USB over IP managed hub

DistKontrolUSB

(USB network connection device)

USER MANUAL

Version 3.15.4

Moscow 2020 г.

Table of contents

ATTENTION!!!

1. Work on the hardware and software parts of the equipment is ongoing. There may be discrepancies between the description and the existing functionality. The options and functions described in this manual are present in various device modifications, and are not necessarily present in YOUR device model.

2. The device works correctly with the bulk of the most common electronic security keys, flash drives, USB cameras and other USB devices, but absolutely all USB devices are not guaranteed to be connected via the network.

3. This "User's Manual" is intended for studying the device, the procedure and rules of operation, installation, setting up a managed USB over IP hub. To use the USB over IP hub, it is recommended to read this manual. When installing a controlled USB over IP hub, one should be guided by the provisions of the "Safety Rules for the Operation of Consumer Electrical Installations" and "Rules for the Operation of Consumer Electrical Installations". To configure a managed USB over IP hub, you must have the skills of a confident PC user.

4. The "User Manual" is relevant for the concentrator software from version 3.14. For software prior to the specified version, see the “User Manual” on the device.

1 COMMON INFORMATION

The USB over IP managed hub is part of the DistKontrolUSB series of USB security and usability products.:

- Managed USB over IP hubs - for remote connection and hardware disconnection and inclusion of USB devices over the network.;
- USB over IP hubs - for remote connection of USB devices over the network;
- Managed USB hubs - for hardware disconnection and incluse of USB devices connected via USB;

1.1PURPOSE OF THE APPLIANCE

Managed USB via an IP hub for connecting USB devices (including electronic security keys, for example, eToken, ruToken and other analogs, keys for 1C software products, scanners, printers, MFPs, sensors, etc.) to a computer networks. By connecting the USB to your computer or laptop, it allows you to use it remotely and control the physical power-up and connection of this USB device.

Managed USB over IP hub provides two-step protection for USB devices when sharing USB over a network:

1. Remote physical power on and off USB devices;

2. Authorization for connecting USB devices by login, password and IP address.

The log of a managed USB over IP hub stores all information about connections and disconnections of both USB inputs (ports) of DistKontrolUSB, and any of USB devices, as well as attempts to enter the password incorrectly and other additional information.

1.2 RANGE OF MANAGED USB OVER IP CONCENTRATORS

USB over IP managed hub

16 USB ports

USB over IP managed hub

32 USB ports

USB over IP managed hub

48 USB ports

USB over IP managed hub

64 USB ports

1.3 APPLICATION AREA OF MANAGED USB OVER IP CONCENTRATORS

The ability to control USB over IP ports allows remotely, via the WEB interface, to disconnect and enable USB devices physically. The USB over IP managed hub supports web-based management, including remote control and alerting. Execution - desktop (with the possibility of installation in a 19 "rack). The USB over IP controlled hub allows you to hardware enable and disable USB devices connected over the network. In the WEB interface of the USB over IP hub, there are pages for managing USB ports, adding users and managing access rights. For users in the WEB interface, only management of allowed USB ports is available, changing the password and email address for sending notifications.

The Managed USB over IP Hub (DistKontrolUSB USB Network Connection Device) is a hardware / software solution that allows USB devices to be used remotely over a network and work directly with it, just as if they were connected locally! This makes it possible to use remote USB devices on your computer, as well as share your USB devices with other users or resources over the network (essentially extending the USB cable over the Internet line).

The DistKontrolUSB device has a built-in Wi-Fi module and an Ethernet network adapter (RJ-45) operating at a speed of 100 Mbps. This allows you to connect the device to the network, both via wired and wireless (Wi-Fi) communication channels. The device comes in a metal case. The operating range of the wireless network when the device is made in a metal case is limited.

Connecting USB devices over a network for sharing allows for more efficient use of computer resources and, most importantly, saves time and money, despite the cost of the USB device itself over the network. The presence of a wireless communication channel in the USB hardware connection device over the network, allows to further ensure the security and physical inaccessibility of shared USB devices.

The ability to remotely connect USB devices over a network using a controlled USB over IP hub will allow your company to raise information security and the security of sharing various USB devices to a new qualitative level. All your carriers of electronic digital signatures will be stored in a place inaccessible for free access (remote) and connected, if necessary, also remotely.

The inability to lose, broke some key will bring significant savings in material resources.

internet network
usb devices

DistKontrolUSB USB Network Connector is ideal for sharing USB devices between multiple users on the network, over the Internet or in the cloud without a USB device that needs to be physically connected to each user's computer. On the user's computer, the USB device looks as if it were connected directly, even if connected to a remote server, so the existing drivers and software work without any changes.

With a USB hardware-over-the-network device, you can provide unprecedented flexibility in using your USB devices and take your USB devices to the next level. The ability to connect a managed USB over IP hub to multiple USB hosts at the same time will allow you to easily continue using USB devices in cluster systems.

DistKontrolUSB USB networking device has been tested and is compatible with VMware and Microsoft Hyper-V virtualization platforms.

1.4 TECHNICAL CHARACTERISTICS OF USB MANAGED OVER IP HUBS

Model	**DistKontrolUSB-4**	**DistKontrolUSB-16**	**DistKontrolUSB-32**	**DistKontrolUSB-48**	**DistKontrolUSB-64**
Network interfaces	Ethernet (RJ-45), 802.11n Wirelless	Ethernet (RJ-45), 802.11n Wirelless	Ethernet (RJ-45), 802.11n Wirelless	Ethernet (RJ-45), 802.11n Wirelless	Ethernet (RJ-45), 802.11n Wirelless
Ethernet port	1 x 10/100 Mb (optional: 1 x 10/100/1000 Mb)	1 x 10/100 Mb (optional: 1 x 10/100/1000 Mb) (optional: 2 x 10/100/1000 Mb)	1 x 10/100 Mb (optional: 1 x 10/100/1000 Mb) (optional: 2 x 10/100/1000 Mb)	1 x 10/100 Mb (optional: 1 x 10/100/1000 Mb) (optional: 2 x 10/100/1000 Mb)	1 x 10/100 Mb (optional: 1 x 10/100/1000 Mb) (optional: 2 x 10/100/1000 Mb)
Number of unmanaged USB ports (inputs)	4	-	-	-	-
Number of controllable USB ports (inputs)	-	16	32	48	64
IP addresses	2 static / DHCP (IPv4/ IPv6)	2 static / DHCP (IPv4/ IPv6)	2 static / DHCP (IPv4/ IPv6)	2 static / DHCP (IPv4/ IPv6)	2 static / DHCP (IPv4/ IPv6)
LEDs indication	Power supply, LAN port status	Power supply, LAN port status, USB device port power supply	Power supply, LAN port status, USB device port power supply	Power supply, LAN port status, USB device port power supply	Power supply, LAN port status, USB device port power supply
Power supply	Built-in 220V power supply 50 Hz, 100 W	Built-in 220V power supply 50 Hz, 150 W (optional: Second power supply in power redundancy mode)	Built-in 220V power supply 50 Hz, 200 W (optional: Second power supply in power redundancy mode)	Built-in 220V power supply 50 Hz, 200 W (optional: Second power supply in power redundancy mode)	Built-in 220V power supply 50 Hz, 100 W (optional: Second power supply in power redundancy mode)
USB support	USB 2.0, 1.1, 1.0	USB 2.0, 1.1, 1.0	USB 2.0, 1.1, 1.0	USB 2.0, 1.1, 1.0	USB 2.0, 1.1, 1.0
USB port protection	-	Limiting USB ports by current, turning off the USB port when overheating, smooth start-up of USB ports	Limiting USB ports by current, turning off the USB port when overheating, smooth start-up of USB ports	Limiting USB ports by current, turning off the USB port when overheating, smooth start-up of USB ports	Limiting USB ports by current, turning off the USB port when overheating, smooth start-up of USB ports
Rated load current per USB port	-	0,5 A	0,5 A	0,5 A	0,5 A
USB port load current limit	-	0,9 A	0,9 A	0,9 A	0,9 A
Ambient temperature	0°C до +50°C	0°C до +50°C	0°C до +50°C	0°C до +50°C	0°C до +50°C

Relative humidity	no more than 80% (at a temperature of + 35 ° C and below)	no more than 80% (at a temperature of + 35 ° C and below)	no more than 80% (at a temperature of + 35 ° C and below)	no more than 80% (at a temperature of + 35 ° C and below)	no more than 80% (at a temperature of + 35 ° C and below)
Operating system support	Windows® Server 2016, Windows® 10, Windows Server® 2012 R2, Windows® Server 2008 R2, Linux, OSX	Windows® Server 2016, Windows® 10, Windows Server® 2012 R2, Windows® Server 2008 R2, Linux, OSX	Windows® Server 2016, Windows® 10, Windows Server® 2012 R2, Windows® Server 2008 R2, Linux, OSX	Windows® Server 2016, Windows® 10, Windows Server® 2012 R2, Windows® Server 2008 R2, Linux, OSX	Windows® Server 2016, Windows® 10, Windows Server® 2012 R2, Windows® Server 2008 R2, Linux, OSX
Overall dimensions (height / width / depth)	35 / 140 / 110	44 / 440 / 285	85 / 440 / 205	130 / 440 / 205	130 / 440 / 205
19 ”rack mount	no	available	available	available	available
Dimensions in Unit	-	1	2	3	3
Safety	https, ssl	https, ssl	https, ssl	https, ssl	https, ssl
USB traffic encryption	available	available	available	available	available
Built-in firewall	available	available	available	available	available
IP restriction for connecting USB device	no	available	available	available	available
Restricting by IP to connect the USB port	no	available	available	available	available
Authorization for connecting a USB device	no	available	available	available	available
Authorization for connecting a USB port	no	available	available	available	available
USB device protection module	no	(Optionally available)	(Optionally available)	(Optionally available)	(Optionally available)

The USB over IP managed hub provides USB ports current limiting to protect the load from abnormal situations. If overheating occurs, the output is blocked until the fault is rectified. Removing the load will reboot the USB input. Also, the hub has a USB port soft-start circuit that minimizes inrush current surges when there is a high capacitive load.

The USB over IP managed hub provides a rated load current of 0.5 A per port and limits the current (load current limit is 0.9 A).

1.5 SUPPLY KIT OF USB MANAGED OVER IP HUB

№	Name	quantity
1	USB over IP managed hub	1
2	Passport	1
3	Power cable	1
4	19 "rack mount	2
5	Mounting screws	8
6	Leg for desktop installation	4

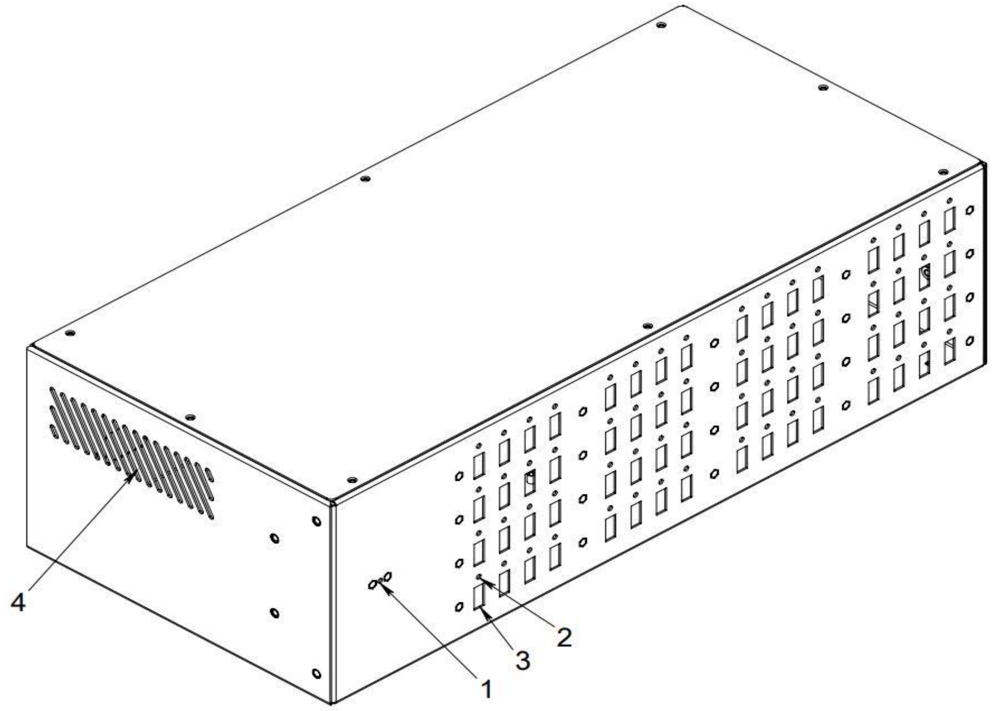
1.6 STRUCTURE AND OPERATION OF THE MANAGED USB OVER IP HUB

1.6.1 OVERALL DIMENSIONS OF USB MANAGED OVER IP HUB (19 "RACK)

Model	height in U	product dimensions in mm.			packing dimensions in mm.		
		height	width	depth	height	width	depth
DistKontrolUSB-16	1	44	440	285	50	500	320
DistKontrolUSB-32	2	85	440	205	128	500	240
DistKontrolUSB-48	3	130	440	205	128	500	240
DistKontrolUSB-64	3	130	440	205	171	500	240

1.6.2 DEVICE STRUCTURE

The hub is housed in a metal case that can be installed on a table or mounted in a 19 '' rack.



The front panel contains:

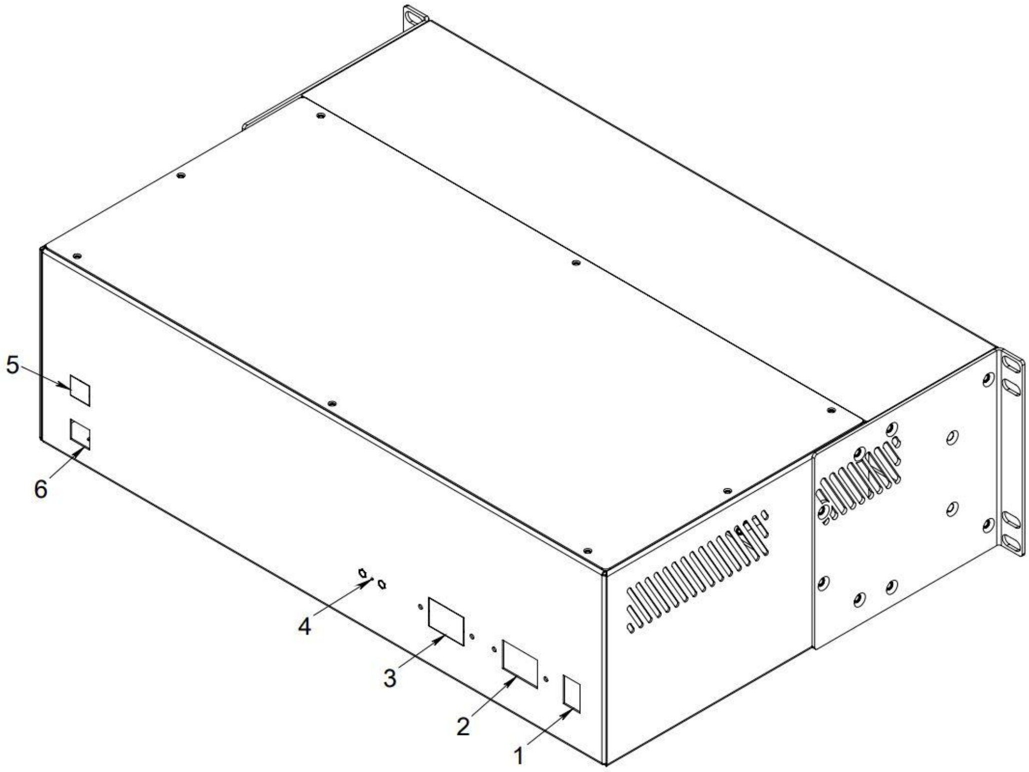
1 - power on indicator;

2 - USB port activity indicator.

3 - USB-A type connectors downstream ports for connecting devices that support the USB protocol;

The side panels contain:

4 - ventilation holes;



The rear panel contains:

1 - Power switch.

2 - Connector for connecting a network cable 1;

3 - Connector for connecting a network cable 2 (optional);

4 - Reset button "Reset"

5 - RJ45 connector for Ethernet "LAN" 2 (optional);

6 - RJ45 connector for Ethernet "LAN" 1;

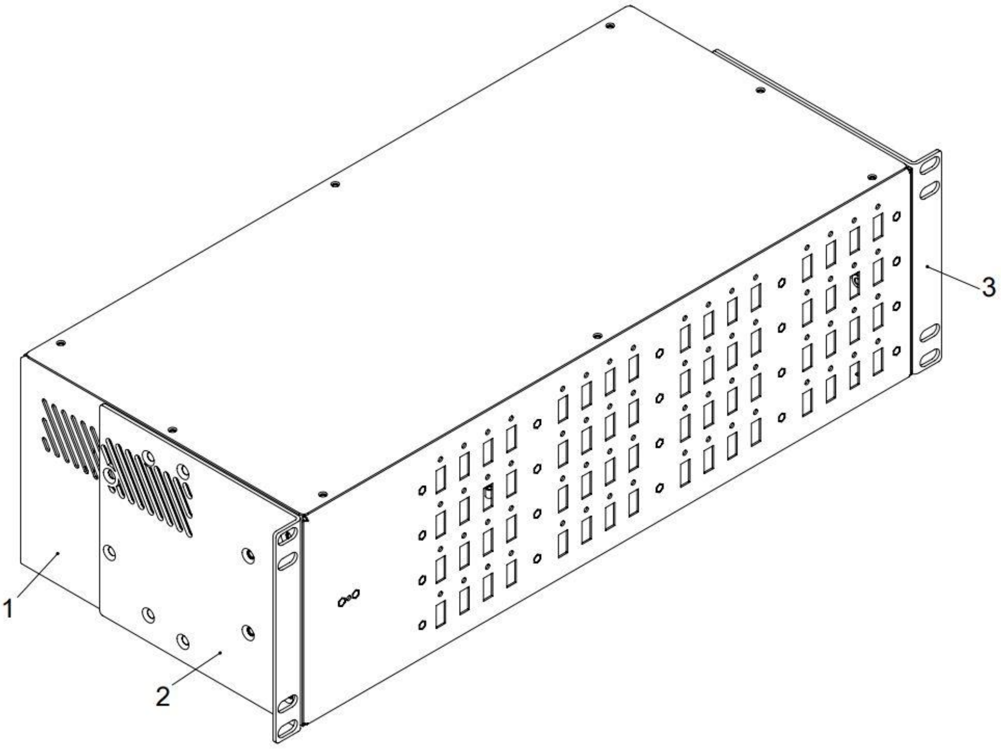
At the corners of the bottom panel concentrator has four holes for mounting legs for mounting on a surface (desk).

The device comes with a 19 ”rack / cabinet mount that can be mounted in two positions.

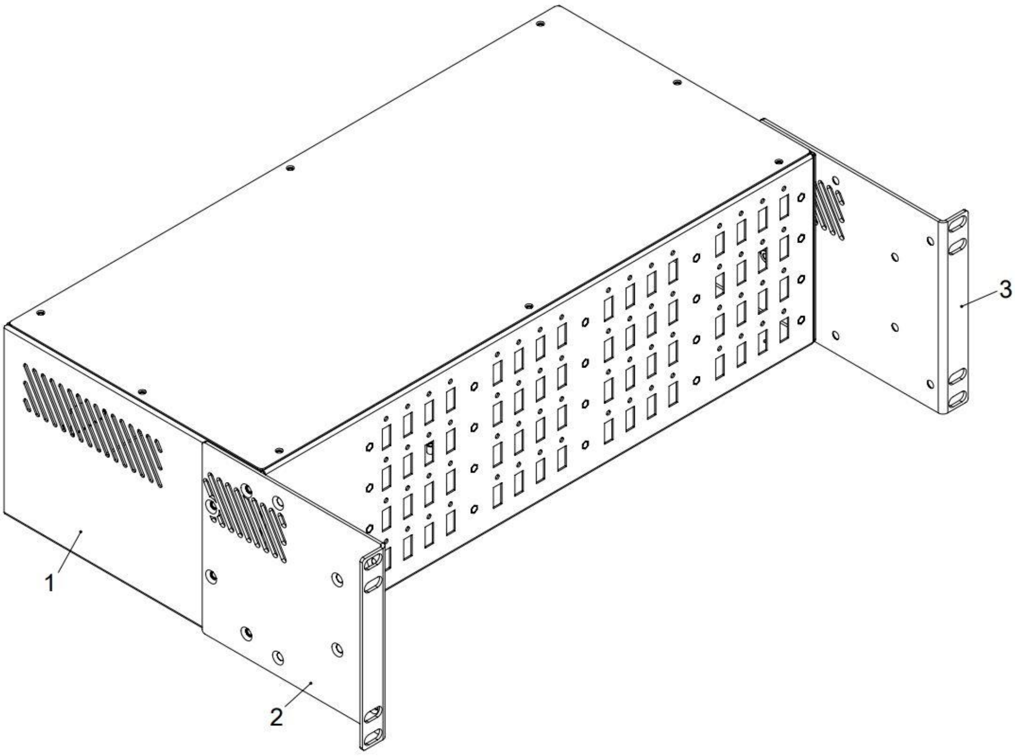
Figure:

1 - Device;

2,3 - Mounts in a rack / cabinet 19 ";



Assembling the 19 ”rack mount device.



Assembly of the device for mounting in a 19 ”cabinet.

1.6.3 PROTECTION MODULE OF CONNECTED USB DEVICES MANAGED USB OVER IP HUB

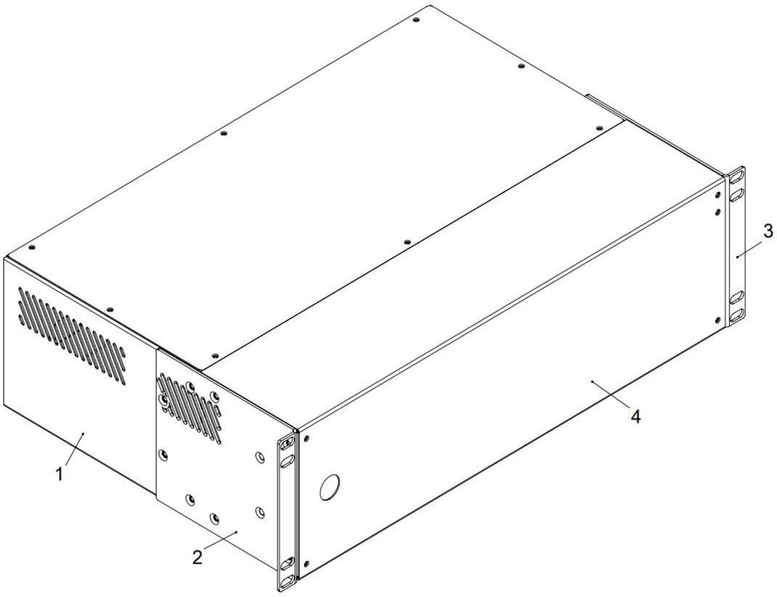
The security module for connected USB devices of a managed USB over IP hub is supplied separately (optional). Not included in the standard package.

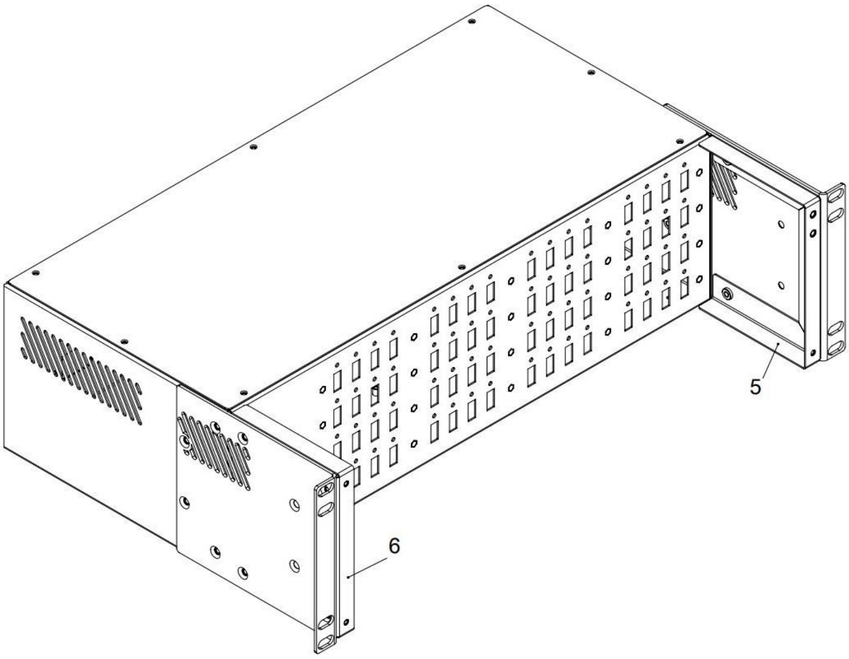
The module is designed to protect connected USB devices from damage and physical access. Includes additional cover mount and protective cover. The lid has a sealing option.

Appearance:

4 - Protective lid;

5,6 - Mounts for the protection module.





1.6.4 OPERATING LIMITS AND RECOMMENDATIONS

The concentrator provides continuous round-the-clock operation and is repairable and maintainable.

The concentrator remains operational when exposed to:

● high ambient temperature up to + 50 ° C;

● low ambient temperature not lower than - 5 ° C;

● increased relative air humidity up to 98% at a temperature of + 25 ° C;

● sinusoidal vibration in the frequency range from 10 to 55 Hz with displacement amplitude up to 0.35 mm (in any direction) in accordance with the requirements of GOST 12997.

1.6.5 SECURITY MEASURES

When using the device, the "Interindustry rules on labor protection (safety rules) during the operation of electrical installations" should be observed.Класс безопасности - I по ГОСТ 12.2.007.0-75

The design of the device ensures the degree of protection IP 20 in accordance with GOST 14254-96.

The sources of danger of the device are ~ 220V mains voltage circuits, ~ 220V contacts of the power cable connector and a built-in voltage converter.Прибор устанавливается горизонтально на столах или других конструкциях, в стойку 19`, в местах, где отсутствует доступ посторонних лиц.

Installation (removal), assembly, repairs should be performed with the mains voltage ~ 220V disconnected from the device.

It is not recommended to cover the ventilation holeson the side panels.

1.6.6 PREPARING A USB MANAGED OVER IP HUB FOR OPERATION

Preparing the hub for use includes the following operations:

- after unpacking, visually check the concentrator for damage;
- place on a stable, level surface (table) or fix it in a 19 "rack;

● connect the power cord to the back of the hub;

● connect the mains plug to the 220V 50 Hz network;

● connect devices supporting the USB protocol to USB ports located on the front panel of the device;

● connect the device to the Ethernet network;

● turn on the power.

Do not turn on the concentrator if its temperature is below room temperature! (This may occur when transporting the concentrator during cold seasons). Allow the concentrator to warm to room temperature before turning it on.

1.6.7 OPERATION OF A MANAGED USB OVER IP HUB

To work with a USB device connected to a USB over IP controlled hub, you must:

1. Turn on the USB device (remotely supply power to the USB device);

2. Connect the USB device to your computer (laptop, tablet, phone, etc.).

Enabling and disabling USB devices connected to a controlled USB over IP hub is possible (enabling and disabling USB inputs of the device):

● Through the WEB interface;

● Using the task scheduler and assigned tasks;

● Using the device management utility (scripts, from the command line or your application).

Connecting and disconnecting USB devices connected to a controlled USB over IP hub is possible:

● Through a client application running in graphical mode or as a service;

● Using API (scripts, command line or your application).

To use a USB over IP controlled hub, you must:

1. Connect the device to LAN (via Ethernet or WiFi) and configure it.

2. On each computer to which you need to forward the USB device, run the DistKontrolUSB Client software running under Linux, Windows, OSX.

3. Configuring and managing the USB device over the network is carried out through the Web interface.

4. Setting up a client computer is simple and intuitive. DistKontrolUSB Client runs Linux, Windows, and OSX versions. The client allows intuitive and easy plugging and unplugging of remote USB devices. DistKontrolUSB Client does not require installation. The client can run as a service.

1.7 SEALING

After the acceptance tests at the manufacturer, the device is sealed.

Installed seals, must exclude the possibility of unauthorized changes to the electrical circuit diagram of the device. Seals are installed on the device in such a way as to exclude the possibility of removing the cover of the device without damaging the seal.

1.8 PACKAGING

A finished product is a device accepted by a technical control representative and packed in a consumer container.

2 TECHNICAL SERVICE

2.1 GENERAL PROVISIONS

The maintenance of the device is carried out according to the planned preventive system and is carried out by the Consumer. The personnel servicing these products must have an electrical safety group of at least III.

Maintenance consists of periodic (at least once a year):

- external inspection of the concentrator, removing dust with a soft cloth;
- checking the functionality of the hub.

During maintenance, safety requirements must be observed, as well as the requirements of GOST 12.1.006, GOST 12.1.019, GOST 12.2.003, "Rules for the technical operation of consumer electrical installations", "Safety rules for the operation of electrical installations of consumers".

2.2 CHECKING THE OPERATION OF A MANAGED USB OVER IP HUB

To check the device, it is necessary to connect a USB flash drive with arbitrary files written to it to each of the ports, and, having connected this drive to a PC via the WEB interface (the port activity indicator should be on), read the file. The ability to read the file indicates the health of the port being checked. After the port is disabled, the port enable LED should go out.

Note: in the absence of the required number of flash drives, you can perform the specified operations with the ports sequentially.

3 CONSERVATION AND STORAGE OF THE MANAGED USB OVER IP HUB

3.1 CONSERVATION

Preservation of the device during long-term storage is not provided.

3.2 STORAGE, TRANSPORTATION AND DISPOSAL

It is recommended to store the device in a heated warehouse. The premises should be free of acid vapors, alkalis, corrosive gases and other harmful impurities that cause corrosion.

The guaranteed shelf life in heated warehouses in consumer containers is at least 3 years.

The device can be transported by any type of road or rail transport in closed bodies (containers, wagons).

Transportation conditions must comply with storage conditions 5 in accordance with GOST 15150-69.

After transportation, the device must be kept in normal conditions for at least 12 hours before being switched on.

There are no special requirements for the disposal of the device.

4 WEB MANAGEMENT INTERFACE DISTKONTROLUSB

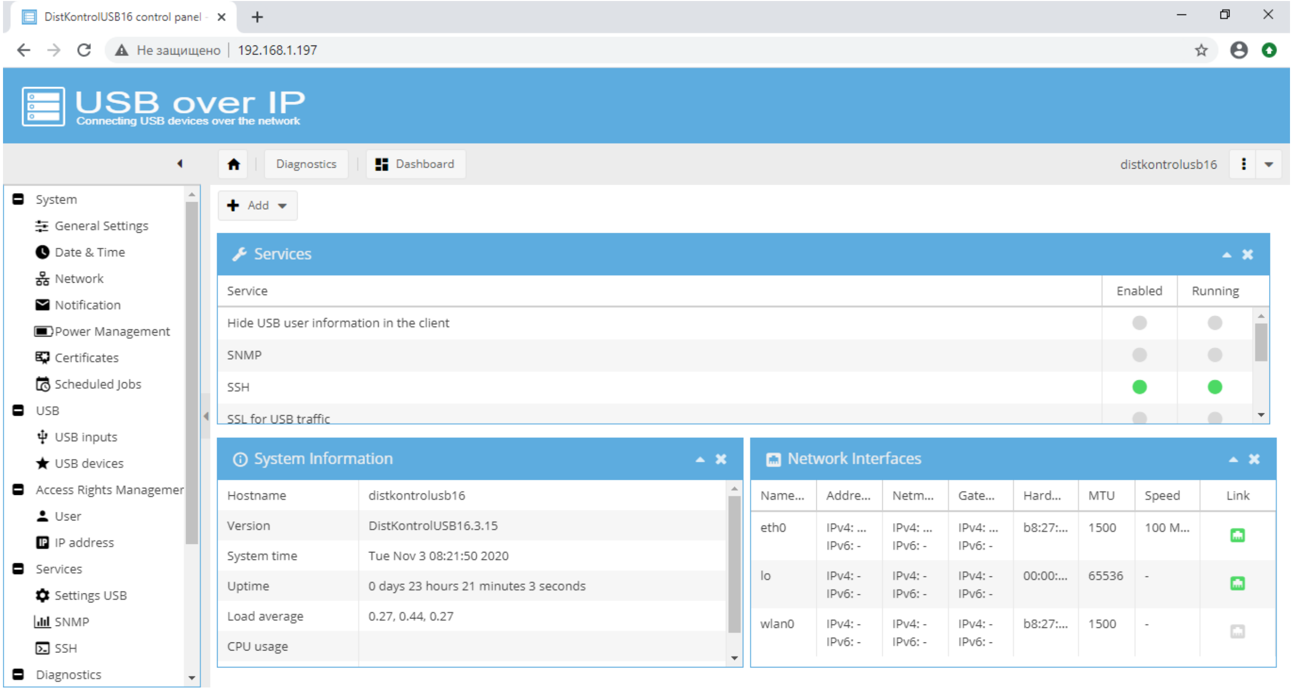
4.1 LOGIN TO WEB INTERFACE AND STARTING SCREEN

The USB over IP hub is controlled via a multilingual WEB administrator interface.

After authorization, settings management is available.

The appearance of the home page can be customized by adding or removing the desired panels.

View of the WEB interface for managing the settings of the USB connection device over the network:



Services

Service	Enabled	Running
Hide USB user information in the client	○	○
SNMP	○	○
SSH	●	●
SSL for USB traffic	○	○

System Information

Hostname	distkontrolusb16
Version	DistKontrolUSB16.3.15
System time	Tue Nov 3 08:21:50 2020
Uptime	0 days 23 hours 21 minutes 3 seconds
Load average	0.27, 0.44, 0.27
CPU usage	

Network Interfaces

Name...	Addre...	Netm...	Gate...	Hard...	MTU	Speed	Link
eth0	IPv4: ... IPv6: -	IPv4: ... IPv6: -	IPv4: ... IPv6: -	b8:27:...	1500	100 M...	🟩
lo	IPv4: - IPv6: -	IPv4: - IPv6: -	IPv4: - IPv6: -	00:00:...	65536	-	🟩
wlan0	IPv4: - IPv6: -	IPv4: - IPv6: -	IPv4: - IPv6: -	b8:27:...	1500	-	□

By default, a USB network device has:

Static IP address - 192.168.1.180

Login to the WEB interface panel - admin

Password for the WEB interface panel - admin

Client connection port - 6565 (default)

SSL client connection port - 6564 (when enabled)

WiFi interface (wlan0) - disabled

Attention!!! If the password is entered incorrectly up to 4 times, the user for whom there were attempts to enter, is blocked for 3 minutes. Each subsequent entry, even the correct password, updates the lock timer.

4.2 SYSTEM

4.2.1 GENERAL SETTINGS

This section contains settings for the Web interface.

SSL is configured for the Web interface, for USB traffic see the section "Client Application Settings"

Attention!!! If you disable previously configured encryption, you need to clear the browser cache, since some browsers cache redirects from http to https.

4.2. 2 DATE AND TIME

NTP server is used by default. To manually enter the time, you must disable "Using NTP Server". The Update Now function is only available with manual time setting.

In the Information section, the current time is static; loaded at the moment of opening the "Date and time" setting.

4.2.3 NETWORK

4.2.3.1 GENERAL

Hostname - the name that will be displayed in the DistKontrolUSB client. Recommended to change when multiple hubs are on the network. If you have multiple network interfaces, it is recommended to add the hub by hostname. In this case, regardless of the active interface, the device will be displayed on the client.

