



# TOSIBOX® Virtual Central Lock User Manual

# Content

1	Introduction .....	4
2	System description .....	5
2.1	Context of use.....	5
2.2	TOSIBOX® Virtual Central Lock 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 virtualisation platforms.....	8
3.2	Requirements for cloud platforms .....	8
4	Installation .....	9
4.1	Installing the VM image .....	9
4.2	VMWare vSphere/ESXi .....	9
4.3	Microsoft Hyper-V .....	9
4.4	Linux KVM .....	10
4.5	Cloud installation .....	10
5	Initial setup .....	10
5.1	Accessing the configuration interface .....	10
5.2	WAN interface configuration and product activation .....	10
5.3	Change password.....	11
5.4	Configuring LAN interfaces.....	11
5.5	Create Remote Matching code .....	11
5.6	Remote Matching.....	12
5.7	Connecting Nodes and Locks .....	12
5.8	Software update.....	13
6	User interface .....	13
6.1	Navigating in the user interface .....	14
6.2	Login.....	15
6.3	Adding admin users .....	16
6.4	Adding virtual LANs .....	16

7	HTTPS login.....	16
8	Access rights management.....	17
8.1	Managing access rights with TOSIBOX® Key.....	17
8.2	Managing access rights with TOSIBOX® Virtual Central Lock.....	18
8.3	Using Access Groups.....	18
8.4	Access Groups UI.....	19
8.5	Filtering.....	19
8.6	Workflow for creating Access Groups.....	21
8.7	Scheduled access.....	22
8.8	Activating scheduled access.....	22
9	Logging and alerts.....	22
9.1	VPN usage logging for Keys.....	23
9.2	Email alerts.....	23
9.3	Admin trail.....	24
9.4	Admin trail events.....	24
10	Software update.....	26
11	Legal notices.....	27

# 1 Introduction

Congratulations for 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® Virtual Central Lock 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 Virtual Central Lock version 2.6.

# 2 System description

## 2.1 Context of use

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

Virtual Central Lock 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. Virtual Central Lock allows connecting over a thousand serialized Nodes and Keys simultaneously.

Virtual Central Lock is a licensed software product that runs on 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 Virtual Central Lock is running on.

## 2.2 TOSIBOX® Virtual Central Lock in brief

Virtual Central Lock is 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.

Virtual Central Lock 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.

Virtual Central Lock 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.

### Virtual Central Lock 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 features

- 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 full version of the Virtual Central Lock you get technical support and as many concurrent connections as is defined by your license type.

The maximum number of concurrent connections is limited with the license. Active connections and the license cap are shown in the Status pane on the Virtual Central Lock front page.

### LITE version

Virtual Central Lock 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 Virtual Central Lock 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 Virtual Central Lock's LAN port or VLAN that it is bridged to. The routed layer 3 connection creates a connection where the Node and the Virtual Central Lock 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 Virtual Central Lock is Layer 3. Additional Keys can be matched to the Virtual Central Lock 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 Virtual Central Lock 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

### Manage any service, run any protocol

Virtual Central Lock 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 Virtual Central Lock includes:

- Automated Linux iptables based firewall at the edge. Everything connected to the Virtual Central Lock 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

Virtual Central Lock provides centralized user management via novel view called Access Groups. Access groups allows 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

Virtual Central Lock collects log data on the events of the Virtual Central Lock and the events of any connected Nodes and Sub Locks. Log collection and monitoring can be enabled from the menu of both the Virtual Central Lock 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

Virtual Central Lock 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)

Virtual Central Lock can be configured to connect to existing VLANs via any of the physical LAN ports. Configuration is available the menu.

