



**TOSIBOX<sup>®</sup> HUB**  
User Manual

# Content

1	Introduction .....	4
2	System description .....	5
2.1	Context of use.....	5
2.2	TOSIBOX® HUB in brief.....	5
2.3	Licensing .....	6
2.4	System components .....	7
2.5	Main features .....	7
3	System Requirements .....	8
3.1	Requirements for cloud and on-premises virtualisation platforms.....	8
3.2	Microsoft Azure.....	9
3.3	Amazon Web Service .....	9
4	Connectivity.....	9
4.1	Tosibox Cloud architecture .....	9
4.2	TCP and UDP connections.....	10
4.3	Installing behind a firewall.....	10
5	Installation .....	11
5.1	Installing the VM image .....	11
5.2	VMWare vSphere/ESXi .....	11
5.3	Microsoft Hyper-V .....	11
5.4	Linux KVM .....	12
5.5	Cloud installation .....	12
6	Initial setup .....	12
6.1	Accessing the configuration interface .....	12
6.2	WAN interface configuration and product activation .....	12
6.3	Change password.....	12
6.4	Configuring LAN interfaces.....	13
6.5	Create Remote Matching code .....	13
6.6	Remote Matching.....	14
6.7	Connecting Nodes and Locks.....	14
6.8	Software update.....	15

7	User interface.....	15
7.1	Navigating in the user interface .....	15
7.2	Login.....	17
7.3	Adding admin users .....	17
7.4	Adding virtual LANs .....	18
8	Static routes .....	18
8.1	introduction .....	18
8.2	Static routes view.....	19
9	HTTPS login.....	20
10	Access rights management .....	21
10.1	Managing access rights with TOSIBOX® Key .....	21
10.2	Managing access rights with TOSIBOX® HUB.....	21
10.3	Using Access Groups .....	22
10.4	Access Groups UI.....	22
10.5	Filtering.....	23
10.6	Workflow for creating Access Groups.....	24
10.7	Access Groups settings .....	26
10.8	IP-to-IP mode.....	26
10.9	Scheduled access.....	28
10.10	Activating scheduled access.....	28
11	Logging and alerts.....	29
11.1	VPN usage logging for Keys.....	29
11.2	Email alerts.....	30
11.3	Admin trail.....	30
11.4	Admin trail events .....	30
12	Software update .....	33
13	Legal notices .....	35

# 1 Introduction

Congratulations on choosing the Tosibox solution!

Tosibox is globally audited, patented and performs at the highest security levels in the industry. The technology is based on two-factor authentication, automatic security updates and the latest encryption technology.

Tosibox solution consists of modular components that offer unlimited expandability and flexibility. All TOSIBOX® products are compatible with each other and are internet connection and operator agnostic. Tosibox creates a direct and secure VPN tunnel between the physical devices. Only trusted devices can access the network.



TOSIBOX® HUB turns your TOSIBOX ecosystem into a controlled OT network of always-on VPN connections for remote maintenance, continuous monitoring, real-time data collection and data logging.

This document applies to HUB version 3.0.0.

# 2 System description

## 2.1 Context of use

TOSIBOX® HUB makes it possible to build a system consisting of many TOSIBOX® Nodes and Keys. HUB is a VPN tunnel concentrator that maintains always-on VPN connections towards TOSIBOX® Nodes and provides centralized user and network management.

HUB is used when the number of users and remote locations is in their dozens or hundreds or when a centralised server software needs to communicate with the remote locations. HUB allows connecting over a thousand serialized Nodes and Keys simultaneously.

HUB is a licensed software product that runs on the customer's own server or virtualization platform and scales easily from just a few connections up to hundreds or thousands. The maximum number of concurrent connections is defined by license type and the performance of the hardware or platform which the HUB is running on.

## 2.2 TOSIBOX® HUB in brief

HUB is a software-only solution for central VPN management running in a virtual server environment. It enables integration of separate Tosibox Nodes into a robust and distributed network of connected devices.

HUB can be deployed e.g. in office networks and cloud infrastructure typically residing in data centers to build centrally managed and connected Tosibox ecosystem. Also, with the help of virtual platforms it is possible to achieve a very high level of redundancy and fault-tolerance where failover time is measured in just seconds.

HUB has high throughput and encryption capacity limited only by available computing resources and the network parameters. This allows building large-scale systems that provide simultaneous access to thousands of Locks, Keys and Mobile Clients and the devices connected to them.

### HUB functionality

#### Logging and alerts

- Network wide audit logging from connected TOSIBOX® Nodes
- System audit trail
- Connection monitoring to detect and notify the user about connection problems
- Email alerts for connection establishment and disconnection

#### User and access rights management

- Account management for the system
- Scalable user access management per Lock and Node
- Scheduled access management

## Network monitoring

- Status of each Lock and Node in the network
- Status of each user in the network
- System overall status

## Security

- Support for VLANs (virtual LANs)
- Built-in firewall
- Encryption and authentication: PKI, 3072-bit RSA
- Data encryption: TLS, AES-256-CBC / AES-192-CBC / AES-128-CBC / Blowfish-128-CBC

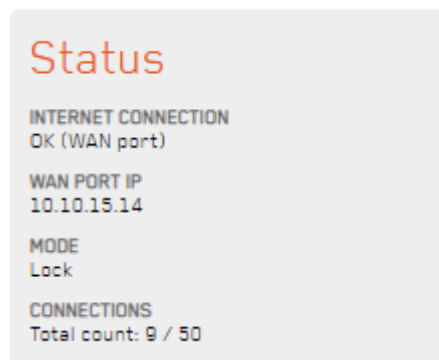
## 2.3 Licensing

### Full version

With a full version of the HUB, you get technical support and as many concurrent VPN tunnel connections as is defined by your license cap. The maximum number of concurrent VPN connections is limited with the license.

Connections total count indicates the number of connected Nodes, Keys and Mobile Clients and the license cap of concurrent VPN connections. Each device can potentially utilize one license when it is online and VPN tunnel is formed between the HUB and the Node, Key or Mobile Client.

HUB starts limiting new VPN connections when the license cap is reached.



*Figure 1: In total of nine connected devices to this HUB and a license cap of 50.*

In the above screen shot the HUB has nine connected devices either online or offline and the license cap of 50 concurrent VPN connections.

### LITE version

HUB LITE is free to download and use after registering. It is limited to five concurrent VPN connections from any TOSIBOX® device. You can add more than five devices to LITE, but you are not able to fully utilise them.

## 2.4 System components

The complete system consists of TOSIBOX® Nodes and Keys that are matched to the HUB in a way that the system owner decides.

Every matched Key uses either a bridged (Layer 2) or a routed (Layer 3) connection type. The bridged layer 2 connection means that the Lock is essentially in the same network with the HUB's LAN port or VLAN that it is bridged to. The routed layer 3 connection creates a connection where the Node and the HUB both have their own IP addresses, and the communication works by routing the IP packets through the network towards the target IP address.

The bridged Key connection allows access only to a specific LAN network and the Locks bridged to it. The routed Key connection allows the selection of multiple LAN networks, Locks and other targets that are accessible for the Key. The desired connection type can be selected for each Key in the Web user interface from [Settings > Keys and Locks](#). The default connection type for Keys matched to a HUB is Layer 3. Additional Keys can be matched to the HUB the same way as they are to a Node.

The matching process for Nodes and Keys is presented in the Key and Lock User Manual. Connecting a Node to the HUB is carried out essentially in the same way as when connecting two Nodes together, except during the process the connection type is defined either as Layer 2 or Layer 3.

## 2.5 Main features

### TosiControl support

HUB is a central component in network management with TosiControl. Access controls created with the Access Groups can be monitored on TosiControl. HUB also sends a list of network elements and their status information for centralized device management.

### Manage any service, run any protocol

HUB enables authentic Layer 2 communication which means you do not need drivers for any ethernet protocol. Use whatever protocol, ethernet capable edge-device, data analytics software, or cloud hosting environment you choose. Leverage our automated networks to build the system you want, not the system that works with your legacy technology.

### Built-in and automated cybersecurity

Automated networking means there is no possibility for human error in properly configuring our cybersecurity profile. Every HUB includes:

- Automated Linux iptables based firewall at the edge. Everything connected to the HUB LAN is invisible to the internet
- Point-to-point networks through 256-bit AES encrypted VPN tunnels without third-party cloud. Data is fully encrypted while in-transit in VPN tunnels

## Central user access management

HUB provides centralized user management via novel view called Access Groups. Access groups allow the administrator to define access rights between the connected devices and users. Configuration is done via Access Groups menu.