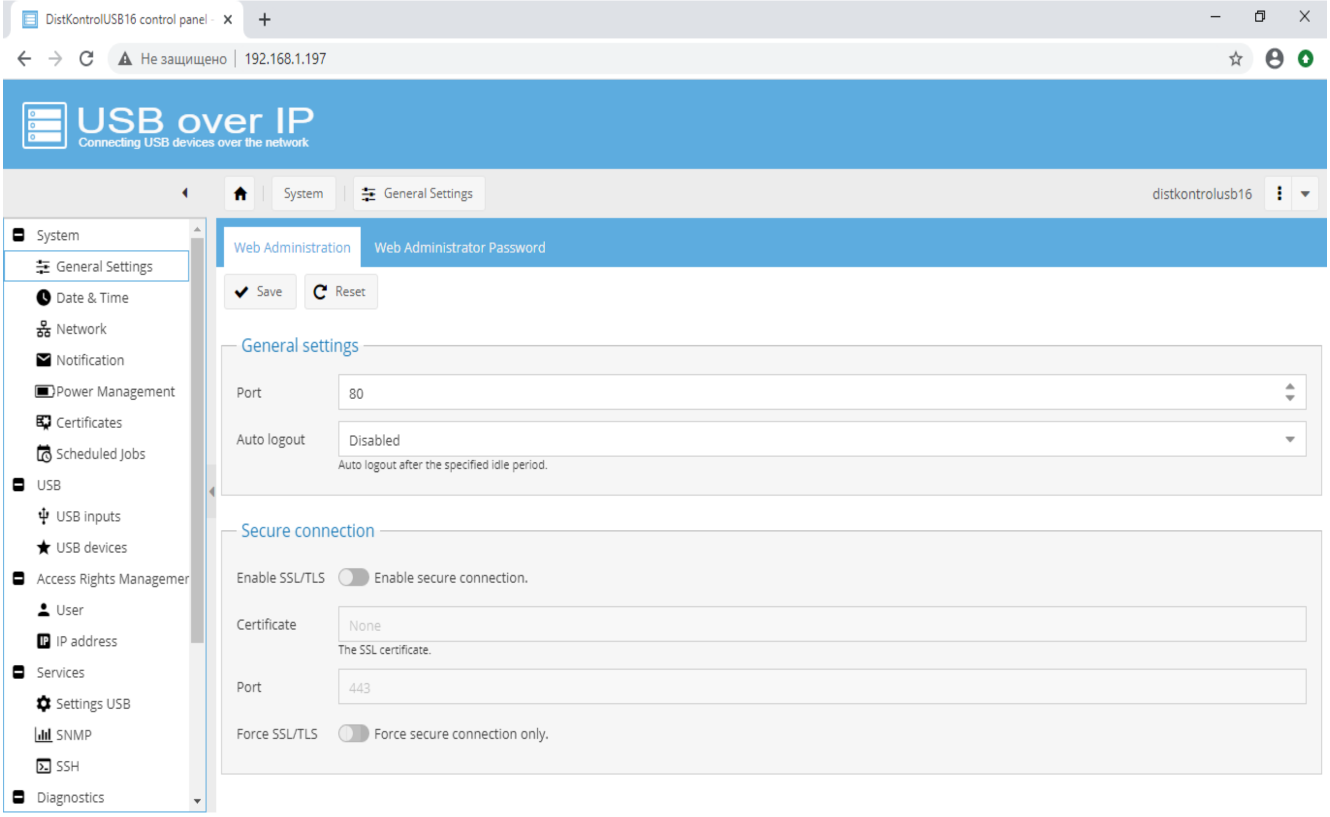
Domain name - adds a domain name of 2 or more levels. Does not affect the connection to the domain, it is used for graphical display in the client application.

4.2.3.2 INTERFACES

To get started, you need to change the IP address of the device and the password of the WEB interface.

The IP address changes when you double click on the corresponding network interface (the Network - Interfaces page). It is possible as a joint use of LAN (eth0) and WiFi (wlan0) interfaces, as well as independent use of any of the interfaces. When using only one network interface, it is recommended to disable the second.

On the general settings page, you can change the password for access to the WEB interface, the WEB interface port.



General settings

Port: 80

Auto logout: Disabled

Auto logout after the specified idle period.

Secure connection

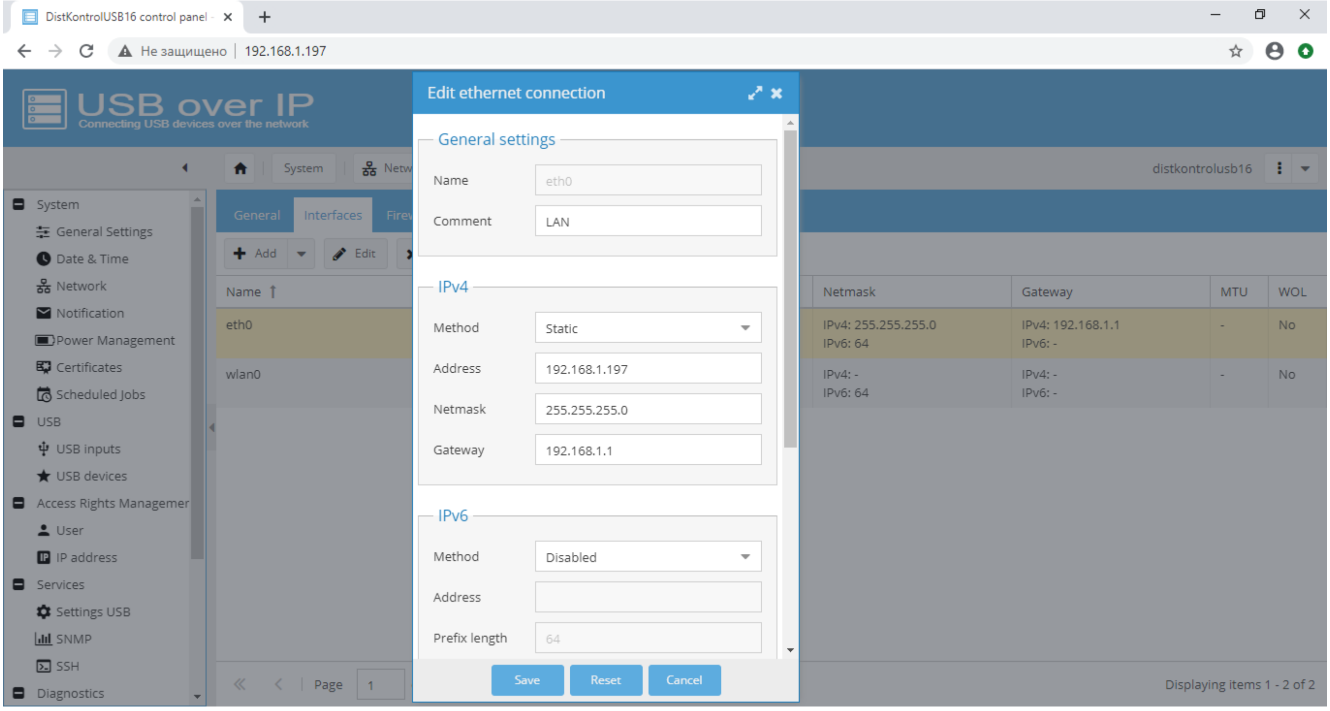
Enable SSL/TLS: Enable secure connection.

Certificate: None

The SSL certificate.

Port: 443

Force SSL/TLS: Force secure connection only.



Name	Netmask	Gateway	MTU	WOL
eth0	IPv4: 255.255.255.0 IPv6: 64	IPv4: 192.168.1.1 IPv6: -	-	No
wlan0	IPv4: - IPv6: 64	IPv4: - IPv6: -	-	No

Edit ethernet connection

General settings

Name: eth0

Comment: LAN

IPv4

Method: Static

Address: 192.168.1.197

Netmask: 255.255.255.0

Gateway: 192.168.1.1

IPv6

Method: Disabled

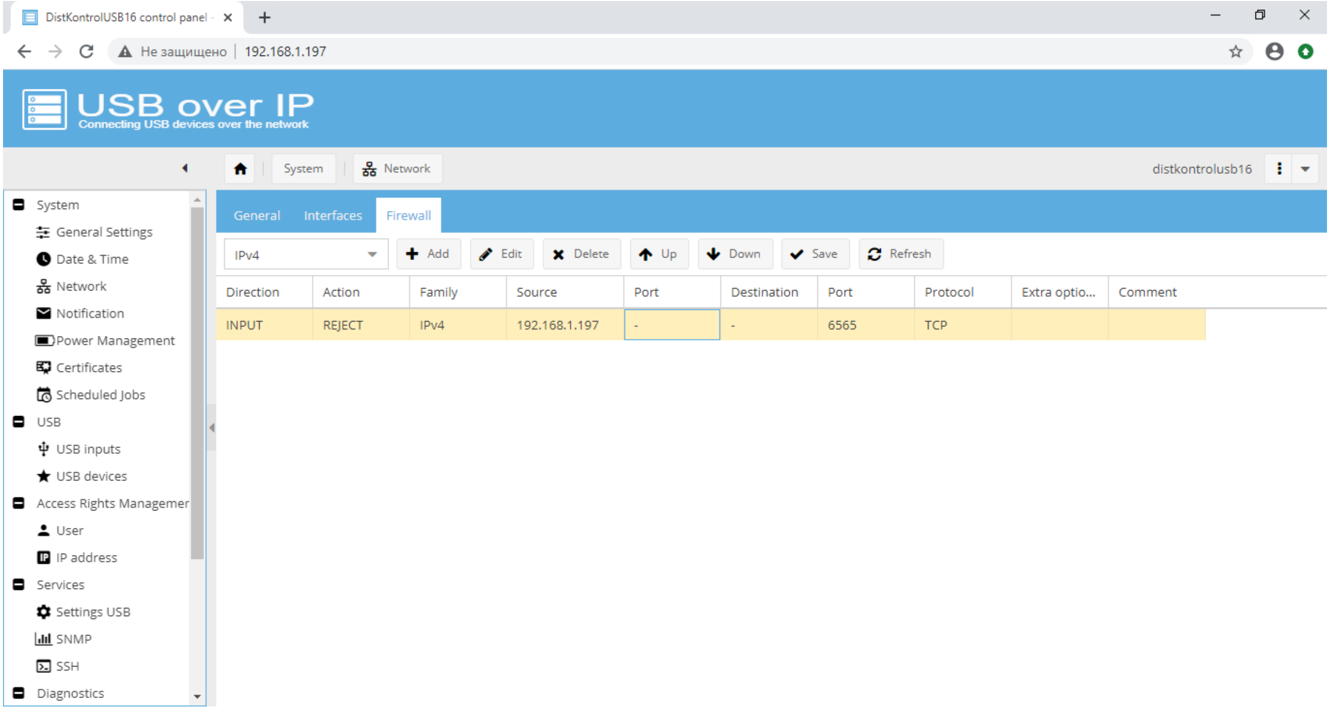
Address:

Prefix length: 64

To create a Bond connection, you must delete all interfaces that will participate in the connection. When eth0 interface is removed, the device's IP address will become dynamic. After applying the settings, go to the Web interface at the new address and configure bond connections by adding all the necessary interfaces.

4.2.3.3 FIREWALL

The hub firewall is based on iptables. It can be useful if you need to completely exclude access to the hub for some computers on the local network. Or grant access only from certain computers. You can create corresponding rules in the filter table.



Direction	Action	Family	Source	Port	Destination	Port	Protocol	Extra optio...	Comment
INPUT	REJECT	IPv4	192.168.1.197	-	-	6565	TCP		

For example, you need to provide access to the hub (WEB interface - port 80 and USB devices - port 6565) from only one computer in the local network with IP 192.168.1.105.

Required (see page screenshot above):

1. Allow access from IP 192.168.1.105 to the hub for the client application.

2. Allow access from IP 192.168.1.105 to the web interface of the concentrator.

3. Allow access from localhost 127.0.0.1

4. Deny all other connections.

The consistency of the rules is important. As a result, from all but the IP address specified in the rules, the client will not have a hub.

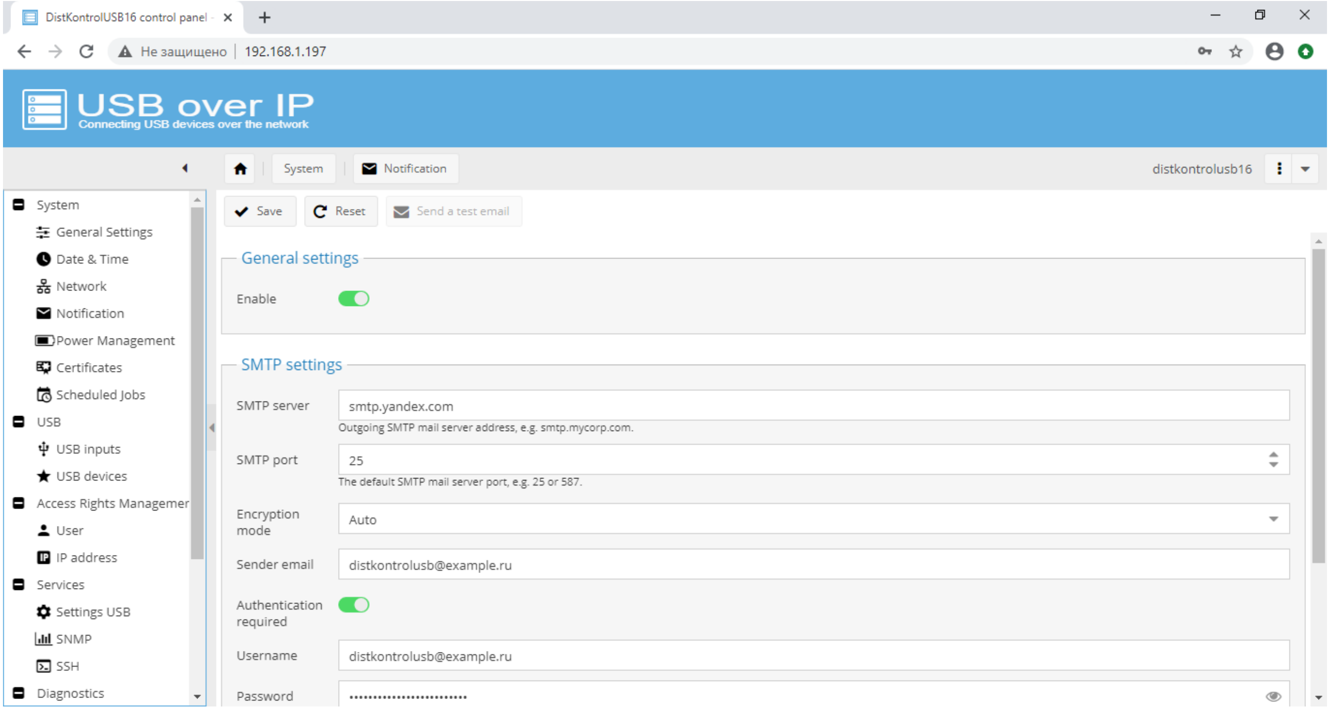
If it is necessary to close access to only one IP address in the local network, then in all the rules change to the opposite "Action"

ATTENTION!!! Carefully configure the rules, do not close access to the hub's WEB interface (to regain control over it, you will need to reset the settings of the USB over IP hub to its original state)

When configuring, it is recommended to temporarily allow for a specific IP and close for everyone, for example, port 22 or 6565 on the device, and only after making sure that the rules are entered correctly, already port 80.

4.2.4 NOTIFICATION

If necessary, you can enable sending notifications by email. The notification system is configured on the web interface page of the System-Notifications hub



General settings

Enable: on

SMTP settings

SMTP server: smtp.yandex.com
Outgoing SMTP mail server address, e.g. smtp.mycorp.com.

SMTP port: 25
The default SMTP mail server port, e.g. 25 or 587.

Encryption mode: Auto

Sender email: distkontrolusb@example.ru

Authentication required: on

Username: distkontrolusb@example.ru

Password: ••••••••••••••••••••••••••

Notifications about user actions are sent to the email addresses specified in their profile. Notification of assigned tasks - to the address specified in the usbcontrol user profile.

- Sending notifications is carried out:
- • Upon successful login to the web management interface of the hub
- • If you enter the wrong username or password to enter the web management interface of the hub
- • When the login to the web management interface of the hub is blocked
- • Service information about the status of the hub

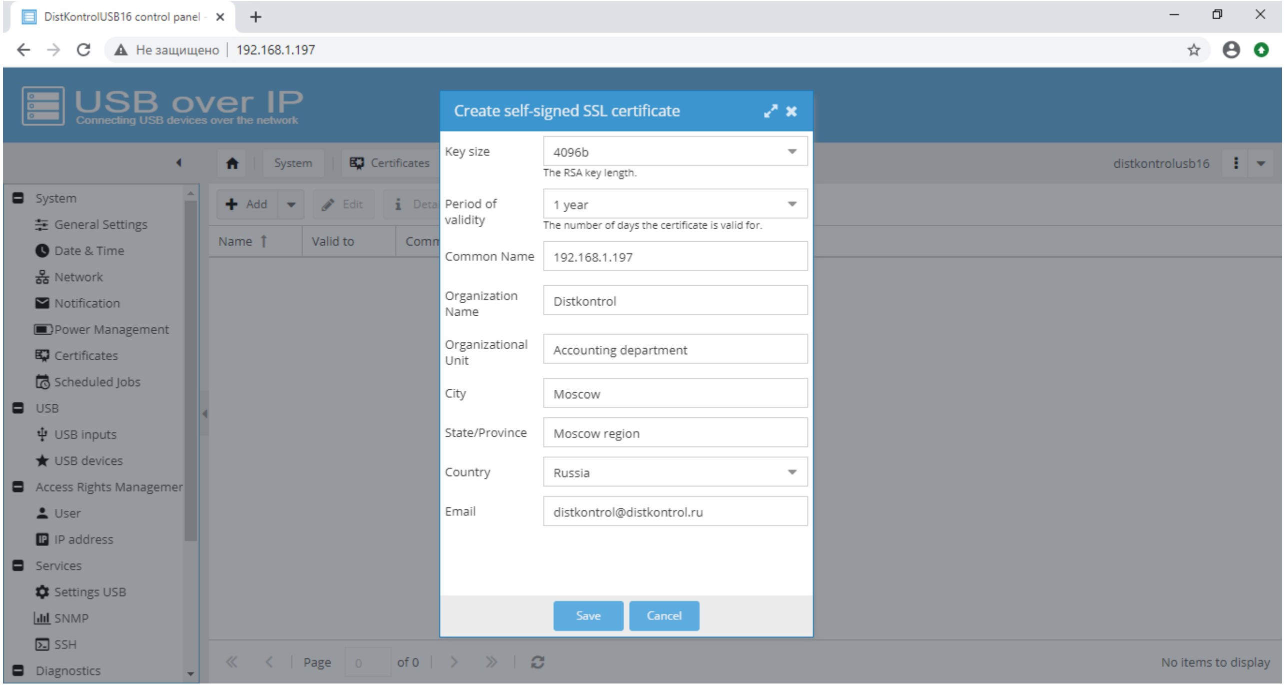
The web management interface of the hub is protected against brute-force login passwords. If the password or username is entered incorrectly five times, the entrance to the control interface is blocked for 3 minutes. Further blocking for 3 minutes at each incorrect entry of credentials, until correct entry. When the entrance is blocked, a notification is sent to the main e-mail, if the notification is enabled and configured.

4.2.5 ENERGY MANAGEMENT

In this section, you can configure a cron task to restart and shutdown the hub.

4.2.6 CERTIFICATES

The USB over IP managed hub supports importing and generating self-signed SSL / SSH certificates. Certificates are managed on the "Certificates" page.



Create self-signed SSL certificate

Key size: 4096b
The RSA key length.

Period of validity: 1 year
The number of days the certificate is valid for.

Common Name: 192.168.1.197

Organization Name: Distkontrol

Organizational Unit: Accounting department

City: Moscow

State/Province: Moscow region

Country: Russia

Email: distkontrol@distkontrol.ru

Save | Cancel

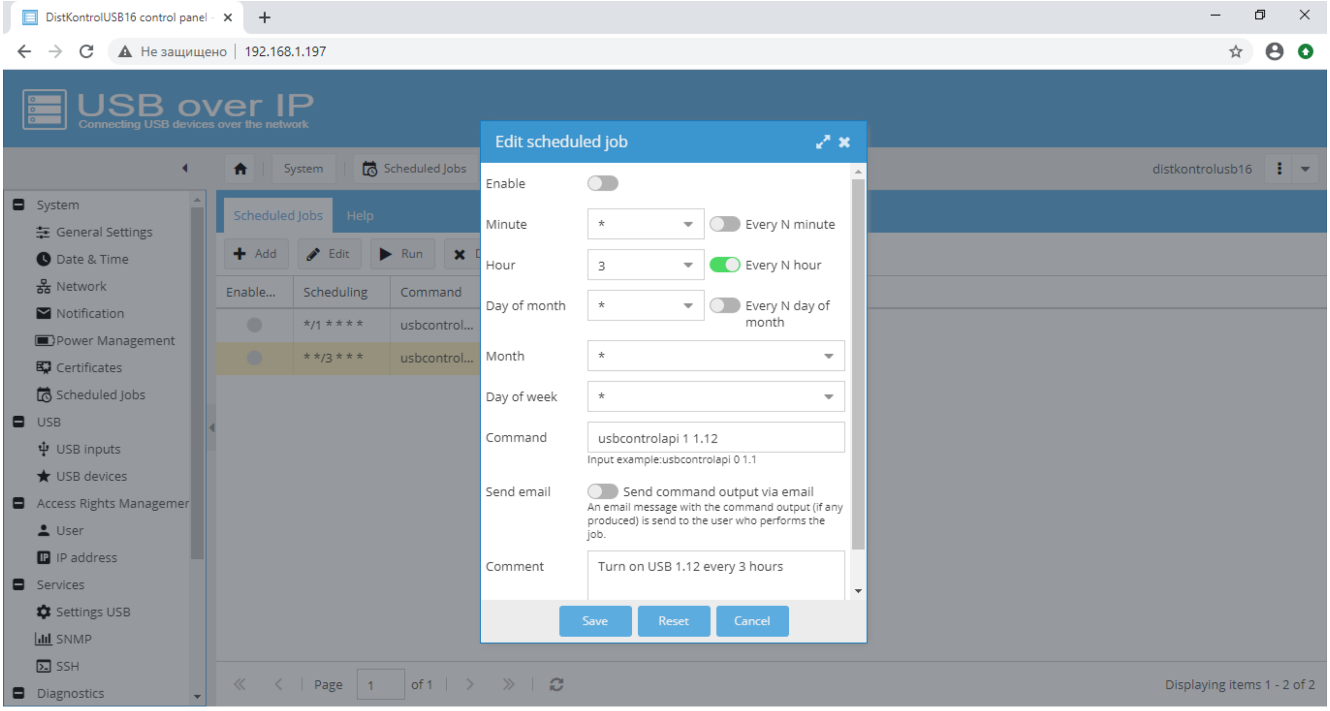
Secure connection for the WEB interface can be enabled on the "General settings" page. There you can also enable the forced use of only a secure connection to access the WEB interface of a managed USB over IP hub.

The procedure for creating and using certificates to encrypt traffic from USB devices is described in detail in the section "Client application settings"

The firewall of the managed USB over IP hub provides additional security for using DistKontrolUSB on the network and flexibly configures access to it

Note: the device must correctly receive the time by NTP (System - Date and Time)

4.2.7 PLANNED TASKS



Enable...	Scheduling	Command
○	*/1 * * * *	usbcontrol...
○	* */3 * * *	usbcontrol...

Edit scheduled job

Enable: off

Minute: * — Every N minute: off

Hour: 3 — Every N hour: on

Day of month: * — Every N day of month: off

Month: *

Day of week: *

Command: usbcontrolapi 1 1.12
Input example:usbcontrolapi 0 1.1

Send email: off — Send command output via email
An email message with the command output (if any produced) is send to the user who performs the job.

Comment: Turn on USB 1.12 every 3 hours

To create a task for controlling USB inputs, on the "Scheduled tasks" page, click the "Add" button, fill in the task fields and click the "Save" button. Created tasks can be disabled and they will not be executed.

The team consists of:

- Team - usbcontrolapi;
- Sign of enabling "1" or disabling "0" port;
- USB port numbers (1.1 to 4.16)

It is also possible to list ports and / or port group indications:

"0.0" - from 1.1 to 4.16;

"1.0" - from 1.1 to 1.16;

"2.0" - from 2.1 to 2.16;

"3.0" - from 3.1 to 3.16;

"4.0" - from 4.1 to 4.16.

Examples of commands:

- usbcontrolapi 0 1.9 (Turn off USB 1.9)
- usbcontrolapi 1 1.12 (Enable USB 1.12)
- usbcontrolapi 1 0.0 (Enable USB 1.1 to 4.16)
- usbcontrolapi 1 2.0,3.0 (Enable USB from 2.1 to 3.16)

- usbcontrolapi 0 1.0,2.1,2.5,3.8,4.0 (Turn off USB from 1.1 to 1.16, 2.1, 2.5, 3.8, from 4.1 to 4.16)

By default, 2 examples are created but disabled.

In the settings of tasks, you can enable sending notifications about the result of their execution by e-mail. Tasks are performed on behalf of the user usbcontrol, notifications will be sent to the email specified in the settings of this user.

To create a task to manage reboot and shutdown of a managed USB over IP hub, on the Power Management - Scheduled Tasks page, click the Add button, fill in the task fields and click the Save button. Created tasks can be disabled and they will not be executed.

Available tasks:

1. Reboot the managed USB over IP hub;

2. Turn off the managed USB over IP hub.

The device uses cron as a task scheduler.

You can familiarize yourself with it and crontab in more detail if you need a more complete understanding of how the scheduler works.

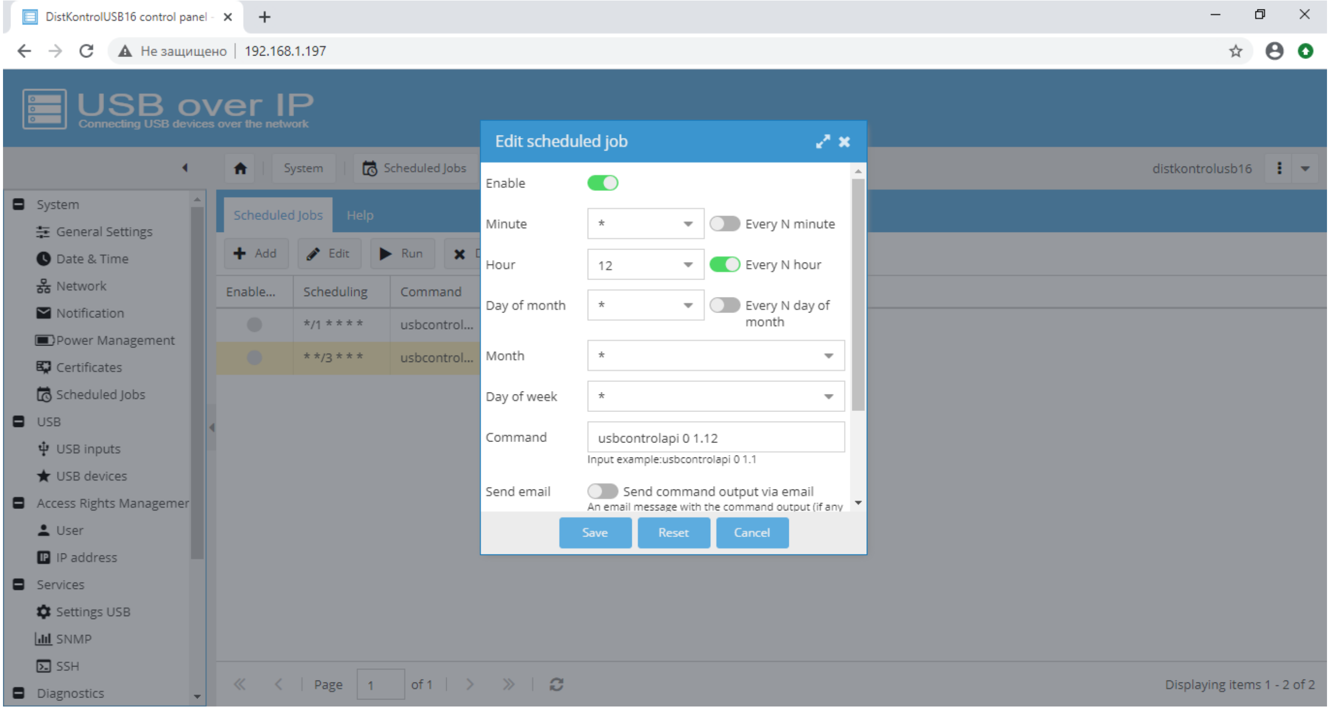
Command format:

```
.---------------- minute (0 - 59)

| .-------------- hour (0 - 23)

| | .------------ day of month (1 - 31)

| | | .---------- month (1 - 12) OR Jan, Feb, Mar ...

| | | | .-------- day of the week (0 - 6) (Sunday = 0 or 7)

| | | | | * * * * * command to execute
```

For example, schedule a task at a specific time (so that command 0 1.12 is executed at 7:00 am 26)

Note: the device must correctly receive the time by NTP (System - Date and Time)

We create a task::



Enable...	Scheduling	Command
●	*/1 * * * *	usbcontrol...
●	* */3 * * *	usbcontrol...

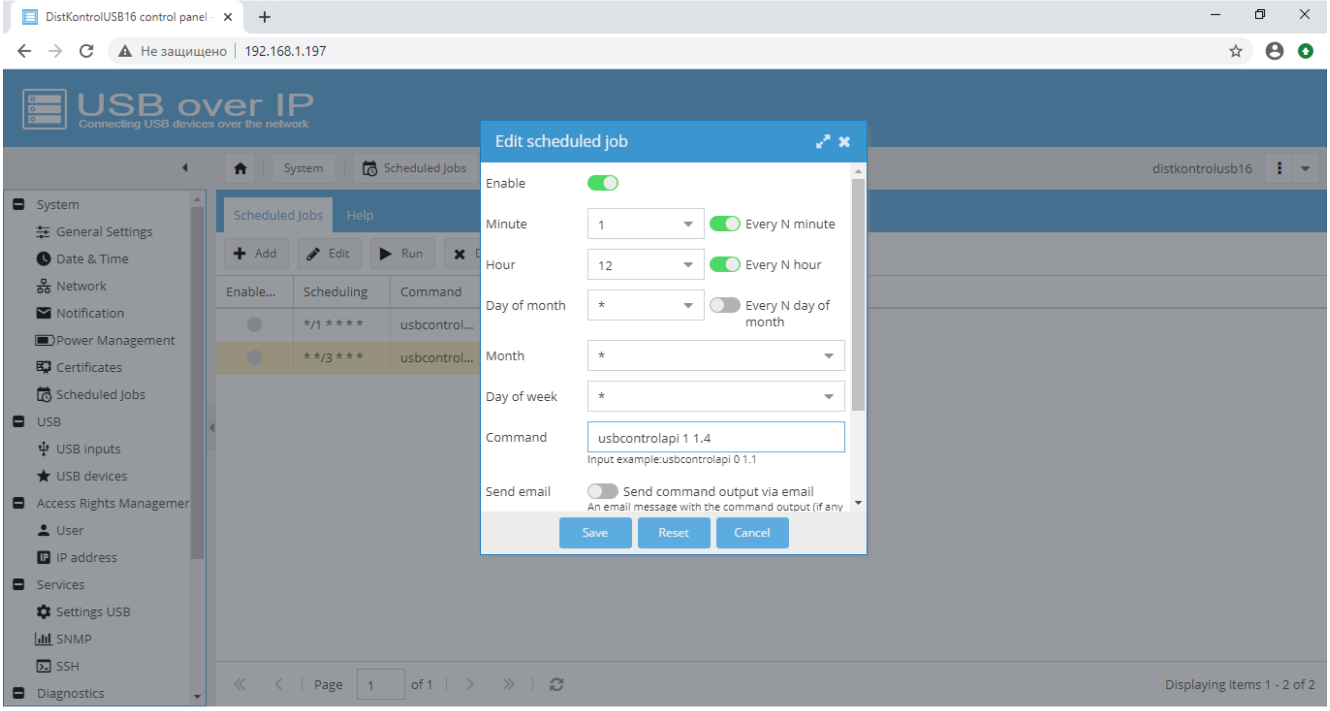
Edit scheduled job

Enable	● on	
Minute	*	○ Every N minute
Hour	12	● Every N hour
Day of month	*	○ Every N day of month
Month	*	
Day of week	*	
Command	usbcontrolapi 0 1.12 Input example:usbcontrolapi 0 1.1	
Send email	○ Send command output via email An email message with the command output (if any	

The "Planned" column will contain: * 7 * * *

An example of repeating a task after 12:01 h

The "Planned" column will contain: * / 1 * / 12 * *



Enable...	Scheduling	Command
●	*/1 * * * *	usbcontrol...
●	* */3 * * *	usbcontrol...

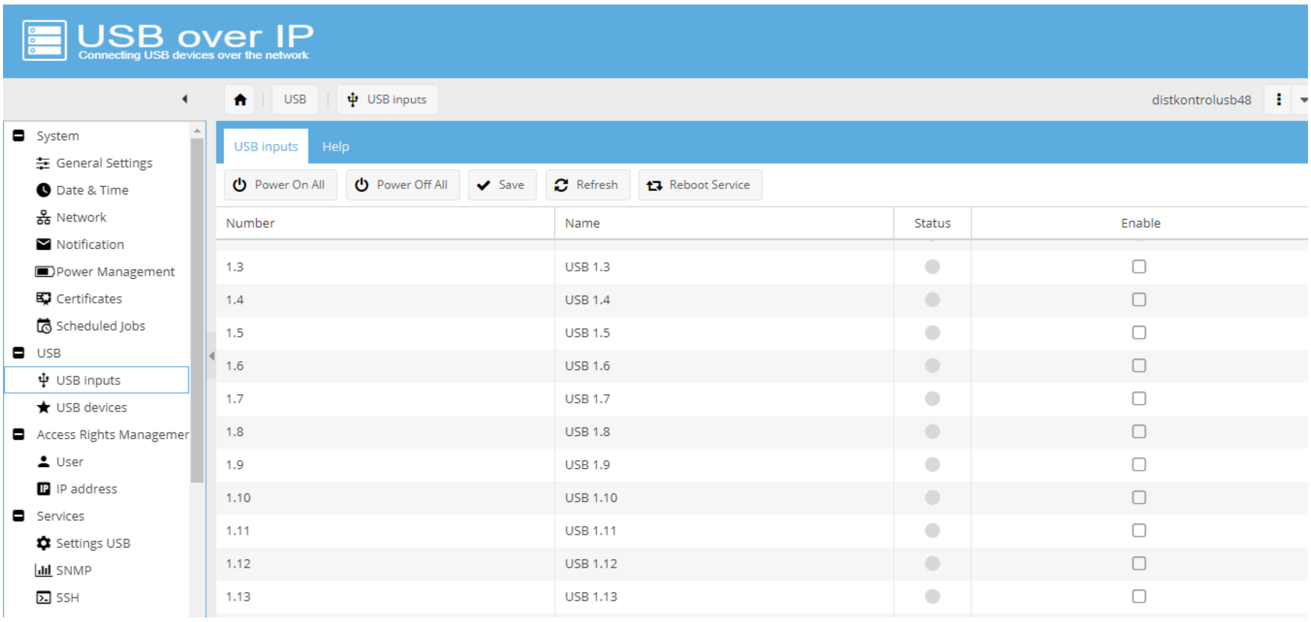
Edit scheduled job

Enable	● on	
Minute	1	● Every N minute
Hour	12	● Every N hour
Day of month	*	○ Every N day of month
Month	*	
Day of week	*	
Command	usbcontrolapi 1 1.4 Input example:usbcontrolapi 0 1.1	
Send email	○ Send command output via email An email message with the command output (if any	

4.3 USB

4.3. 1 USB PORTS

The name of the USB port can be changed. Turning on and off the USB ports of the managed USB over IP hub is done by clicking on the corresponding button on the device.



Number	Name	Status	Enable
1.3	USB 1.3	●	□
1.4	USB 1.4	●	□
1.5	USB 1.5	●	□
1.6	USB 1.6	●	□
1.7	USB 1.7	●	□
1.8	USB 1.8	●	□
1.9	USB 1.9	●	□
1.10	USB 1.10	●	□
1.11	USB 1.11	●	□
1.12	USB 1.12	●	□
1.13	USB 1.13	●	□

The "Enable All", "Disable All" buttons control all available ports. Name column for USB port names.

If "Display Name" = "DEFAULT" or "default" or "0" will reset the default name.

To apply the changes, you must click on the "Save" button.

To apply changes in the client application, you must click on the "Restart service" button. The service will be restarted.

4.3.2 USB DEVICES

This section is necessary to configure access rights, for more details see "Access settings"

By default, 2 USB devices are added for example. Devices can be added, edited, deleted. Adding manual and Autosearch for connected USB devices to a managed USB over IP hub. The device must have one of the unique parameters: Vendor ID, Product ID or Serial No. It is recommended to add devices via Autosearch.

The Users column lists the users who have been assigned rights to this device.

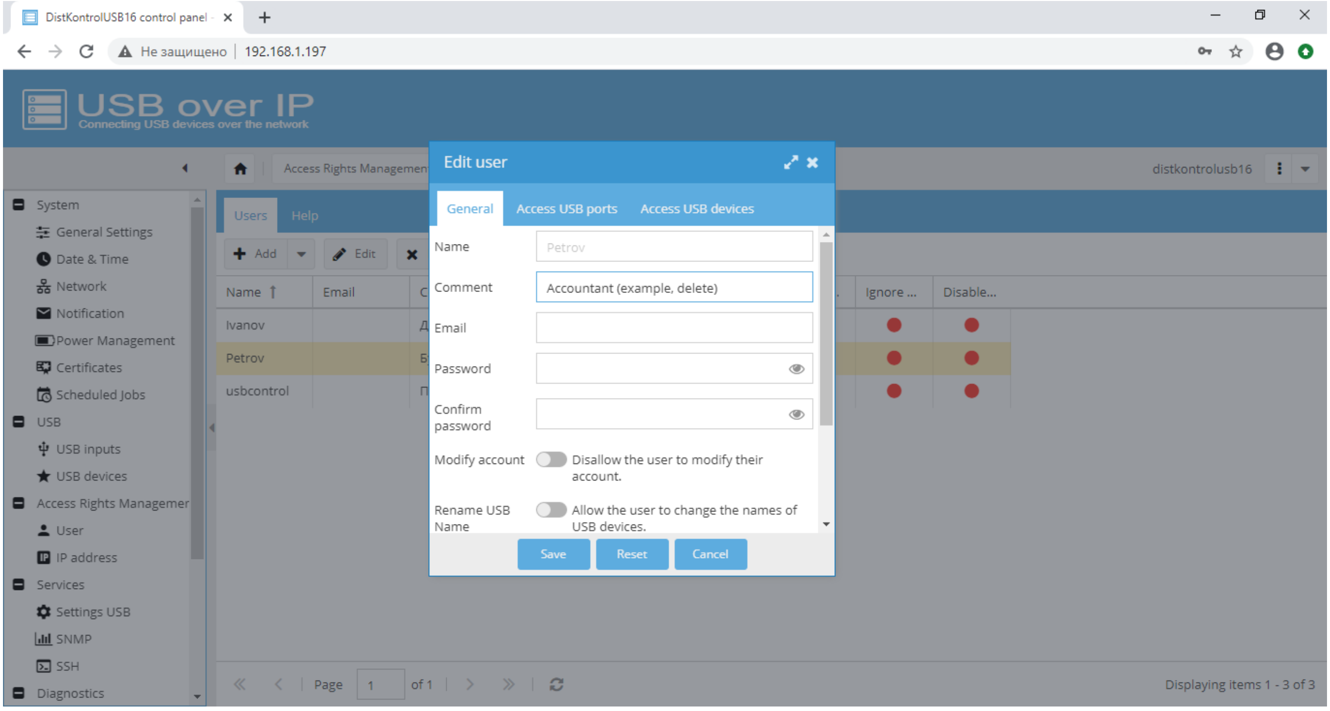
Attention!!! Some USB devices may not work properly. In this case, they will be skipped during autosearch. The search list may not be displayed correctly. Disconnect and reconnect the power to the USB port and search for devices again.