# 3 System Requirements

## 3.1 Requirements for virtualisation platforms

Virtualisation platform based on one of the following:

- VMWare vSphere/ESXi v7.0 GA
- Microsoft Hyper-V on Windows Server 2016 and 2019
- Linux KVM
- Microsoft Azure Cloud
- Amazon AWS Cloud

Minimum HW and computing requirements common for all 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 Virtual Central Lock, you will also need:

- Internet connectivity to download the Virtual Central Lock VM image and possible software updates
- License key to activate Virtual Central Lock

## 3.2 Requirements for cloud platforms

- Linux / MacOS workstation to run the installer (on Windows these steps can be done manually, or with Linux subsystem)
- Azure or AWS subscription
- Command line tool “az” for Azure or “aws” for AWS installed if installing via command line
- Installation image for the cloud platform



# 4 Installation

## 4.1 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.

Virtual Central Lock images are distributed at <https://downloads.tosibox.com/VCL/>.

## 4.2 VMWare vSphere/ESXi

- Download the latest *TOSIBOX\_Virtual\_Central\_Lock\_latest\_esx.ova* appliance
- Use the Deploy OVF Template function of the vSphere client to import the downloaded .ova file. Alternatively, it is possible to download the *TOSIBOX\_Virtual\_Central\_Lock\_latest.vmdk* virtual disk file and create the virtual machine out of it
- 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

## 4.3 Microsoft Hyper-V

- Download the latest *TOSIBOX\_Virtual\_Central\_Lock\_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
- Disable hardware Secure Boot

## 4.4 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.

## 4.5 Cloud installation

How to install TOSIBOX® Virtual Central Lock on cloud via CLI (command line interface). Links to Tosibox Helpdesk articles.

- [How to install VCL on Microsoft Azure Cloud via CLI](#)
- [How to install VCL on Amazon AWS Cloud via CLI](#)

How to install TOSIBOX® Virtual Central Lock on cloud via web UI interface. Links to Tosibox Helpdesk articles.

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

# 5 Initial setup

## 5.1 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.

## 5.2 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 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 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 reboot, you can proceed with the configuration.

### 5.3 Change password

After the virtual machine has booted up again, the graphical console provides now access to the Virtual Central Lock 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.

### 5.4 Configuring LAN interfaces

The Virtual Central Lock can have multiple LAN and VLAN interfaces that can provide access to your own local networks and services. The initial configuration of Virtual Central Lock 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 Virtual Central Lock, 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).

### 5.5 Create Remote Matching code

After the Virtual Central Lock is activated and has Internet connection, the Master Key needs to be matched to the Virtual Central Lock 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 1: 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 Virtual Central Lock to the network.

## 5.6 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*.

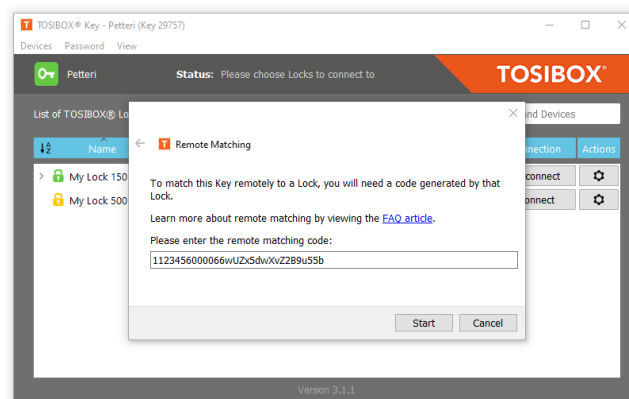


Figure 2: Remote Matching on TOSIBOX® Key client application

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, Virtual Central Lock has been added to your network. You can see it on the Key application interface immediately.

## 5.7 Connecting Nodes and Locks

Now that you have Virtual Central Lock 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 Virtual Central Lock in the selection. Click Next.
3. For Select Connection Type choose either Layer 2 or Layer 3, click Next.

- Confirmation dialog is displayed, click Save and the VPN tunnel is created between each selected node and the Virtual Central Lock separately and the devices start to appear on the Virtual Central Locks 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 Virtual Central Lock.