## Audit log data collection and monitoring

HUB collects log data on the events of the HUB and the events of any connected Nodes and Sub Locks. Log collection and monitoring can be enabled from the menu of both the HUB and the Nodes that are expected to report events. Only Nodes from which log data is desired should have the logging enabled.

## Connection monitoring and alerts

HUB can be set to send email alerts for connections being established and closed. The alerts can be configured freely for any or all matched Nodes. Activating alerts does not require any additional services. Alerts can be taken in use from the menu.

## Virtual LANs (VLANs)

HUB can be configured to connect to existing VLANs via any of the physical LAN ports. Configuration is available on the menu.

# 3 System Requirements

## 3.1 Requirements for cloud and on-premises virtualisation platforms

Virtualisation platform based on one of the following:

- VMWare vSphere/ESXi v7.0 GA
- Microsoft Hyper-V on Windows Server 2019
- Linux KVM
- Microsoft Azure cloud platform (update from previous version, new installations are done on Azure Marketplace)
- Amazon AWS cloud platform (update from previous version, new installations are not supported)

Minimum HW and computing requirements for cloud and on-premises virtualisation platforms:

- x86-64 processor architecture, processor with two high performance server CPU cores. Additional cores can be required based on the intended system load
- Minimum 2 GB RAM, recommended 8 GB RAM for large environments
- Minimum 16 GB of permanent storage, recommended 20GB for VMWare, Hyper-V and KVM environments



- Two or more network interfaces for the virtual machine
- One non-restricted IP address, recommended public IP address
- Working DNS connectivity

Minimum 10/10 Mbit/s internet connection, recommended 100/100 Mbit/s

To install and setup the HUB, you will also need:

- Internet connectivity to download the HUB VM image and possible software updates
- License key to activate HUB

Note that Secure Boot is not supported and should be disabled if available on the platform.

### 3.2 Microsoft Azure

HUB can be installed on Microsoft Azure from the Azure Marketplace. The above requirements apply to Azure.

- <https://azuremarketplace.microsoft.com/>

### 3.3 Amazon Web Service

Currently HUB 3.0.0 cannot be installed on AWS. Virtual Central Lock 2.6 should be installed using the scripting installation method as explained in Helpdesk and upgraded to HUB 3.0.0. The above requirements apply to AWS.

## 4 Connectivity

### 4.1 Tosibox Cloud architecture

Typically, TOSIBOX® products facilitate direct establishment of VPN connections between one another. However, certain scenarios preclude this direct connection, such as instances where outbound UDP is obstructed by a firewall, or a proxy server is necessitated. In such circumstances, a fallback mechanism is employed, utilizing the Tosibox Cloud environment to establish relayed VPN connection.

The relay server serves as a Tosibox-hosted router, redirecting encrypted VPN data between the connected endpoints. Relay servers possess known addresses and are perpetually accessible to Tosibox products via the TCP protocol.

Due to the latencies inherent in the communication between VPN endpoints and relay servers, as well as the characteristics of the TCP protocol and limitations of server capacity, relayed connections may not deliver performance on par with direct UDP connections. To optimize latencies and ensure optimal performance, it is advisable to permit all outbound UDP connections in the firewall configuration.

## 4.2 TCP and UDP connections

The Tosibox ecosystem, encompassing the HUB among other components, offers support for two distinct VPN connection types: TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) connections. Within the ecosystem, a VPN tunnel can be established using either of these protocols.

TCP and UDP are transport layer protocols within the Internet Protocol (IP) suite, governing the transmission of data over networks while presenting different sets of features and trade-offs.

TCP can create a dependable and sequentially ordered connection between two devices before transmitting data. It ensures that data packets transmitted from one device are received accurately and in the same order by the receiving device. Notably, the TCP connection type is always relayed, meaning the connection is routed through servers in the Tosibox Cloud. Consequently, TCP connections typically exhibit slower performance compared to UDP connections.

On the other hand, UDP operates differently, as it does not establish a dedicated connection prior to data transmission. Instead, it independently sends packets, known as datagrams, to the recipient without providing guarantees of reliability, ordering, or congestion control. UDP prioritizes simplicity and minimizes overhead.

The UDP connection type, in contrast to TCP, is always a direct connection from the HUB to the respective Node or Key. This inherent directness results in faster performance when compared to the TCP connection type.

## 4.3 Installing behind a firewall

HUB is designed to work best with a non-restricted public IP address. Often this is the optimal solution providing the best connectivity with the easiest setup.

If separate network edge firewall is required in front of the HUB this can be achieved with the following remarks. The firewall must be configured with:

- UDP enabled for direct VPN connections to work. Without UDP enabled all network connections will be routed via relays which can cause increased latency
- No port translation
- No restrictions towards the Internet

Note, that all ports from the internet towards the HUB can be closed.

# 5 Installation

## 5.1 Installing the VM image

In most cases, one of the images referenced earlier can be imported to the virtualisation platform directly or converted to a suitable format. Please refer to the documentation of your virtualization platform for the supported image formats and import method.

HUB images are distributed at <https://downloads.tosibox.com/HUB/>.

## 5.2 VMWare vSphere/ESXi

- Download the latest .ova image
- Use the Deploy OVF Template function of the vSphere client to import the downloaded .ova file
- Adjust the CPU and RAM hardware settings according to your needs, keeping in mind the minimum requirements
- Make sure that the video memory setting is set to "auto-detect" or at least 32 MB is available for the VM if configured manually
- Make sure that the network adapter is in bridged mode and satisfies the requirement of the non-firewalled public IP address
- Check from VMWare virtual switch security settings your virtual LAN adapter has security options are set to
  - Promiscuous mode – Accept
  - MAC address changes – Reject
  - Forged transmits – Accept

## 5.3 Microsoft Hyper-V

- Download the latest .vhdx image
- If needed, create a new Virtual Switch using type External and the interface that is connected to the Internet
- Create a new VM with the downloaded vhdx image, select Generation 2
- Edit the settings of the created VM
- Add new Network Adapter (not Legacy)
- In the Network Adapter's settings, select the correct Virtual Switch (if you created one earlier, select it)
- In the Network Adapter's settings, go to Advanced Features and select Enable MAC address spoofing

## 5.4 Linux KVM

In most cases, one of the distributed images can be imported to the virtualisation platform directly or converted to a suitable format. Please refer to the documentation of your virtualization platform for the supported image formats and import method.

## 5.5 Cloud installation

For instructions how to install the HUB on Azure see Tosibox Helpdesk.

# 6 Initial setup

## 6.1 Accessing the configuration interface

Start the virtual machine that was installed. The virtual machine will automatically boot into graphical console / desktop and launch the activation user interface through a browser. The browser will automatically close after it has been inactive for a long time. In this case it can be restarted by interacting on the desktop with mouse or keyboard.

## 6.2 WAN interface configuration and product activation

In the activation user interface, configure the IP address settings for the WAN interface. The IP address must be assigned dynamically with DHCP during activation. After activation is complete, you can configure the IP address manually. When configuring the IP address manually, it is very important to enter also working DNS servers as many product features, including the activation, require a working DNS service.

Enter the delivered license key into its own field and click Activate. The product is now activated, and it will download the rest of the product components using the defined WAN connection. This can take up to 15 minutes, depending on the Internet connection speed. After the activation and installation is finalized, a message “Activation completed, rebooting...” will appear and the VM will automatically reboot. After rebooting, you can proceed with the configuration.

## 6.3 Change password

After the virtual machine has booted up again, the graphical console now provides access to the HUB web user interface. Log in with the default admin credentials (admin / admin) and go to [Settings > Change password](#) to change the password.

The web user interface can be accessed also remotely over VPN connection from master Key. If there is a need to access the web user interface from other Keys or networks, the access rights can be explicitly allowed in the Access Groups.

## 6.4 Configuring LAN interfaces

The HUB can have multiple LAN and VLAN interfaces that can provide access to your own local networks and services. The initial configuration of HUB contains a default LAN1 interface that is not connected to any real adapter. To assign LAN1 to a real adapter, it must be first deleted by navigating to Interfaces page and selecting Delete next to interface 'LAN1'.