4.4 MANAGEMENT OF ACCESS RIGHTS

4.4.1 USER

For limited granting of rights to enable and disable USB devices, you need to create users of the managed USB over IP hub on the page "Access rights management" - "User".

ATTENTION!!! Username can only be entered in Latin keyboard.



Edit user

Name: Petrov

Comment: Accountant (example, delete)

Email:

Password:

Confirm password:

Modify account: Disallow the user to modify their account.

Rename USB Name: Allow the user to change the names of USB devices.

Name	Email	C	Ignore ...	Disable...
Ivanov		Д	●	●
Petrov		Б	●	●
usbcontrol		П	●	●

Page 1 of 1

Displaying items 1 - 3 of 3

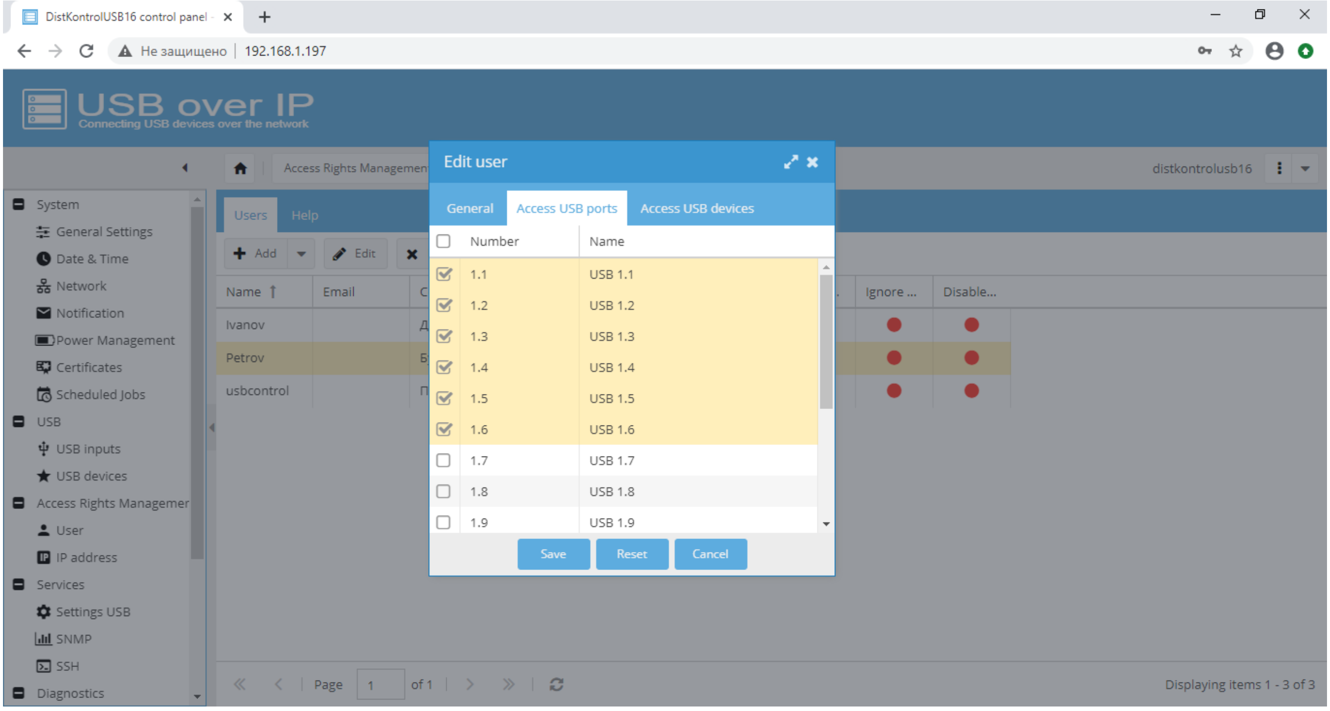
In the initial state, demo users are created on the device (it is recommended to delete them before using the device) and a user - usbcontrol (it is recommended to change the password, but not delete the user).

The usbcontrol user is used for the service function of enabling and disabling the USB ports of the device using the usbcontrol and ssh utility.

ATTENTION!!! When deleting the usbcontrol user, the ability to enable and disable the USB ports of the device using the usbcontrol and ssh utility will be unavailable. **Restoring the usbcontrol user is possible only by resetting the device to its original settings.**

The device has a number of system accounts whose names cannot be used to create a user. When you try to create such a user, the system will display a corresponding warning.

When adding users on the "Access to USB ports" and "Access to USB devices" tabs, you can assign them rights to control USB inputs and rights to connect to USB devices, USB ports. For details, see the section "Restricting access to USB devices, USB ports". Editing user rights and settings is possible after adding.

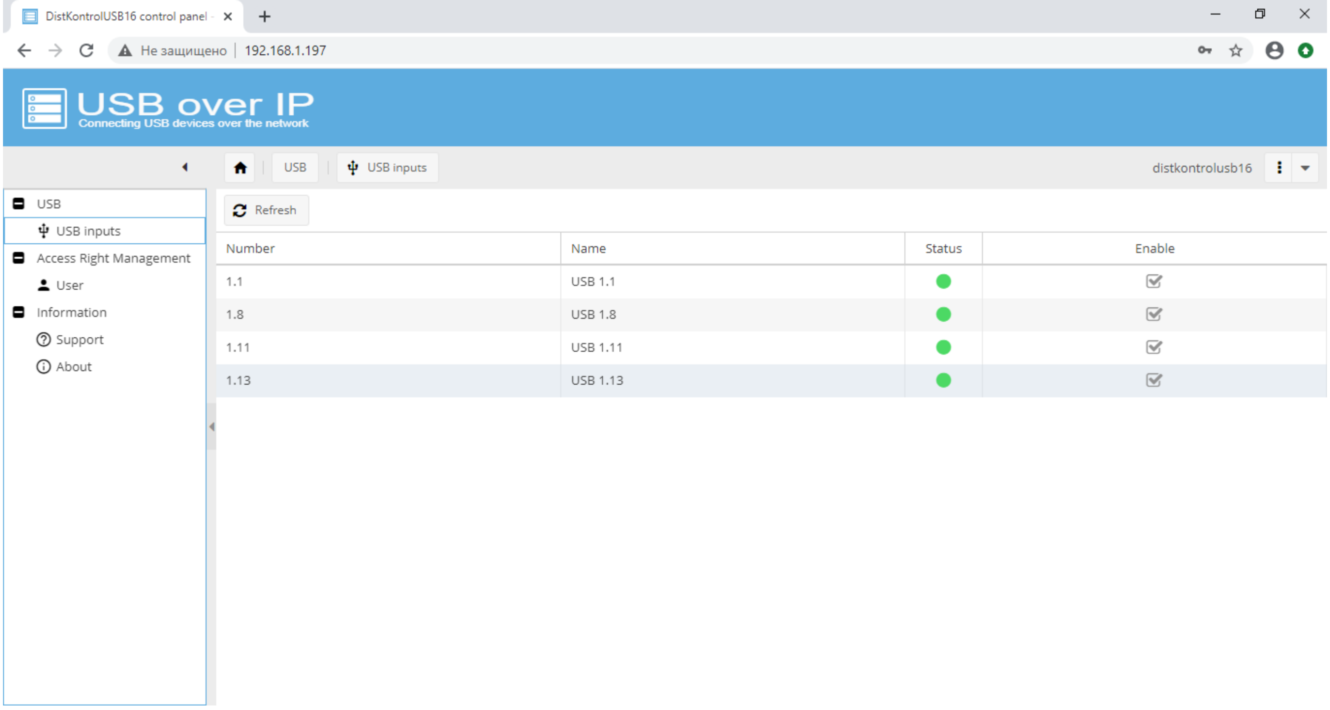


Name	Email	C	Ignore ...	Disable...
Ivanov		Д	●	●
Petrov		Б	●	●
usbcontrol		П	●	●

□	Number	Name
☑	1.1	USB 1.1
☑	1.2	USB 1.2
☑	1.3	USB 1.3
☑	1.4	USB 1.4
☑	1.5	USB 1.5
☑	1.6	USB 1.6
□	1.7	USB 1.7
□	1.8	USB 1.8
□	1.9	USB 1.9

When entering the WEB interface of a managed USB over IP hub under the rights of created users, they can only manage the allowed USB inputs (ports), change the password and e-mail address for sending notifications. The ability to change user data can be disabled in the settings.

To control (turn on and off) the USB inputs of DistKontrolUSB, only the assigned inputs are available to the user, and in the WEB user interface on the “User” page, only those inputs to which the user is granted control rights . See the section on configuring access restrictions.



Number	Name	Status	Enable
1.1	USB 1.1	●	☑
1.8	USB 1.8	●	☑
1.11	USB 1.11	●	☑
1.13	USB 1.13	●	☑

Importing users from Active Directory (AD).

1.Connection:

Enter the correct details to connect to your AD.

Username - the user must have access to get the list of users.

Password - the user's password in AD.

Server address - IP address of the AD server.

User group - a group in AD from which usernames will be unloaded.

Domain Name - The domain name of your network, for example "myad".

Domain zone - the zone of your network, for example "com" or "local".

The domain name and zone will look like "myad.local".

Click the "Connect" button to go to the next step.

If you entered incorrect data, you will receive a corresponding notification from the system.

2.Selection of users:

Select from the list the users you want to add.

The added users will have random passwords.

Users will have default settings.

Click the "Import" button to go to the next step.

You need to apply the settings after completing the next step.

3.Editing users:

Click on the "Update" button to get an up-to-date list of users.

Edit all added users.

Enter the correct password.

Assign the required rights.

Apply the settings.

(Yellow pop-up at the top of the screen.)

4.4.2 IP ADDRESS

This section is necessary to configure access rights, for more details see "Access settings"

By default, 2 IP addresses are added for example. IP can be added, edited, deleted. When creating, editing a device, select the IP family (IPv4 or IPv6).

4.5 SERVICES

4.5.1 USB SETTINGS

4.5.1.1 ACCESS SETTINGS

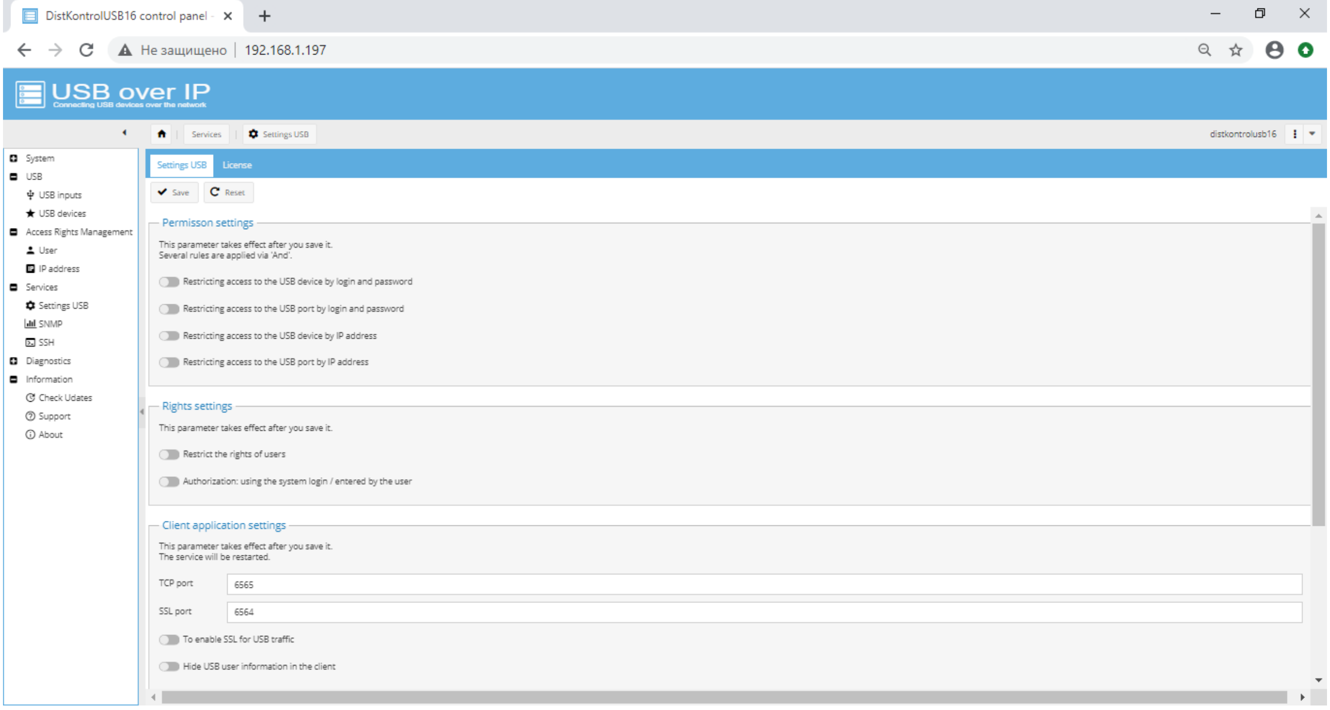
The controlled USB over IP hub has the ability to restrict user access to connected USB devices and ports (authorization to access USB devices and / or ports). There are four ways to limit:

1. Restricting access to a USB device by login and password (authorization by login and password to access a USB device);

2. Restricting access to the USB port by login and password (authorization by login and password to access the USB port);

3. Restricting access to a USB device by IP address (authorization by IP address).

4. Restricting access to the USB port by IP address (authorization by IP address to access the USB port).



Permisson settings

This parameter takes effect after you save it.
Several rules are applied via 'And'.

- Restricting access to the USB device by login and password
- Restricting access to the USB port by login and password
- Restricting access to the USB device by IP address
- Restricting access to the USB port by IP address

Rights settings

This parameter takes effect after you save it.

- Restrict the rights of users
- Authorization: using the system login / entered by the user

Client application settings

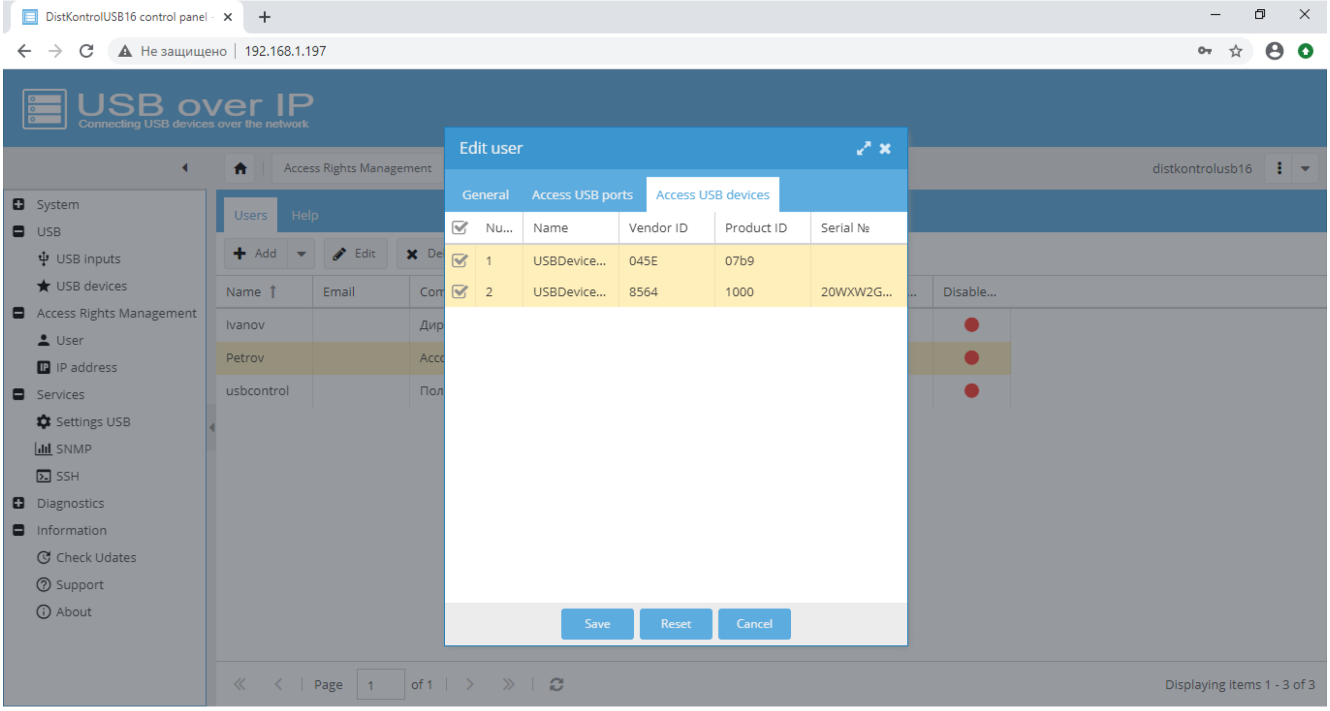
This parameter takes effect after you save it.
The service will be restarted.

TCP port: 6565

SSL port: 6564

- To enable SSL for USB traffic
- Hide USB user information in the client

Restriction modes are enabled on the WEB interface page "Access rights management" - "Access rights" page. By default, all authorization methods are disabled. To enable restriction of user access to connected USB devices, press the corresponding interface button.



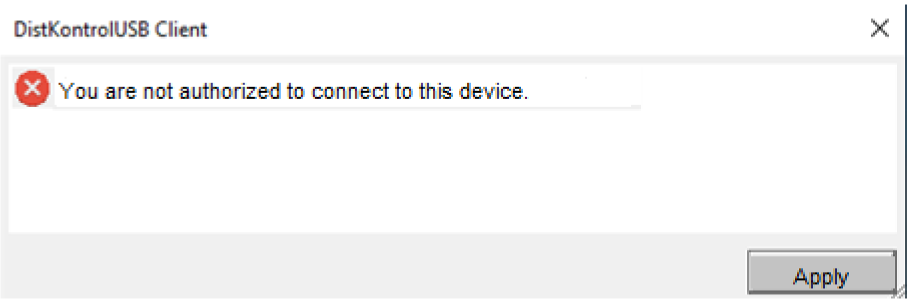
☑	Nu...	Name	Vendor ID	Product ID	Serial №
☑	1	USBDevice...	045E	07b9	
☑	2	USBDevice...	8564	1000	20WXW2G...

Name	Email	Com	Disable...
Ivanov		Дир	●
Petrov		Acc	●
usbcontrol		Пол	●

Modes of restricting user access to USB devices (authorization for access to USB devices) can be used both independently of each other and together in order to increase the security of using USB devices

ATTENTION!!! When used together, the rules are applied through "AND". All enabled rules must be met to grant access to the device. It is recommended to configure access rules one rule at a time, and then enable joint restriction modes..

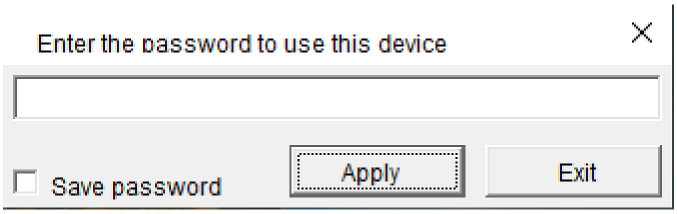
When trying to connect a USB device, without permission, the user will be prompted with a corresponding message:



You are not authorized to connect to this device.

4.5.1.1.1 RESTRICTING ACCESS TO USB DEVICE BY LOGIN AND PASSWORD

When restricting access to a USB device by login and password is enabled - when connected to a USB device, the user will be prompted to enter a password to access the USB device (not the port of a controlled USB over IP hub, namely the USB device, regardless of which port it is connected). The system login is used when connecting (the name of the current computer user from which the connection to the USB device is made) and you do not need to enter it when connecting.



Enter the password to use this device

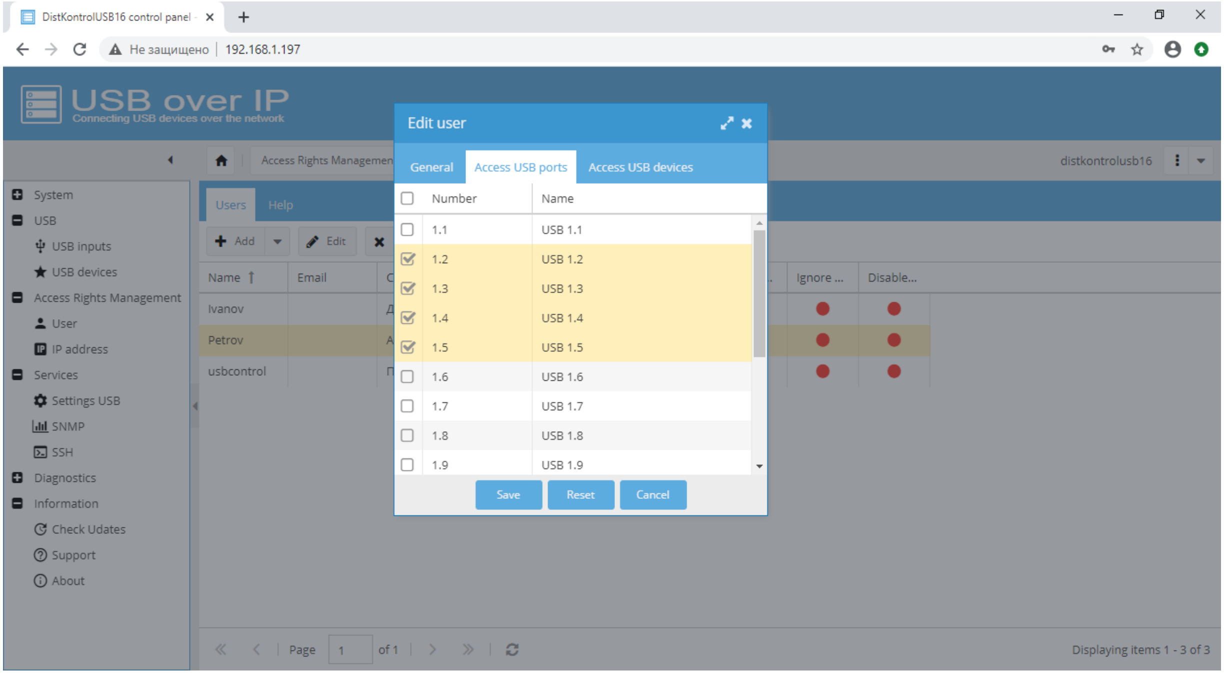
☐ Save password

If the password is entered correctly, the USB device will be connected to the user's computer and will no longer be required to enter the password until the client restarts, even if disconnected and reconnected to the device.

When connected to a USB device (port), when prompted for a password, you can select "Save Password", the user password will be saved and will not be required to enter it on subsequent launches of the application. If the user password is changed, you must first delete the stored password from the user settings file, and at the next password request, enter a new one. To delete the memorized password, you must close the application (do not collapse, which is the default action when you click on the cross in the upper right corner of the program interface). To make changes to the client application settings file, see p. "Configuring a client application controlled by a USB over IP hub" (you can simply delete the settings file to reset all settings of the client application to the original ones).

To configure the mode of restricting access to a USB device by login and password, you must:

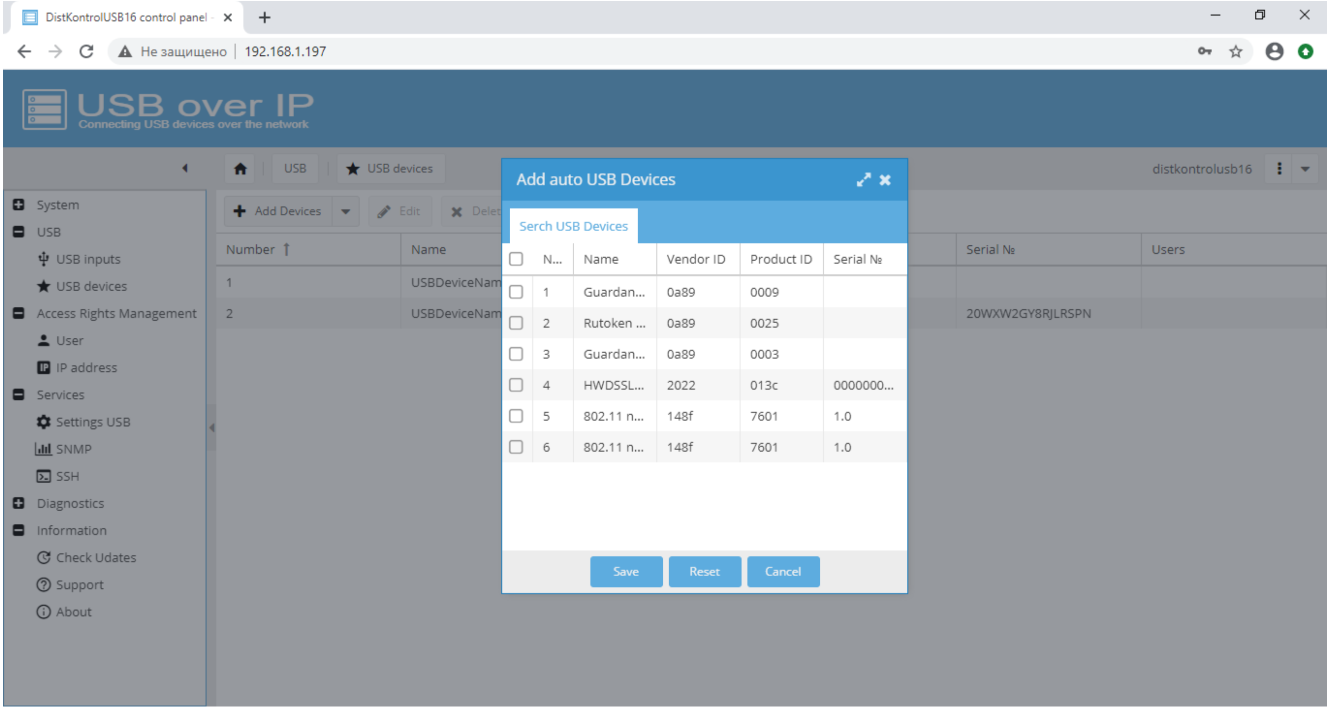
1. On the page of the WEB administrator interface "Services" - "USB devices" add ALL USB devices that will be used. The device works according to the principle: "Everything that is clearly not allowed is prohibited."



☐	Number	Name
☐	1.1	USB 1.1
☑	1.2	USB 1.2
☑	1.3	USB 1.3
☑	1.4	USB 1.4
☑	1.5	USB 1.5
☐	1.6	USB 1.6
☐	1.7	USB 1.7
☐	1.8	USB 1.8
☐	1.9	USB 1.9

USB devices can be added:

- 1. From the automatically generated list of USB devices connected to the hub (included on the "USB inputs" page). "Add devices" - "Auto search". Select the USB devices to be added from the list and click the "Save" button.



Number	Name		Serial №	Users
1	USBDeviceNam			
2	USBDeviceNam		20WXW2GY8RJLRSPN	

Add auto USB Devices

Serch USB Devices

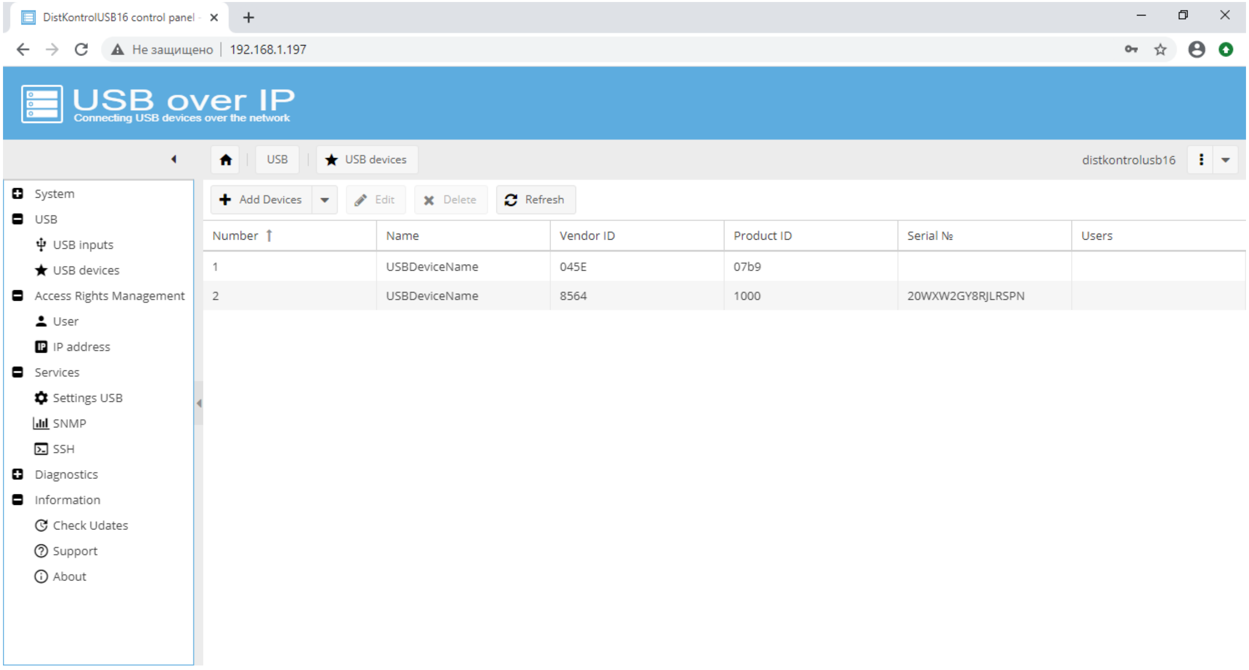
☐	N...	Name	Vendor ID	Product ID	Serial №
☐	1	Guardan...	0a89	0009	
☐	2	Rutoken ...	0a89	0025	
☐	3	Guardan...	0a89	0003	
☐	4	HWDSSL...	2022	013c	0000000...
☐	5	802.11 n...	148f	7601	1.0
☐	6	802.11 n...	148f	7601	1.0

Save | Reset | Cancel

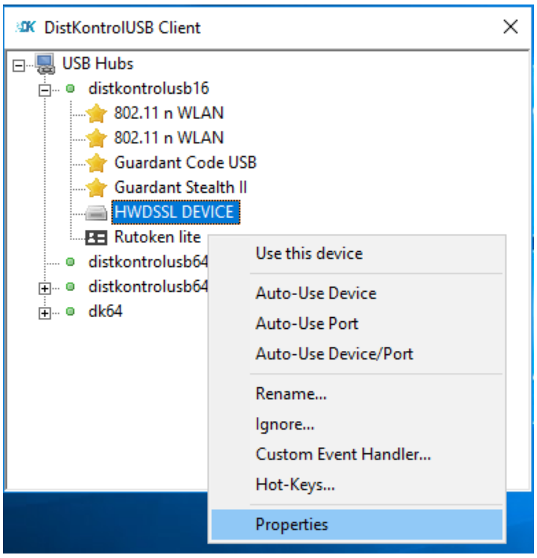
A report on the result of adding USB devices to the list will be issued.

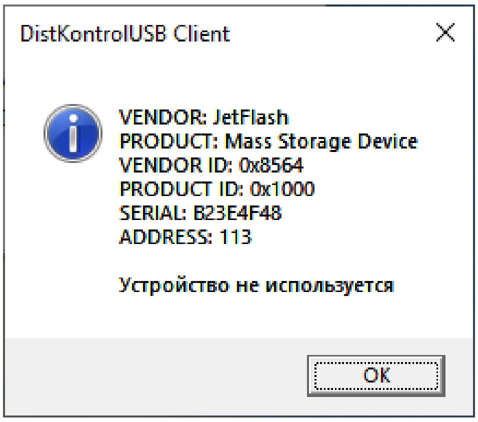
- 2. Manually:

To add USB devices manually, you need to know their VendorID, ProductID and Serial No. They can be viewed in the client



Number	Name	Vendor ID	Product ID	Serial №	Users
1	USBDeviceName	045E	07b9		
2	USBDeviceName	8564	1000	20WXW2GY8RJLRSPN	





VENDOR: JetFlash
PRODUCT: Mass Storage Device
VENDOR ID: 0x8564
PRODUCT ID: 0x1000
SERIAL: B23E4F48
ADDRESS: 113

Устройство не используется

or on the page of the WEB administrator interface "Diagnostics" - "System logs" in the stock of the form:

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

VendorID - 8564

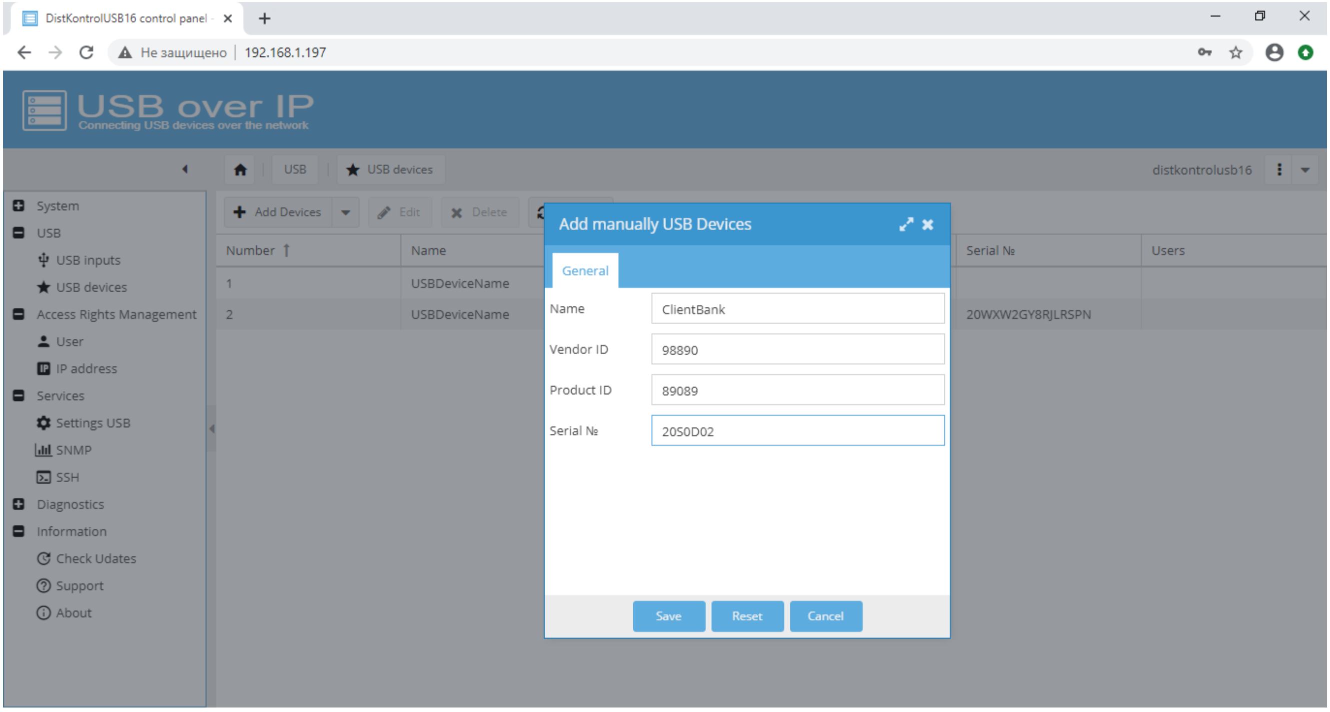
ProductID - 1000

Serial no. - '05KVOF66TU4IHDTZ'

VendorID and ProductID and Serial No. must contain only numbers and Latin letters.