## 5.8 Software update

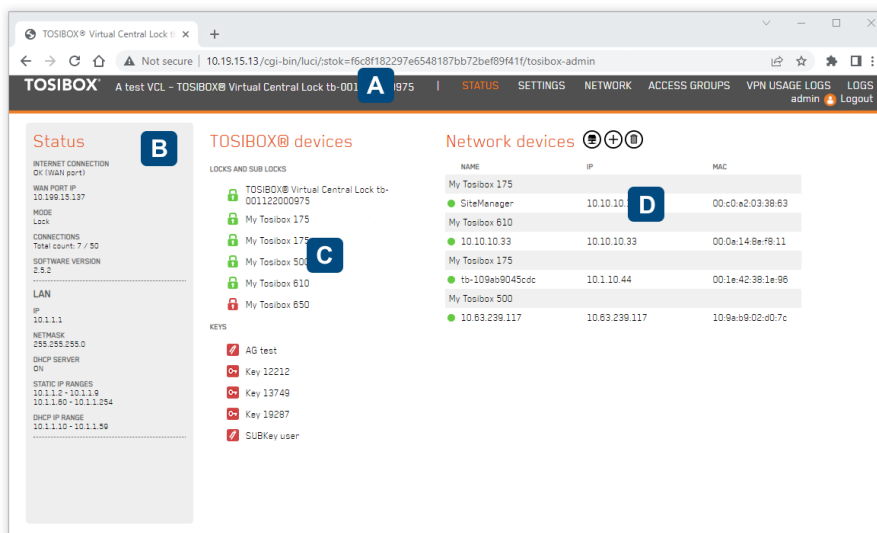
Software updates can be checked and installed from Virtual Central Lock *Settings > Software update*. Opening the Software update view displays the option to check for possible available updates.

It is recommended to update to the latest available software version before taking the Virtual Central Lock to production environment.

# 6 User interface

The TOSIBOX® Virtual Central Lock 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 Virtual Central Lock
- Network devices – Devices connected to the selected Node discovered during network scan



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

## 6.1 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® Virtual Central Lock 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 Virtual Central Lock 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 Virtual Central Lock periodically.

### Settings menu

The Settings menu contains various settings related to TOSIBOX® Nodes and TOSIBOX® Keys, change the name for the Virtual Central Lock, reset to default settings, change the password of the admin account, restart the Virtual Central Lock, 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
- Virtual Central Lock time zone
- VPN cipher selection
- NTP service on Virtual Central Lock
- 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 Virtual Central Lock
- 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 Virtual Central Lock
- DHCP Server – Configure Dynamic Host Configuration Protocol server on the Virtual Central Lock

## 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 Virtual Central Lock, the Virtual Central Lock 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 Virtual Central Lock 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.

## 6.2 Login

Virtual Central Lock 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 Virtual Central Lock'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 Virtual Central Lock's name in the Key user interface.

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

## 6.3 Adding admin users

Virtual Central Lock supports 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 new user is created an unambiguous username is required. System generates a one-time password for the user. When new user logs in for the first time, they must change the password. If password for 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.

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

## 6.4 Adding virtual LANs

When the system local network has multiple VLAN networks available, adding a new virtual LAN can be used to connect the Virtual Central Lock 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 Virtual Central Lock 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.

