TOSI BOX®

VIRTUAL CENTRAL LOCK

INSTALLATION GUIDE

Table of contents

1. Introduction

TOSIBOX® Virtual Central Lock is a licensed software product that runs in a virtual server environment. The main functionality and features of the Virtual Central Lock are similar to the software of the Central Lock. In addition to the features of the Central Lock, the Virtual Central Lock supports up to 4094 virtual LAN interfaces.

Because the product is a virtual machine, it can be deployed e.g. in office networks and cloud infrastructures. 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.

1.1. Main features

- Supports up to thousands concurrent VPN connections from Keys, Locks or Mobile Clients
- Scalable access rights management by using Access groups
- Possibility to collect audit log data from connected TOSIBOX® Locks
- Monitoring service for VPN connections
- Encryption and authentication: PKI, 3072 bit RSA
- Data encryption: TLS, AES-256-CBC / AES-192-CBC / AES-128-CBC / Blowfish-128-CBC

1.2. Technical requirements

A supported virtualisation platform based on one of the following:

- VMWare vSphere/ESXi v5.0 or later
- Microsoft Hyper-V
- Linux KVM

The common requirements for all virtualisation platforms are:

- x86-64 processor architecture, two or more CPU cores
- Minimum of 2 GB of RAM
- Minimum of 5 GB of permanent storage (HDD or SSD)
- Two or more network interfaces for the virtual machine (one WAN connection + at least one LAN connection)
- WAN interface needs to be set as DHCP client during activation
- One non-firewalled public IP address
- At least 10/10 Mbit/s Internet connection

In order to install and setup the TOSIBOX® Virtual Central Lock, you will also need:

- Internet connectivity to download the TOSIBOX® Virtual Central Lock VM image
- License key that was delivered to you upon the purchase

2. Installing TOSIBOX® Virtual Central Lock

Installing the VM image:

2.1. VMWare vSphere/ESXi

1. Download the latest TOSIBOX_Virtual_Central_Lock_*YYYYMMDDNN*_esx.ova appliance
2. 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_*YYYYMMDDNN*.vmdk virtual disk file and create the virtual machine out of it.

3. Adjust the CPU and RAM hardware settings according to your needs, keeping in mind the minimum requirements mentioned above.
4. 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.
5. Make sure that the network adapter is in bridged mode and satisfies the requirement of the non-firewalled public IP address.

2.2. Microsoft Hyper-V

1. Download the latest TOSIBOX_Virtual_Central_Lock_*YYYYMMDDNN*.vhdx image
2. If needed, create a new Virtual Switch using type External and the interface that is connected to the Internet
3. Create a new VM with the downloaded .vhdx image, select Generation 2
4. Edit the settings of the created VM (right-click on the VM and select Settings)
    1. Add new Network Adapter (not the Legacy one) on Hardware → Add Hardware
    2. In the Network Adapter's settings, select the correct Virtual Switch (if you created one earlier, select it)
    3. In the Network Adapter's settings, go to Advanced Features and tick *Enable MAC address spoofing*
    4. Disable *Secure Boot* from Hardware → Security

2.3. KVM

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

2.4. VMWare Workstation/Fusion (not officially supported)

1. Download the latest TOSIBOX_Virtual_Central_Lock_*YYYYMMDDNN*_vbox.ova appliance
2. Use the import function of the VMware product to load the downloaded .ova file
3. If you get a dialog saying that the .ova file "did not pass OVF specification conformance or virtual hardware compliance checks", click "Retry" to continue with the import.
4. Adjust the CPU and RAM hardware settings according to your needs, keeping in mind the minimum requirements mentioned above.

2.5. Oracle VirtualBox (not officially supported)

1. Download the latest TOSIBOX_Virtual_Central_Lock_*YYYYMMDDNN*_vbox.ova appliance.
2. Use the import function to load the downloaded .ova file.
3. Adjust the CPU and RAM hardware settings according to your needs, keeping in mind the minimum requirements mentioned above.
4. Make sure that the network adapter is in bridged mode and satisfies the requirement of the non-firewalled public IP address. The detailed settings of Network Adapter 1 should be:
    1. Check Enable Network Adapter
    2. Attached to: Bridged Adapter
    3. Name: (choose the correct physical interface)
    4. Advanced → Adapter Type: Intel PRO/1000 T Server (82543GC)

3. Initial setup

3.1. Accessing the configuration interface

Start the virtual machine that was installed in the previous step. 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.

3.2. WAN interface configuration and product activation

In the activation user interface, configure the IP address settings for the WAN interface. The IP address has to 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 will be 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.

3.3. Change admin 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 admin password* to change the password. The web user interface can be accessed also remotely over VPN connection from master Key(s). 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* (see User Manual).

3.4. 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. In order to assign LAN1 to a real adapter, it must be first deleted by navigating to *Network → Interfaces* and selecting *Delete* next to interface 'LAN1'.

In order 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 virtualisation platform and typically requires restarting the virtual machine. In case layer 2 VPN connections from Keys or Locks 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).

3.5. Matching the Master Key

After the Virtual Central Lock is activated and has Internet connection, the Master Key needs to be matched to the Virtual Central Lock instance. This is done with the *remote matching feature*.

After the Virtual Central Lock has been matched with the Master Key, the product is ready to be used. Additional networks, Keys, and Locks can be connected to the Virtual Central Lock as explained in the User Manual.

Tosibox Oy
sales@tosibox.com
support@tosibox.com
Sales within Finland, tel. 044 70 90 100
Sales, international, tel. +358 44 70 90 200
www.tosibox.com

TOSIBOX®
Simplifying IoT