"Add devices" - "Add manually"

In the future, it is possible to delete and edit information about the USB device:

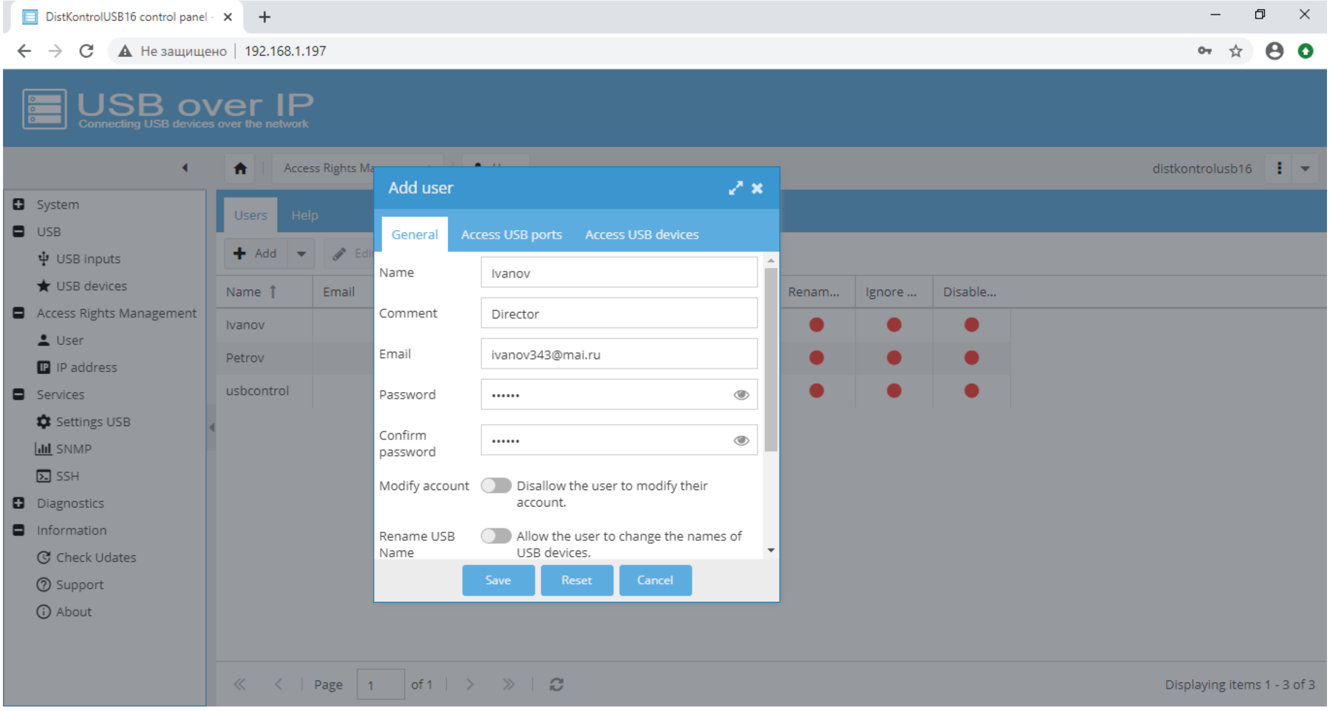


Number	Name	Serial №	Users
1	USBDeviceName		
2	USBDeviceName	20WXW2GY8RJLRSPN	

Name: ClientBank
Vendor ID: 98890
Product ID: 89089
Serial №: 20S0D02

In the factory setting of the product, sample keys are created that can be deleted or edited to use DistKontrolUSB.

2. On the page "Manage access rights" - "User" add users.



Name	Email	Renam...	Ignore ...	Disable...
Ivanov		●	●	●
Petrov		●	●	●
usbcontrol		●	●	●

Add user

General | Access USB ports | Access USB devices

Name	Ivanov
Comment	Director
Email	ivanov343@mai.ru
Password	••••••
Confirm password	••••••
Modify account	Disallow the user to modify their account.
Rename USB Name	Allow the user to change the names of USB devices.

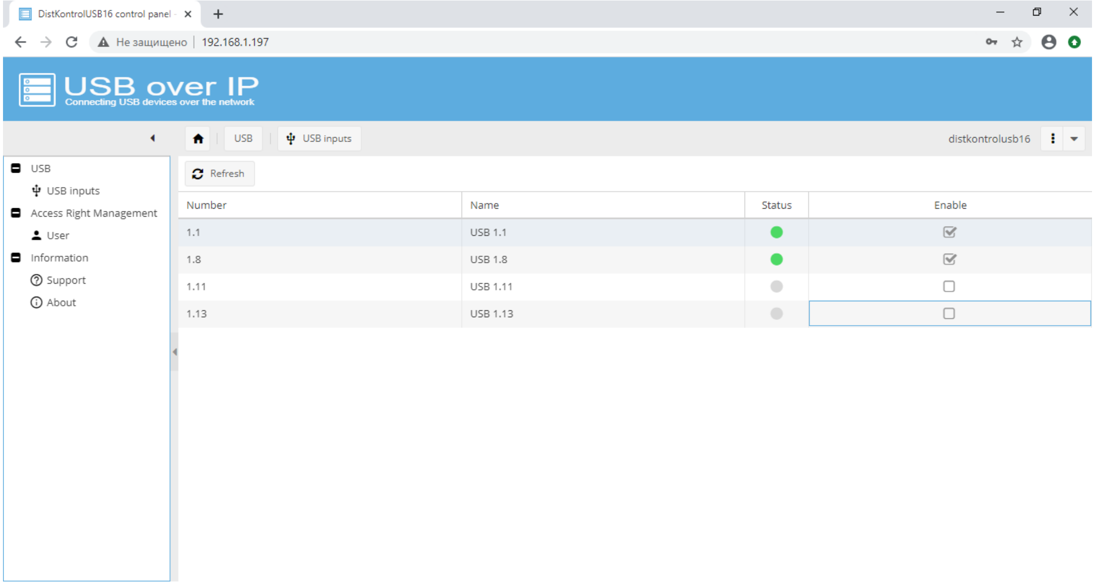
Save | Reset | Cancel

Usernames must MATCH the system username (the name of the current computer user from which the USB device is connected). If necessary, you can also see it (after trying to connect to a USB device) in the system log. See example above. User's email and password - any. It is recommended to use complex passwords.

3. On the tabs "Access to USB ports", "Access to USB device" assign the user access rights to USB ports and / or USB devices. Click the "Save" button in the dialog box.

When assigning rights in the "Access to USB ports" tab, the user will be able to control the power supply of USB ports via the WEB interface and connect USB devices to the selected ports. If no ports are assigned, the user will receive a corresponding notification that they do not have port control rights.

When connecting USB devices, only the designated USB devices and / or USB devices connected to the allowed ports will be available for connection. If you try to connect USB devices that are not assigned to the user, the client application will display a message about the lack of access to the USB device.



Number	Name	Status	Enable
1.1	USB 1.1	●	☑
1.8	USB 1.8	●	☑
1.11	USB 1.11	●	☐
1.13	USB 1.13	●	☐

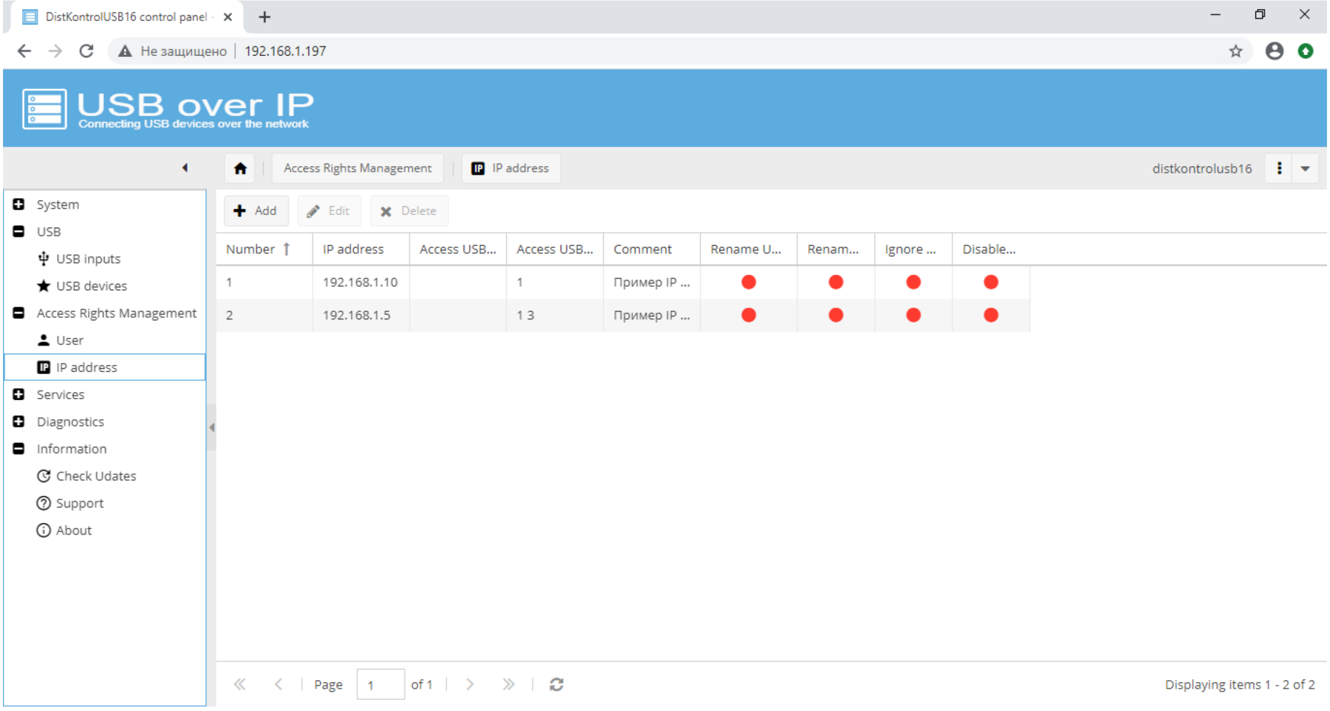
4.5.1.1.2 RESTRICTING ACCESS TO USB PORT BY LOGIN AND PASSWORD

When restricting access to the USB port by login and password is enabled - when connected to a USB device, the user will be prompted to enter a password to access the USB device. The system login is used when connecting (the name of the current computer user from which the connection to the USB device is made) and you do not need to enter it when connecting. Regardless of which USB device is connected to the port, if the user is allowed to use the USB port, they will be given access to the USB device.

Configuring port access rights is described in detail in the previous paragraph.

4.5.1.1.3 RESTRICTING ACCESS TO USB DEVICE BY IP ADDRESS

When restricting access to a USB device by IP address is enabled, the user will be able to connect a USB device only from an IP address with the right to access a USB device (not a port of a controlled USB over IP hub, namely a USB device, regardless of which port it is connected to).



Number	IP address	Access USB...	Access USB...	Comment	Rename U...	Renam...	Ignore ...	Disable...
1	192.168.1.10		1	Пример IP ...	●	●	●	●
2	192.168.1.5		1 3	Пример IP ...	●	●	●	●

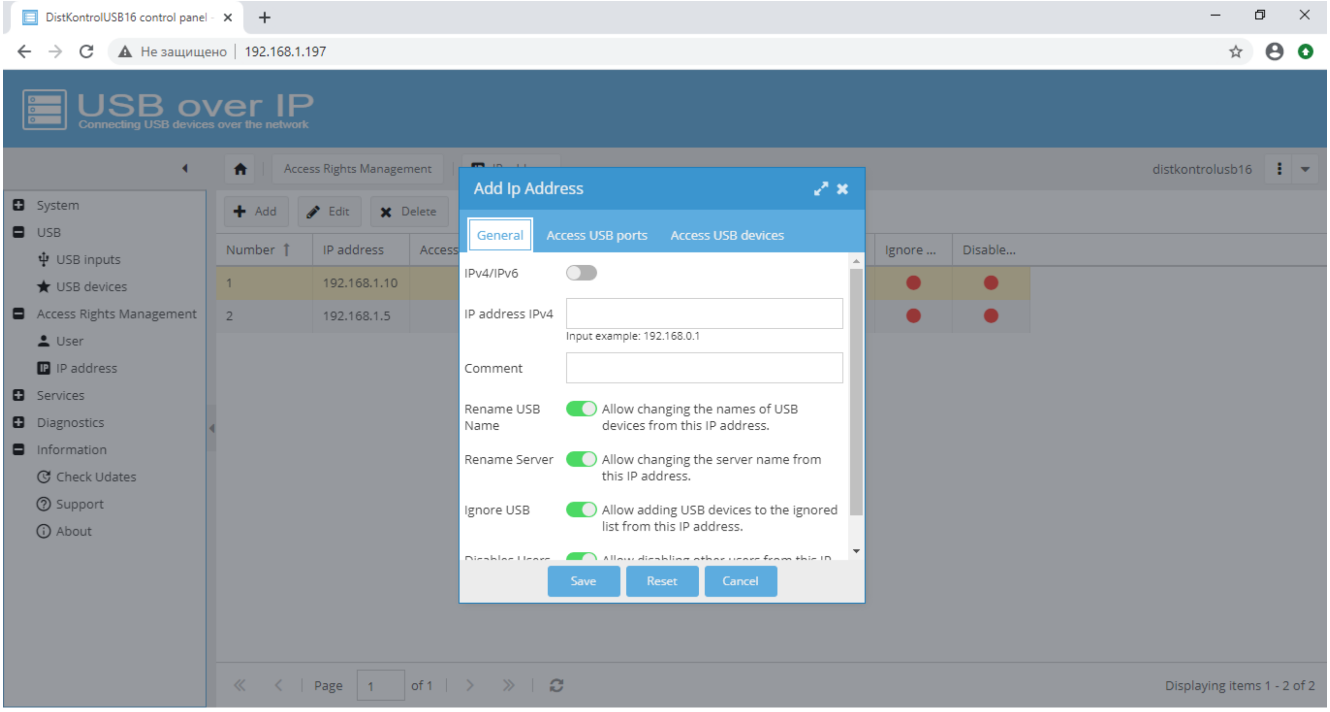
To configure the mode, you must:

1. On the web page of the administrator's interface "Access rights management" - "IP addresses" add ALL IP addresses that will be used. The device works according to the principle: "Everything that is clearly not allowed is prohibited."

It is possible to add and remove information. When adding, you must assign all the necessary rights in the tabs "Access to USB ports", "Access to USB device". Editing is not possible.

.

IP addresses of 192.168.1.1 format are available for input. If you want to add IPv6 format, turn on the IPv4 / IPv6 switch.



Number	IP address	Access	Ignore ...	Disable...
1	192.168.1.10		●	●
2	192.168.1.5		●	●

Add Ip Address

General | Access USB ports | Access USB devices

IPv4/IPv6 ○

IP address IPv4
Input example: 192.168.0.1

Comment

Rename USB Name ● Allow changing the names of USB devices from this IP address.

Rename Server ● Allow changing the server name from this IP address.

Ignore USB ● Allow adding USB devices to the ignored list from this IP address.

Disables Users ● Allow disabling other users from this IP

4.5.1.1.4 RESTRICTING ACCESS TO USB PORT BY IP ADDRESS

When restricting access to the USB port by IP address is enabled, the user will be able to connect a USB device only from an IP address with the right to access the USB port (not a USB device, namely the USB port of a controlled USB over IP hub, regardless of which USB device is connected to connected to it).

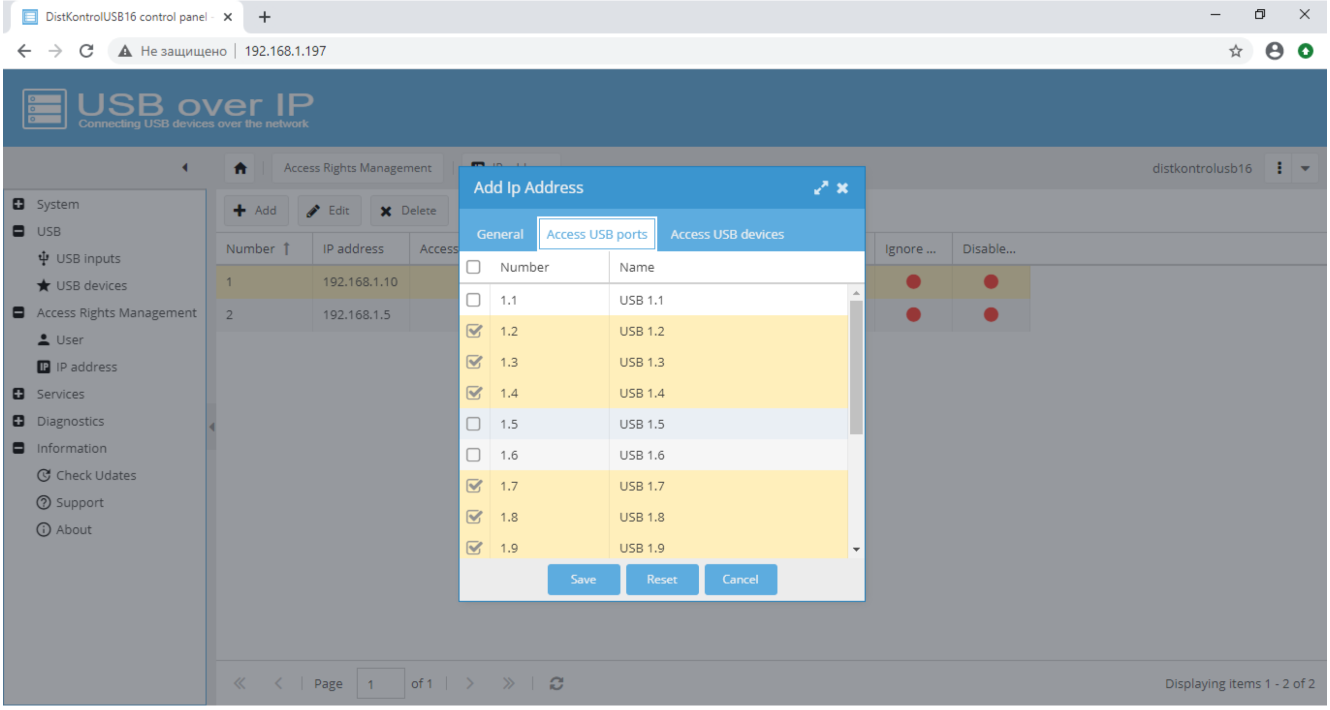
To configure the mode, you must:

1. On the web page of the administrator's interface "Access rights management" - "IP addresses" add ALL IP addresses that will be used. The device works according to the principle: "Everything that is clearly not allowed is prohibited."

It is possible to add and remove information. When adding, you must assign all the necessary rights in the tabs "Access to USB ports", "Access to USB device". Editing is not possible.

IP addresses of 192.168.1.1 format are available for input. If you want to add IPv6 format, turn on the IPv4 / IPv6 switch.

In the "Access to USB devices" tab, check the USB devices to which the user will be allowed access.



Number	IP address	Access	Ignore ...	Disable...
1	192.168.1.10		●	●
2	192.168.1.5		●	●

☐	Number	Name
☐	1.1	USB 1.1
☑	1.2	USB 1.2
☑	1.3	USB 1.3
☑	1.4	USB 1.4
☐	1.5	USB 1.5
☐	1.6	USB 1.6
☑	1.7	USB 1.7
☑	1.8	USB 1.8
☑	1.9	USB 1.9

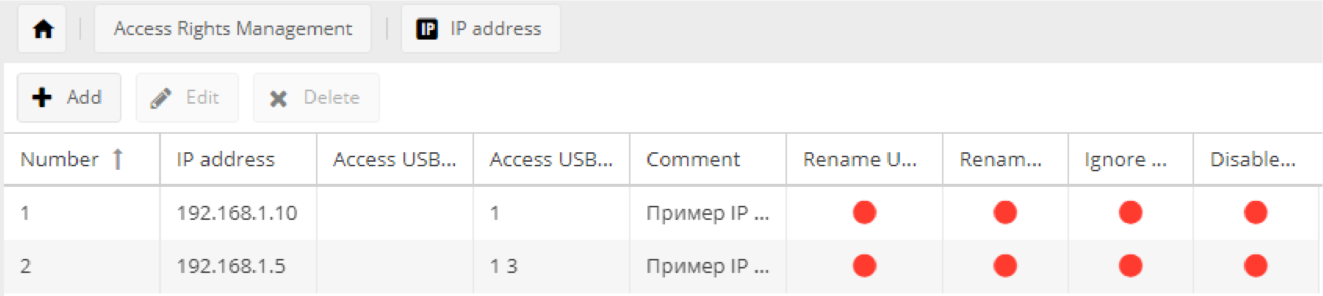
Similarly, in the "Access to USB ports" tab, check the USB ports (inputs) to which the user will be allowed access.

To complete the creation, click on the "Save" button in the dialog box.

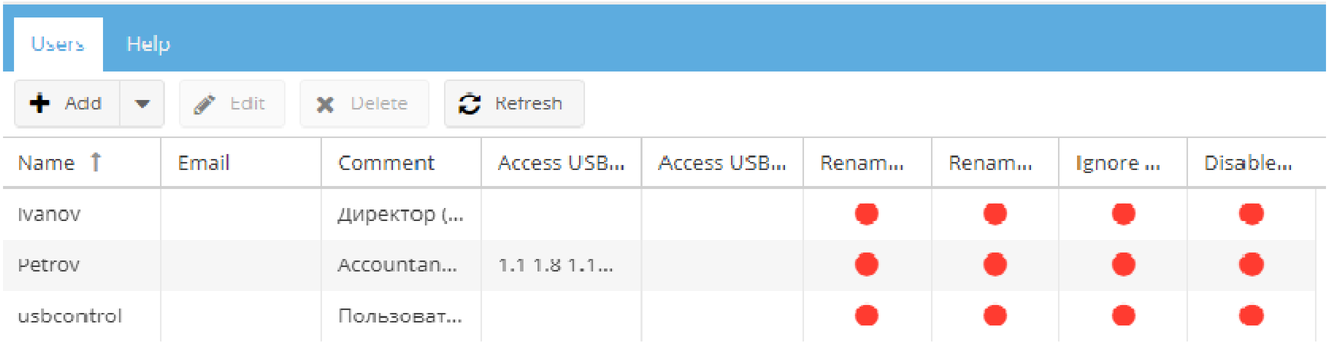
4.5.1.2 ACCESS RIGHTS SETTINGS

The option "Restrict user rights" is disabled by default. In the interface, all rights are marked with a red marker. All users have the rights:

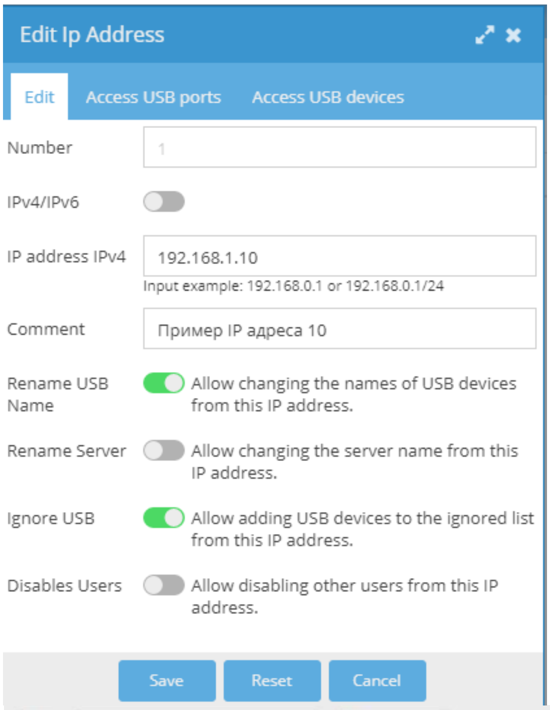
- changing the name of the USB device;
- changing the name of the hub;
- adding USB devices to the list of ignored;
- Disable other users in the DistKontrolUSB Client application (when starting the client application with the -a parameter).



Number	IP address	Access USB...	Access USB...	Comment	Rename U...	Renam...	Ignore ...	Disable...
1	192.168.1.10		1	Пример IP ...	🔴	🔴	🔴	🔴
2	192.168.1.5		1 3	Пример IP ...	🔴	🔴	🔴	🔴



Name	Email	Comment	Access USB...	Access USB...	Renam...	Renam...	Ignore ...	Disable...
Ivanov		Директор (...			🔴	🔴	🔴	🔴
Petrov		Accountan...	1.1 1.8 1.1...		🔴	🔴	🔴	🔴
usbcontrol		Пользоват...			🔴	🔴	🔴	🔴



Number: 1

IPv4/IPv6: ○

IP address IPv4: 192.168.1.10
Input example: 192.168.0.1 or 192.168.0.1/24

Comment: Пример IP адреса 10

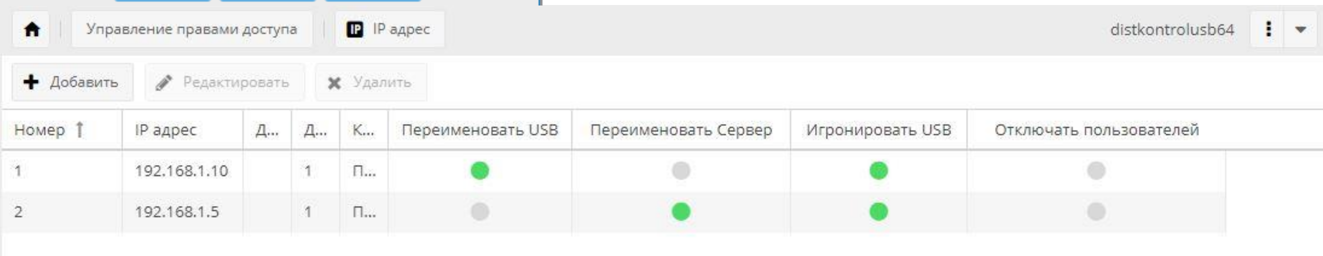
Rename USB Name: ● Allow changing the names of USB devices from this IP address.

Rename Server: ○ Allow changing the server name from this IP address.

Ignore USB: ● Allow adding USB devices to the ignored list from this IP address.

Disables Users: ○ Allow disabling other users from this IP address.

When this option is activated, the rights to use the above options will be determined from the settings of user rights and IP addresses. Permitted actions will be marked with a green marker, not allowed in gray.



Номер	IP адрес	Д...	Д...	К...	Переименовать USB	Переименовать Сервер	Игнорировать USB	Отключать пользователей
1	192.168.1.10		1	П...	🟢	⚪	🟢	⚪
2	192.168.1.5		1	П...	⚪	🟢	🟢	⚪

Permissions for users and IP addresses work according to the "OR" rule

Example 1:

Enabled the option "Restrict user rights"

User Ivanov was not allowed any of the rules

IP address 192.168.1.10 allowed to change the name of the USB device

User Ivanov will not be able to change the name of the USB device if his IP address is not 192.168.1.10

Anyone with the address 192.168.1.10 will be able to change the name of the USB device.

Example 2:

Enabled the option "Restrict user rights"

User Ivanov was allowed to disconnect other users

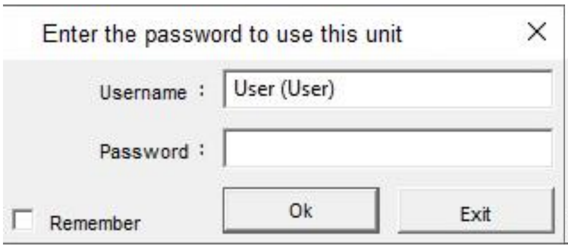
IP address 192.168.1.10 was allowed to change the server name

User Ivanov will be able to disconnect other users if his IP address is 192.168.1.10 he can also change the server name.

All users with the address 192.168.1.10 will be able to change the server name.

The option "Authorization: use system username / entered by user" by default is "use system username". A window with a password request will be displayed only when restrictions on access rights by login and password are enabled.

When activated, the user will be able to enter a login different from the system one while connecting the USB device.

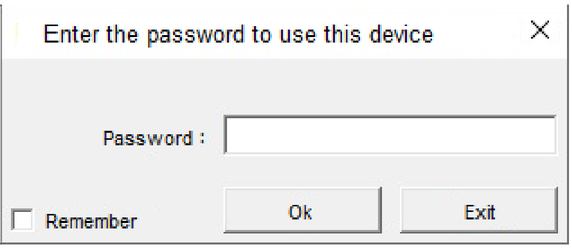


Enter the password to use this unit

Username : User (User)

Password :

□ Remember



Enter the password to use this device

Password :

□ Remember

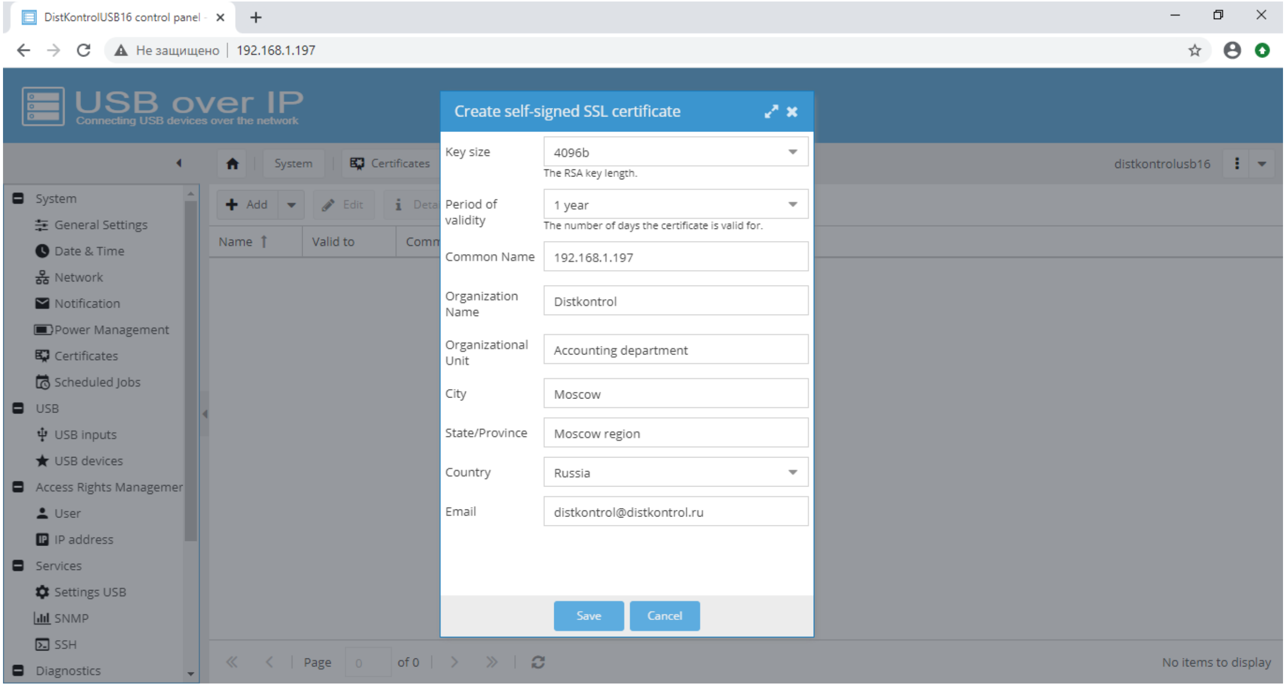
4.5.1.3 CLIENT APPLICATION PARAMETERS

The USB over IP managed hub supports Secure Socket Layer (SSL) for client / server communications. This is useful when sharing USB devices over the Internet to provide better protection against eavesdropping. Commercial or self-signed certificates can be used.

The mode is enabled on the "Services" - "USB settings" - "Enable SSL for USB traffic" page. After enabling the mode and (or) adding certificates, you need to reboot the device for the changes to take effect

Create a self-signed server certificate (or buy one from a Certification Authority). You can also use the self-signed DistKontrolUSB certificate. It can be downloaded on the page: "System" - "Certificates" - "SSL" - "Download certificate" or "Information" - "Support" - "DistKontrolUSB self-signed certificate" When setting up the device, it is recommended to use it first. Next, use a commercial or create your own self-signed certificate.

You can create your own self-signed certificate in the device WEB interface on the page: "System" - "Certificates" - "SSL" select "Add" - "Create"



Create self-signed SSL certificate

Key size: 4096b
The RSA key length.

Period of validity: 1 year
The number of days the certificate is valid for.

Common Name: 192.168.1.197

Organization Name: Distkontrol

Organizational Unit: Accounting department

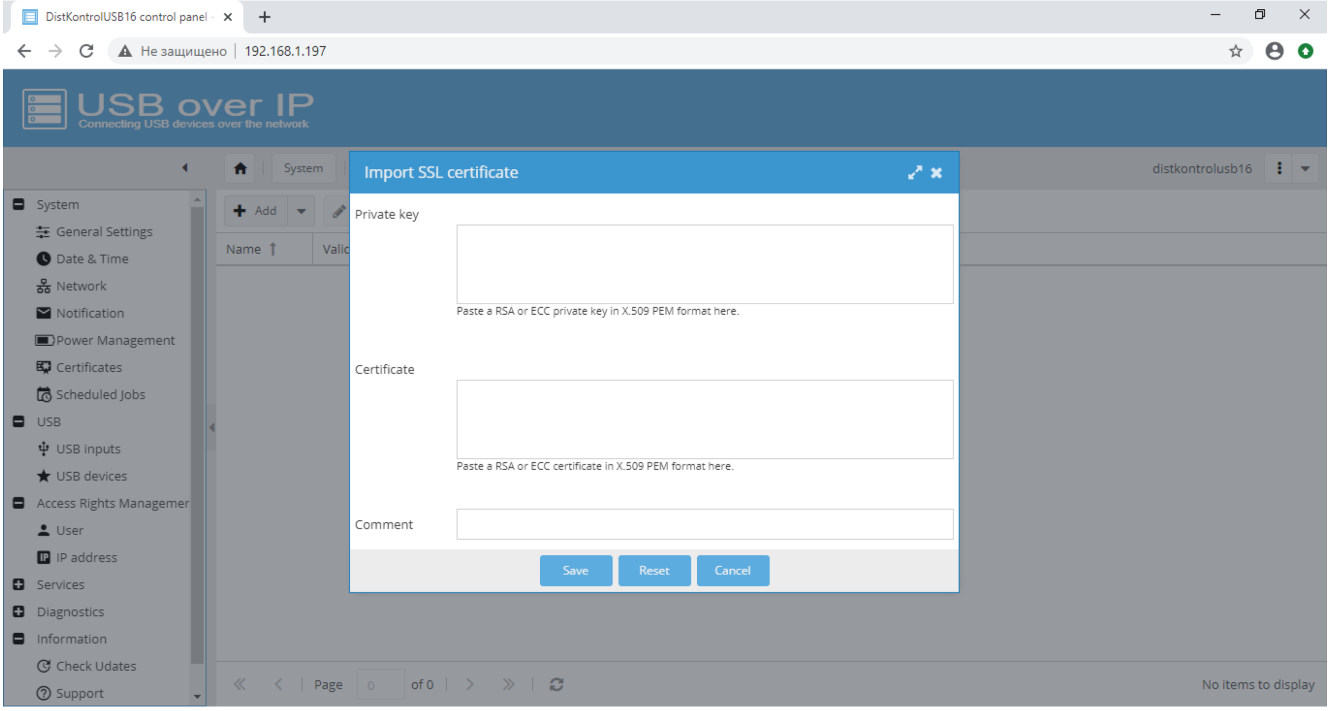
City: Moscow

State/Province: Moscow region

Country: Russia

Email: distkontrol@distkontrol.ru

It is possible to import an existing certificate. (required: private RSA key in X.509 PEM format and RSA certificate X.509 in PEM format), for this select "Add" - "Import"



Import SSL certificate

Private key

Paste a RSA or ECC private key in X.509 PEM format here.

Certificate

Paste a RSA or ECC certificate in X.509 PEM format here.

Comment

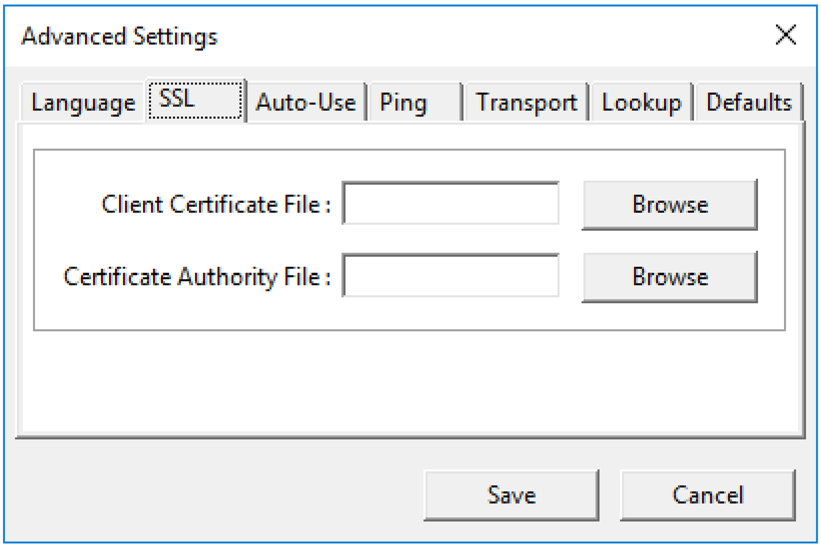
When creating multiple SSL certificates, the last one created (imported) will be used to encrypt USB traffic. The certificate for the client application can be downloaded on the page: "System" - "Certificates" - "SSL" - "Download certificate" or "Information" - "Support" - "DistKontrolUSB self-signed certificate". It will be updated to match the last one created (imported).