# 7 HTTPS login

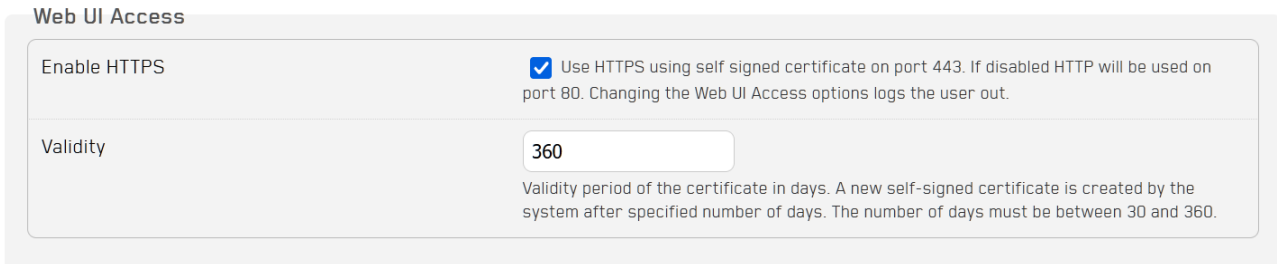
Starting from Virtual Central Lock 2.6 web UI access can be made via secure https protocol. Https encrypts traffic between the end user device and the web server and thus provides increased security. Default protocol is http. If https is enabled, it is used always when accessing from the Virtual Central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



The screenshot shows a configuration panel titled "Web UI Access". It contains two main sections:

- Enable HTTPS:** A checkbox is checked. To its right, a text label reads: "Use HTTPS using self signed certificate on port 443. If disabled HTTP will be used on port 80. Changing the Web UI Access options logs the user out."
- Validity:** A text input field contains the number "360". Below the field, a text label reads: "Validity period of the certificate in days. A new self-signed certificate is created by the system after specified number of days. The number of days must be between 30 and 360."

## Self-signed certificate

Virtual Central Lock https implementation relies on self-signed certificates.

The security certificate is generated and signed by the Virtual Central Lock 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.

# 8 Access rights management

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

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, Virtual Central Lock becomes a necessity and the central point of management. In a network with Virtual Central Lock, 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 Virtual Central Locks' 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 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 Virtual Central Lock is used for always-on, bidirectional protected connections that enables for instance data collection and real-time direct service connections to the devices installed in the field. Virtual Central Lock can operate for instance as a data collection point, connection status log recorder or a connection supervisor.

## 8.2 Managing access rights with TOSIBOX® Virtual Central Lock

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

Centralized model enables an easy to use and versatile deployment of access rights management using the Virtual Central Locks' 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 Virtual Central Lock 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 Virtual Central Lock.

## 8.3 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 Virtual Central Lock and from there onwards access to the LAN side devices is possible as configured by the Administrator in the Virtual Central Locks' Access Groups. Once a Lock is added to Virtual Central Lock, 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 has 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.

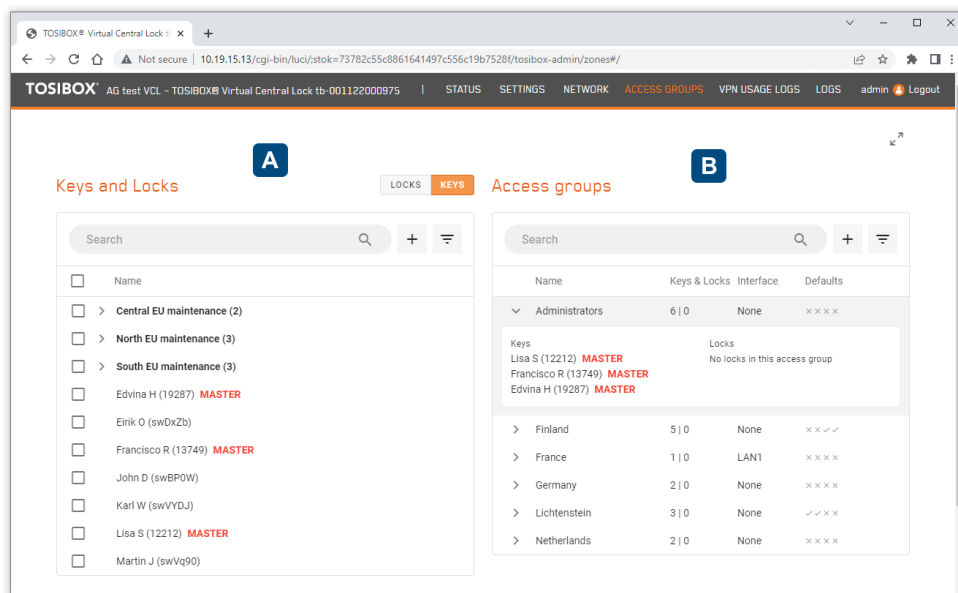
## 8.4 Access Groups UI

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

- 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.
- 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



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.

