



Tosibox HUB 4.0

User Manual

Contents

1	Introduction	4
2	System description	5
2.1	Context of use.....	5
2.2	HUB in brief	5
2.3	Licensing.....	6
2.4	System components.....	6
2.5	Main features	7
3	System Requirements	8
3.1	Requirements for cloud and on-premises virtualisation platforms.....	8
3.2	Microsoft Azure	8
3.3	Amazon Web Service.....	8
4	Connectivity.....	9
4.1	Tosibox Cloud architecture.....	9
4.2	TCP and UDP connections	9
4.3	Installing behind a firewall	9
5	Installation.....	10
5.1	Installing the VM image.....	10
5.2	VMWare vSphere/ESXi.....	10
5.3	Microsoft Hyper-V	10
5.4	Linux KVM	11
5.5	Cloud installation.....	11
6	Initial setup.....	11
6.1	Accessing the configuration interface.....	11
6.2	WAN interface configuration and product activation	11
6.3	Change password	11
6.4	Configuring LAN interfaces	11
6.5	Create Remote Matching code.....	12
6.6	Remote Matching.....	12
6.7	Connecting Nodes and Locks	13
6.8	Software update.....	13
7	User interface.....	13
7.1	Navigating in the user interface.....	14
7.2	Login.....	15
7.3	Adding admin users	16
7.4	Adding virtual LANs.....	16

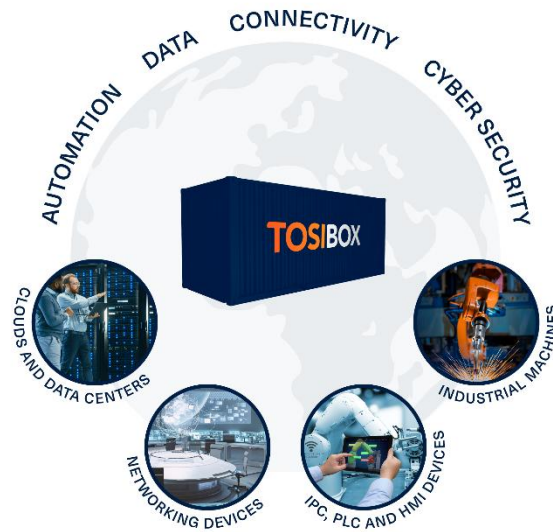
8	Access rights management	16
8.1	Managing access rights with Key	17
8.2	Managing access rights with HUB.....	17
9	Logging and alerts.....	17
9.1	VPN usage logging for Keys	17
9.2	Email alerts	18
9.3	Admin trail.....	19
9.4	Remote logging.....	19
10	Software update.....	19
11	Legal notices.....	20

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 4.0.

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 centralized 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 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 1.2 and 1.3, ChaCha20 / AES-256-CBC / AES-192-CBC / AES-128-CBC / Blowfish-128-CBC

2.3 Licensing

HUB 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 total 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.

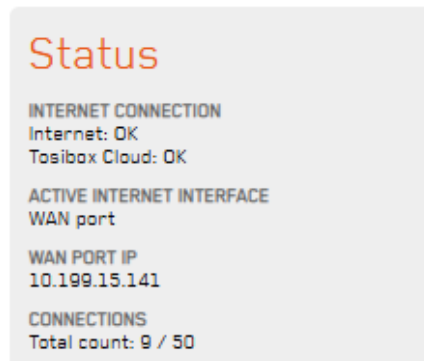


Figure 1: In total of nine connected devices to this HUB and a license cap of 50.

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

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 integration

The HUB serves as a central component in network management with TosiControl. Access controls configured through Access Groups can be monitored via TosiControl. The HUB transmits network element listings and their status information for centralized device management.

Unrestricted Service and Protocol Support

The HUB enables authentic Layer 2 communication, eliminating the need for specific ethernet protocol drivers. Deploy any protocol, ethernet-capable edge device, data analytics software, or cloud hosting environment. Our automated networks allow you to build your desired system without legacy technology constraints.

Built-in automated cybersecurity

Our automated networking eliminates human error in cybersecurity configuration. Every HUB includes:

- Automated Linux iptables-based firewall at the edge, rendering HUB LAN-connected devices invisible to the internet
- Point-to-point networks through 256-bit AES encrypted VPN tunnels without third-party cloud involvement, ensuring full data encryption during transit

Central user access management

The HUB offers centralized user management through Access Groups. This feature enables administrators to define access rights between connected devices and users. Configuration is managed through the Access Groups menu.

Audit log data collection and forwarding

The HUB collects log data from events occurring on both the HUB itself and any connected Nodes and Sub Locks. Log collection and monitoring can be enabled through the menu interfaces of both the HUB and individual Nodes. HUB can be configured to forward log data to a remote logging server.

Connection monitoring and alerts

The HUB can send email alerts for established and closed connections. Alerts can be configured selectively for any Node and implemented without additional services. Alert configuration is available through the menu.