ATTENTION!!! The device uses OpenSSL to encrypt traffic. If you need to create a certificate outside the device, we recommend generating it using 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
```

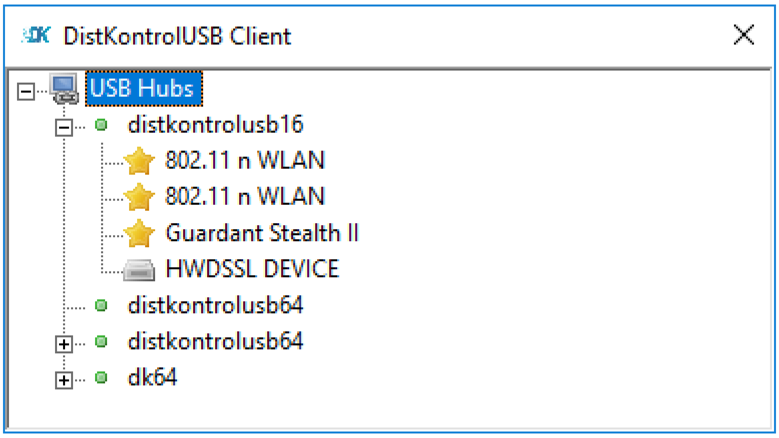
In the client application, right-click "USB Hubs" - "Advancent Settings". On the SSL tab, in the Sertificate Authority File line, click Browse and select your pem certificate. Click “Save” and agree to restart the client application.

ATTENTION!!! On a number of OSes, the path to the certificate should not be in Cyrillic for correct operation. It is recommended to use the Latin alphabet for the names of the folders where the certificate is stored.



After configuration, the client automatically connects to the USB over IP managed hub using TLSv1.2 through the default SSL port 6564. If you do not use Auto Search, you need to enter the address of the managed USB over IP hub in the Specify Hubs and specify port 6564.

After successful connection of the client application to DustKontrolUSB, the device in the client will be displayed with the corresponding icon.



SSL port can be changed in the WEB interface. If you want to use a port other than the default ssl port, you will need to make changes to the INI file with client settings. Close the client application. Edit the INI file for the client and add a line under

[General]

………………

SSLPort = 5554 (SSL port set in the WEB interface)

then start the client. The client will now expect the connection on port 5554 to use ssl.

4.5.1.4 CLEANING AND RESET

In some cases, it becomes necessary to prohibit the use of a USB device. This can be done from the client application. Right click on the corresponding USB device and select "Ignore". If the USB device has a serial number, you will be prompted to add to the list of unused only this device or all with the same VendorID and ProductID.

Clearing the list of unused USB devices is carried out in the WEB interface of the managed USB over IP hub on the "Services" - "USB settings" - "Clear list of ignored devices" page. After clearing the list of unused devices, a device restart is required.

It is possible to rename USB devices in the client application. With the right mouse button on the device, call the window - Rename. Enter the desired name - Click OK. All users will see the name change.

In the WEB interface of the device on the page "Services" - "USB settings" - "Reset the name of USB devices to the original", it is possible to reset the names to the original ones. A reset will restart the service.

To reset all settings of the client application, in the WEB interface of the device on the page "Services" - "USB Settings" - "Reset USB over IP service parameters to their original values." A reset will restart the service.

This will reset port numbers, ssl settings and hidden device display, device names and hiding.

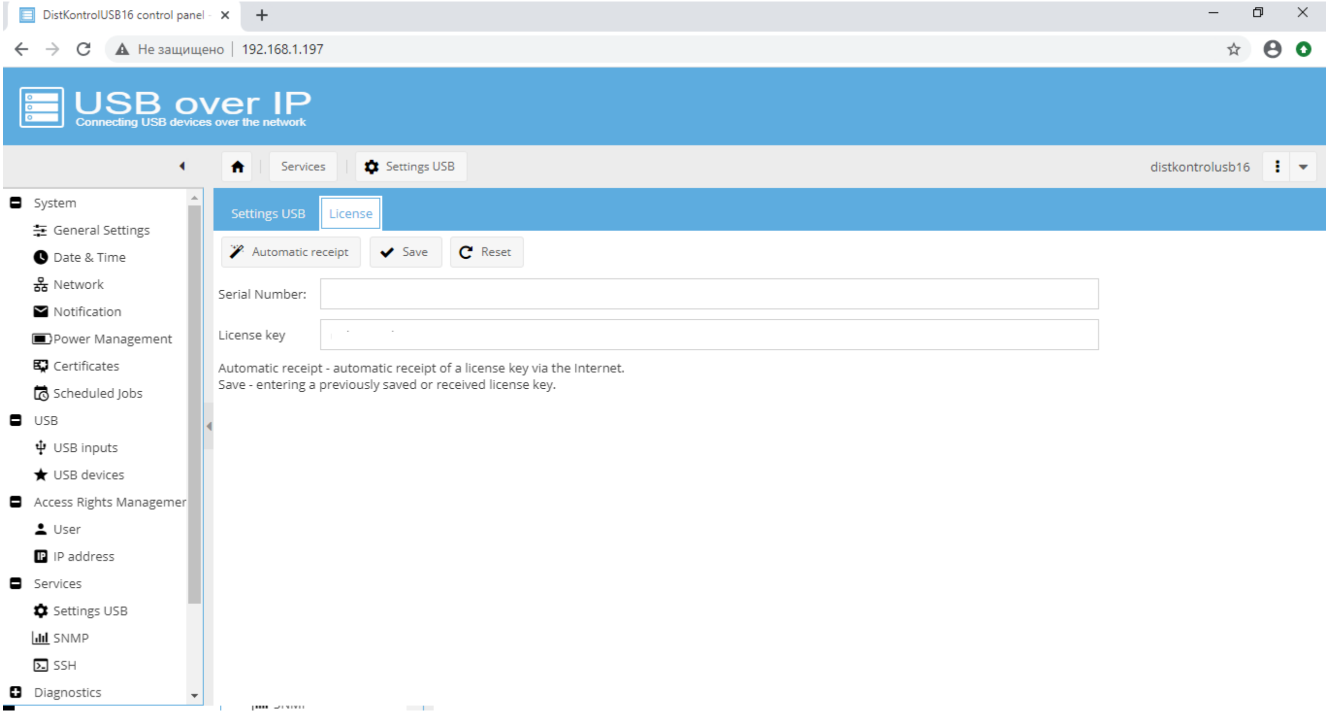
.

4.5.1.5 LICENSE

After resetting the device to original settings or updating, you must turn on the device and wait for it to boot. The end of the download is indicated by the appearance of the device, and the client application and the availability of the device's WEB interface.

After downloading, you must enter the license key for the software. It can be entered in any of three ways:

1. In the WEB interface of the hub automatically - by clicking on the "Get automatically" button on the "Services" - "USB settings" - "License" page. The key will be obtained automatically (the hub must have access to the Internet) and no additional steps are required.



Serial Number:

License key

Automatic receipt - automatic receipt of a license key via the Internet.
Save - entering a previously saved or received license key.

2. In the WEB interface of the concentrator manually - enter the previously saved or received license key and click the "Save" button.

3. Through the client application manually. To enter the license key, after launching the client application, right-click on “USB Hubs” in the client, select “License” - “Enter License” and in the window that opens, insert the received key and click “OK”.

To manually enter the license key:

1. It can be copied and saved on the License page before upgrading or resetting the hub to factory settings.

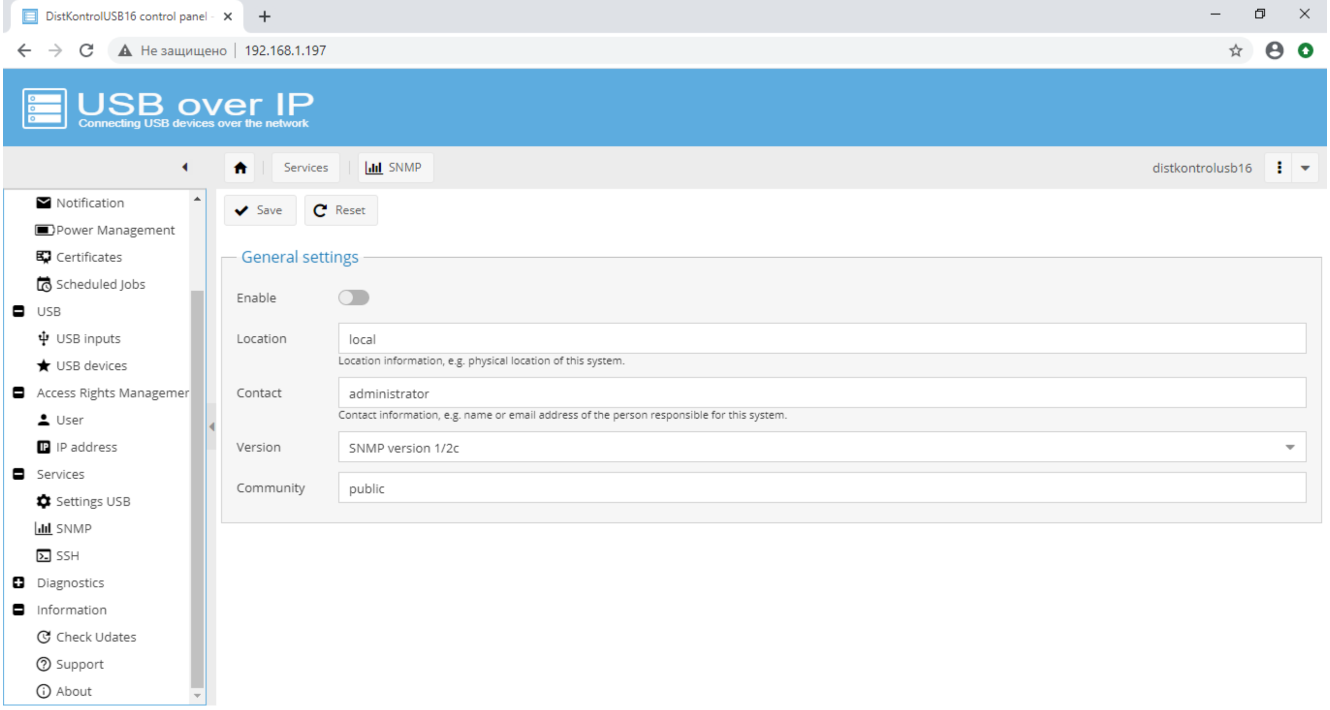
2. Request by e-mail support@distkontrol.ru, indicating the serial number of the product.

The serial number of the product can be viewed on the page "Services" - "USB settings" - "License" or by starting the client application. Right-click on the device name in the client, select the "Properties" menu item and copy from the "SERIAL NUMBER" line (RECOMMENDED) or in the device passport (on the last page below).

4.5.2 SNMP

The USB over IP managed hub supports SNMP versions 1, 2c, 3. The SNMP support makes it easy to monitor the status of the hub and USB inputs using various monitoring systems. For example, Zabbix, Nagios, etc.

By default, SNMP (Simple Network Management Protocol) is disabled. The protocol is enabled and configured on the "Services" - "SNMP" page.



General settings

Enable ○

Location: local
Location information, e.g. physical location of this system.

Contact: administrator
Contact information, e.g. name or email address of the person responsible for this system.

Version: SNMP version 1/2c

Community: public

To configure SNMP versions 1, 2c:

Element	Description
Enable	Select whether the hub will use SNMP.
Location	Location information, such as the physical location of this system. It can contain up to 64 characters.
Contact Person	Contact information, such as the name or email address of the person in charge of this system. It can contain up to 64 characters.
Version	SNMP version used
Communities	Enter the community name to authenticate requests. It can contain up to 32 characters. (Can be used as a password)

To configure SNMP version 3, you must additionally specify:

- Username,
- Security level. This security feature allows you to set up authentication based on user requirements. 3 levels of authentication:
  - NoAuthNoPriv: Users who use this mode / level have no authentication and no privacy when sending / receiving messages.
  - AuthNoPriv: This level requires the user to authenticate, but there will be no encryption of sent / received messages.
  - AuthPriv: Finally, the most secure layer in which authentication is required and messages sent / received are encrypted.
- Authentication Type and User Password (when you select a security level with authentication),
- Confidentiality Type (data encryption) and Password (if you select the confidentiality security level).

List of OID (Object Identifier) for information

about the state of the managed USB over IP hub via SNMP:

OID (Object Identifier)	**Parameter**	**Notes**
.1.3.6.1.4.1.2021.9.12.1	CPU temperature	
.1.3.6.1.4.1.2021.9.12.2	CPU Load	
.1.3.6.1.4.1.2021.10.1.3.1	1 minute CPU Load	
.1.3.6.1.4.1.2021.10.1.3.2	5 minute CPU Load	
.1.3.6.1.4.1.2021.10.1.3.3	15 minute CPU Load	
.1.3.6.1.4.1.2021.11.11.0	Idle CPU time (%)	
.1.3.6.1.4.1.2021.4.6.0	Total RAM used	

.1.3.6.1.4.1.2021.4.11.0	Total RAM Free	
.1.3.6.1.2.1.25.1.1.0	Uptime устройства	
.1.3.6.1.4.1.2021.20.1.1	USB port status 1.1	On / off (1/0)
.1.3.6.1.4.1.2021.20.1.2	USB port status 1.2	On / off (1/0)
.1.3.6.1.4.1.2021.20.1.3	USB port status 1.3	On / off (1/0)
.1.3.6.1.4.1.2021.20.1.4	USB port status 1.4	On / off (1/0)
.1.3.6.1.4.1.2021.20.1.5	USB port status 1.5	On / off (1/0)
.1.3.6.1.4.1.2021.20.1.6	USB port status 1.6	On / off (1/0)
.1.3.6.1.4.1.2021.20.1.7	USB port status 1.7	On / off (1/0)
.1.3.6.1.4.1.2021.20.1.8	USB port status 1.8	On / off (1/0)
.1.3.6.1.4.1.2021.20.1.9	USB port status 1.9	On / off (1/0)
.1.3.6.1.4.1.2021.20.1.10	USB port status 1.10	On / off (1/0)
.1.3.6.1.4.1.2021.20.1.11	USB port status 1.11	On / off (1/0)
.1.3.6.1.4.1.2021.20.1.12	USB port status 1.12	On / off (1/0)
.1.3.6.1.4.1.2021.20.1.13	USB port status 1.13	On / off (1/0)
.1.3.6.1.4.1.2021.20.1.14	USB port status 1.14	On / off (1/0)
.1.3.6.1.4.1.2021.20.1.15	USB port status 1.15	On / off (1/0)
.1.3.6.1.4.1.2021.20.1.16	USB port status 1.16	On / off (1/0)
.1.3.6.1.4.1.2021.20.2.1	USB port status 2.1	On / off (1/0)
.1.3.6.1.4.1.2021.20.2.2	USB port status 2.2	On / off (1/0)
.1.3.6.1.4.1.2021.20.2.3	USB port status 2.3	On / off (1/0)
.1.3.6.1.4.1.2021.20.2.4	USB port status 2.4	On / off (1/0)
.1.3.6.1.4.1.2021.20.2.5	USB port status 2.5	On / off (1/0)
.1.3.6.1.4.1.2021.20.2.6	USB port status 2.6	On / off (1/0)
.1.3.6.1.4.1.2021.20.2.7	USB port status 2.7	On / off (1/0)

.1.3.6.1.4.1.2021.20.2.8	USB port status 2.8	On / off (1/0)
.1.3.6.1.4.1.2021.20.2.9	USB port status 2.9	On / off (1/0)
.1.3.6.1.4.1.2021.20.2.10	USB port status 2.10	On / off (1/0)
.1.3.6.1.4.1.2021.20.2.11	USB port status 2.11	On / off (1/0)
.1.3.6.1.4.1.2021.20.2.12	USB port status 2.12	On / off (1/0)
.1.3.6.1.4.1.2021.20.2.13	USB port status 2.13	On / off (1/0)
.1.3.6.1.4.1.2021.20.2.14	USB port status 2.14	On / off (1/0)
.1.3.6.1.4.1.2021.20.2.15	USB port status 2.15	On / off (1/0)
.1.3.6.1.4.1.2021.20.2.16	USB port status 2.16	On / off (1/0)
.1.3.6.1.4.1.2021.20.3.1	USB port status 3.1	On / off (1/0)
.1.3.6.1.4.1.2021.20.3.2	USB port status 3.2	On / off (1/0)
.1.3.6.1.4.1.2021.20.3.3	USB port status 3.3	On / off (1/0)
.1.3.6.1.4.1.2021.20.3.4	USB port status 3.4	On / off (1/0)
.1.3.6.1.4.1.2021.20.3.5	USB port status 3.5	On / off (1/0)
.1.3.6.1.4.1.2021.20.3.6	USB port status 3.6	On / off (1/0)
.1.3.6.1.4.1.2021.20.3.7	USB port status 3.7	On / off (1/0)
.1.3.6.1.4.1.2021.20.3.8	USB port status 3.8	On / off (1/0)
.1.3.6.1.4.1.2021.20.3.9	USB port status 3.9	On / off (1/0)
.1.3.6.1.4.1.2021.20.3.10	USB port status 3.10	On / off (1/0)
.1.3.6.1.4.1.2021.20.3.11	USB port status 3.11	On / off (1/0)
.1.3.6.1.4.1.2021.20.3.12	USB port status 3.12	On / off (1/0)
.1.3.6.1.4.1.2021.20.3.13	USB port status 3.13	On / off (1/0)
.1.3.6.1.4.1.2021.20.3.14	USB port status 3.14	On / off (1/0)
.1.3.6.1.4.1.2021.20.3.15	USB port status 3.15	On / off (1/0)
.1.3.6.1.4.1.2021.20.3.16	USB port status 3.16	On / off (1/0)

.1.3.6.1.4.1.2021.20.4.1	USB port status 4.1	On / off (1/0)
.1.3.6.1.4.1.2021.20.4.2	USB port status 4.2	On / off (1/0)
.1.3.6.1.4.1.2021.20.4.3	USB port status 4.3	On / off (1/0)
.1.3.6.1.4.1.2021.20.4.4	USB port status 4.4	On / off (1/0)
.1.3.6.1.4.1.2021.20.4.5	USB port status 4.5	On / off (1/0)
.1.3.6.1.4.1.2021.20.4.6	USB port status 4.6	On / off (1/0)
.1.3.6.1.4.1.2021.20.4.7	USB port status 4.7	On / off (1/0)
.1.3.6.1.4.1.2021.20.4.8	USB port status 4.8	On / off (1/0)
.1.3.6.1.4.1.2021.20.4.9	USB port status 4.9	On / off (1/0)
.1.3.6.1.4.1.2021.20.4.10	USB port status 4.10	On / off (1/0)
.1.3.6.1.4.1.2021.20.4.11	USB port status 4.11	On / off (1/0)
.1.3.6.1.4.1.2021.20.4.12	USB port status 4.12	On / off (1/0)
.1.3.6.1.4.1.2021.20.4.13	USB port status 4.13	On / off (1/0)
.1.3.6.1.4.1.2021.20.4.14	USB port status 4.14	On / off (1/0)
.1.3.6.1.4.1.2021.20.4.15	USB port status 4.15	On / off (1/0)
.1.3.6.1.4.1.2021.20.4.16	USB port status 4.16	On / off (1/0)

4.5.2.1 EXAMPLES OF CHECKING SNMP CONFIGURATION OF A MANAGED USB OVER IP HUB.

Before configuring the monitoring system, it is recommended to make sure that data is received from the device correctly. Port 161 / TCP must be open.

Linux example using snmpget (must be installed).

We input:

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

or (depending on the selected SNMP version)

```
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
```

We get:

```
iso.3.6.1.4.1.2021.9.12.1 = INTEGER: 52
```

Example for **Windows**, using SnmpGet (must be installed):

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

or (depending on the selected SNMP version)

```
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
```

We get:

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

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

OID=.1.3.6.1.4.1.2021.9.12.1

Type=Integer

Value=52
```

4.5.2.2 EXAMPLE OF ZABBIX CONFIGURATION FOR MONITORING STATUS OF A MANAGED USB OVER IP HUB.

To start monitoring the status of the USB over IP hub and its USB inputs via SNMP using the Zabbix monitoring system, the following steps must be performed:

Step 1

Create a host for the device.

Enter the IP address. Click on "Add" to save the host.

Step 2

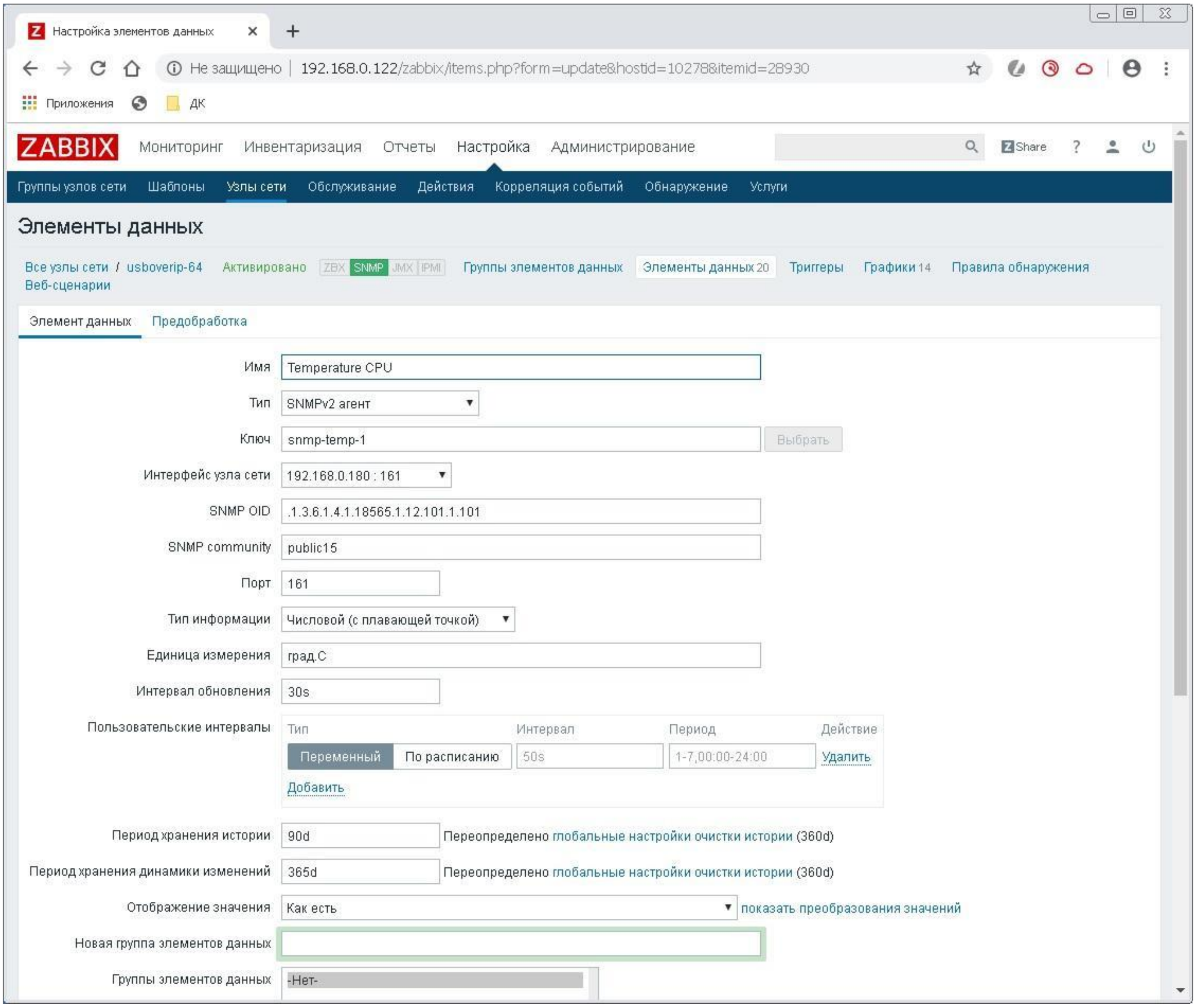
Check the user manual for the SNMP OID of the item you want to monitor.

Step 3

Create an item to monitor.

In Zabbix click on Items, select the SNMP host you created earlier. Enter a simple description in Russian (or English) in the 'Description' field in the new item dialog. Make sure your hub is in the Host field and change the Type field to SNMPv * agent. Enter “community” (usually public) and enter the numeric OID you received earlier in the “SNMP OID” field, for example: .1.3.6.1.4.1.2021.9.12.1

Enter SNMP Port - 161 and Key - something meaningful like SNMP-Temperature. Set "Information Type" to Numeric (floating point). Select a multiplier if you want, and specify the "Refresh interval", and "History retention" if you want the parameter values to differ from the default.



Элементы данных

Все узлы сети / usboverip-64 Активировано ZBX SNMP JMX 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 [Выбрать]
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
Пользовательские интервалы	Тип: [Переменный] По расписанию; Интервал: 50s; Период: 1-7,00:00-24:00; Действие: Удалить Добавить
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 ▾ показать преобразования значений
Новая группа элементов данных	
Группы элементов данных	-Нет-

All required input fields are marked with a red asterisk.

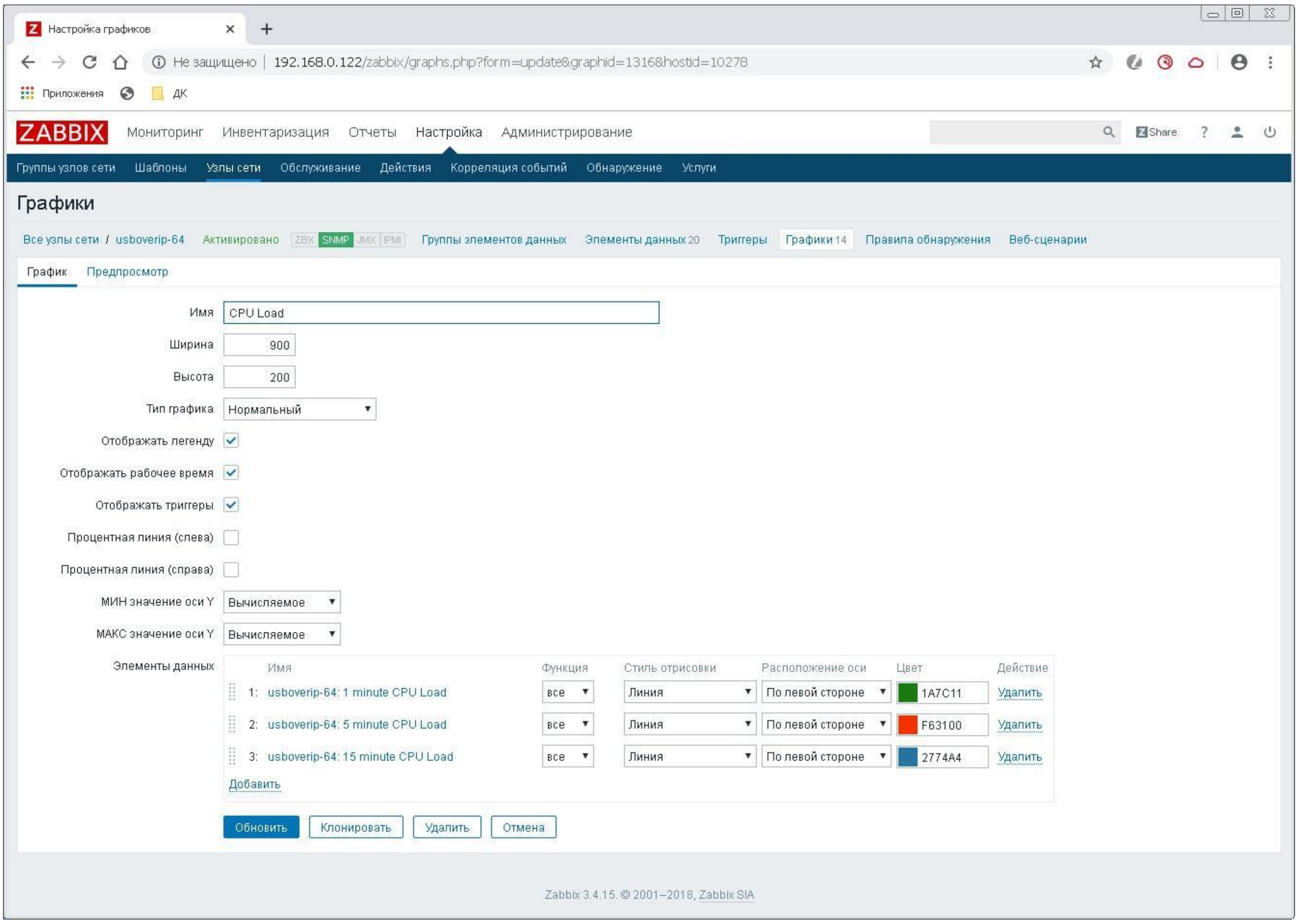
Save the item and go to Monitoring → Latest Data to see SNMP data.

Note the specific options available only for SNMPv3 items. In case of incorrect SNMPv3 credentials (security name, authentication protocol / passphrase, security protocol) Zabbix will receive ERROR from net-snmp, except for an erroneous Security Passphrase, in which case Zabbix will receive a TIME OUT error from net-snmp.

If you make changes to the Authentication Protocol, Authentication Passphrase, Security Protocol, or Security Passphrase, you must restart the server for these changes to take effect.

Step 4

Next, we create graphs for the required data items.



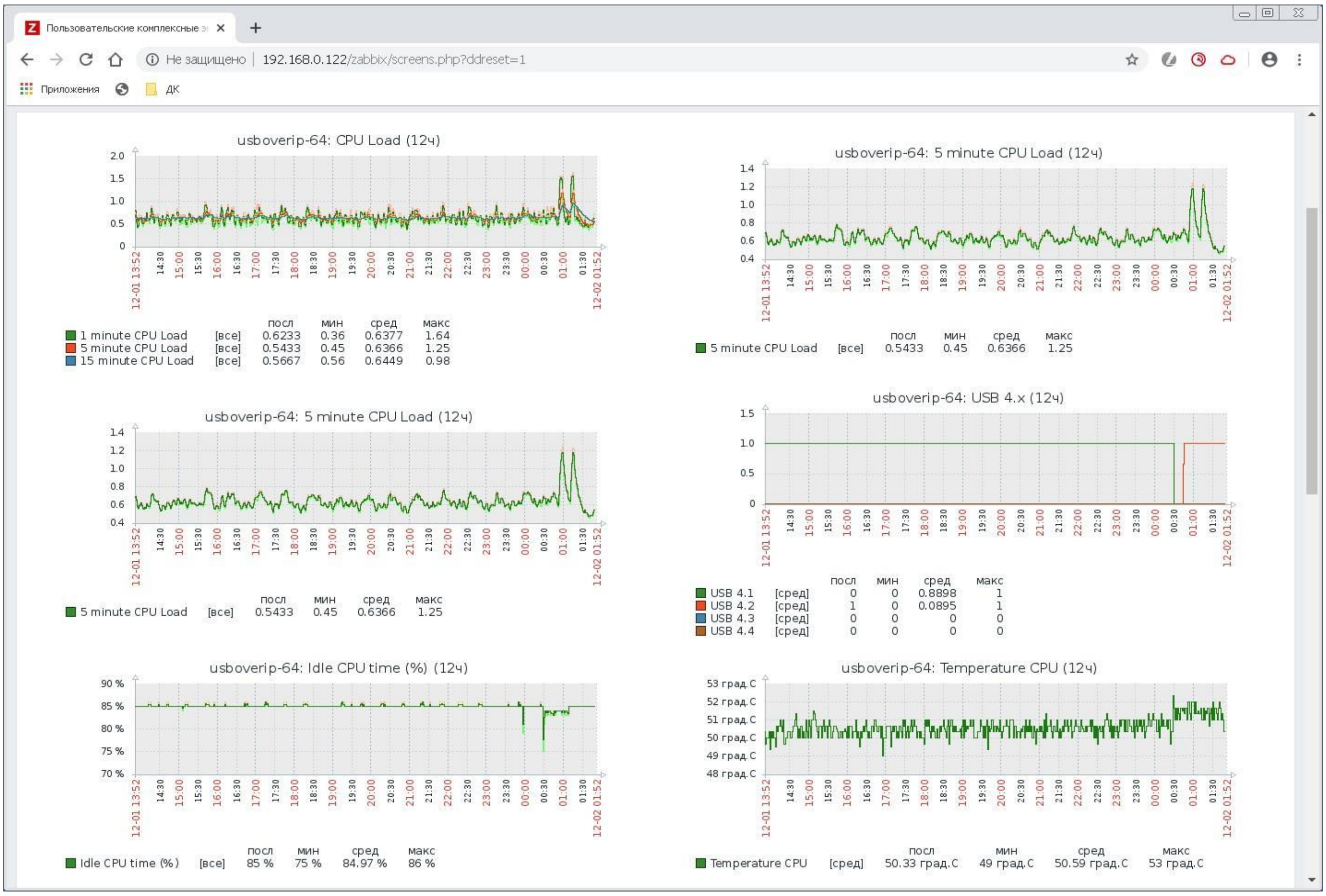
Графики

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

Step 5: Next, create complex screens:



usboverip-64: CPU Load (12ч)

		посл	мин	сред	макс
🟩 1 minute CPU Load	[все]	0.6233	0.36	0.6377	1.64
🟥 5 minute CPU Load	[все]	0.5433	0.45	0.6366	1.25
🟦 15 minute CPU Load	[все]	0.5667	0.56	0.6449	0.98

usboverip-64: 5 minute CPU Load (12ч)

		посл	мин	сред	макс
🟩 5 minute CPU Load	[все]	0.5433	0.45	0.6366	1.25

usboverip-64: 5 minute CPU Load (12ч)

		посл	мин	сред	макс
🟩 5 minute CPU Load	[все]	0.5433	0.45	0.6366	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	1
🟦 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.C	49 град.C	50.59 град.C	53 град.C

4.5.3 SSH

SSH is used to work with the UsbControl utility. More details on how to work with the utility can be found in the section "Brief instructions on using the utility for managing ports of a managed USB over IP hub"

4.6 DIAGNOSTICS

4.6.1 BOARD

Board with information. It is possible to add, hide, close, resize and drag windows. It is the start page for entering the Web interface.

4.6.2 SYSTEM INFORMATION

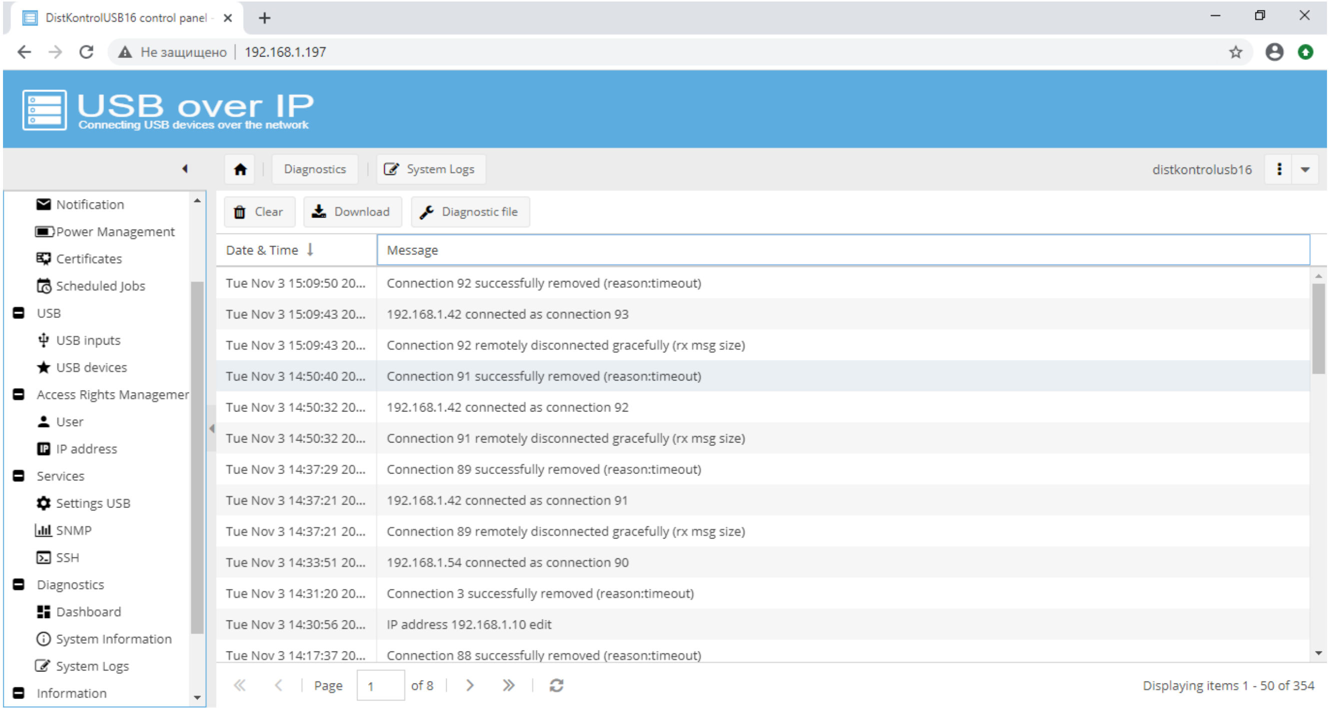
This section provides information about the firmware version, system time, CPU and RAM load parameters.

4.6.3 SYSTEM JOURNAL

Viewing the system log is possible on the page of the WEB administrator interface "Diagnostics" - "System logs".

The log contains all information about connections and disconnections of both USB inputs (ports) of DistKontrolUSB, and any of the USB devices, as well as attempts to enter the password incorrectly. Changes to the hub settings and other service information are also recorded.

The diagnostic file is required when contacting technical support.