To add additional LAN interfaces for the HUB, you must first configure a new network adapter for the virtual machine. This is done differently depending on your virtualization platform and typically requires restarting the virtual machine. In case layer 2 VPN connections from Keys or Nodes are required, the network adapter should be configured to allow MAC address spoofing or promiscuous mode:

- Hyper-V: In the Network Adapter's settings, go to Advanced Features and tick Enable MAC address spoofing
- VirtualBox: In the Network Adapter's settings, open Advanced menu and set Promiscuous Mode: Allow All

After the new network adapter is added, it can be configured in the web user interface by selecting *Network > Interfaces > Add*. In the "Add interface" view, set the port role as 'LAN', define a number for the interface (e.g. starting from '1'), choose the IP address assignment method (DHCP or static) and finally choose the newly added network adapter. After clicking Submit, the IP address and DHCP server settings can be configured if protocol was set to static. After clicking Save, the new interface is ready to be used and it can be included in Access Groups or additional VLANs utilising the interface can be created (see User Manual).

## 6.5 Create Remote Matching code

After the HUB is activated and has Internet connection, the Master Key needs to be matched to the HUB to add it to the network. This is done with the remote matching feature.

1. Go to *Settings > Keys and Locks*. Scroll down to the bottom of the page to find Remote Matching.



Figure 2: Remote Matching Code generation

2. Click the Generate button to create the Remote Matching Code.
3. Copy and send the code to the network administrator who has the Master Key for the network. Only the network administrator can add the HUB to the network.

## 6.6 Remote Matching

Insert the network Master Key in your workstation and TOSIBOX® Key client application opens. If Key application is not installed browse to [www.tosibox.com](http://www.tosibox.com) for more information. Note that you must use the Master Key for your network.

Log in with your credentials and go to *Devices > Remote Matching*.

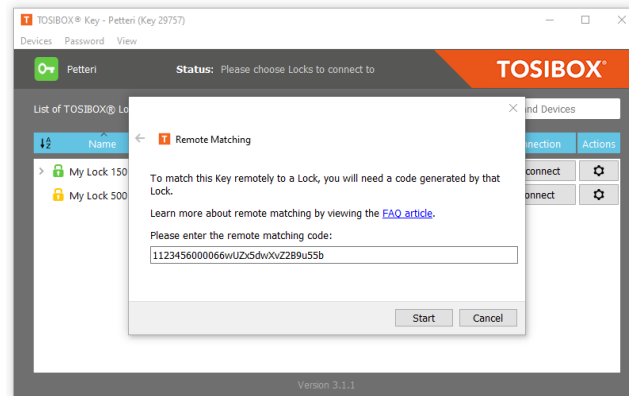


Figure 3: Remote Matching on TOSIBOX® Key client application

Paste the Remote Matching code on the text field and click Start. The Key application will connect to the TOSIBOX® infrastructure. When “Remote Matching completed successfully” appears on the screen, HUB has been added to your network. You can see it on the Key application interface immediately.

## 6.7 Connecting Nodes and Locks

Now that you have HUB installed in your network you can connect all your Nodes and Locks for always-on, secure VPN connectivity.

1. Open TOSIBOX® Key application and go to *Devices > Connect Locks*.
2. Tick all the wanted Nodes and Locks and make sure you also include the HUB in the selection. Click Next.
3. For Select Connection Type choose either Layer 2 or Layer 3, click Next.
4. Confirmation dialog is displayed, click Save and the VPN tunnel is created between each selected node and the HUB separately and the devices start to appear on the HUBs Status view.

If you need to revert the connection, you can go through the *Devices > Revert Lock Connections* wizard in the Key client application and remove those devices you do not want connected to HUB.

## 6.8 Software update

Software updates can be checked and installed from HUB *Settings > Software update*. Opening the Software update view displays the option to check for possible available updates.

It is recommended to update to the latest available software version before taking the HUB to production environment.

# 7 User interface

The TOSIBOX® HUB web user interface screen is divided into four sections:

- Menu bar – Product name, menu commands and Login/Logout command
- Status area – System overview and general status
- TOSIBOX® devices – Nodes and Keys matched to this HUB
- Network devices – Devices connected to the selected Node discovered during network scan

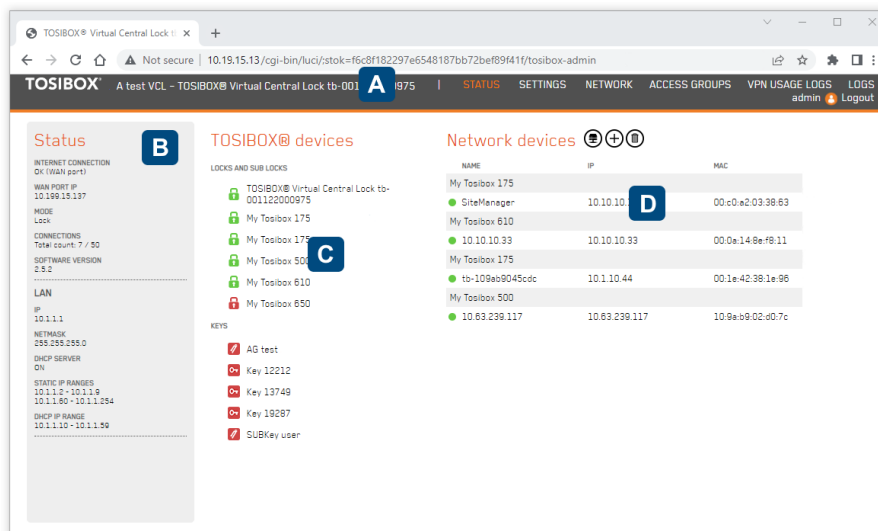


Figure 4: HUB user interface overview

Note that your screen can look different depending on the settings and your network.

## 7.1 Navigating in the user interface

### Status menu

The Status menu command opens the Status view with basic information about the network configuration, all matched TOSIBOX® Nodes and TOSIBOX® Keys and possible LAN or manually added devices.

The TOSIBOX® HUB scans the configured network interfaces. The LAN network scan can be configured to discover physical LAN devices with the Scan for LAN devices button.

New network devices can be added either

- automatically by clicking the network icon ("Scan for LAN devices"), which searches for all the devices within the LAN networks of the product
- manually by clicking the plus icon ("Add network device") and filling in the required details on the page that opens.

The network device list consists of devices connected to HUB LAN or VLAN. The list can be cleared by clicking the Clear network device list button. Devices connected to any Nodes' LAN are not cleared as the list of devices is managed by the Nodes and sent to HUB periodically.

## Settings menu

The Settings menu contains various settings related to TOSIBOX® Nodes and TOSIBOX® Keys, change the name for the HUB, reset to default settings, change the password of the admin account, restart the HUB, update the software, set email alerts and change the advanced settings.

The advanced settings page allows control to

- Remote support access from Tosibox Technical Support
- Logging server and audit logging settings
- HUB time zone
- VPN cipher selection
- NTP service on HUB
- Local user password minimum and maximum length requirement
- VPN access from the Mobile Clients
- Force computers using the Key to route all Internet traffic through the HUB
- HTTP/HTTPS selection

## Network menu

All networking settings can be edited in the Network menu.

- Interfaces – Configure WAN and LAN interfaces
- VLANs – Configure virtual LAN settings. VLANs can be added to any of the product's LAN interfaces
- Static routes – Configure active static routes on the HUB
- DHCP Server – Configure Dynamic Host Configuration Protocol server on the HUB

## Access Groups menu

Access Groups is the central user management view. Access Groups are used to define access rights between the connected devices and users.



Access Groups menu allows the administrator to define access control between Keys and Locks already matched with the HUB, the HUB LANs or VLANs, IP address ranges or single IP address even on port and protocol level. It also allows defining an access schedule for Sub Keys in this access group.

## VPN usage logs menu

VPN usage logs collect logging information on Keys accessing Nodes or IP addresses on HUB LAN. This data can be used for analysing how much data is consumed over the traced VPN connections.

## Logs menu

Logs view creates audit trail of various admin actions such as configuration modifications to keep track of changes in the system for system auditing purposes.

## 7.2 Login

HUB UI is protected from unauthorized access with a username/password. Login is possible only over VPN connection if accessing from the internet or from any workstation via private LAN side.