Virtual LANs (VLANs)

The HUB supports VLAN configuration through any physical LAN port, accessible via the menu interface.

Prometheus Resource Monitoring

The HUB features integration with Prometheus monitoring system, enabling comprehensive resource tracking and performance analysis. Monitor CPU usage, memory consumption, and system health metrics in real-time. The built-in Prometheus support provides standardized metrics that can be easily integrated with existing monitoring dashboards and alerting systems.

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 2022
- Linux KVM
- Microsoft Azure cloud platform (new installations are done on Azure Marketplace)
- Amazon AWS cloud platform (update from previous version, new installations on HUB 4.x branch are now 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
- 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/>
- [How to install HUB from Azure Marketplace](#)

3.3 Amazon Web Service

HUB 4.X image can be found in AWS AMI (Amazon Machine Images) catalog. The above system requirements apply also to AWS.

Installation instructions:

- [How to install VCL / HUB on Amazon AWS Cloud via WEB-GUI](#)

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/>.

See also the helpdesk article: [How to Install HUB](#)

5.2 VMWare vSphere/ESXi

- Download the latest image named ...esx.ova
- 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, select Generation 2
- Download the latest .vhdx image and "use an existing virtual hard disk" and select the downloaded .vhdx file as disk image.
- 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

- Disable secure boot

5.4 Linux KVM

In most cases, one of the distributed images can be imported to the virtualization 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. 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.



At minimum HUB must have one LAN interface configured when using Mobile Clients. The interface does not have to be connected to a physical interface but must exist.

NOTE. In Cloud environment, one cannot access the UI, and remote matching needs to be made via console. See the helpdesk document https://tosibox.service-now.com/customer_portal?id=kb_article_view&sysparm_article=KB0010061

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 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**.

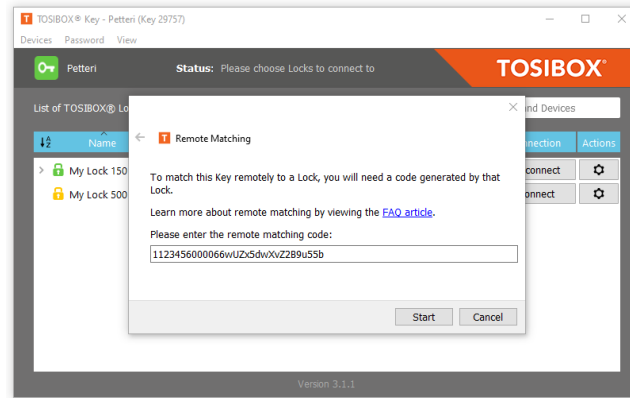


Figure 3: Remote Matching on Tosibox Key client application

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:

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

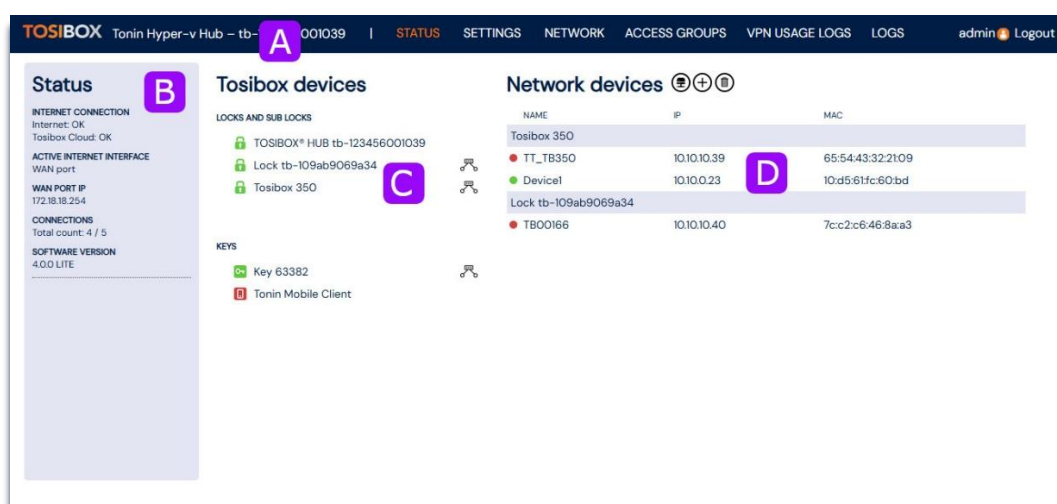


Figure 4: HUB user interface overview

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, changing the name for the HUB, changing the password of the admin account, restart the HUB, update the software, set email alerts, configure the Prometheus monitoring, remote logging 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
- VPN details – Displays details on active VPN connections

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 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.

8.1 Managing access rights with 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.

8.2 Managing access rights with 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.

9 Logging and alerts

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

- VPN usage logging for Keys
- Email alerts
- Admin trail with or without Remote logging

9.1 VPN usage logging for Keys

VPN usage logging is available at the main level in the main menu at [VPN USAGE LOGS](#).