Date & Time	Message
Tue Nov 3 15:09:50 20...	Connection 92 successfully removed (reason:timeout)
Tue Nov 3 15:09:43 20...	192.168.1.42 connected as connection 93
Tue Nov 3 15:09:43 20...	Connection 92 remotely disconnected gracefully (rx msg size)
Tue Nov 3 14:50:40 20...	Connection 91 successfully removed (reason:timeout)
Tue Nov 3 14:50:32 20...	192.168.1.42 connected as connection 92
Tue Nov 3 14:50:32 20...	Connection 91 remotely disconnected gracefully (rx msg size)
Tue Nov 3 14:37:29 20...	Connection 89 successfully removed (reason:timeout)
Tue Nov 3 14:37:21 20...	192.168.1.42 connected as connection 91
Tue Nov 3 14:37:21 20...	Connection 89 remotely disconnected gracefully (rx msg size)
Tue Nov 3 14:33:51 20...	192.168.1.54 connected as connection 90
Tue Nov 3 14:31:20 20...	Connection 3 successfully removed (reason:timeout)
Tue Nov 3 14:30:56 20...	IP address 192.168.1.10 edit
Tue Nov 3 14:17:37 20...	Connection 88 successfully removed (reason:timeout)

Displaying items 1 - 50 of 354

The line [Connect Client] -> displays the parameters of connecting a USB device by the user in the following sequence:

User: User login

Pswd: User password (MD5 hash) (if a password is entered)

IP: user's IP address

Port: USB port

Name: Alias of the USB device (in case the device was renamed)

V_ID: VENDOR_ID of USB device

P_ID: PRODUCT_ID of USB device

Serial: Serial No. of USB device

Path: Current USB device number used by user (internal service)

The line is written to the log every time a client connects a USB device, regardless of the mode of access to USB devices.

4.6.3.1 AUTHORIZATION MESSAGES

Login and password authorization to access the USB device.

[Authorization Client] The user ‘NAME’ was not found in the database - The user was not found in the hub database.

[Authorization Client] The user 'NAME' found - The user was found in the hub database.

[Authorization Client] Password OK (or BAD) - Unsuccessful (or successful) verification of the username and password for connecting to the USB device. In square brackets Username to connect from.

[Authorization Client] The USB device was not found in the database - The USB device to be connected is not in the list of USB devices.

[Authorization Client] The user 'NAME' does not have permission to connect USB devices. - The user does not have any permitted USB devices.

[Authorization Client] DEVICE OK (or BAD) - Unsuccessful (or successful) verification of the user's permission to use the connected USB device. The first parameter in square brackets is the No. of the USB device to which the connection is made, the second is the list of USB devices allowed for the user.

Authorization by IP address to access the USB device.

[Authorization Client] The IP 'IP address' not found in the database - The IP address was not found in the hub database.

[Authorization Client] The IP 'IP address' found - The IP address was found in the hub base.

[Authorization Client] DEVICE OK (or BAD) - Unsuccessful (or successful) check of permission to connect USB devices from this IP. In square brackets, the first parameter is the number of the USB device from the list of USB devices, the second is the list of USB devices allowed for this IP.

Authorization by IP address to access the USB port of the hub.

[Authorization Client] The IP 'IP address' not found in the database - The IP address was not found in the hub database.

[Authorization Client] The IP 'IP address' found - The IP address was found in the hub base.

[Authorization Client] PORT OK (or BAD) - N Unsuccessful (or successful) check of permission to connect USB port from this IP. In square brackets, the first parameter is the number of the USB port to which the connection is made, the second is the list of allowed ports for this IP.

BOUND to connection X - Successful connection of the USB device;

UNBOUND from connection X - Successfully disconnected the USB device.

4.6.3.2 USB POWER MANAGEMENT MESSAGES

[USB PORTS] // Control port // USER: Petrov USB in: 2.3 STATUS: turnOn (turnoff) - Enable (disable) USB port 2.3 by the user "Petrov"

4.6.3.3 OTHER MESSAGES

All messages in the system log of the USB over IP managed hub are recorded with date and time. For the correct operation of the device time service, it must be configured in the "System" - "Date and Time" section.

Also, other service information about the operation of the device is recorded in the system log of the managed USB over IP hub.

It is possible to clear the log and download it to the user's computer for further storage and analysis.

Thus, when analyzing the syslog messages, you can diagnose various problems when restricting access to USB devices and ports to configure it as required.

General message structure:

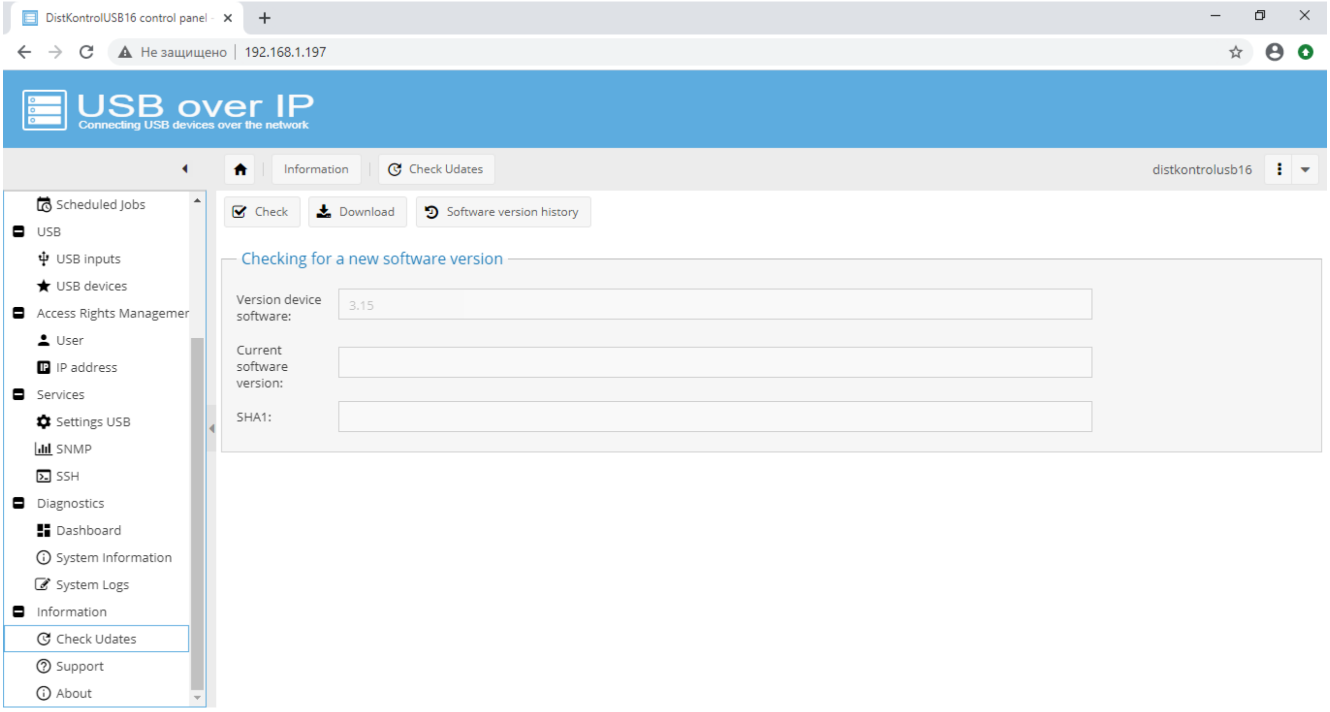
[USB Settings] Restricting access to the USB port by login and password - DISABLED:

- [USB Settings] - Log of the "USB Settings" section
- Restricting access to the USB port by login and password - the name of the changed parameter
- DISABLED - parameter status.

4.7 INFORMATION

4.7.1 CHECK FOR UPDATES

The page allows you to check the current software version and compare with the installed version on the hub.



Checking for a new software version

Version device software: 3.15

Current software version:

SHA1:

To request the current version, you must click on the "Check" button (Requires hub access to the Internet).

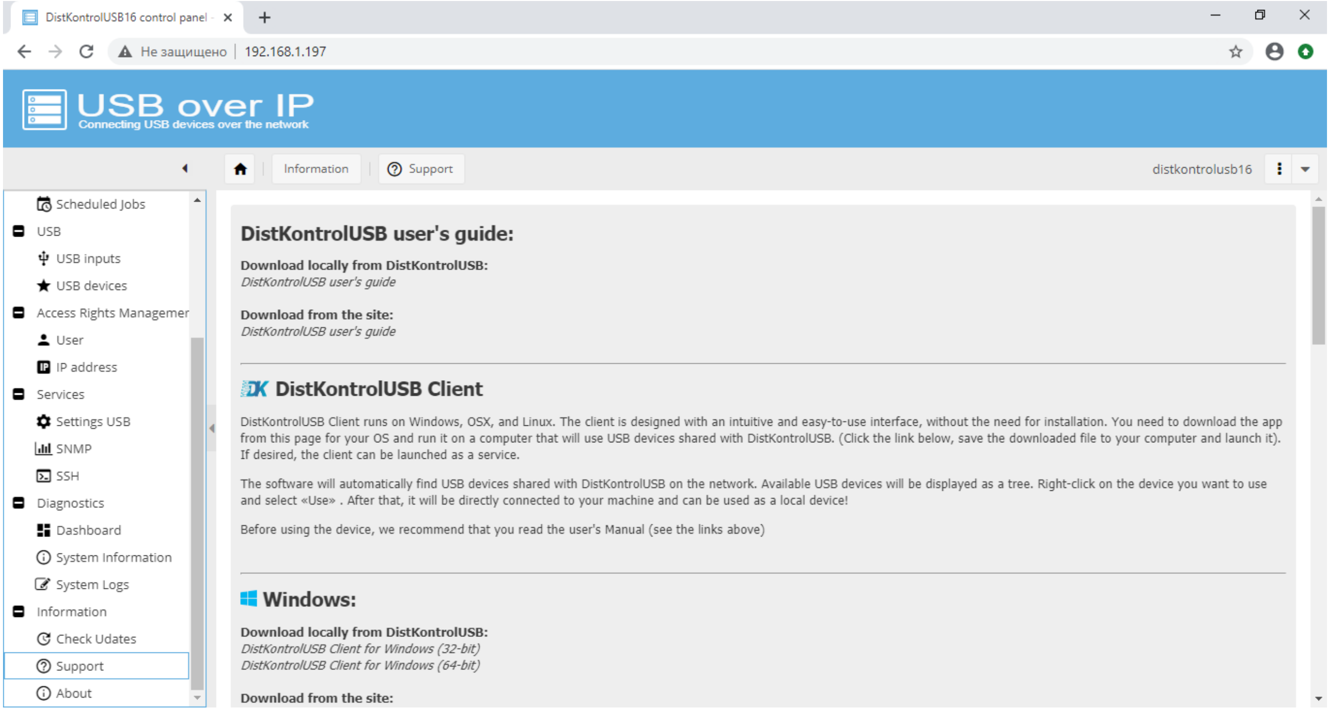
"Download" button - allows you to download the latest available software version for updating the hub from a flash drive. For details, see "Software Update".

Button "Software version history" - opens the page with the history of changes in a new window.

"SHA1" - checksum of the firmware file.

4.7.2 SUPPORT

In this section, you can download the User's Guide, as well as the DistKontrolUSB client for your operating system. Downloading is available locally and from the site via the Internet.



DistKontrolUSB user's guide:

Download locally from DistKontrolUSB:
DistKontrolUSB user's guide

Download from the site:
DistKontrolUSB user's guide

DistKontrolUSB Client

DistKontrolUSB Client runs on Windows, OSX, and Linux. The client is designed with an intuitive and easy-to-use interface, without the need for installation. You need to download the app from this page for your OS and run it on a computer that will use USB devices shared with DistKontrolUSB. (Click the link below, save the downloaded file to your computer and launch it). If desired, the client can be launched as a service.

The software will automatically find USB devices shared with DistKontrolUSB on the network. Available USB devices will be displayed as a tree. Right-click on the device you want to use and select «Use» . After that, it will be directly connected to your machine and can be used as a local device!

Before using the device, we recommend that you read the user's Manual (see the links above)

Windows:

Download locally from DistKontrolUSB:
DistKontrolUSB Client for Windows (32-bit)
DistKontrolUSB Client for Windows (64-bit)

Download from the site:

4.7.3 ABOUT US

Contact Information.

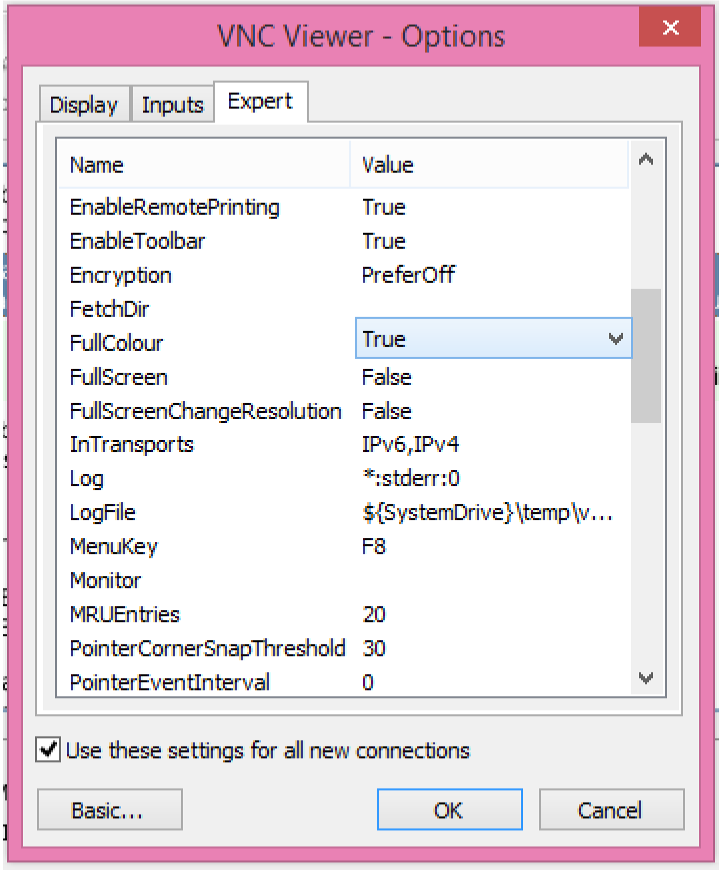
4.8 RESET SETTINGS MANAGED BY USB OVER IP HUB TO DEFAULT STATE.

There are two ways to reset the settings:

1. Using the hardware "Reset" button located on the back of the device. To reset, turn off the hub, press the "Reset" button and, without releasing the button, apply power to the device. After 20 seconds, you can release the "Reset" button. The device has been reset to factory settings.

2. To reset USB over IP settings to initial settings, you need to install any VNC client.

The VNC client you are using must request a 24-bit color (color picker mode * not * 256). TightVNC and krdc work fine by default, for RealVNC make sure you enable full Color in the settings:



Name	Value
EnableRemotePrinting	True
EnableToolbar	True
Encryption	PreferOff
FetchDir	
FullColour	True
FullScreen	False
FullScreenChangeResolution	False
InTransports	IPv6,IPv4
Log	*:stderr:0
LogFile	${SystemDrive}\temp\v...
MenuKey	F8
Monitor	
MRUEntries	20
PointerCornerSnapThreshold	30
PointerEventInterval	0

☑ Use these settings for all new connections

Using a VNC client that asks for the wrong number of colors will cause the application to crash (displaying a “rescue shell” on the screen).

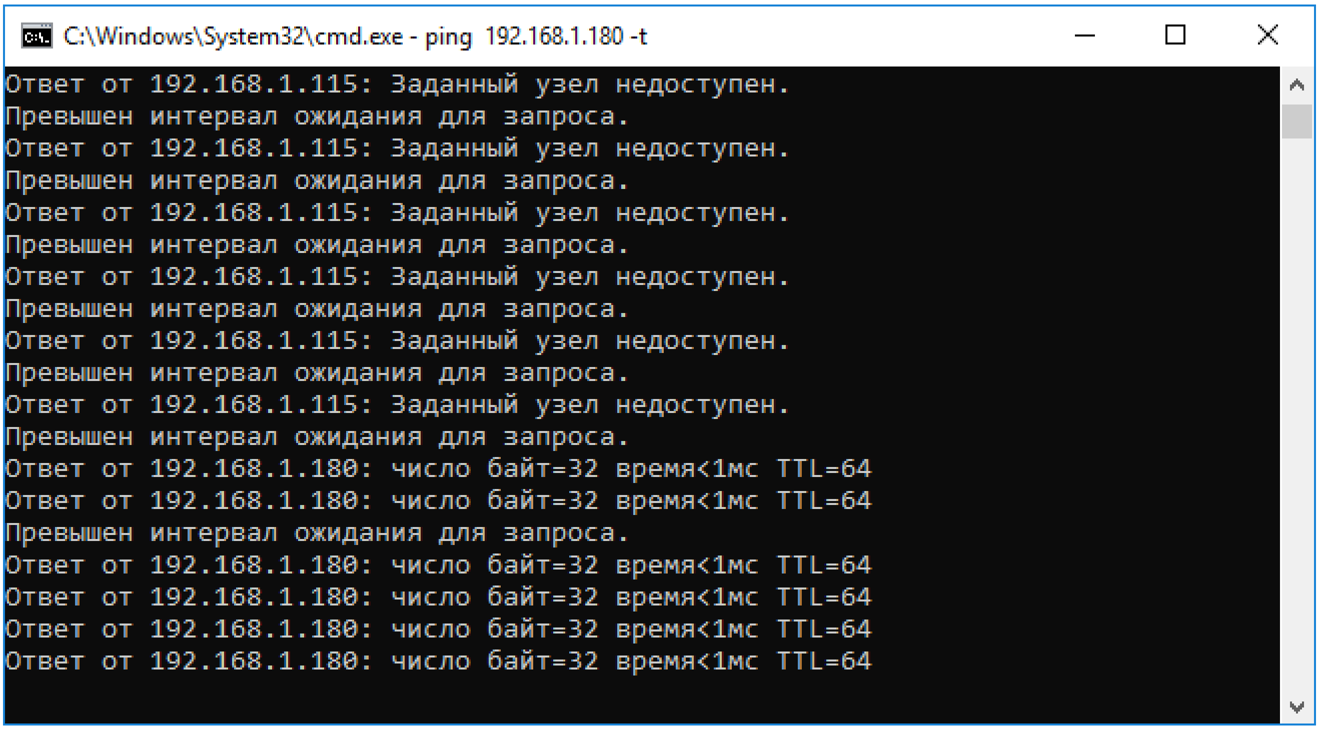
Connection for resetting the settings is possible within 20 seconds after the power is supplied to USB over IP. It is recommended to run the command on the command line:

```
ping -t 192.168.1.180
```

and wait for a response from USB over IP. Then you can run the VNC client program on a regular computer and connect to the device at the IP address 192.168.1.180

ATTENTION!!! To reset the settings and update the hub, you must connect exactly to the IP address 192.168.1.180, regardless of the address set for the main software.

The connection must be completed within 20 seconds, or the device will continue to boot normally to operate in normal mode, it will no longer be possible to connect to it until the next reboot.

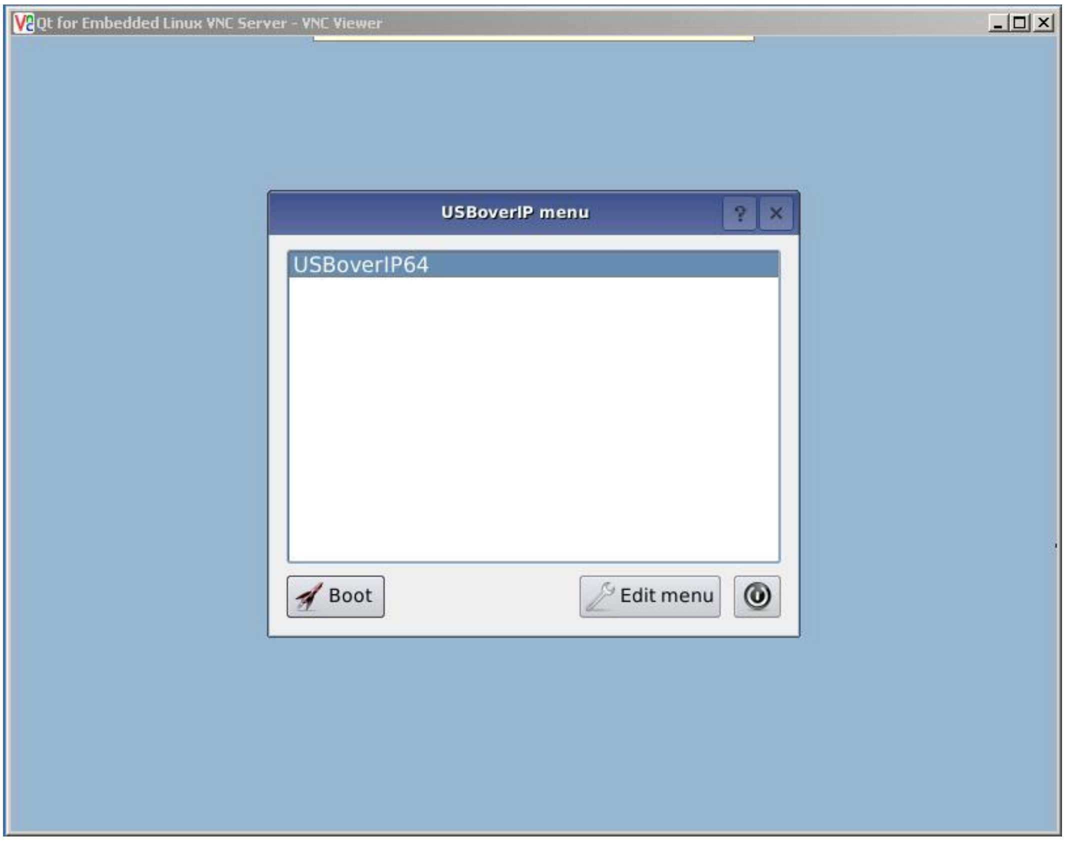


```
Ответ от 192.168.1.115: Заданный узел недоступен.
Превышен интервал ожидания для запроса.
Ответ от 192.168.1.115: Заданный узел недоступен.
Превышен интервал ожидания для запроса.
Ответ от 192.168.1.115: Заданный узел недоступен.
Превышен интервал ожидания для запроса.
Ответ от 192.168.1.115: Заданный 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
```

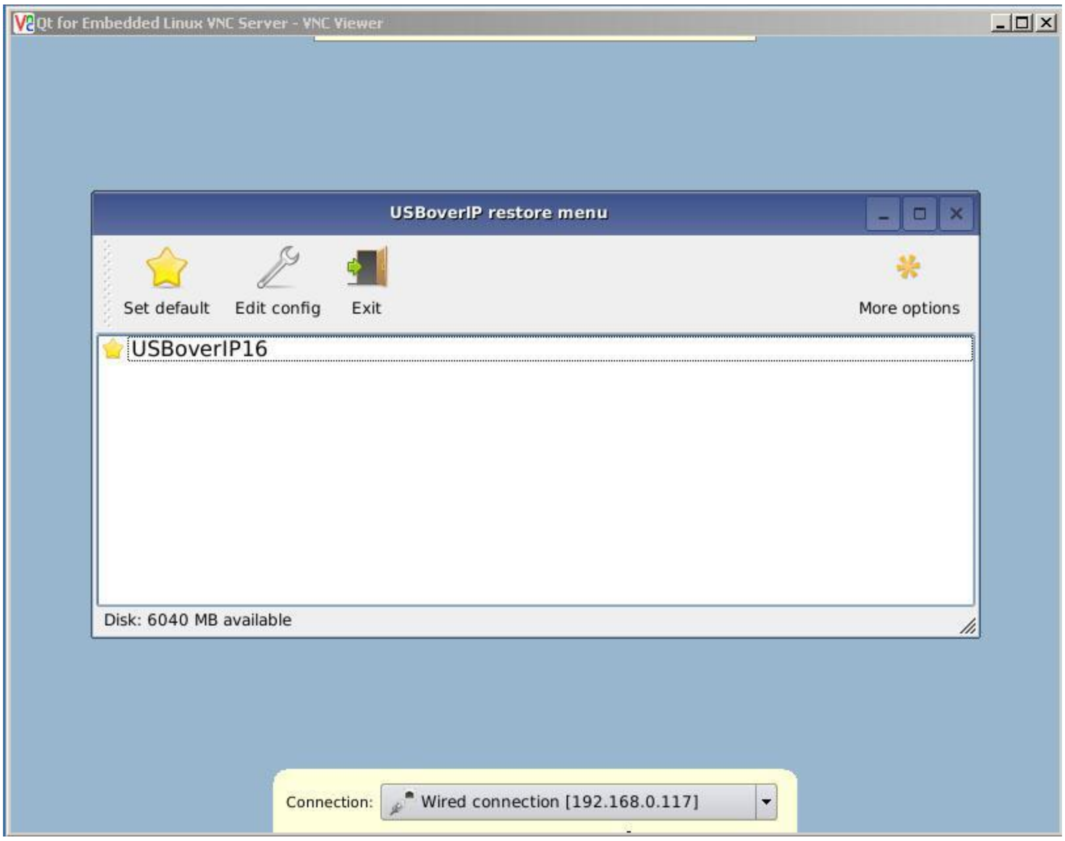
To reset the settings, you must:

Sequentially in the USBoverIP boot and recovery menu select:

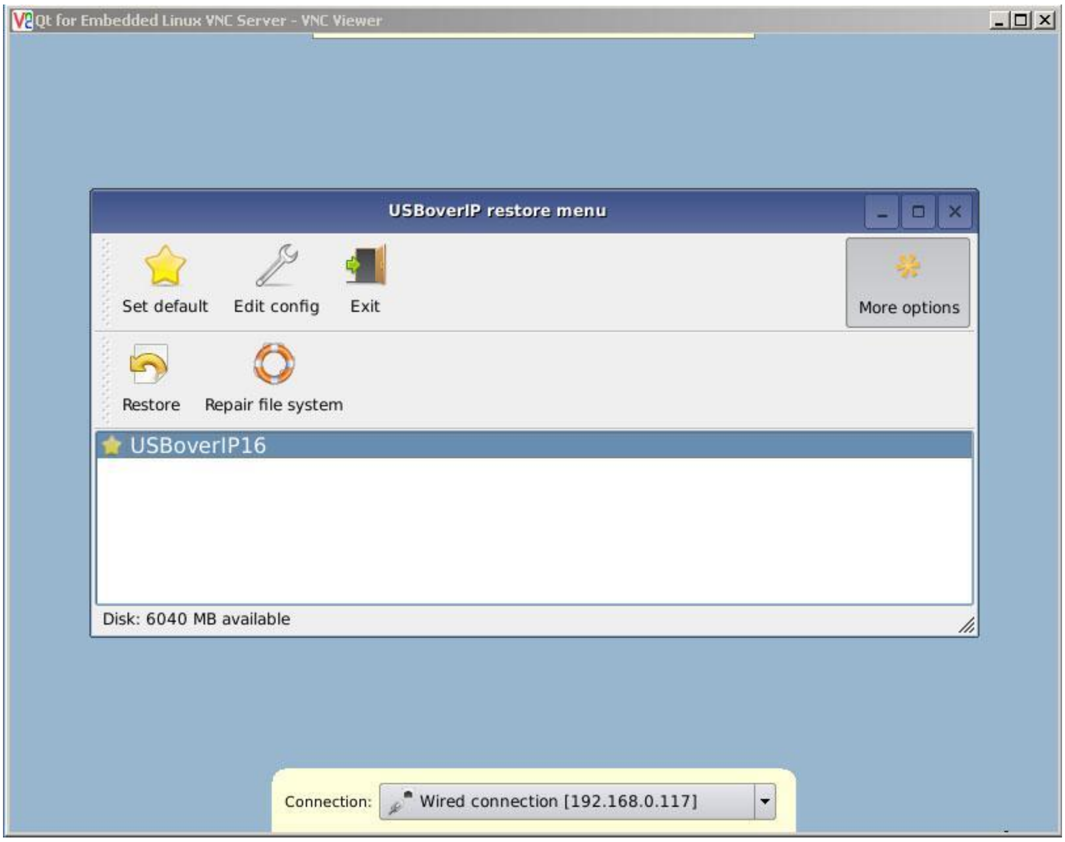
a. «Edit menu»



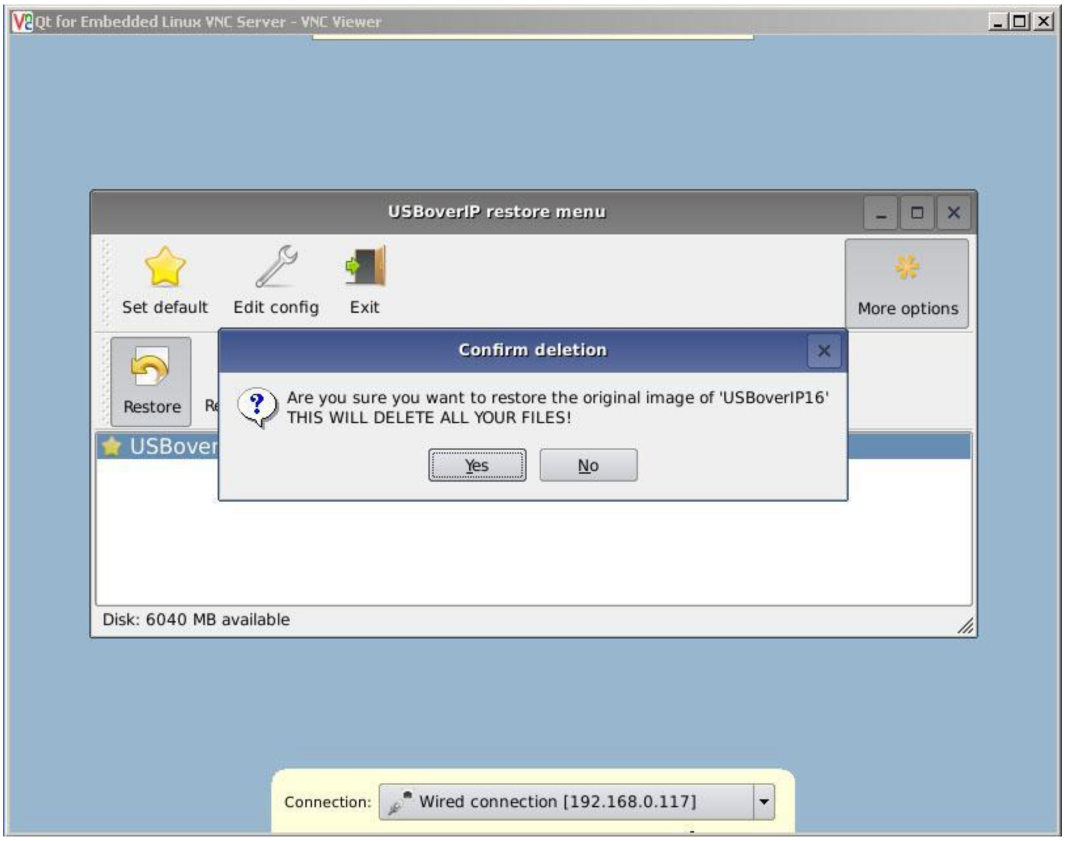
b. «More options»



c. «Restore»

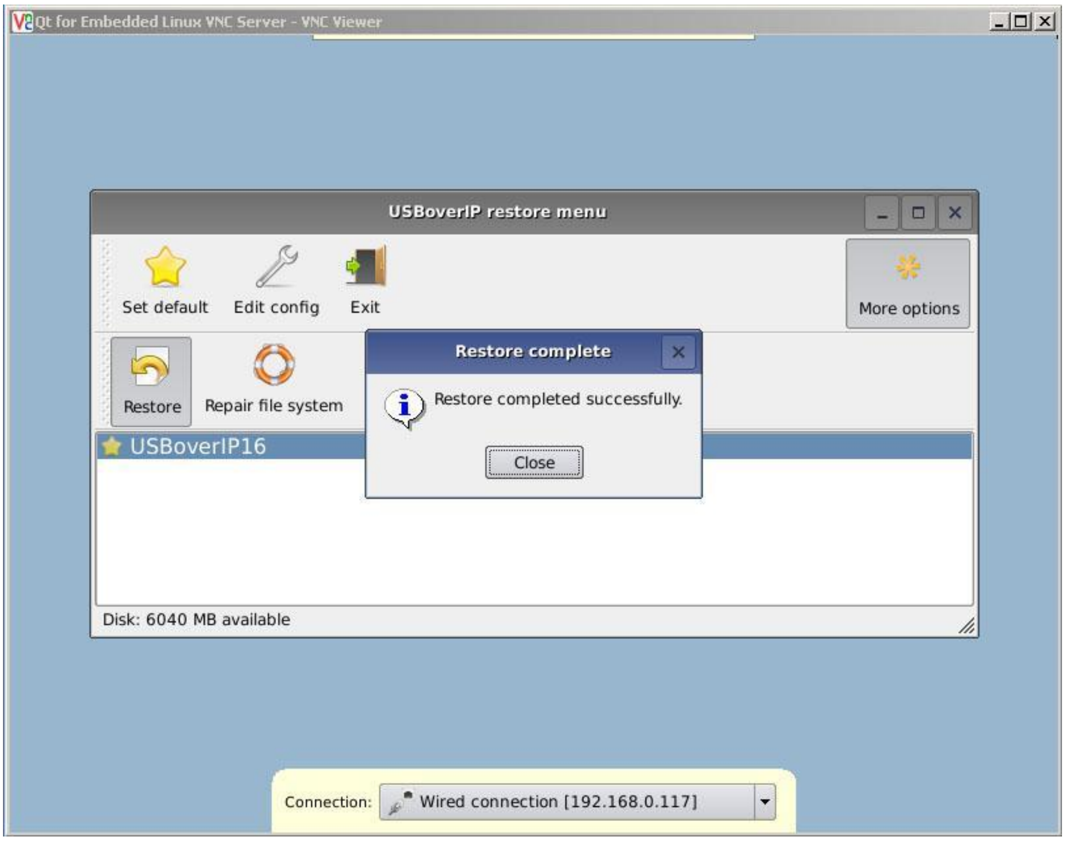


d. «Yes»



Are you sure you want to restore the original image of 'USBoverIP16'
THIS WILL DELETE ALL YOUR FILES!

e. «Close» и «Exit»



Restore complete

Restore completed successfully.

ATTENTION!!! After resetting the device to the original settings and updating, the first boot of the device can take about 5 minutes.

After resetting the device to the original settings and updating, you will need to enter the license key for the USB over IP hub software as described in the License section.

4.9 UPDATE SOFTWARE CONTROLLED BY USB OVER IP HUB.

ATTENTION!!! When updating the software of a USB over IP hub, its settings are not saved and are reset to the original ones. Before updating the device, it is necessary to export the settings and import them after the update (see the section "Saving and restoring settings" of the manual) or to re-configure the device, and you will need to enter the license key to the software of the controlled USB over IP hub according to the method described in section "License".

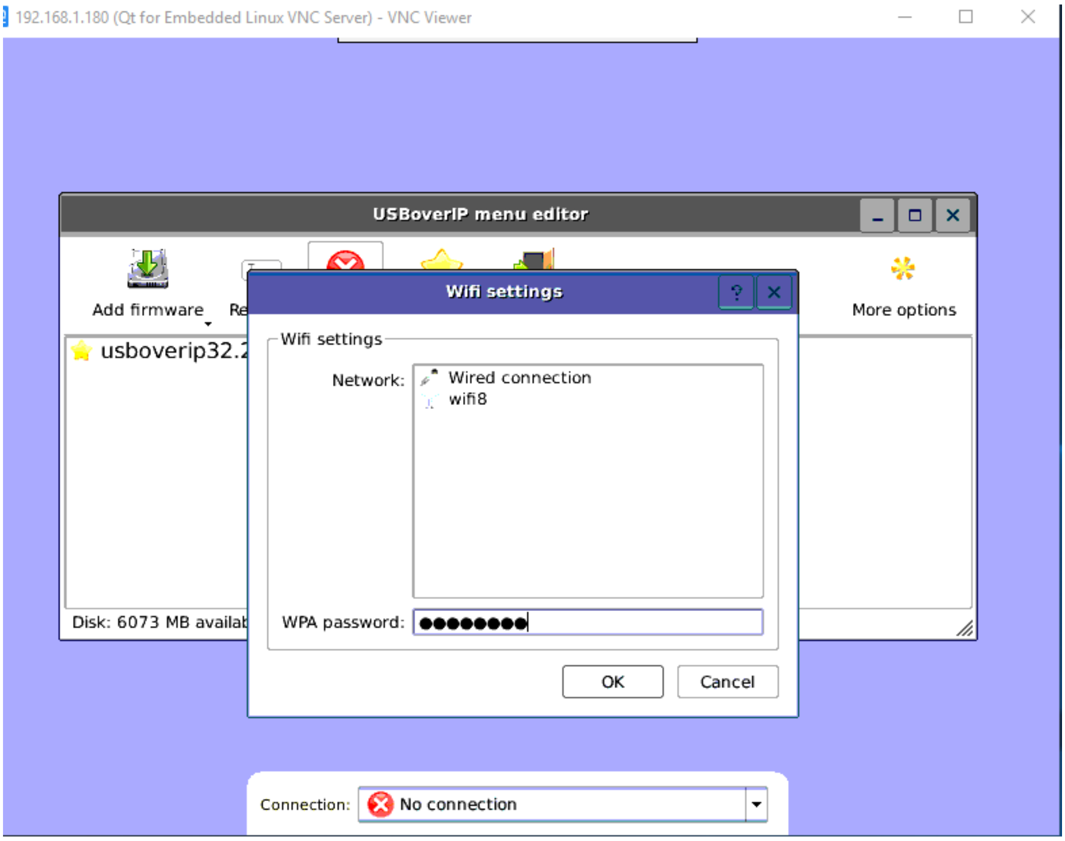
To update the software of a controlled USB over IP hub, you need to connect to it using VNC as described above.