You can log in to the product's web user interface in the following ways:

- Using the virtual machine's graphical console
- Using any of the HUB's configured LAN or VLAN interfaces. The connecting computer must be connected to the same network with the LAN/VLAN interface and the LAN/VLAN interface must belong to an access group that provides access to the web user interface. The IP address of the product's LAN/VLAN interface is entered as the address in the browser.
- Over a VPN connection from a serialized master Key. The browser opens by double-clicking the HUB's name in the Key user interface.

There is a single administrator level access and one pre-defined username (admin). The default password is generated during the installation.



*Login session timeouts automatically in 1h if there is no user activity. Timeout length is not configurable.*

---

## 7.3 Adding admin users

HUB supports a maximum of 50 admin users. Default administrator user 'admin' can create and delete new users, but the default user cannot be removed. Only one user can be logged in at the same time.

When a new user is created an unambiguous username is required. The system generates a one-time password for the user. When a new user logs in for the first time, they must change the password. If a password for the user is lost, admin can reset it from the same menu, creating a new one-time password for the user.

Users can change their own password any time. HUB enforces mandatory password change during the first login.

Password constraints (min, max length) are set on Advanced settings view. Audit log will record configuration changes done by all admin users.

## 7.4 Adding virtual LANs

When the system local network has multiple VLAN networks available, adding a new virtual LAN can be used to connect the HUB to these networks. Each VLAN is configured to work over one of the product's virtual network adapters.

- To add a new VLAN interface, open the VLANs page and click Add
- Set the interface name, select the physical LAN port and VLAN tag (an integer between 1 and 4094). Note that VLAN ID can be set to one single interface at a time. Remove used VLAN ID before assigning it to another VLAN.
- Click Submit.
- Set the IP address and netmask used by the HUB in this VLAN and define DHCP settings if needed.
- Accept the settings by clicking the Save button. The newly added virtual LANs are summarized on the VLANs page together with their settings.

# 8 Static routes

## 8.1 introduction

A "static route" in networking refers to a predefined and manually configured path that data packets should follow to reach a specific network or destination. Unlike dynamic routing protocols that automatically determine the best path based on real-time network conditions, a static route is configured and maintained by a network administrator.

Network administrators set up static routes by specifying the destination network or IP address and the next-hop router or gateway that should be used to reach that destination. This information is entered into the routing table of a network device, such as a router or switch.

Static routes are typically used in specific situations, such as when a particular network segment should always use a specific path to reach a certain destination. They are also employed when the network environment is simple, stable, and changes rarely, making dynamic routing unnecessary.

Static routes are global settings in HUB. They are delivered to all connecting clients independently of how Access Groups are configured. Static routes should be considered only after Access Groups configuration is not enough.

## 8.2 Static routes view

Tosibox HUB static routes view can be configured with the Network / Static routes menu command.

The view consists of *Active IPv4 Routes* table that lists default routes, active static routes already in the system and routes related to VPNs, and *Static IPv4 Routes* table where new routes can be defined and edited with the provided UI controls.

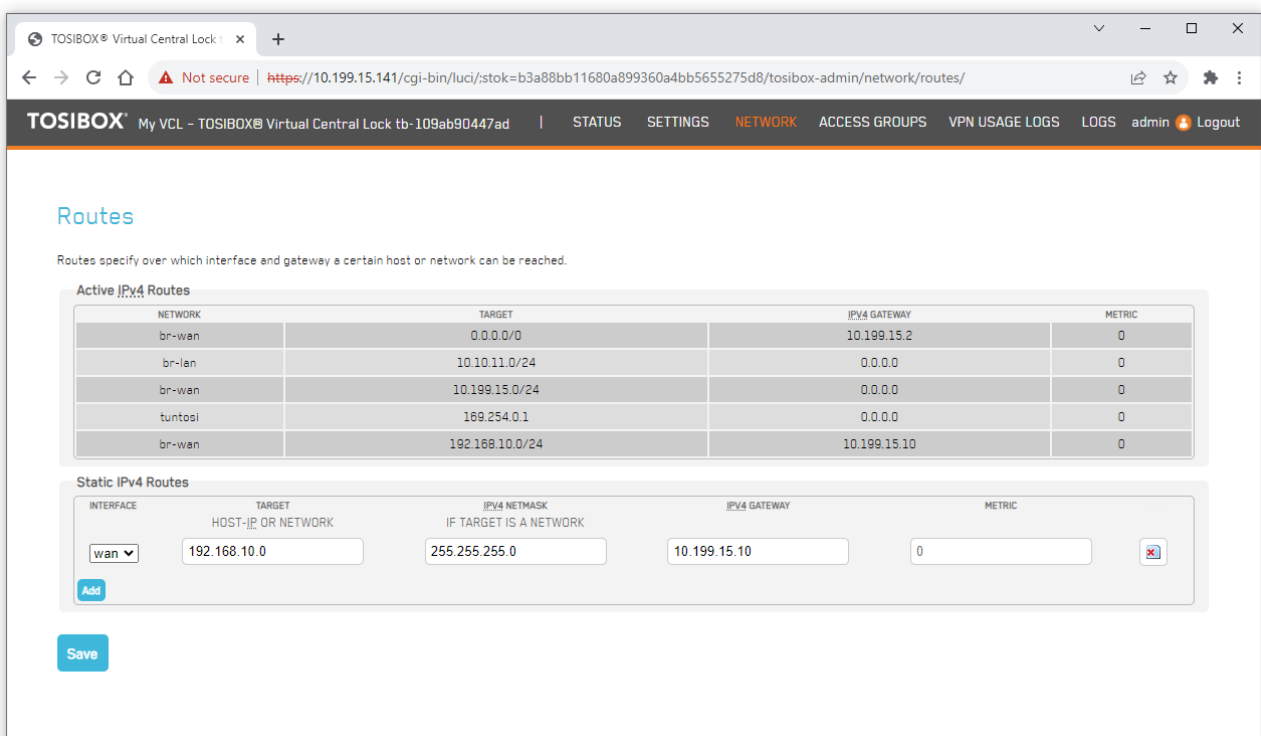


Figure 5: Static routes view

The above example has five default or static routes active, each on its own line.

1. br-wan, this is the default route if any other route does not match the target of the ethernet packet being routed
2. br-lan, the one and only configured LAN network on this instance of the HUB
3. br-wan, WAN network the HUB is connected to
4. tuntosi, Tosibox VPN tunnel open to the HUB (Remote support connection)
5. br-wan, configured static route

Adding a route that conflicts with predefined system routes can have undefined consequences and are not allowed. HUB will notify if a route is added that conflicts with system default routes.

HUB will notify if a gateway for a route is not reachable. If gateway is defined, it must be within the interface subnet/network. A gateway of 0.0.0.0 is also accepted, but that indicates the route is configured to use the default gateway.

Examples of erroneous situations:

- Target network address has more bits defined than netmask, for example Target 192.168.10.1 and IPv4 Netmask 255.255.0.0 violates this rule.
- Duplicate route entry
- Route conflicts with default network interface route

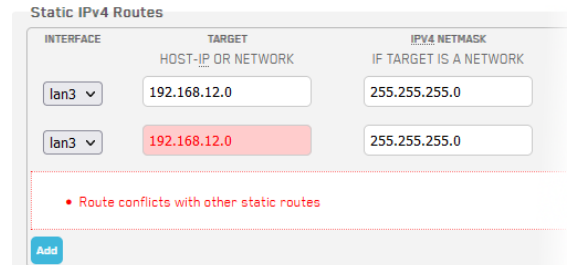


Figure 6: Static routes view with error

## 9 HTTPS login

Starting from HUB 2.6 web UI access can be made via secure https protocol. Https encrypts traffic between the end user device and the web server and thus provides increased security. Default protocol is http. If https is enabled, it is always used when accessing from the HUB LAN or over VPN connection.

Https uses security certificates that identify the server for the web browser. When the web browser receives the security certificate it analyses it and typically shows a lock icon in the address bar that distinguishes the connection being secure.

### Https

To enable https login, check the Enable HTTPS option and define the validity period. The security certificate is valid for the period you define. After the period lapses a new certificate is generated automatically. If https is disabled and enabled again a new certificate is generated always.

