



TOSIBOX® Virtual Central Lock (HUB)

TOSIBOX® Virtual Central Lock is an operative network for your devices and service personnel. The 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.

The Virtual Central Lock cuts centralized access management work time from days into minutes, enabling easy management of big networks without special IT skills.

Access groups

Virtual Central Lock revolutionizes the creation and management of access groups, making it a breeze. You can create access groups and add relevant members (Keys, Nodes, IP addresses, network ranges or MAC addresses) by drag and drop. Members of the same access group can communicate freely, and members can belong to several access groups.

Network monitoring

The Virtual Central Lock has some very interesting features for a controlled network, such as audit log data collection and connection monitoring. You can see log data about the events of connected TOSIBOX Nodes, always tracking who were using the TOSIBOX VPN at a certain time. The Virtual Central Lock can also be set to send email alerts for connections for any or all serialized TOSIBOX® Nodes being established and closed.






Virtual LAN

Virtual Central Lock supports Virtual LANs enabling adding workstations or servers from one or more networks connected to the VCL LAN into an access group. You may have different networks defined per customer, or you may want to separate your office network from production network, and arrange remote access to these networks differently.

Unlimited expandability

TOSIBOX® Virtual Central Lock is infinitely scalable. The LITE license includes max. 5 VPN connections.

Advantages of TOSIBOX

-  **Simple**
Build and manage secure OT infrastructure in minutes
-  **Secure**
Tested & audited security
-  **Modular**
Unlimited expandability and flexibility
-  **Timeless**
Deals with legacy and future systems
-  **Unique**
Globally patented point-to-point connection



Properties

- With Virtual Central Lock and always-on VPN connections you can easily enable applications like data logging, continuous monitoring or remote maintenance.
- Possibility to collect audit log data from connected TOSIBOX Nodes
- Monitoring service for VPN connections
- Improved and scalable access management that is enterprise-ready.
- With virtual platforms, it is possible to achieve a very high level of redundancy and fault-tolerance where failover time is measured in seconds.
- Because it's virtual, it can be deployed in your office network, in your favorite cloud infrastructure, or anywhere else where you prefer.
- Supports up to thousands concurrent VPN connections from Keys, Nodes or Mobile Clients. The LITE license includes max. 5 VPN connections.

System requirements

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

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