Updating is possible in two ways:

1. Via the Internet (recommended update method).

2. From a flash drive.

1. To update via the Internet, it is necessary to provide access to the global network from the 192.168.1.180 address via the device's LAN. It is also possible to update software via WiFi. To connect to WiFi, click on the "Wired connection" inscription at the bottom of the screen, select a network from the list of available ones and enter a password.



192.168.1.180 (Qt for Embedded Linux VNC Server) - VNC Viewer

USBoverIP menu editor

Wifi settings

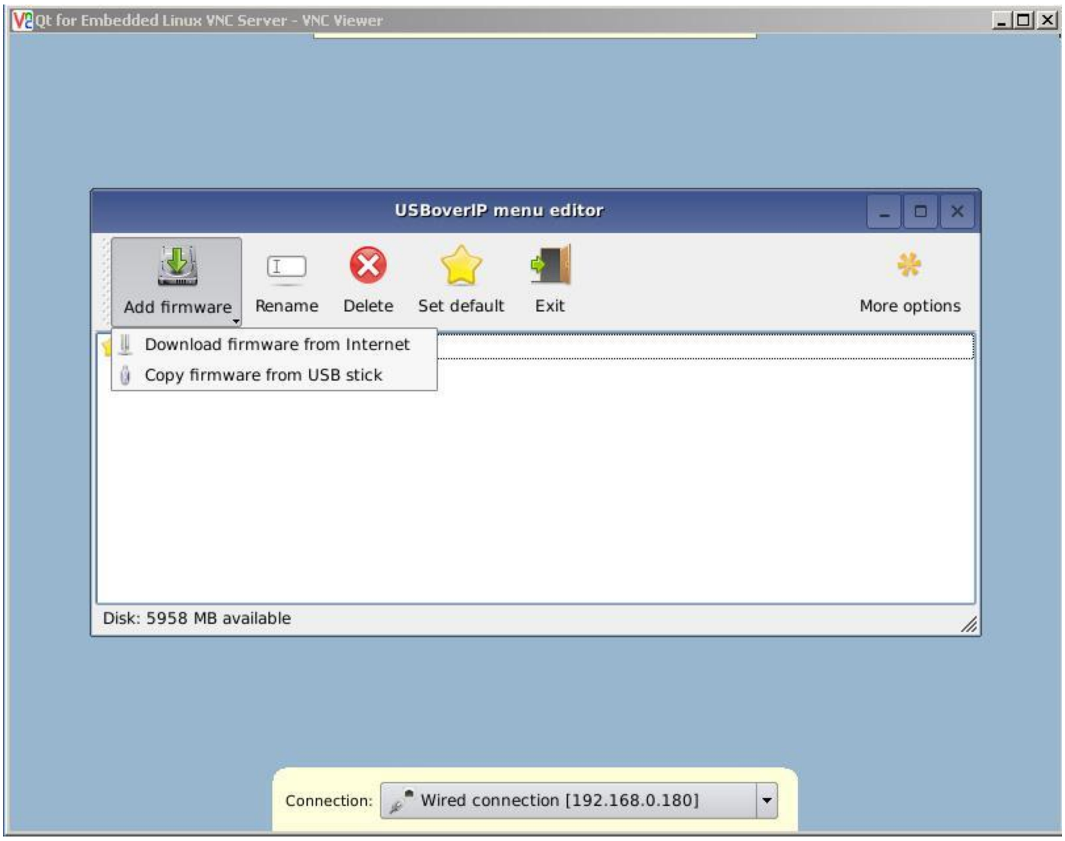
Network: Wired connection, wifi8

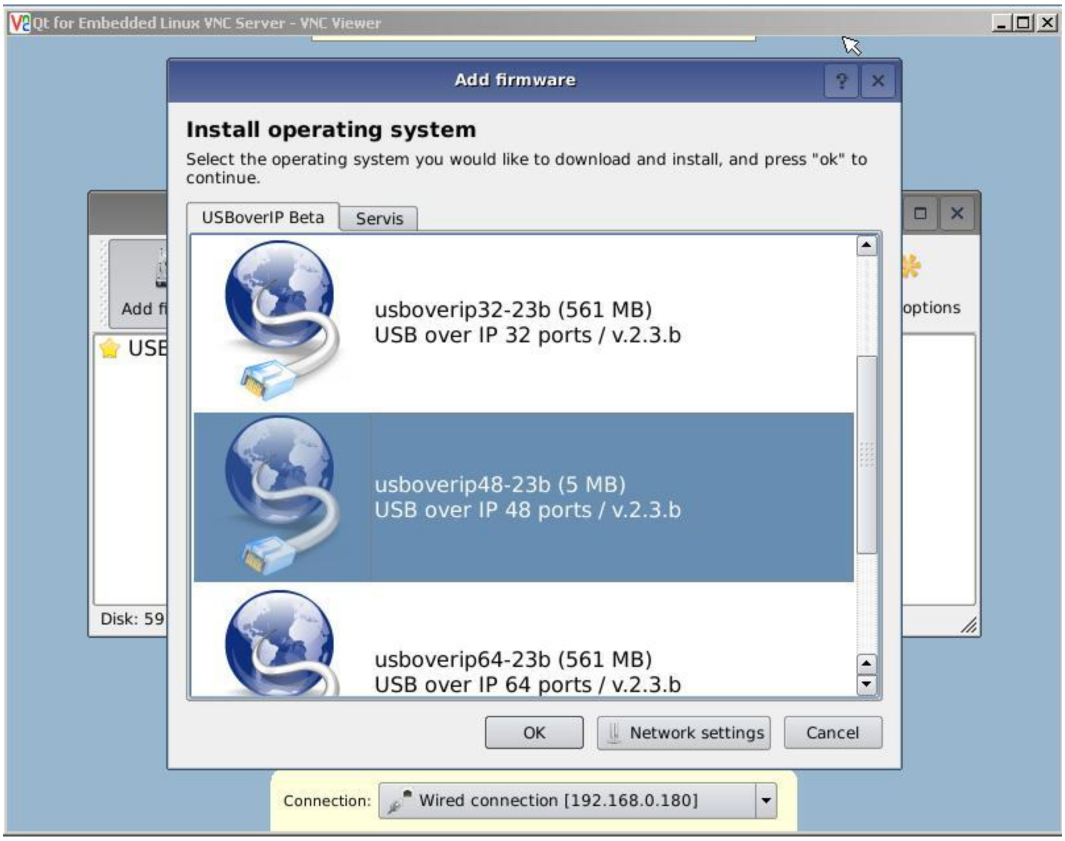
WPA password: ●●●●●●●●

Connection: No connection

Disk: 6073 MB availat

To start the update, you must sequentially select in the USBoverIP boot and recovery menu: "Edit menu" - "Add firmware" and select the appropriate submenu item.


Qt for Embedded Linux VNC Server - VNC Viewer
USBoverIP menu editor
Add firmware
Rename
Delete
Set default
Exit
More options
Download firmware from Internet
Copy firmware from USB stick
Disk: 5958 MB available
Connection:
Wired connection [192.168.0.180]


Qt for Embedded Linux VNC Server - VNC Viewer
Add firmware
USBoverIP Beta
Servis
OK
Network settings
Cancel
Connection:
Wired connection [192.168.0.180]

Install operating system

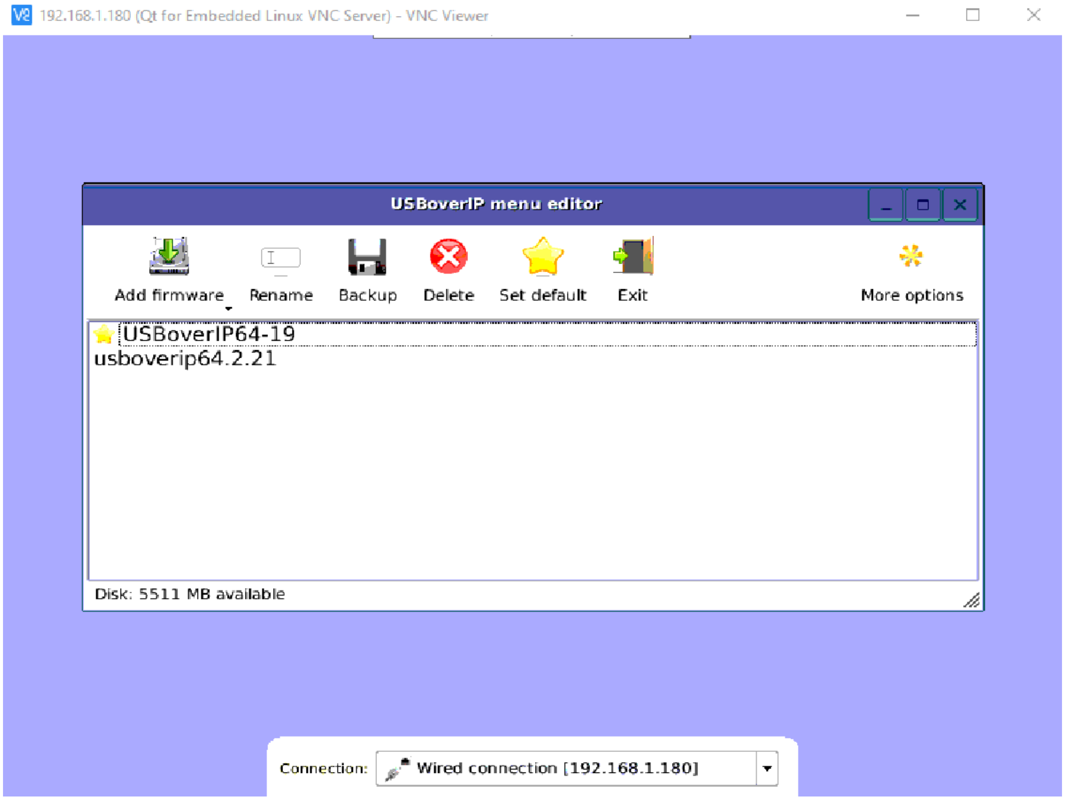
Select the operating system you would like to download and install, and press "ok" to continue.

usboverip32-23b (561 MB)
USB over IP 32 ports / v.2.3.b

usboverip48-23b (5 MB)
USB over IP 48 ports / v.2.3.b

usboverip64-23b (561 MB)
USB over IP 64 ports / v.2.3.b

Then select the software version and click OK. The new software version will be downloaded and installed on the device.



USBoverIP64-19
usboverip64.2.21

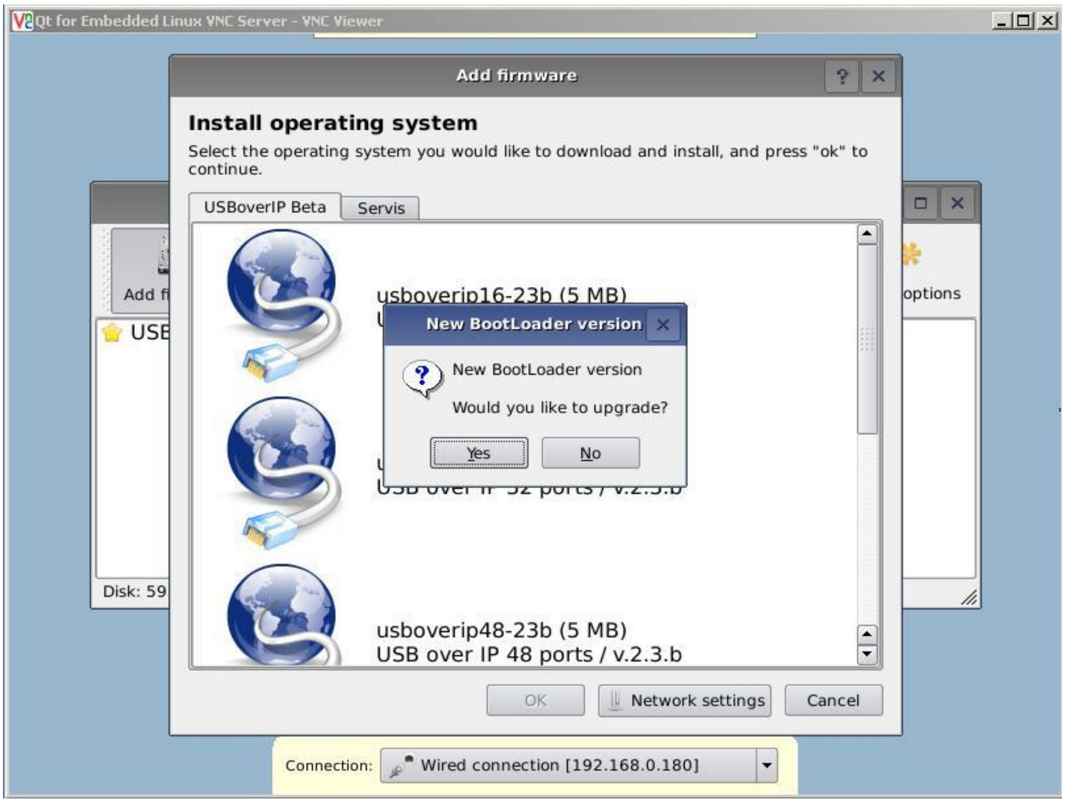
Disk: 5511 MB available

Connection: Wired connection [192.168.1.180]

If, when updating the device, you see a message about the availability of a new version of the bootloader, then first you need to update the bootloader software by clicking on the "YES" button. Updating the bootloader is only possible via the Internet.

After updating the bootloader, update the main software of the device.

If you do not plan to update the main software of the hub, it is not recommended to update the bootloader.



Install operating system

Select the operating system you would like to download and install, and press "ok" to continue.

usboverip16-23b (5 MB)

USB over IP 32 ports / v.2.3.b

usboverip48-23b (5 MB)
USB over IP 48 ports / v.2.3.b

New BootLoader version

Would you like to upgrade?

Connection: Wired connection [192.168.0.180]

1. If the Internet connection is poor, it is possible to update the main software of the managed USB over IP hub using a flash drive.

To update software from a flash drive, you must:

- Download the new software version on the "Information" - "Check for updates" page or follow the link.
- When updating from a flash drive, the checksum of the firmware file is not checked. It is necessary to independently check the checksum of the downloaded file from the one indicated on the update download page.
- Write the software to the flash media (it is recommended to use media with a volume of 4 - 16GB) and connect the media to USB port 1.1. The port is automatically enabled when entering the edit menu.
- To call the submenu, click and hold the “Add firmware” button. Selecting the corresponding item of the “Add firmware” submenu will open the software selection dialog box. It is necessary to select the recorded version of the software on the flash drive and press the "Open" button.
- The new software version will be copied and installed on the device.

After installation, you will see a new item in the list of installed software. To use a new version of the software, select it in the menu and click on the "Set default" button, then "Exit". The device will reboot with the new software version.

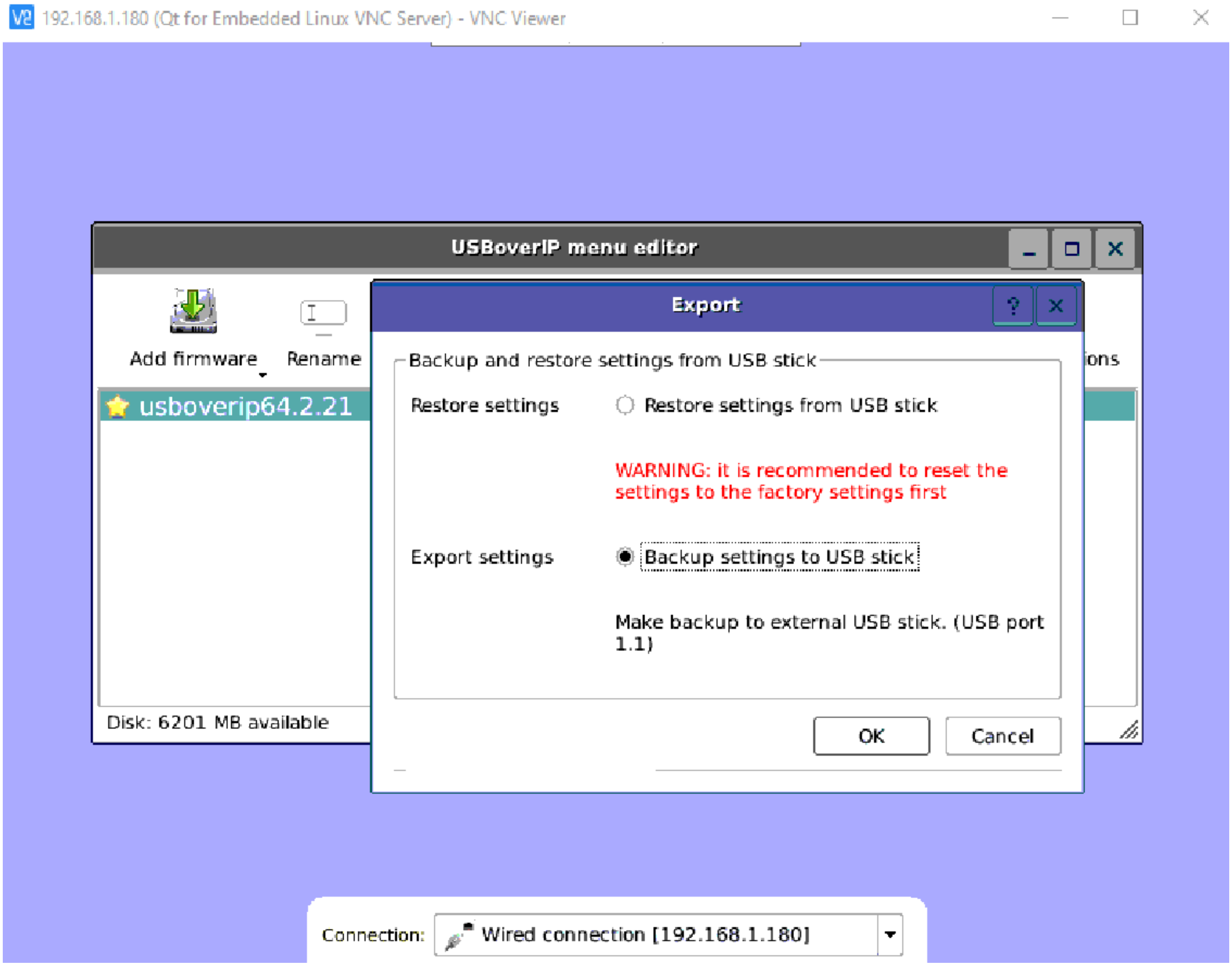
Additionally, the editing menu provides the ability to rename and delete unnecessary software versions.

4. 10 SAVING AND RESTORING SOFTWARE CONTROLLED BY USB OVER IP HUB.

ATTENTION!!! Saving the settings of the software controlled by the USB over IP hub or restoring them is possible for software versions not lower than 2.21. If necessary, the imported settings can be deleted by simply resetting the settings of the USB over IP hub to its original state. Read more in "Resetting a USB over IP Controlled Hub to its original state."

To save the settings of the software controlled by the USB over IP hub or restore them, you must connect to the hub using VNC as described above. In the USB port 1.1 of the hub, you need to connect a flash drive (it is recommended to use media with a volume of 4 - 16GB) formatted in FAT32. The port is automatically enabled when entering the edit menu.

To save the settings of the software controlled by the USB over IP hub, click the "Backup" menu button. In the export window that opens, select "Backup settings to USB stick" and click the "OK" menu button. Then confirm the export of the settings and wait for the operation to complete.



192.168.1.180 (Qt for Embedded Linux VNC Server) - VNC Viewer

Export

Backup and restore settings from USB stick

Restore settings ○ Restore settings from USB stick

WARNING: it is recommended to reset the settings to the factory settings first

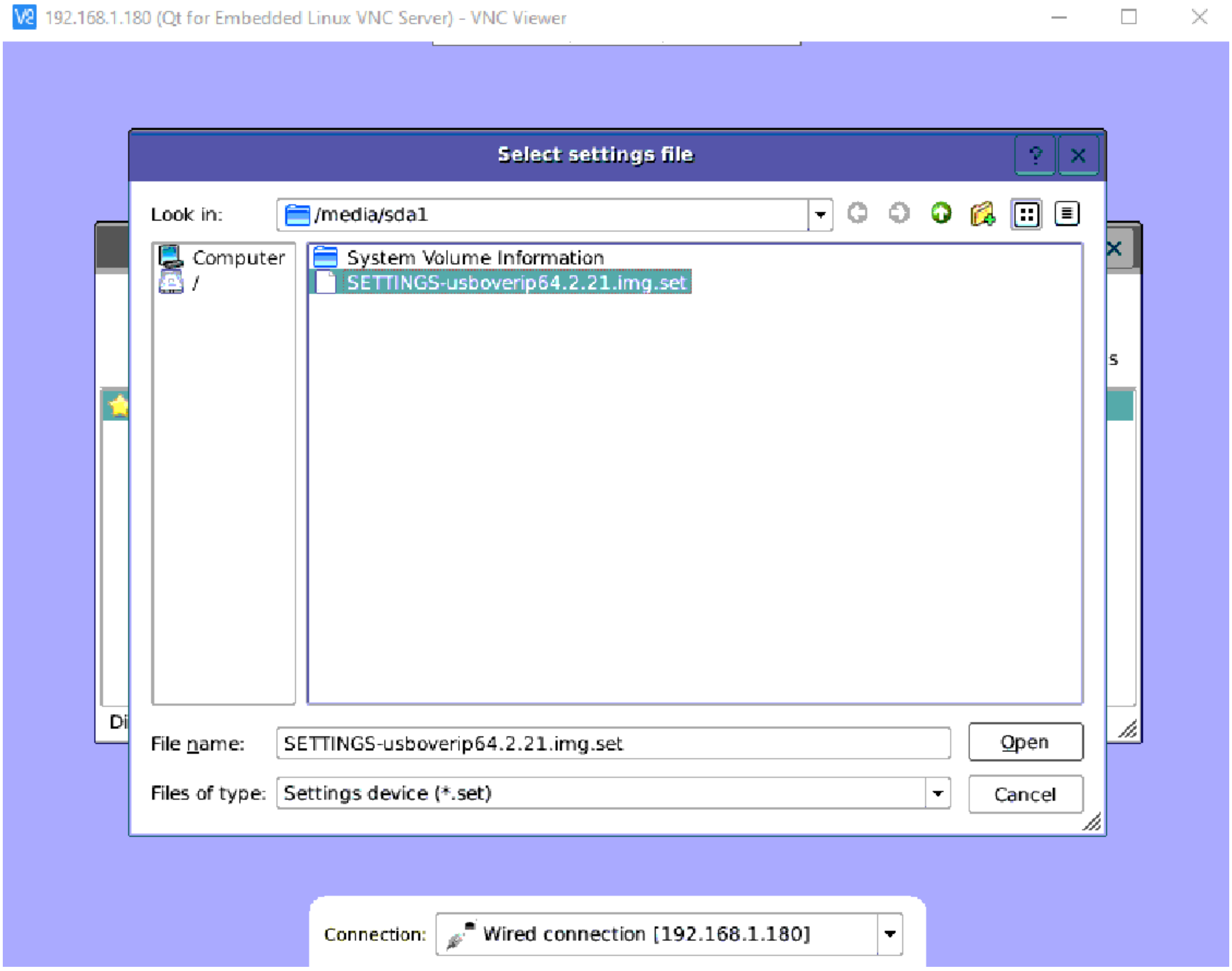
Export settings ● Backup settings to USB stick

Make backup to external USB stick. (USB port 1.1)

Connection: Wired connection [192.168.1.180]

Before restoring the settings of the software controlled by the USB over IP hub, it is recommended to reset the settings of the controlled USB over IP hub to its original state according to the method described in clause 4.18 of the Guide.

To restore the settings of the software controlled by the USB over IP hub, click on the name of the firmware to which you want to export the settings, then click the "Backup" menu button. In the export window that opens, select "Restore settings from USB stick" and click the "OK" menu button. Then select the settings file and wait for the operation to complete.



192.168.1.180 (Qt for Embedded Linux VNC Server) - VNC Viewer
Select settings file
Look in:
Computer
/
Open
Cancel
Connection:

/media/sda1

System Volume Information

SETTINGS-usboverip64.2.21.img.set

File name: SETTINGS-usboverip64.2.21.img.set

Files of type: Settings device (*.set)

Wired connection [192.168.1.180]

After restoring the settings of the software controlled by the USB over IP hub, click the “Exit” menu button to reboot the hub.

4.11 HARDWARE RESET OF THE MANAGED USB OVER IP HUB.

To reboot the hub press and hold the “Reset” button located on the back of the device for 5 seconds. The hub will restart gracefully.

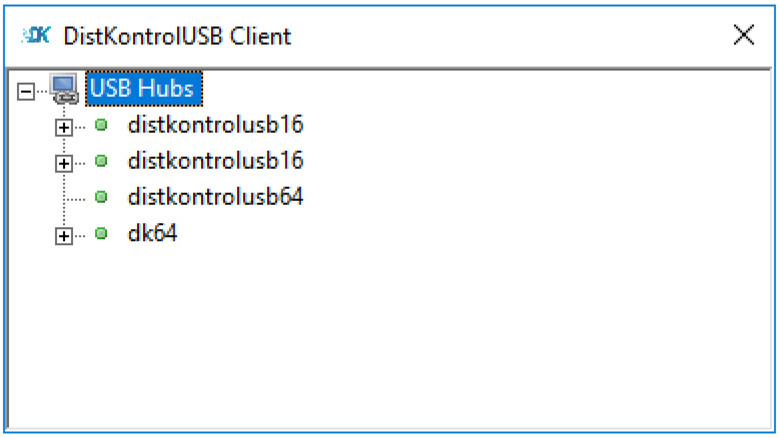
5 DISTKONTROLUSB CLIENT

5.1 INSTALLING THE DISTKONTROLUSB CLIENT

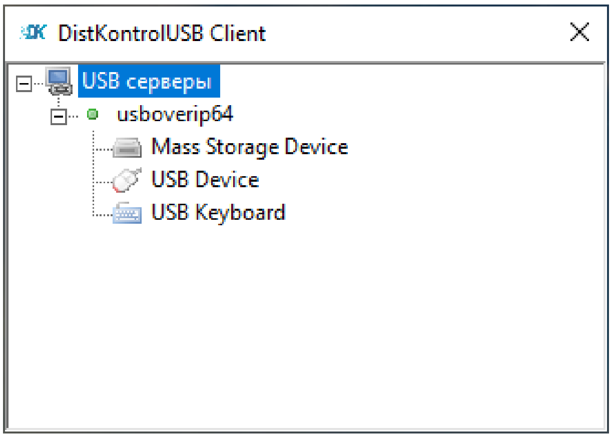
The USB client can be downloaded from the USB device itself over the network or from the website (links on the Information - Support page).

You need to download and run the appropriate software.

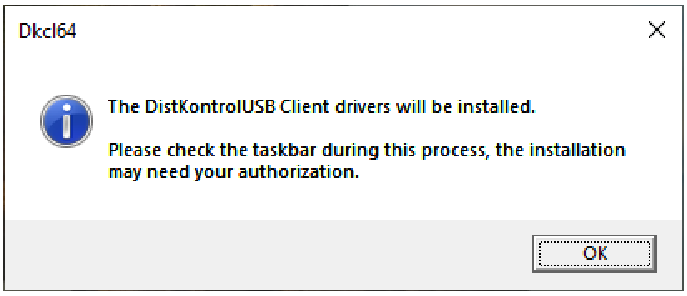
A Windows Security Center notification will appear during installation. The application must be allowed to make changes.



When connected to USB over IP USB devices, they will be visible in the client and can be connected to the computer:



The first time you connect to a USB device, you will be prompted to install the USB over IP driver:

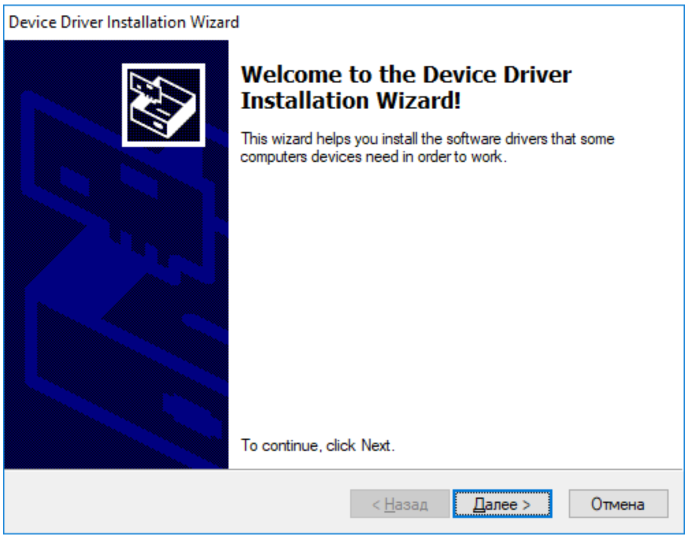


Dkcl64

The DistKontrolUSB Client drivers will be installed.

Please check the taskbar during this process, the installation may need your authorization.

A Windows Security Center notification will appear during installation. The application must be allowed to make changes.



Device Driver Installation Wizard

Welcome to the Device Driver Installation Wizard!

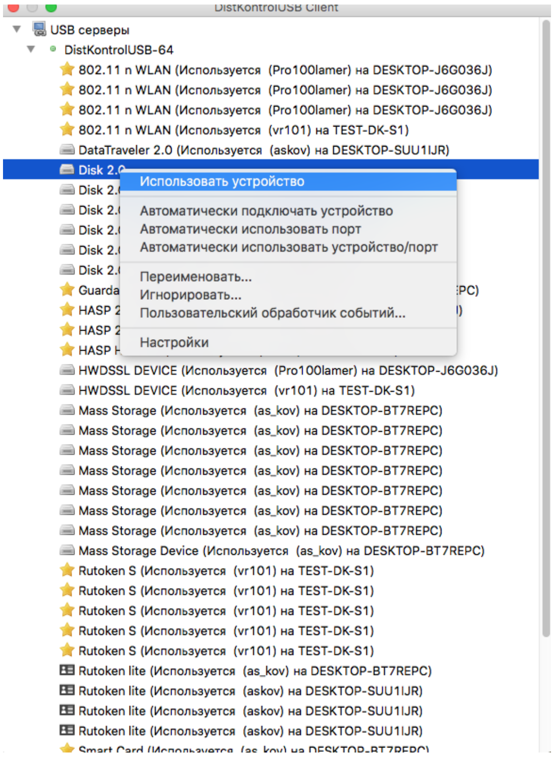
This wizard helps you install the software drivers that some computers devices need in order to work.

To continue, click Next.

Click "Install".

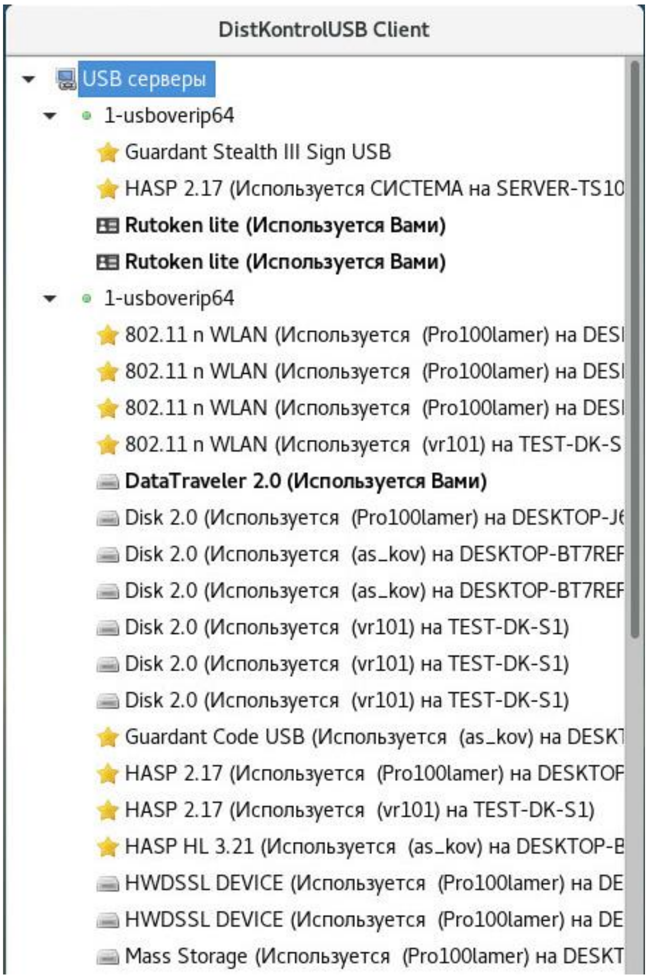
Once launched, the USB client window will appear.

The software will automatically find USB devices shared by servers on the network. Available USB devices will be displayed as a tree. Right click on the device you want to use and select Use. After that, it will be directly connected to your computer (machine) and can be used as a local device.


DistKontrolUSB Client
Использовать устройство
Автоматически подключать устройство
Автоматически использовать порт
Автоматически использовать устройство/порт
Переименовать...
Игнорировать...
Пользовательский обработчик событий...
Настройки

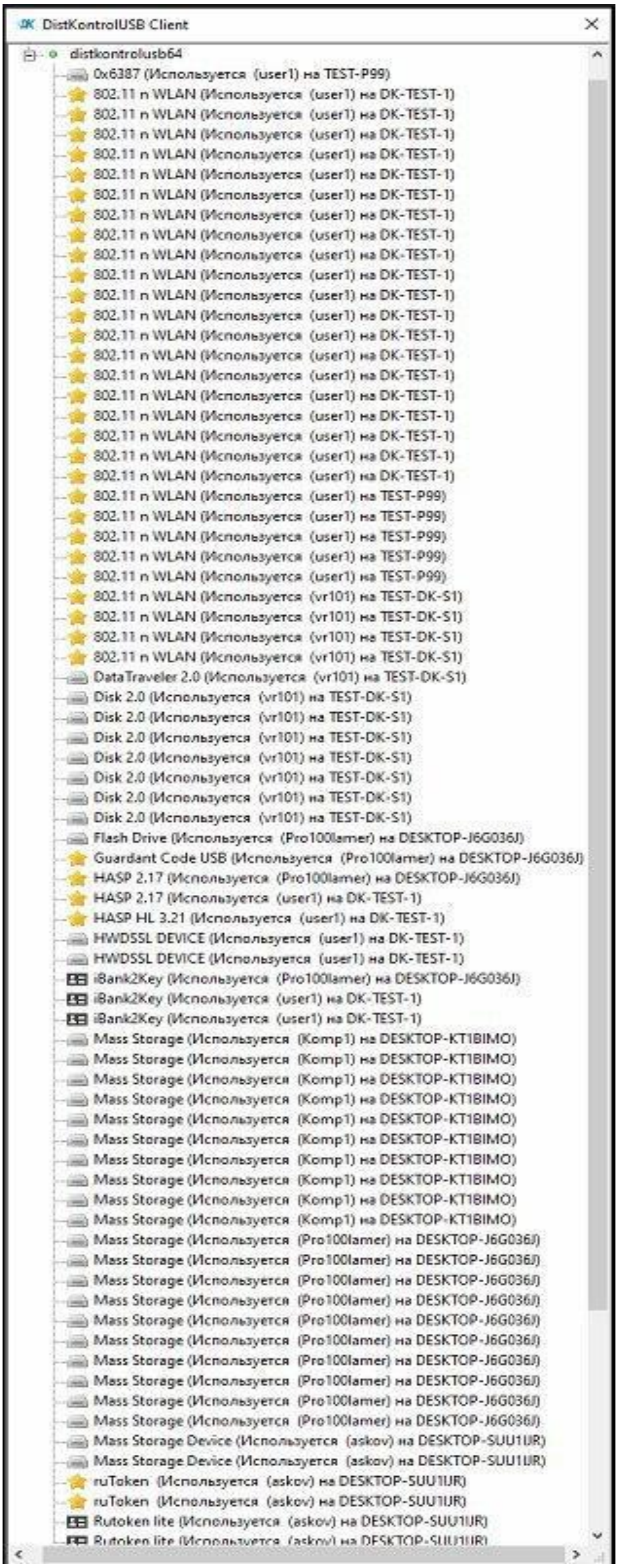
```
USB серверы
  DistKontrolUSB-64
    802.11 n WLAN (Используется  (Pro100lamer) на DESKTOP-J6G036J)
    802.11 n WLAN (Используется  (Pro100lamer) на DESKTOP-J6G036J)
    802.11 n WLAN (Используется  (Pro100lamer) на DESKTOP-J6G036J)
    802.11 n WLAN (Используется  (vr101) на TEST-DK-S1)
    DataTraveler 2.0 (Используется  (askov) на DESKTOP-SUU1IJR)
    Disk 2.0
    Disk 2.
    Disk 2.
    Disk 2.
    Disk 2.
    Disk 2.
    Guarda                                                  PC)
    HASP 2                                                  )
    HASP 2
    HASP H
    HWDSSL DEVICE (Используется  (Pro100lamer) на DESKTOP-J6G036J)
    HWDSSL DEVICE (Используется  (vr101) на TEST-DK-S1)
    Mass Storage (Используется  (as_kov) на DESKTOP-BT7REPC)
    Mass Storage (Используется  (as_kov) на DESKTOP-BT7REPC)
    Mass Storage (Используется  (as_kov) на DESKTOP-BT7REPC)
    Mass Storage (Используется  (as_kov) на DESKTOP-BT7REPC)
    Mass Storage (Используется  (as_kov) на DESKTOP-BT7REPC)
    Mass Storage (Используется  (as_kov) на DESKTOP-BT7REPC)
    Mass Storage (Используется  (as_kov) на DESKTOP-BT7REPC)
    Mass Storage Device (Используется  (as_kov) на DESKTOP-BT7REPC)
    Rutoken S (Используется  (vr101) на TEST-DK-S1)
    Rutoken S (Используется  (vr101) на TEST-DK-S1)
    Rutoken S (Используется  (vr101) на TEST-DK-S1)
    Rutoken S (Используется  (vr101) на TEST-DK-S1)
    Rutoken S (Используется  (vr101) на TEST-DK-S1)
    Rutoken lite (Используется  (as_kov) на DESKTOP-BT7REPC)
    Rutoken lite (Используется  (askov) на DESKTOP-SUU1IJR)
    Rutoken lite (Используется  (askov) на DESKTOP-SUU1IJR)
    Rutoken lite (Используется  (askov) на DESKTOP-SUU1IJR)
    Smart Card (Используется  (as_kov) на DESKTOP-BT7REPC)
```

Linux:



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

Windows:

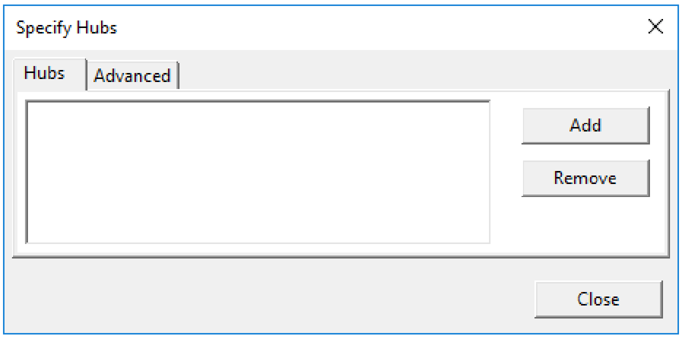


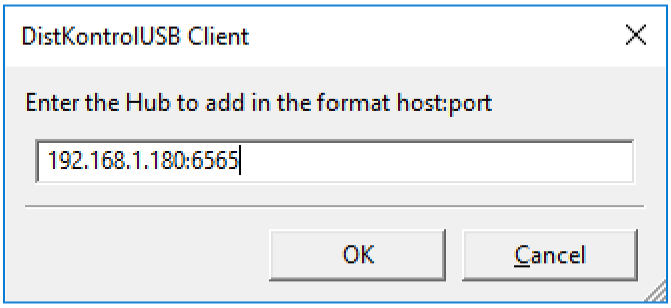
DistKontrolUSB Client

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

The DistKontrolUSB Client for Linux uses the native usbip driver for Linux. (It is recommended to use the kernel (4.9+) for maximum compatibility).