<div> <div>TOSIBOX</div> <div>Tonin Hyper-v Hub – tb-123456001039</div> </div> <div> <div>STATUS</div> <div>SETTINGS</div> <div>NETWORK</div> <div>ACCESS GROUPS</div> <div>VPN USAGE LOGS</div> <div>LOGS</div> </div> <div> <div>admin</div> <div>Logout</div> </div>						
VPN Usage Logs						
Export						
KEY	VPN OPEN TIME ↓	VPN CLOSE TIME	TOTAL RX (BYTES)	TOTAL TX (BYTES)		
token-63382	2025-03-24 12:55:58+02:00	2025-03-24 15:27:50+02:00	720	720		
	LAST ACTIVITY	FIRST ACTIVITY	TARGET HOST	TARGET IP	TARGET NETWORK	RX (BYTES) TX (BYTES)
	2025-03-24 13:05:01+02:00	2025-03-24 13:05:01+02:00	Device1	10.10.0.23	109ab9069d5b	720 720
token-63382	2025-03-24 12:06:24+02:00	2025-03-24 12:51:00+02:00		0	0	▼
token-63382	2025-03-24 12:06:09+02:00	2025-03-24 12:06:18+02:00		0	0	▼
token-63382	2025-03-24 12:00:54+02:00	2025-03-24 12:06:02+02:00		0	0	▼
token-63382	2025-03-21 13:55:47+02:00	2025-03-21 15:12:59+02:00		0	0	▼
token-63382	2025-03-21 13:35:02+02:00	2025-03-21 13:41:21+02:00		0	0	▼
token-63382	2025-03-18 09:47:24+02:00	2025-03-18 21:59:47+02:00		0	0	▼

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.

9.2 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.

9.3 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.

Supported Admin trail events are listed in an article on Tosibox Knowledgebase.

Admin trail events can also be forwarded to a remote logging server.

9.4 Remote logging

Remote logging enables the transmission of audit events to an external server for centralized storage and analysis. This capability improves real-time monitoring, troubleshooting, and security maintenance throughout your network infrastructure.

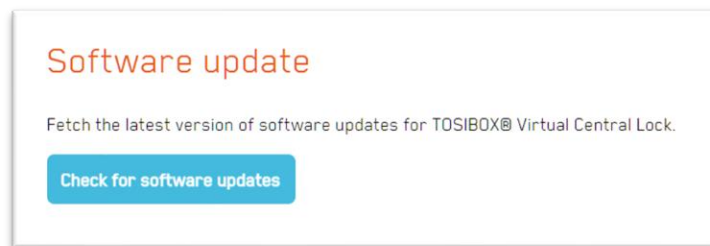
The main advantage of remote logging is its ability to centralize security auditing and enhance incident response by retaining long-term audit logs. Through remote logging, you can guarantee that crucial system events and audit trails are stored securely off-device, creating a dependable record for forensic analysis, security inquiries, and compliance reporting.

10 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.

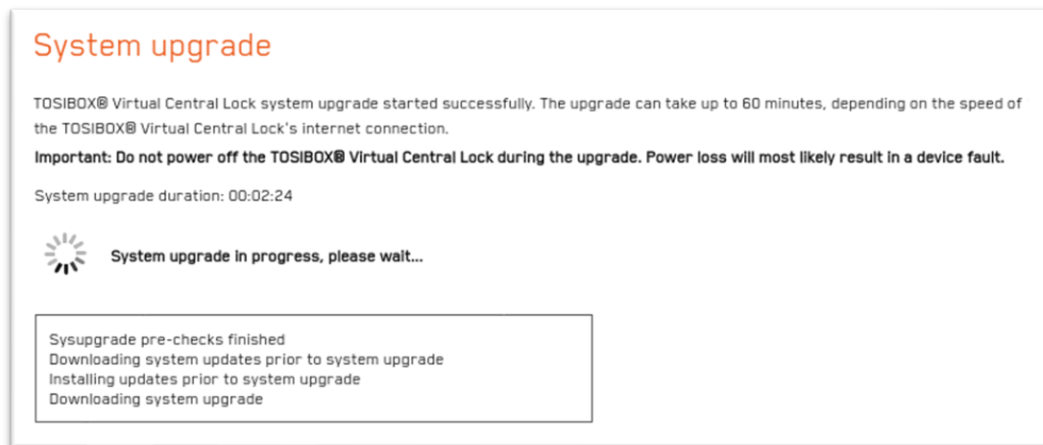


HUB 3.0 system upgrade requires two updates. A System update is offered first that prepares HUB for kernel update. In the second phase a System upgrade is offered that brings the system to version 3.0.

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.

11 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 or by mail: Tosibox Oy, Elekroniikkatie 2A, 90590 Oulu, Finland.