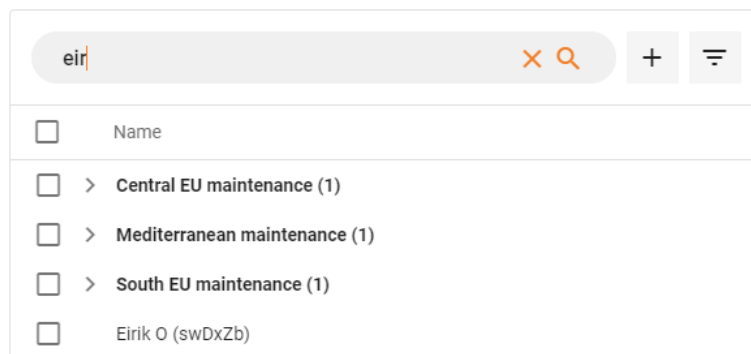
## 8.5 Filtering

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.

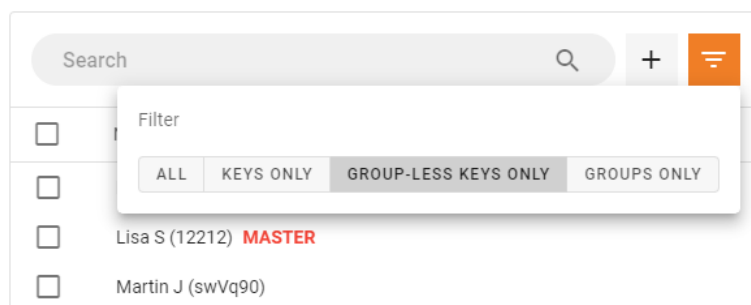
In the below example the search condition “eir” shows three groups where the user Eirik O is a member of as well as the single individual Key. Note how the filter bar symbols are shown in orange to indicate active filtering. To clear filtering click the X symbol.



## 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

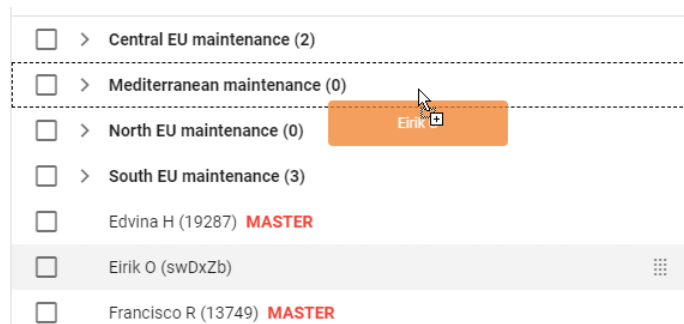


Note also how the quick filter symbol is shown in orange to indicate active filtering. To clear filtering select the ALL option.

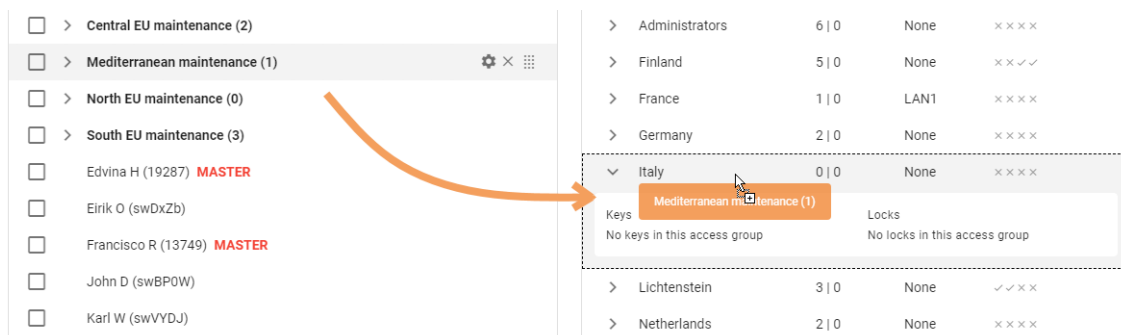
## 8.6 Workflow for creating Access Groups