The address of a managed USB over IP hub can be specified (for use, for example, in a global network), for this, right-click on USB Hubs and select Specify Hubs.



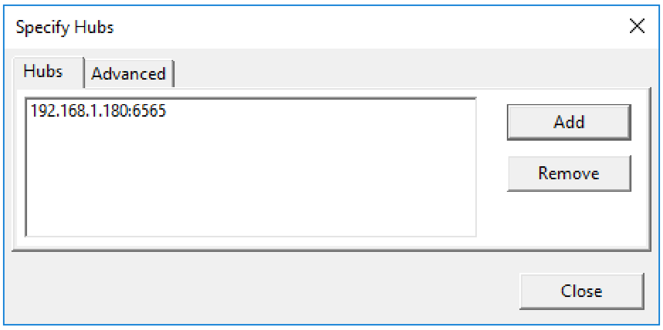


Enter the Hub to add in the format host:port

192.168.1.180:6565

In the Specify Hubs window, click Add.

Enter the server settings in the format address: port and click OK. Port: 6565 (6564 when using SSL). Here you need to specify the IP address of the hub.



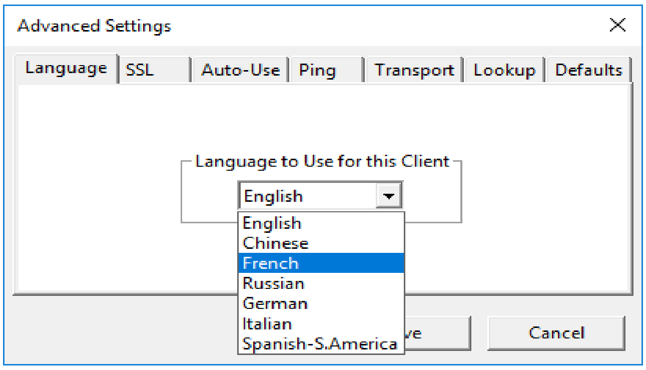
192.168.1.180:6565

In the Specify Hubs window, click Close.

The client interface is multilingual. To select In the client/

1. Right click on USB Habs -> Advanced Setting

2. On the Lenguage tab, select the interface language -> Save



Language to Use for this Client

English

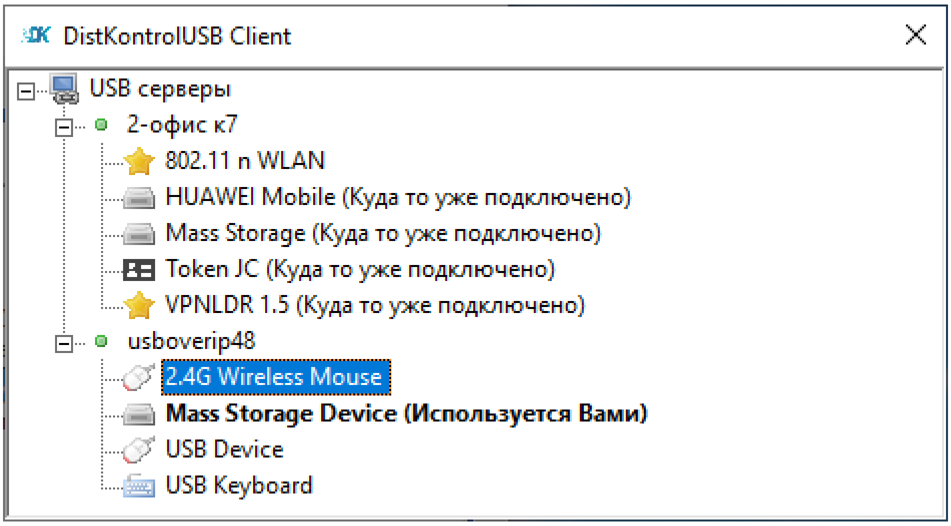
English
Chinese
French
Russian
German
Italian
Spanish-S.America

5.2 DISTKONTROLUSB CLIENT SETUP

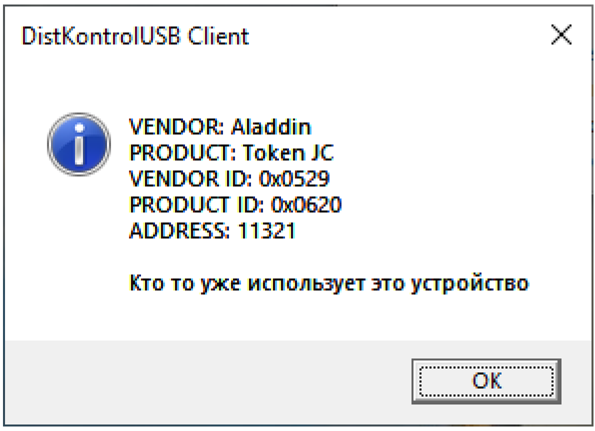
5.2.1 USB DEVICE USER INFORMATION CONTROL

The USB over IP controlled hub allows you to enable or disable the display of information in the client application about users using USB devices.

By default, information display is enabled. In the example below, information display is enabled on the USBoverIP64 hub, and disabled on the USBoverIP32 hub.

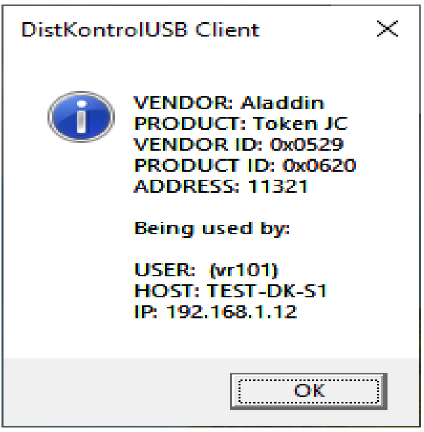


USB серверы
- 2-офис к7
  - 802.11 n WLAN
  - HUAWEI Mobile (Куда то уже подключено)
  - Mass Storage (Куда то уже подключено)
  - Token JC (Куда то уже подключено)
  - VPNLDR 1.5 (Куда то уже подключено)
- usboverip48
  - 2.4G Wireless Mouse
  - **Mass Storage Device (Используется Вами)**
  - USB Device
  - USB Keyboard



VENDOR: Aladdin
PRODUCT: Token JC
VENDOR ID: 0x0529
PRODUCT ID: 0x0620
ADDRESS: 11321

Кто то уже использует это устройство



VENDOR: Aladdin
PRODUCT: Token JC
VENDOR ID: 0x0529
PRODUCT ID: 0x0620
ADDRESS: 11321

Being used by:

USER: (vr101)
HOST: TEST-DK-S1
IP: 192.168.1.12

Managing the display of information about users of USB devices is carried out in the WEB interface of the device on the page "Services" - "USB Settings" - "Hide information about USB users in the client" (For use, enable and save)

5.2.2 CHANGE USB DEVICE NAME IN CLIENT APPLICATION.

It is possible to rename USB devices in the client application. With the right mouse button on the device, call the window - Rename. Enter the desired name - Click OK. All users will see the name change. The default device name is set by the USB port number.

To restrict the rights to rename USB devices, configure the rights: "Rights Settings"

In the WEB interface of the device on the page "Services" - "USB settings" - "Reset the name of USB devices to the original", it is possible to reset the names to the original ones. A reset will restart the service.

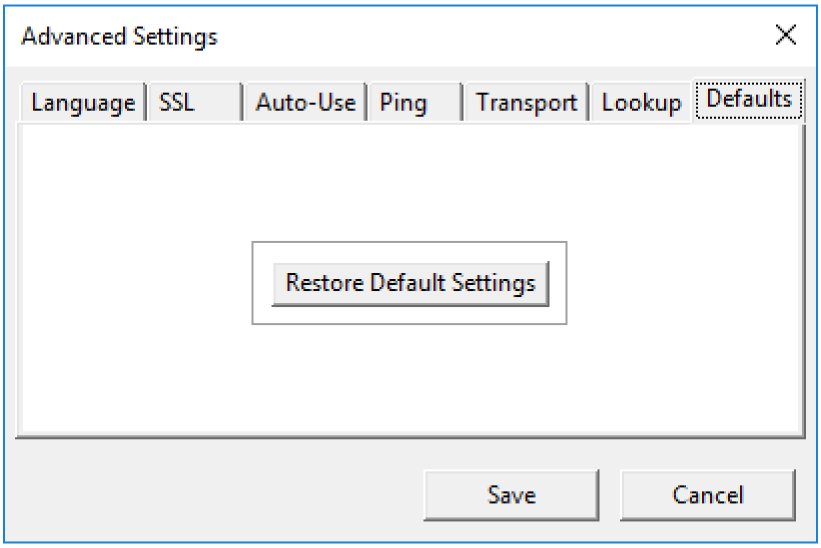
5.2.3 CUSTOMIZING THE DISTKONTROLUSB CLIENT APP MENU

The client saves all his parameters in one text file

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

This file is updated when the settings are changed. On first launch, the client creates a default configuration file.

To reset a previously saved password, you must reset the client settings. Right click on “USB Servers” - “Additional Settings”. The Default Settings tab is located at the very end.



5.2.4 RESETTING DISTKONTROLUSB CLIENT APPLICATION PARAMETERS

To reset all settings of the client application, in the WEB interface of the device on the page "Services" - "USB settings" - "Reset the parameters of the USB over IP service to the original ones." A reset will restart the service.

This will reset port numbers, ssl settings and hidden device display, device names and hiding.

5.3 RUNNING THE DISTKONTROLUSB CLIENT AS A SERVICE (DEMON)

The USB client can run as a regular application or as a service (daemon). Running the client as a service allows devices to be shared without requiring a user to log on, the client will run in the background continuously.

When you install a USB client as a service, it automatically starts when the operating system boots up and automatically connects to any devices you specify. The Message log can be viewed in Event Viewer (Windows), Console Viewer (OSX), or tail / var / log / syslog (Linux).

Чтобы установить USB клиента в качестве службы Windows или OSX:

Right click "USB Hubs-> Install Client as a Sevice" (if the service is already installed, Uninstall Client Service will be available).

The DistKontrolUSB client will be installed as a service.

When the client restarts, it will interact with the running service in the background.

You can log out of the client and the client service will continue to run as usual in the background.

To install a client on USB as a daemon in Linux, you need to start the client with the - n parameter. This will launch it in daemon mode.

For example: to run a client in the background under Ubuntu / Debian use:

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

The daemon does not need to use sudo to run in console mode as a non-root user, just run from the command line.

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

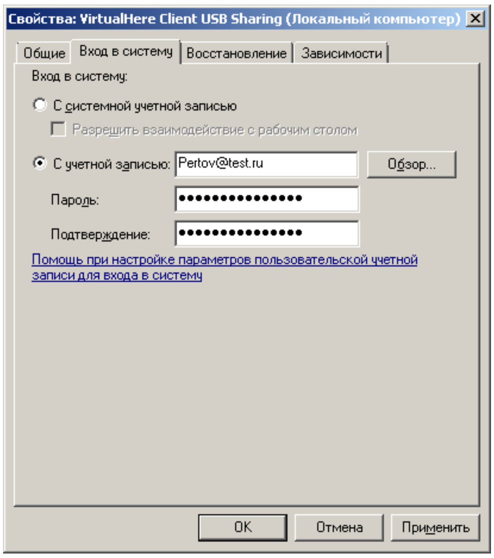
By default, the service runs as the System user.

Since the service mode is for background work (daemon), device management is carried out through the graphical interface of the client application, and using bat files (scripts).

Through the client application in graphical mode, in this case only monitoring is possible.

Authorization on behalf of the user is possible in two ways:

1. Start the service on behalf of the user from which the USB devices will be connected:



Свойства: VirtualHere Client USB Sharing (Локальный компьютер)

Вход в систему:

○ С системной учетной записью

□ Разрешить взаимодействие с рабочим столом

● С учетной записью: Pertov@test.ru

Пароль: ••••••••••••••••

Подтверждение: ••••••••••••••••

Помощь при настройке параметров пользовательской учетной записи для входа в систему

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

(password - the password of the user on behalf of which the service is running)

2. Specify in bat files, when connecting USB devices, the corresponding parameters:

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

(user - username (case matters), pssword - user password)

Running the client as a service has additional permissions (similar to starting in graphical mode with the -a option). This is useful when users need to be able to disconnect USB devices used by others.

To restrict the rights to disconnect users, configure the rights: "Rights Settings"

5.4 DISTKONTROLUSB CLIENT MANAGEMENT FROM SCRIPTS OR FROM COMMAND LINE

USB client can be controlled by scripts or the command line. This is useful when:

- You want to manage the client when run as a service
- You want to control the client only through a console session, for example ssh
- You want to create your own GUI
- You want to manage with a batch file (Windows) or bash (OSX / Linux) script

Start the client with the -t HELP argument to get a list of available commands.

```
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"
```

Returns "OK" on success,

If the server does not exist, or the address is invalid - "error: error string".

For example, on Windows:

Make sure the client is already running normally as an application (displayed as a green USB icon in the taskbar) or as a background service.

```
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>
```

From this report, you can see the hubs client to two USBoverIP and have 13 devices connected.

For example, 2-TokenJC connected to USBoverIP16 at USBoverIP16.1122, to use it, force execution

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

and see the "OK" response in the console.

To stop using the USB storage

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

To automatically use any device connected to your computer:

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

5.5 ADDITIONAL OPPORTUNITIES WHEN WORKING WITH THE DISTKONTROLUSB CLIENT

The USB over IP managed hub client has several command line arguments, described below. To use them on Windows, just call dkcl32.exe <argument> or dkcl64.exe <argument>, on OSX you have to call directly / Applications / DistKontrolUSB / DistKontrolUSB.app/Contents/MacOS/dkcl <argument>, on Linux - dkclt64 , or dkclientx86_64.

List and purpose of arguments:

-h Command line help.

-l = <path> File for logging all messages (instead of logging in the System Messages window.

-c Configuration file to use instead of the default file.

-a Run the client in administrator mode. This allows the client to disconnect other users from devices remotely.

-d install client drivers and shutdown. This argument is useful for performing an enterprise-wide installation over a network through a Microsoft Systems Management Server. (Administrator rights are required when using this argument.)

-x Extract drivers. This is useful for manually installing drivers on Windows XP Embedded.

-i On Windows and OSX, install the client as a service. (Administrator rights are required when using this argument).

-b Same as the -i argument, but installs the client as a service with autosearch enabled by default.

-u Remove client service (Administrator rights required when using this argument).

-y Remove all USB client drivers (if any) (Administrator rights are required when using this argument).

-t Send the command to the running client.

-r = <file> When used with the t / x / i / u / d argument, will redirect the output to the file specified after the argument. This is useful for parsing results in batch files on Windows.

5.6 DISTKONTROLUSB CLIENT MANAGEMENT EXAMPLES FOR WINDOWS AND LINUX

5.6.1 ALGORITHM FOR CREATING CLIENT MANAGEMENT BATCH FILE FOR WINDOWS

Run dkcl64.exe as a service or GUI in Windows.

We start the command line, go to the program directory.

We recruit:

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

Copy the device address (what's in brackets).

For example, it is USBoverIP16.115, then

To connect a USB device

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

To disconnect a USB device

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

(the address of the USB device is entered without a space after the comma)

To connect the USB port

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

To disconnect the USB port

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

(the address of the USB device is entered without a space after the comma)

5.6.2 DEMON SETUP AND SETTING ALGORITHM FOR LINUX

An example of installing and configuring (for connecting USB devices with SSL encryption and authorization) of the USB over IP hub console client as a daemon on Debian (Ubuntu):

The USB over IP hub client for Linux uses the embedded Linux usbip driver. Most Linux versions have it enabled by default. It is recommended to use the latest kernel (4.9+) for maximum compatibility.

The user must have sudo permission to run the daemon. Daemon control commands are executed without sudo. (connect via ssh to the OS, create a user, add it to the sudo group).

IP address of the hub 192.168.1.180 from the example - replace with the address of your device, user "testuser" and password "pass" with your corresponding ones.

Download the certificate and the console client from the hub:

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

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

Install the rights to the client and run it as a daemon:

```
chmod +x ./dkclientx86_64

sudo ./dkclientx86_64 -n
```

Add the IP address of the hub:

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

./dkclientx86_64 -t 'list'
```

Next, let's configure SSL and authorization. Turn on SSL encryption, restrict access to the USB port by login and password, and add the user to the hub's WEB interface (see the corresponding sections of the instructions).

Add the path to the certificate to the client's configuration file (replace the "testuser" user with your username):

```
echo "[General]" >> ./.dkcl

echo "SSLCAFile=/home/testuser/distkontrolusb.pem" >> ./.dkcl

cat ./.dkcl
```

We check that the output should contain the following lines:

```
…..

[Settings]

ManualHubs=192.168.1.180:6564

[General]

SSLCAFile=/home/ testuser /distkontrolusb.pem

.....
```

Restart the daemon:

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

We see:

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

We input:

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

We check:

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

Should be;

```
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
```

We connect a USB device, access to the port which is allowed for the user testuser from the device side:

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

You should see in the output:

```
OK
```

The USB device is connected to the OS with SSL encryption and limited access to the USB port of the managed USB over IP hub by login and password.

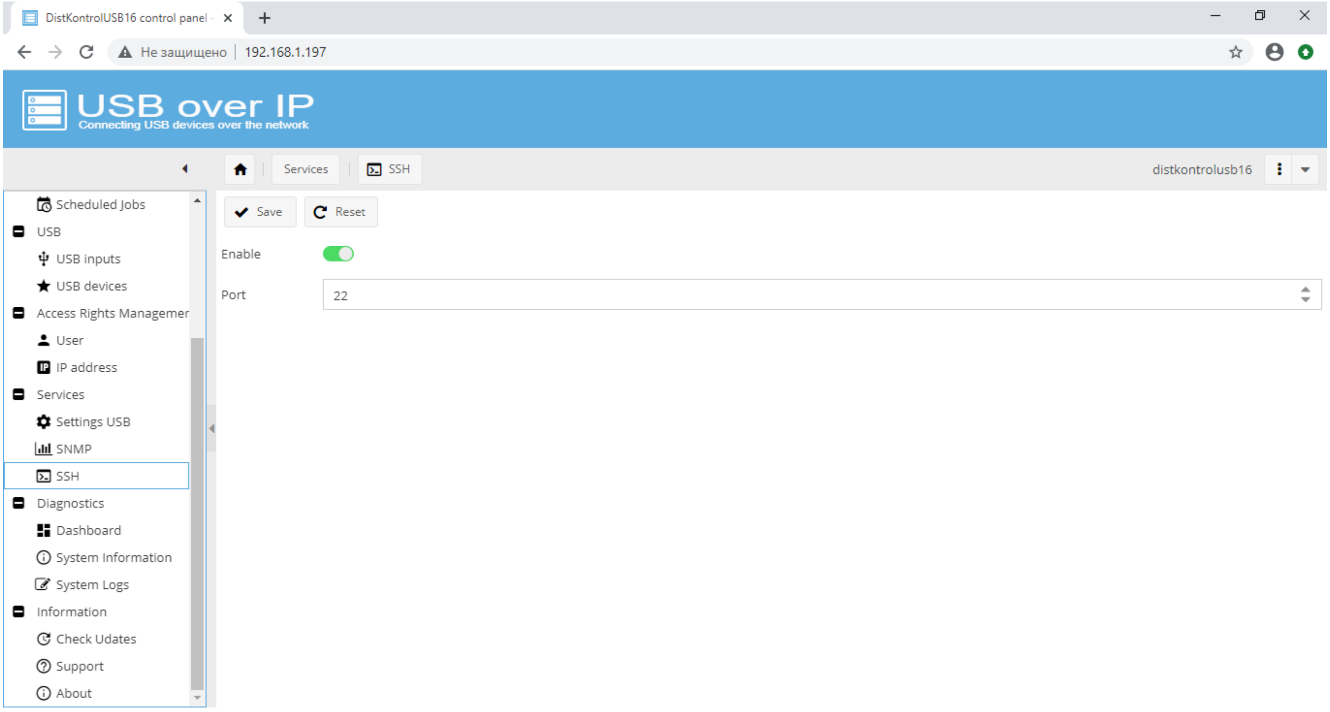
If in the output:

```
FAILED
```

We look at the result of an attempt to connect in the WEB interface of the device (for more details, see the Messages of the authorization system in the section Viewing the system log of DistKontrolUSB). We analyze what was done wrong, make adjustments.

6 BRIEF INSTRUCTIONS FOR USING THE PORT CONTROL UTILITY OF A USB MANAGED OVER IP HUB

To use the utility, you must enable "API SSH" on the "Services" - "USB Settings" page. The utility works with port 22.



Enable ●

Port 22

The general format for launching the utility:

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

All arguments are separated by spaces.

If the utility is run without parameters (without arguments), a brief help in English will be displayed.

Description of arguments:

1) ipaddress - IP address (or network name) of the device to which you want to connect;

2) status - "0" or "1". 0 - Disable USB port. 1 - Enable USB port.

3) UsbPort - the number of the USB port to be enabled / disabled (from 1.1 to 4.16);

4) pass - the password for the usbcontrol user (set in the WEB interface: Access rights management - User - usbcontrol)

Example:

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

(Enable USB port # 3.12)

Example of running in a bat file: see usbcontrol.bat

ATTENTION!!! The usbcontrol user password is transmitted to the device in a secure way, but storing it in control script files is not secure. It is necessary to take additional measures to ensure the security of the scripts, applications, etc. you use.

It is also possible to independently write a script for controlling USB ports via ssh. Connection is possible from the user "usbcontrol". The password is set when editing user rights. Commands available:

```
q  (exit)

usbcontrolapi status UsbPort
```

Description of arguments:

1) status - "0" or "1". 0 - Disable USB port. 1 - Enable USB port.

2) UsbPort - the number of the USB port to be enabled / disabled (from 1.1 to 4.16);

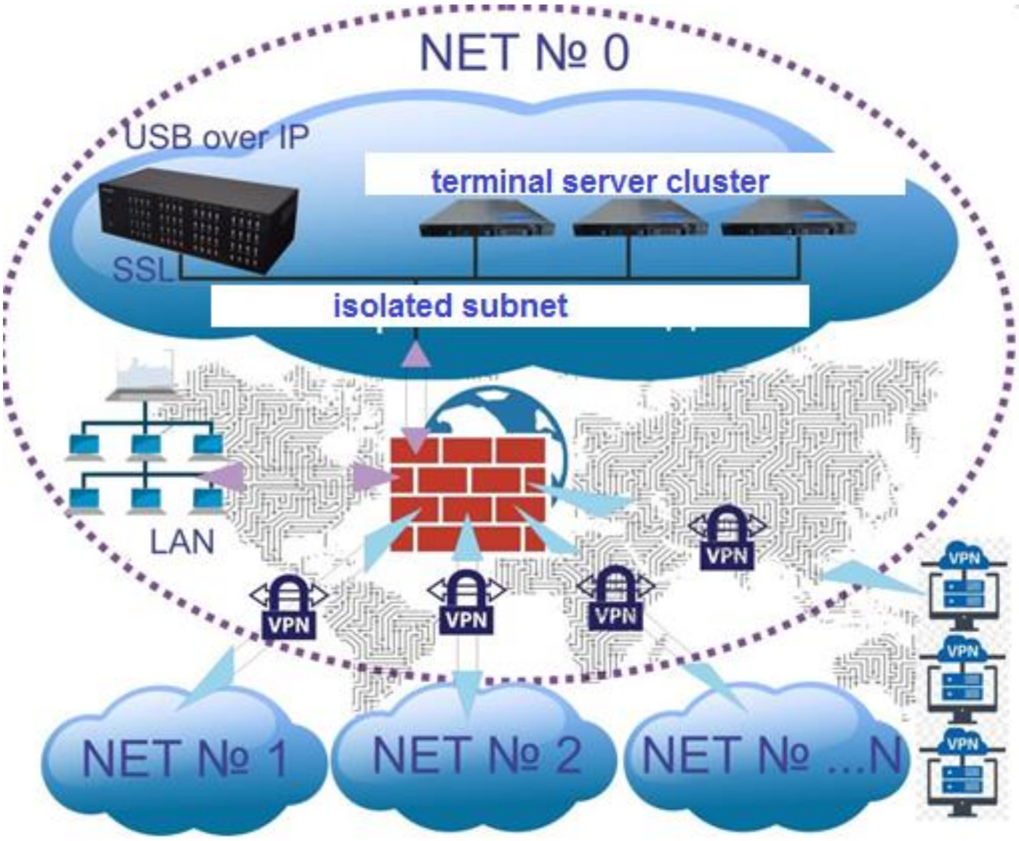
Example:

```
usbcontrol@192.168.1.180's password:

> ucbcontrol-api 1 3.15

Status OK. USB port: 3.16 Status: 1
```

7 OPTION OF USE MANAGED BY USB OVER IP HUB.

A USB over IP managed hub is not an absolute security feature when connecting USB devices over a network. It is necessary to combine its use with additional organizational and technical measures to ensure information security.

- Possible use case:
- Task: organization of access to USB devices:
- from regional offices (conditionally NET # 1 …… NET # N),
- for a limited number of computers and laptops that connect USB devices via a global network,
- for users published on terminal application servers.



1. Organizational security measures.

The controlled USB over IP hub is installed in a high-quality, key-locked server cabinet. Physical access to it is streamlined (ACS to the room itself, video surveillance, keys and access rights for a strictly limited circle of people).

All USB devices used in the organization are conditionally divided into 3 groups:

- Critical. Financial EDS - used in accordance with the recommendations of banks (not via USB over IP)
- Important. EDS for trading floors, services, EDI, reporting, etc., a number of keys for software - are used using a controlled USB over IP hub.

● Not critical. A number of keys for software, cameras, a number of flash media and disks with non-critical information, USB modems - are used using a controlled USB over IP hub.

2. Technical security measures.

Network access to the USB over IP managed hub is provided only within an isolated subnet. Access to an isolated subnet is provided:

- from a terminal server farm,
- via VPN (certificate and password) a limited number of computers and laptops, via VPN they are given permanent addresses,
- via VPN tunnels connecting regional offices.

On the managed USB over IP hub DistKontrolUSB using its standard tools, the following functions are configured:

- The USB over IP hub uses encryption to access USB devices (SSL encryption is enabled on the hub).
- "Restricting access to USB devices by IP address" is configured. Depending on the IP address, the user is given access to the assigned USB devices or not.
  - "Restricting access to the USB port by login and password" is configured. Accordingly, users are assigned rights to access USB devices, since all USB keys are permanently connected to the USB over IP hub and cannot be moved from port to port.

Physical activation and deactivation of USB ports is carried out:

  - For software and EDM keys - using the task scheduler and assigned tasks of the concentrator (a number of keys were programmed to turn on at 9.00 and turn off at 18.00, a row from 13.00 to 16.00);
  - For keys from trading floors and a number of software - by authorized users through the WEB interface;
  - ● Cameras, a number of flash drives and disks with non-critical information are always on.

8 FREQUENTLY ASKED QUESTIONS

8.1 FREQUENTLY ASKED QUESTIONS ABOUT USB OVER IP CONCENTRATOR SETUP.

Received the device. When connecting a USBoverIP-controlled hub with a patchcord to a laptop, it does not ping and you cannot enter the WEB interface.

Connect your device and laptop via a network switch.

Received the device. Why can't I connect a USB device over the network to my computer via the DistKontrolUSB USB over IP managed hub?

Make sure the USB device functions properly when connected to a computer with a USB cable. If you need a driver for your USB device, such as a USB printer or multifunction device, make sure you have it installed on your computer. Restarting your computer after installing the USB device driver can also help. Although the USB over IP managed hub can work with a very wide range of USB devices, it is not guaranteed to work with absolutely all USB devices.

Received the device. The set includes only a passport for the product. Where can I find instructions?

All documentation and software can be downloaded from the site.

Managed USB over IP hub. User mannual

Managed USB over IP hub. Booklet

Managed USB over IP hub. The passport

Managed USB over IP hub. GOST R Certificate of Conformity

Managed USB over IP hub. Fire safety certificate

Managed USB over IP hub. Notification of the Center for Licensing, Certification and Protection of State Secrets of the FSB of Russia

Managed USB over IP hub. Report on entry into the Unified Register of notifications by the Center for Licensing, Certification and Protection of State Secrets of the FSB of Russia

Managed USB over IP hub. Eurasian Economic Commission. Unified register of notifications about the characteristics of encryption (cryptographic) means and goods containing them

Managed USB over IP hub. EAC Declaration of Conformity

Managed USB over IP hub. ROSACCREDITATION

Managed USB over IP hub. Prices

Managed USB over IP hub. Payment and delivery

Received the device. The kit contains only a passport for the product, but it does not indicate the factory IP address of the device and login / password. Where can I find them?

By default, a USB network device has:

Static IP address - 192.168.1.180

Login to the WEB interface panel - admin

Password for the WEB interface panel - admin

Client connection port - 6565 (default)

SSL client connection port - 6564 (when enabled)

WiFi interface (wlan0) - disabled Got a device. Why can't I see any servers in the DistKontrolUSB USB over IP managed hub client list after installation?

Make sure the USB over IP managed hub is properly connected to the network. Some antivirus programs may also use a firewall that prevents the managed USB over IP setup program from accessing the network. Make sure the client application of the USB over IP managed hub is not blocked by antivirus software.

Problem when working with SberBank keys VPN-Key-TLS in a terminal session. The key is connected to a USBoverIP hub, it is visible on the client machine (virtual machine on Windows), but after launching it gives the following error: "error cannot open infocrypt hwdssl device"

The system for working with VPN-Key-TLS tokens provides protection against remote access to the key, so if you try to start the key from the remote desktop (when the key is inserted into the server, and the RDP client tries to start it), this error will be issued, and the key will work will not be.

Outputs:

1. Connect the key to the client via usboverip and then connect to the terminal server.

2. Or use not RDP, but programs like VNC, Radmin and the like for console access.

For your VPN-Key-TLS connection scheme, we recommend:

1. Connect the dongle via USB over IP to the client PC (in the connection properties, enable the connection of ports and disks (or the Infocrypt HWDSSL disk)).

2. Connect to the server via RDP

3. Open the disk corresponding to the disk Infocrypt HWDSSL

4. Run start.exe

The connection process or part of it can be automated with a script:

1. We connect to the VPN server.

2. Turn on the power of the USB port.

3. Connect the key

4. Connect to the RDP server

5. We work

6. At the end of the RDP session, turn off the power to the USB port.

Also, to ensure security, it is recommended to take additional measures (VPN channel, authorization, etc.)

The problem when connecting the SberBank VPN-Key-TLS key in the console session.

1. Remove all token drivers on the server (computer)

2. Reboot the server (computer)

3. Connect the token to the server (computer) via USB over IP

4. Install the drivers

The Sberbank token has a number of problems with the OS, but with the OS. As a rule, the steps described above are enough.

For more see:

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

If a USB device is connected via a DistKontrolUSB hub, can several computers work with it AT THE SAME TIME?

It is not possible to operate multiple devices (PC) with one USB device at the same time. USB 2.0 does not allow this.

The key can be accessed by any number of PCs and switch between them manually or automatically.

How do I use one SSL certificate across multiple hubs?

In the "System" - "Certificates" section, it is necessary to IMPORT the certificate to all hubs as indicated in the "Client application settings" instructions.

A downloaded certificate from any device will work for all devices on which the same certificate is imported.

8.2 FREQUENTLY ASKED QUESTIONS FOR CONFIGURING THE USB OVER IP HUB CLIENT APPLICATION.

When authorization is enabled, no password is required to connect to a USB device (port). The connection result is recorded in the system log:

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

When connected to a USB device (port), the "Remember password" checkbox is checked in the client application, see p. "Configuring a client application controlled by a USB over IP hub"

When authorization is enabled, USB devices are visible in the client application, but when connected, they are not connected. The connection result is recorded in the system log:

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

When connecting to a USB device (port), the “Remember password” checkbox is checked in the client application and the connection to the USB device is made. Further, the user's password was changed, but the old one is automatically transferred. It is necessary to close the application (do not minimize, which is the default action when you click on the "cross" in the upper right corner of the program interface). To make changes to the client application settings file, see p. “Configuring the client application of a managed USB over IP hub” (you can simply delete the settings file to reset all settings of the client application to the original ones) If you need to delete the password remembered by the user, you need to delete the line like (will differ after the equal sign):

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

The client application does not work on Linux OS. The message is displayed: "USBIP client drivers are not available, you will have to compile / install your own from the linux kernel source"

Most likely the kernel is missing usbip.

You can check:

```
modprobe vhci_hcd
...
```

```
lsmod | grep vhci
```

Most Linux versions are already compiled with usbip, however sometimes you need to recompile the kernel to support them. (make menuconfig and select Drivers -> USBIP to check if it is enabled and then rebuild the kernel kernel make)

Can the client menu be customized? The client application does not need any menu item.

*Yes, you can. The client saves all of its parameters in one text file**:***

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

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

Linux: ~/.dkcl

This file is updated when settings are changed and usually does not need to be changed by the end user. On first launch, the client creates a default configuration file. To hide menu items in the client:

1. Log out of the client.

2. Edit the file c: \ Users \\ AppData \ Roaming \ dkcl.ini (for Windows)

3. In the [General] section, add the HideMenuItems line and specify the exact name of the menu items, separated by commas, to be hidden.

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

Can I add port numbers to the client app's device list? Now, if several devices are connected (especially of the same name), then it is very unclear which device a particular client needs to use

Yes. Rename (connect one by one) USB devices and you can use simple names (if desired, you can use port numbers in the name).

Can't rename the USB device in the client application.

Update the device software to the latest current version. Download the latest version of the client from the website. Download links are available in the Web interface in the "Support" section

How to start DistKontrolUSB Client as systemctl service (Debian 9+ / Ubuntu 18.04 Server +) at system startup

1. SSH to your OC

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

(or wget http://www.distkontrol.ru/usbclient/dkclienti386 depending on the bitness of the OS)

2.sudo chmod + x ./dkclientx86_64

3.sudo mv dkclientx86_64 / usr / sbin

4. Create a text file

nano /etc/systemd/system/dkclient.service

with the following content:

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

5. systemctl daemon-reload

6. systemctl enable dkclient

7. systemctl start dkclient

We check:

/usr/sbin/dkclientx86_64 -t 'MANUAL HUB ADD,192.168.1.180:6565'

/usr/sbin/dkclientx86_64 -t 'list'

/usr/sbin/dkclientx86_64 -t 'AUTO USE HUB,distkontrolusb64'

For more see:

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