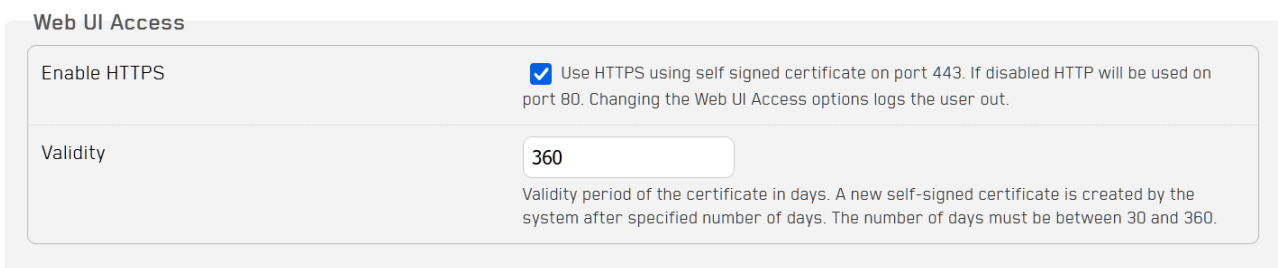


Figure 7: HTTPS settings

### Self-signed certificate

HUB https implementation relies on self-signed certificates.

The security certificate is generated and signed by the HUB itself. Since the web browser cannot know whether a certificate signed by the server itself can be relied on it typically shows a warning “Your connection is not private”.

To access the web UI, you must tell your browser the server is reliable and that the certificate can be trusted. You do this by clicking “Proceed to <address>” or similar button shown on the web browser.

# 10 Access rights management

In Tosibox ecosystem there are two principal methods for managing access rights: using the TOSIBOX® Key or with TOSIBOX® HUB.

The basic, always available, and best suited model for small networks is where the Key users have direct VPN connections from their workstations to Nodes and Locks at remote locations. Access rights are managed with the TOSIBOX® Key application.

When the network grows and more Nodes, Locks and users are added, HUB becomes a necessity and the central point of management. In a network with HUB, Key applications’ role for administrator is to add new Nodes and Locks and users to the network but not to manage access rights, this is done with HUB’s Access Groups. Administrator can continue to use the Key application to grant access to Nodes and Locks to other administrators or users.

## 10.1 Managing access rights with TOSIBOX® Key

In the basic model Key users have direct VPN connections to Nodes and Locks at remote locations. Administrator can manage access rights to Nodes and Locks for SubKey users. Access to LAN devices cannot be limited, all LAN devices under a Lock are accessible automatically when a user is given access to the Lock. For administrator Key application is the primary tool to manage user access rights to the Locks.

If there is a need to define access rights to individual network devices behind a Node, it is done on each Node individually.

In the basic model HUB is used for always-on, bidirectional protected connections that enable for instance data collection and real-time direct service connections to the devices installed in the field. HUB can operate for instance as a data collection point, connection status log recorder or a connection supervisor.

## 10.2 Managing access rights with TOSIBOX® HUB

In centralized model Keys have access to the remote locations via the HUB and direct access from the Key application to the Nodes and Locks is disabled.

The centralised model enables an easy to use and versatile deployment of access rights management using the HUB’s Access Groups view. Access Groups define access rights

between group members which can be Keys, Nodes, IP addresses or network ranges, or MAC addresses. Members of an Access group can communicate freely.

Access can be granted to Locks' LAN networks, devices (IP addresses or ranges on Lock's network or on HUB LANs / VLANs) or devices with port and protocol restrictions, allowing protected, customer specific "server / field device / remote user" networks to be created, all of which are separated from each other. Access rights are instantly deployed.

Care must be taken to ensure adequate Internet connection bandwidth as all remote connection traffic flows through the HUB.

### 10.3 Using Access Groups

Access Groups are used to manage access to the devices on the Locks' LAN side. Operators and field engineers use Key application to open connection to the HUB and from there onwards access to the LAN side devices is possible as configured by the Administrator in the HUB's Access Groups. Once a Lock is added to HUB, access to the LAN side devices is managed with the Access Groups, but not to the Lock itself.

Access Group consists of logical sets of users and devices that are combined to provide users access permissions to physical devices. Access Group UI uses concepts of a Lock group, Key group and Access group.

- **Lock group** is a collection of TOSIBOX® Nodes and Locks connected to your network. A single Node or a Lock can form a group.
- **Key group** is a collection of users with TOSIBOX® Key or TOSIBOX® SoftKey who have access to manage the network. A single user can form a group.
- **Access group** is a combination of a Lock group and a Key group (or groups) where the users belonging to the Key group shall have access to the devices belonging to Lock groups. Individual users or devices which do not belong to any group can be added to Access group as well.

### 10.4 Access Groups UI

The Access Groups web user interface screen is divided into two panes.

- A. Keys and Locks – Left part of the screen is shared between Keys or Locks. You can select the wanted content with the LOCKS and KEYS buttons.
- B. Access groups – Created Access groups are listed on the right.

A group is differentiated from a single object with a greater-than sign (>). Clicking the symbol expands the group and displays the content.

- You can search and filter for specific objects using the search text field
- You can add new Lock, Key or Access group with the + symbol
- Quick filtering is available through the Filter button

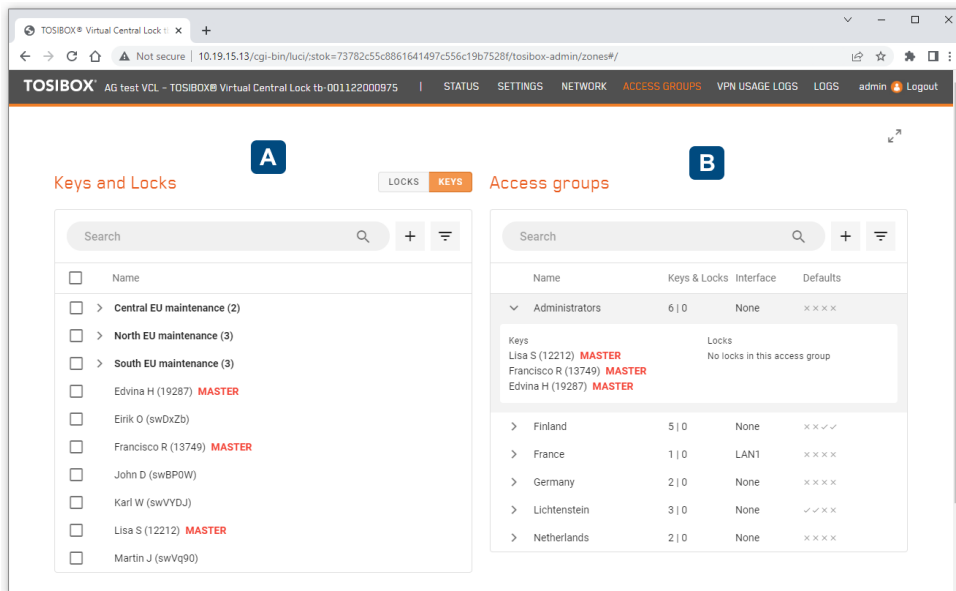


Figure 8: Access Groups user interface overview

In the above screen shot on the left in Keys and Locks pane there are three Key groups and individual Key users listed below. Master Key holders are shown with a red MASTER label.

On the right in Access groups pane there are several Access groups for different physical maintenance locations. Administrators group is expanded to show the admin users and the devices they have access to.

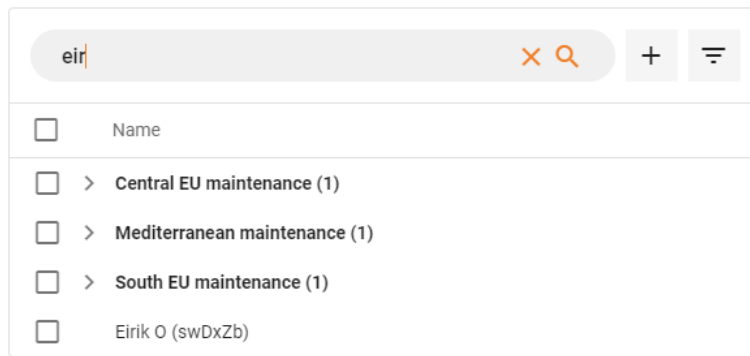
## 10.5 Filtering

There are two methods for filtering: free form text-based filtering and quick filtering. Filtering behaves the same way for Locks and Keys depending on which list you are filtering. You can also combine both the free form text-based filtering and quick filtering.

### Text filtering

Text filtering works by typing in the search condition. Condition can be one character or longer string as needed. Filtering takes effect immediately when you start typing. All respective groups and individual for Locks or Keys are filtered that match the search condition.