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.
- A Layer 3 Key or a 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 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 as long as the Key or Lock is present in the Access group once.

### 8.7 Scheduled access

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

Scheduled access gives you a better control over who can access resources inside the network. If a Sub Key connects a Virtual Central Lock 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.

### 8.8 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.

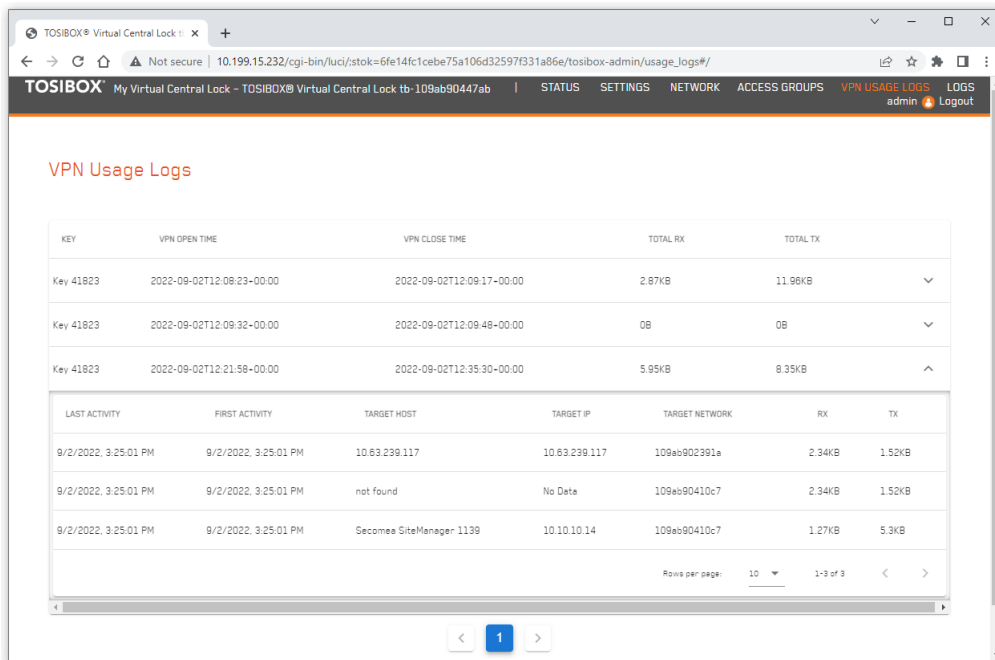
All times will be defined in Virtual Central Lock time zone, defined in [Settings > Advanced settings](#). Modifications to the schedules or rules will take effect immediately upon saving the settings. However, active connections will not be dropped upon saving the settings.

## 9 Logging and alerts

There are in total of three different variations of logging in Virtual Central Lock; VPN usage logging for Keys, Email alerts and Admin trail.

## 9.1 VPN usage logging for Keys

VPN usage logging is available the main level in 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	109aa902391a	2.34KB	1.52KB
9/2/2022, 3:25:01 PM	9/2/2022, 3:25:01 PM	not found	No Data	109aa90410c7	2.34KB	1.52KB
9/2/2022, 3:25:01 PM	9/2/2022, 3:25:01 PM	Secomes SiteManager-1139	10.10.10.14	109aa90410c7	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.