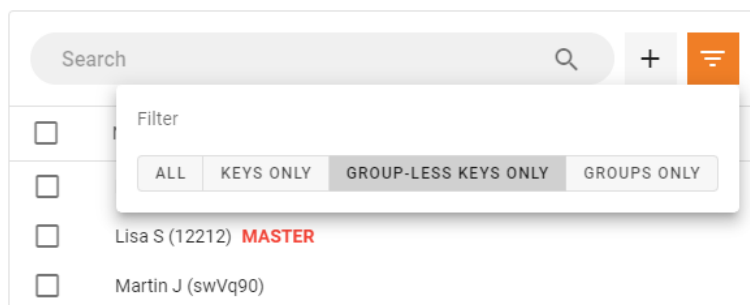
In the below example the search condition “eir” shows three groups where the user Eirik O is a member of as well as the single individual Key. Note how the filter bar symbols are shown in orange to indicate active filtering. To clear filtering click the X symbol.



## Quick filtering

Quick filtering has three modes. These modes are impossible to achieve with the free form text-based filtering.

- **Keys only** – filter shows only individual Keys, all groups are filtered
- **Group-less Keys only** – filter shows those Keys that do not belong to any group yet. This filter is handy when you have large number of Keys and you are struggling to know if all Keys have already been added to groups
- **Groups only** – filter shows only groups, all individual Keys are filtered



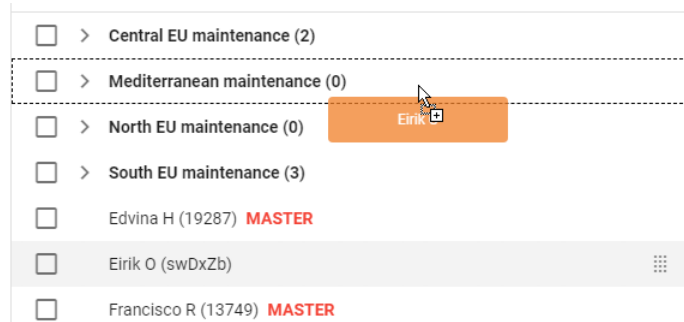
Note also how the quick filter symbol is shown in orange to indicate active filtering. To clear filtering select the ALL option.

## 10.6 Workflow for creating Access Groups

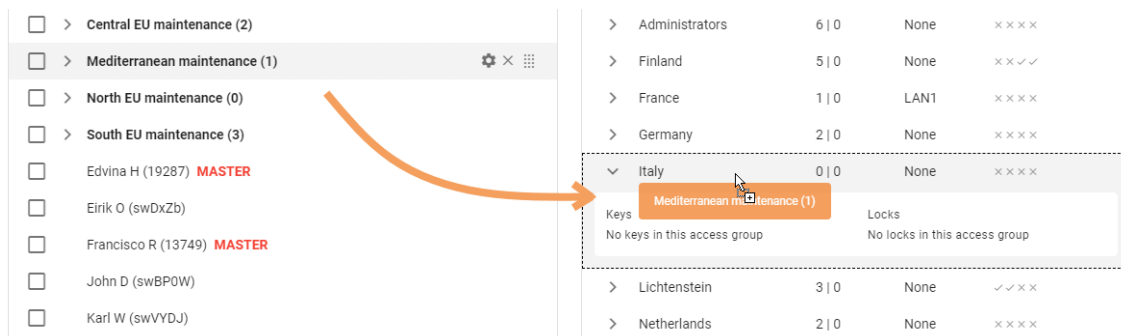
Creating new Access Group consists of three steps; creating a Lock group, creating a Key group and finally creating an Access Group.

- Choose whether you are creating a Lock or a Key group by clicking either the LOCKS or KEYS button.
- Click the + symbol to create a new group. Give the group a name.
- Drag and drop the wanted Layer 3 users to a new Keys group or Layer 3 devices into the new Locks group. You can drag and drop several objects by checking their checkbox and dragging the objects. Note that you cannot add Layer 2 Keys or Nodes to a group. To use Layer 2 Key or a Node in Access Group they must be added as an individual object. Layer 2 Key or a Node can belong to a one single Access Group only.





- Once you have created both the Keys group and the Locks group create a new Access Group by clicking the + symbol.
- Edit access group view will open. You can edit the settings now or modify them later. Click Save to save the changes. The Access group is still blank at this stage.
- Drag and drop the wanted Keys group from the Keys pane and Lock group from the Locks pane into the newly created Access Group. Watch the Access Group build as you drag and drop groups and individual users or remove them.

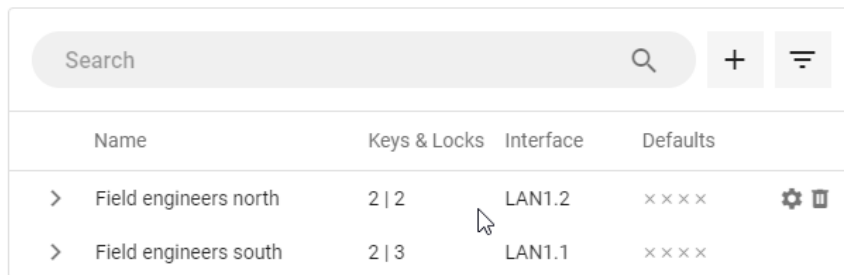


## Notes

- Access Group is saved automatically and takes effect immediately when you add or remove users, devices or groups, there is no need to save the settings.
- Layer 3 Key or Layer 3 Lock does not necessarily have to belong to a group but can belong to one or several groups at the same time.
- Layer 2 Key or Layer 2 Lock cannot belong to a Key or Lock group. They must be managed as individual objects in Access Groups. This is due to Layer 2 object being a part of the bridge connection.
- It is possible to add several groups that contain the same Key or Lock to the same Access group. In this case the permissions do not stack, the impact is the same whether a Key or a Lock is in one or several groups if the Key or Lock is present in the Access Group at least once.

## 10.7 Access Groups settings

Settings for each Access Groups can be viewed and edited with the Edit button found on the right side of the Access group when hovering over the line with the mouse.



Name	Keys & Locks	Interface	Defaults
> Field engineers north	2   2	LAN1.2	x x x x
> Field engineers south	2   3	LAN1.1	x x x x

The Access Groups overview displays

- Name – the user friendly name given to the Access group
- Keys & Locks - the total number of unique Keys and Locks that belong to the Access group
- Interface – The physical interface or the VLAN the Access group is linked to. Every interface can belong to one Access group only.
- Defaults – the Access group where newly added L2 or L3 Keys or Locks are added automatically when matched to the HUB.
- Edit button – opens the edit view to configure Access group settings.
- Delete button – deletes the Access group. Be careful when deleting Access groups, this action cannot be undone.

## 10.8 IP-to-IP mode

IP-to-IP mode can be configured and taken in use on the Access Groups settings view.

IP-to-IP mode provides isolated access between two or more addresses on the LAN networks without allowing access to any other devices on the networks. With the IP-to-IP mode, traffic in Access Group is only allowed between manually specified IP addresses.

### HUB LAN to Node LAN access

IP-to-IP mode allows creating connections on IP level from the LAN side of one or more Nodes to the LAN side of the HUB. Both the Node LAN device IP address and the HUB LAN device IP address must be defined on the IP Addresses list.

### Node LAN to Node LAN access

IP-to-IP mode allows creating connections on IP level from the LAN side of one Node to the LAN side of another Node. With the IP-to-IP mode it is possible to limit the access between the LAN side devices even if there are more devices present on the Node LANs. The IP address of both Node LAN devices must be defined on the IP Addresses list.

## Key access

IP-to-IP mode is designed for machine-to-machine communication, Key access cannot be restricted with the IP-to-IP mode.

Keys can be added to the same Access Group, but their access is not restricted by the IP address table and will have access to all devices in the LANs.

## Example

For example, in the following illustration orange camera on the Node A LAN can be configured to communicate with the orange server on the Node B LAN, but the camera won't have access to any other server or vice versa.

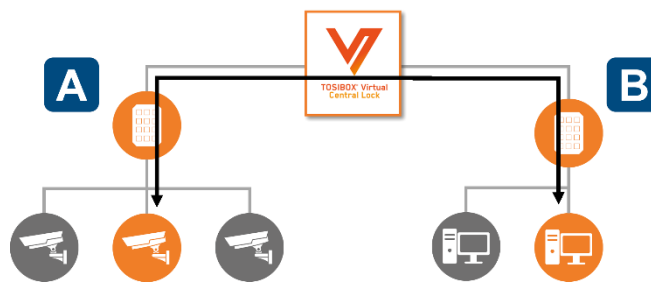


Figure 9: Example network configuration with device from LAN A communicating to device in LAN B

IP level access rules are created with the *IP Addresses* area settings in the *Edit access group* view. Checking the *IP-to-IP mode for traffic between locks* checkbox enables the mode. When IP-to-IP mode is enabled *Allow traffic between Locks* is automatically disabled. These two modes are mutually exclusive.

You can also limit access to certain protocols or services only by defining the port or port range.

### Steps to configure above example

- Add the Node A and Node B in the same Access Group
- Turn the IP-to-IP mode on
- Enter the IP addresses of the camera and the server that need to communicate together
- Optionally, add the user Key to the Access Group

The same restrictions can be extended to multiple IP addresses within the same Access Group if needed. All defined addresses will have access to each other.



*IP-to-IP mode is a new feature introduced in HUB 2.6.1.*

## 10.9 Scheduled access

Scheduled access allows you to limit the Sub Key access and devices connected to HUB. Schedules are added for an access group.

Scheduled access gives you better control over who can access resources inside the network. If a Sub Key connects a HUB outside the schedule, the access to resources is disabled and a notification is shown on the Key user interface, describing the reason for the missing connectivity. This feature does not limit other connections than Sub Key devices.

## 10.10 Activating scheduled access

Scheduled access is activated on the Access Group Settings page by editing existing access group or creating a new. You can add new schedules for the Sub Keys by configuring the rules related to the schedule. One access group can have multiple schedules defined.

Admin can see all current schedules on the access group configuration page and modify or remove them. Rules inside a schedule can be enabled or disabled with a single click. If disabled, the rule is not controlling the access. If all the rules inside a schedule are disabled, the whole schedule is automatically disabled.

All times will be defined in HUB time zone, defined in [Settings > Advanced settings](#). Modifications to the schedules or rules will take effect immediately upon saving the settings. However, active connections will not be dropped upon saving the settings.

# 11 Logging and alerts

There are in total three distinct variations of logging in HUB.

- VPN usage logging for Keys
- Email alerts
- Admin trail

## 11.1 VPN usage logging for Keys

VPN usage logging is available at the main level in the main menu at *VPN usage logs*.

KEY	VPN OPEN TIME	VPN CLOSE TIME	TOTAL RX	TOTAL TX
Key 41823	2022-09-02T12:08:23-00:00	2022-09-02T12:09:17-00:00	2.87KB	11.96KB
Key 41823	2022-09-02T12:09:32-00:00	2022-09-02T12:09:48-00:00	0B	0B
Key 41823	2022-09-02T12:21:58-00:00	2022-09-02T12:35:30-00:00	5.95KB	8.35KB

LAST ACTIVITY	FIRST ACTIVITY	TARGET HOST	TARGET IP	TARGET NETWORK	RX	TX
9/2/2022, 3:25:01 PM	9/2/2022, 3:25:01 PM	10.63.239.117	10.63.239.117	109ae902391a	2.34KB	1.52KB
9/2/2022, 3:25:01 PM	9/2/2022, 3:25:01 PM	not found	No Data	109ae90410c7	2.34KB	1.52KB
9/2/2022, 3:25:01 PM	9/2/2022, 3:25:01 PM	Secomea SiteManager-1139	10.10.10.14	109ae90410c7	1.27KB	5.3KB

VPN usage logging collects usage statistics for transmitted VPN data. Collected data includes used Key, the VPN end-point IP address or accessed Lock, time the tunnel is open in accuracy of seconds and the amount of data transferred. Data can be used e.g. for billing purposes.

VPN usage logging can be enabled for each Key independently from *Settings > Keys and Locks*. Logging is disabled by default.

Once logging is activated, Keys and Locks view can be used to select the Keys to be traced. Activating VPN usage logging has performance impact if large number of Keys is being traced.

The summary view shows the information about connecting Key, the start and end times for the connection, and amount of data transferred (RX and TX). The data amount calculations assume KB is equal to 1024 bytes.

## 11.2 Email alerts

Email alerts are disabled by default. Alerts can be taken in use in [Settings > Alerts](#). Alerts require configuring email server using SMTP (Simple Mail Transfer Protocol server).

Email alerts can be enabled for each Node independently.

### Email alerts

Title	Message content	Example
[TOSIBOX] Alert: <node> connected	Lock <ID> (<node>) connected to HUB <ID> at <date> <time>	Lock tb-109ab9026b99 (Lock150) connected to HUB tb-001122000975 at 2022-09-14 19:55:27+0300.
[TOSIBOX] Alert: <node> disconnected	Lock <ID> (<node>) disconnected from HUB <ID> at <date> <time>	Lock tb-109ab9026b99 (Lock150) disconnected from HUB tb-001122000975 at 2022-09-17 04:24:06+0300.

## 11.3 Admin trail

Audit logging stores various admin actions such as system state and configuration changes. Admin actions can be traced as audit log events on the Logs view. Audit logging is enabled by default but can be switched off by demand.

Admin trail can be filtered based on the event type. Filtered log events can be exported to a CSV file.

Audit logging is enabled and disabled from [Settings > Advanced settings](#).

## 11.4 Admin trail events

### Access control category

ID	Text	Notes
105	Password was changed for user <user>	User has changed his/her password
150	Added user <user>	New Web UI user has been created
151	Deleted user <user>	Web UI user has been removed from the system
152	Password reset for user <user>	User has clicked Reset password button on the User management view
153	Session timeout for user <user>	User has successfully logged out of the system. Shown also during session timeout.
154	Failed login attempt, wrong credentials for user <user>	User has entered erroneous credentials
-	Web UI logout: <user>	User has successfully logged out of the system
-	Web UI login: <user>	User has successfully logged in to the system
-	VPN opened from <a> to <b>	Raised either when:

		<ul style="list-style-type: none"> <li>• User opens connection from the Key &lt;a&gt; to Node &lt;b&gt;. The originating source is the Node.</li> <li>• Node &lt;a&gt; connects to the HUB &lt;b&gt;. The originating source is the HUB.</li> <li>• Node &lt;a&gt; connects to the HUB &lt;b&gt;. The originating source is the Node.</li> </ul> <p>Note that the HUB raises the VPN opened event when a Node comes online.</p>
-	VPN closed from <a> to <b>	<p>Raised either when:</p> <ul style="list-style-type: none"> <li>• User closes connection from the Key &lt;a&gt; to Node &lt;b&gt;. The originating source is the Node.</li> <li>• Node &lt;a&gt; connection is closed or cut between the Node and the HUB &lt;b&gt;. The originating source is the HUB.</li> <li>• Node &lt;a&gt; connection is closed or cut between the Node and the HUB &lt;b&gt;. The originating source is the Node.</li> </ul> <p>Note that the HUB raises the VPN closed event when a Node goes offline.</p>
160	Key user added	New Key application or Mobile Client user is granted access
161	Key user removed	Key application or Mobile Client user is removed

## Control system event category

ID	Text	Notes
106	System reboot	
3010	System started	VCL has started. Created during system initialization, typically is the first event when system is powered
3011	System shutdown started	System shut down is requested. Created when user pushes the reboot button or a command from the CLI is received to shut down the system. Logged when the first signal of a shutdown is received, Shutdown can still be potentially canceled after this. Is not logged in AWS instances.
3012	System shutdown succeeded	The system is now shut down. Created when system is requested to reboot or shutdown. Typically, is the last event when system is powered off
3013	System shutdown canceled	System shutdown signal was sent but some component denied shutdown
3016	Node added, <type> (Lock / Sub Lock <ID>)	Layer 3 Tosibox Node (Lock) or Layer 2 Tosibox Node (Sub Lock) is matched to this HUB. <type> is the Lock model. <ID> is the MAC address of the Node.
3017	Node removed, <type> (Lock / Sub Lock <ID>)	Layer 3 Tosibox Node (Lock) or Layer 2 Tosibox Node (Sub Lock) is removed from this HUB. <type> is the Lock model. <ID> is the MAC address of the Node.