## 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 or a Lock independently.

### Email alerts

Title	Message content	Example
-------	-----------------	---------

[TOSIBOX] Alert: <node> connected	Lock <ID> (<node>) connected from Virtual Central Lock <ID> at <date> <time>	Lock tb-109ab9026b99 (Lock150) connected to Virtual Central Lock tb-001122000975 at 2022-09-14 19:55:27+0300.
[TOSIBOX] Alert: <node> disconnected	Lock <ID> (<node>) disconnected from Virtual Central Lock <ID> at <date> <time>	Lock tb-109ab9026b99 (Lock150) disconnected from Virtual Central Lock 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.

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](#).

### 9.4 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 <source> to <target>	User has created VPN tunnel from point a to point b
-	VPN closed from <source> to <target>	User has closed VPN tunnel from point a to point b

#### Control system event category

ID	Text	Notes
106	System reboot	



3010	System started	VCL is 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	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
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

## 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

## Audit log category

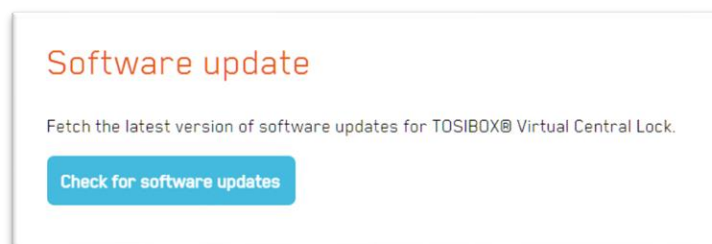
ID	Text	Notes
191	CSV log export	User has exported audit log

# 10 Software update

There are three 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
- **Security patches** – Availability of security patches are constantly being checked in the background and if found, automatically installed. Receiving security patches cannot be disabled.

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 Virtual Central Lock connects to the update service and verifies if update is available and displays information accordingly. Virtual Central Lock does not automatically check or install system upgrades or software updates, this is always a manual task.

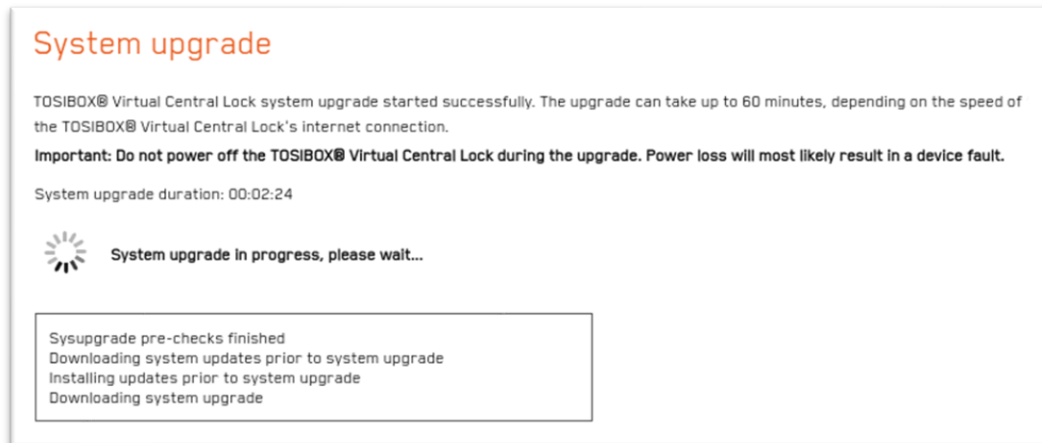
When upgrade is complete you get “System upgrade finished successfully” message.



*Virtual Central Lock 2.6 system upgrade requires two updates. A System update is offered first that prepares Virtual Central Lock for kernel update. In the second phase a System upgrade is offered that brings the system to version 2.6.*

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 system update is offered.

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



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

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



---

*Update from previous versions can require increased disk partition size. Requirements for current version are listed in chapter System requirements. If your system has less resources available update 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

© 2022 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, Teknologiantie 12A, 90590 OULU, FINLAND