3023	Connection license cap near or exceeded limit, Limit: <n> Devices: <m>	Logged when a new device is added to HUB, but the license cap is nearly or fully utilized. <n> is the cap limit, <m> is the currently used license amount
3027	License change: VPN usage logs enabled / disabled	Support for VPN Usage Logs is enabled or disabled.
3028	License change: Scheduled access enabled / disabled	Support for scheduled access in Access Groups is enabled or disabled.
3029	License change: Multi-user mode enabled / disabled	Support for several Web UI users is enabled or disabled.
3030	License change: Audit logging enabled / disabled	Support for audit logs is enabled or disabled.
3031	License connection cap changed from <a> to <b>	VPN connection license cap has been changed. <a> is the starting limit, <b> is the new limit

## Configuration change category

ID	Text	Notes
100	Keys and Locks page saved	Logged when save button is pressed on the page
102	Remote matching code created	Logged when save button is pressed on the page
103	Lock name saved	System name is changed
104	Serializations reset	Logged when reset serializations button is pressed on the page
107	Alerts page saved	Logged when save button is pressed on the page
108	Advanced settings page saved	Logged when save button is pressed on the page
120	Interface <name> added	New WAN or LAN interface created
121	Interface <name> edited	Interface edited
122	Interface <name> deleted	WAN or LAN interface deleted
125	VLAN <name> added	VLAN interface created
126	VLAN <name> deleted	VLAN interface deleted
130	Static routes saved	Logged when save button is pressed on the page
135	DHCP Server page saved	Logged when save button is pressed on the page
140	Access group <name> added	New Access Group is created with the given name
141	Access group <name> renamed to <newname> and saved	Access Group changes saved
141	Access group <name> saved	Access Group changes saved
142	Access group <name> deleted	Access Group deleted
190	EULA accepted	Logged when accept button is pressed on the page
192	New master key <name> added	New master key generated and added



5043	Created new self-signed certificate for web UI with a validity period of <x>	Logged with https using self-signed cert for web UI whenever certificate is rotated
5044	Web UI protocol changed from <a> to <b>	Logged when protocol changed from http to https or vice versa. <a> and <b> is either http or https.
5024	user <name>: Remote support enabled	Secure remote support tunnel for Tosibox technical support is enabled on the Advanced Settings page
5025	user <name>: Remote support disabled	Secure remote support tunnel for Tosibox technical support is disabled on the Advanced Settings page
5026	user <name>: VPN cipher changed from <a> to <b>	VPN cipher on the Advanced settings page changed. <name> is the username, <a> is the original cipher previously in use e.g. AES-128-CBC, <b> is the new cipher taken in use e.g. AES-256-CBC
5021	Software update started from <a> to <b>	New software update installation was just launched and is ongoing. <a> is the starting level, <b> is the new installation level.
5022	Software update succeeded from <a> to <b>	Software update completed and installation succeeded. <a> is the starting level, <b> is the new installation level.
5023	Software update failed (<reason>)	Software update completed but installation failed. <reason> is the failure reason, printed if known.
5053	Software update available from <a> to <b>	Notification that a new minor software update is available. <a> is the starting level, <b> is the new installation level.
5054	System upgrade started from <a> to <b>	A new software upgrade installation was just launched and is ongoing. <a> is the starting level, <b> is the new installation level
5055	System upgrade succeeded from <a> to <b>	Software upgrade completed and installation succeeded. <a> is the starting level, <b> is the new installation level.
5056	System upgrade failed (<reason>)	Software upgrade completed but installation failed. <reason> is the failure reason, printed if known.
5057	System upgrade available from <a> to <b>	Notification that a new major software upgrade is available. <a> is the starting level, <b> is the new installation level.

## Audit log category

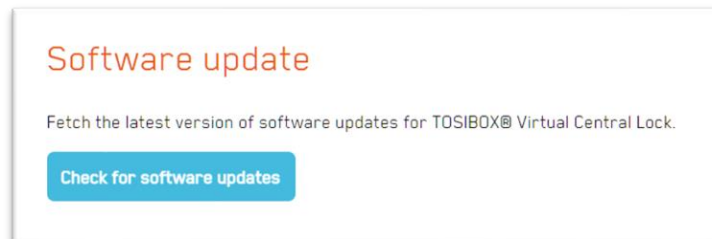
ID	Text	Notes
191	CSV log export	User has exported audit log

# 12 Software update

There are two types of updates

- **System upgrade** – System upgrade is a major release containing foundational changes to the platform and applications
- **Software update** – Software update is a minor release containing updates to selected parts of the system

Software updates can be checked and installed from *Settings > Software update*. Opening the Software update view displays the option to check for possible available updates.



By clicking the *Check for software updates* button HUB connects to the update service and verifies if update is available and displays information accordingly. SW updates are also checked automatically once a day. If a new update is found a notification is shown on the UI along with an audit event. Update can be installed from the SW Update page as wanted.

When the upgrade is complete you get “System upgrade finished successfully” message.



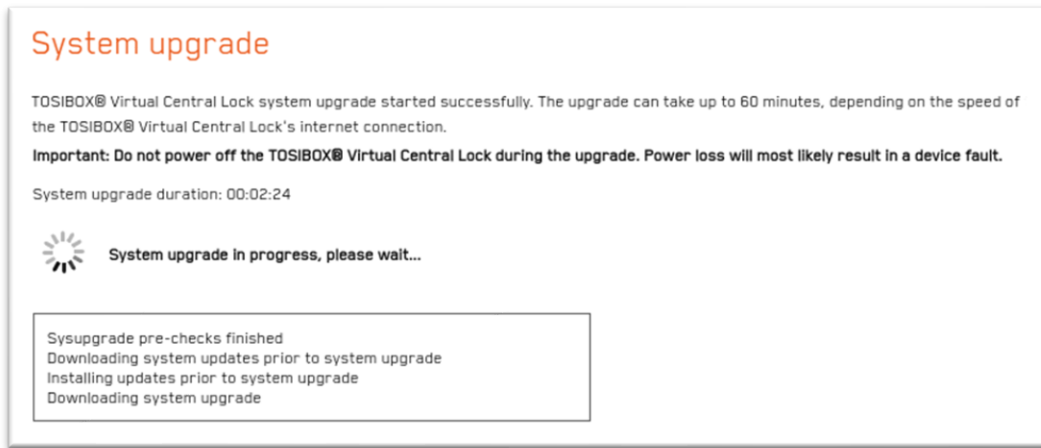
*HUB 3.0 system upgrade requires two updates. A System update is offered first that prepares HUB for kernel update. In the second phase a System upgrade is offered that brings the system to version 3.0.*

---

Depending on the availability of the software upgrades and updates UI can show the option to start either of the processes. If both options are available system upgrade installs required system updates if update is not run first. System upgrade is a safe option even if a system update is offered.

Software update process is enhanced with checking for Azure and AWS specific extensions. HUB can warn about extensions coming from unknown sources. It is up to the user to determine the risk level of offered extensions.

System upgrade can be a lengthy process and require restarting the HUB. It is recommended to perform system upgrades only during planned maintenance breaks.



Software update typically takes less time and does not necessarily require reboot. VPN connections can go down temporarily during software update installation.

When the upgrade is complete you get “System upgrade finished successfully” message. If a reboot is required after the SW update, HUB will notify about this.



---

*Updates from previous versions can require increased disk partition size. Requirements for the current version are listed in chapter System requirements. If your system has less resources available updates will not start, and you get a message on screen accordingly. Contact Tosibox support if help is needed.*

---

Virtual machine snapshot is highly recommended before any type of update.

## 13 Legal notices

© 2024 Tosibox Oy. All rights reserved. Tosibox logo is registered trademark of Tosibox Oy.

Reproduction, distribution or storage of part or all of the content of this document without the prior written permission of Tosibox is prohibited.

Because of continuous product development, Tosibox Oy reserves the right to change and improve any product mentioned herein without prior notice.

Tosibox shall not take responsibility of any loss of information or income or any special, incidental, consequential or indirect damages.

The contents of this document are provided "as is". No warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, are made in relation to the accuracy, reliability or contents of this document. Tosibox reserves the right to revise this document or withdraw it at any time without prior notice.

Tosibox products contain software that is based on open-source software. When requested by the customer, Tosibox will deliver more detailed information from the parts that the

licenses require. The source code requests shall be submitted to: [sourcecode.request@tosibox.com](mailto:sourcecode.request@tosibox.com) or by mail: Tosibox Oy, Elektriikkatie 2A, 90590 OULU, FINLAND