TOSIBOX® Lock for Container

User Manual

V1.4

Content

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® Lock for Container works both in private and public networks when Internet connection is available.

- TOSIBOX® Key is a client used to access the network. The workstation where the TOSIBOX® Key is used is the starting point for the VPN tunnel
- TOSIBOX® Lock for Container is the endpoint of the VPN tunnel providing secure remote connectivity to the host device where it's installed

This document applies to Lock for Container version 1.1.

2 System description

2.1 Context of use

TOSIBOX® Lock for Container serves as the endpoint of a highly secure VPN tunnel initiated from a user workstation running TOSIBOX® Key, a user mobile device running TOSIBOX® Mobile Client or a private data center running TOSIBOX® Virtual Central Lock. The end-to-end VPN tunnel is routed through the Internet towards the Lock for Container residing anywhere in the world, without a cloud in the middle.

TOSIBOX® Lock for Container can run on any device supporting Docker container technology. Lock for Container provides secure remote connection to the host device where it's installed, and access to the LAN side devices connected to the host itself.

TOSIBOX® Lock for Container is ideal for industrial OT networks where simple user access control complemented with ultimate security is needed. Lock for Container is also suitable for demanding applications in building automation and for machine builders, or in hazardous environments such as marine, transport and other industries. In these scenarios Lock for Container brings secure connectivity to hardware devices designed to meet demanding requirements.

2.2 TOSIBOX® Lock for Container in brief

TOSIBOX® Lock for Container is a software-only solution based on Docker technology. It enables users to integrate networking devices such as IPCs, HMIs, PLCs and controllers, industrial machines, cloud systems, data centers into their Tosibox ecosystem.

Any service running on the host or, if configured, on the LAN devices can be accessed over the VPN tunnel such as Remote Desktop Connection (RDP), web services (WWW), File Transfer Protocol (FTP) or Secure Shell (SSH) just to mention some. LAN side access must be supported and enabled on the host device for this to work.

No user input is required after setup, Lock for Container runs silently in the system background. Lock for Container is a software-only solution comparable to TOSIBOX® Lock hardware.

2.3 Main features

Secure connectivity to nearly any device

The patented Tosibox connection method is now available virtually to any device. You can integrate and manage all your devices with your TOSIBOX® Virtual Central Lock with the familiar Tosibox user experience. TOSIBOX® Lock for Container can be added to TOSIBOX® Virtual Central Lock access groups and accessed from the TOSIBOX® Key software. Using it together with TOSIBOX® Mobile Client ensures convenient usage on the go.

Build end-to-end highly secure VPN tunnels

TOSIBOX® networks are known to be ultimately secure yet flexible to fit many different environments and uses. TOSIBOX® Lock for Container supports one-way, Layer 3 VPN tunnels between a TOSIBOX® Key and TOSIBOX® Lock for Container or two-way, Layer 3 VPN tunnels between TOSIBOX® Virtual Central Lock and Lock for Container, without a third-party cloud in the middle.

Manage any service running on your network

TOSIBOX® Lock for Container does not limit the number of services or devices you need to manage. You can connect any service over any protocol between any devices. Lock for Container provides unlimited access if supported by and enabled on the host device.

Install without activation, or activate for immediate access

TOSIBOX® Lock for Container can be installed without being activated, keeping the software ready and waiting for activation. Once activated, Lock for Container connects to the Tosibox ecosystem and is ready to be taken in production use. Lock for Container user license can be transferred from one device to another.

Runs silently in the system background

TOSIBOX® Lock for Container runs silently in the system background. It does not interfere with the operating system level processes or middleware. Lock for Container installs cleanly on top of the Docker platform separating Tosibox connectivity application from system software. Lock for Container does not need access to system files, and it doesn’t change system level settings.

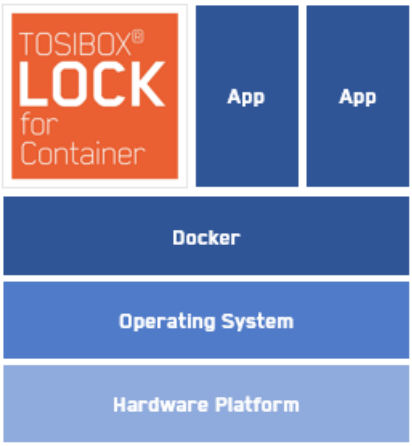
2.4 Comparison of TOSIBOX® Lock and Lock for Container

The following table highlights the differences between a physical TOSIBOX® Node device and Lock for Container.

Feature	TOSIBOX® Node	TOSIBOX® Lock for Container
Operating environment	Hardware device	Software running on Docker platform
Deployment	Plug & Go™ connectivity device	Available in Docker Hub and in well-equipped marketplaces
SW auto-update	✓	Update via Docker Hub
Internet connectivity	4G, WiFi, Ethernet	-
Layer 3	✓	✓
Layer 2 (Sub Lock)	✓	-
NAT	1:1 NAT	NAT for routes
LAN access	✓	✓
LAN device scanner	For LAN network	For Docker network
Matching	Physical and remote	Remote
Open firewall ports from internet	-	-
End-to-end VPN	✓	✓
User access management	From TOSIBOX® Key Client or TOSIBOX® Virtual Central Lock	From TOSIBOX® Key Client or TOSIBOX® Virtual Central Lock

3 Docker fundamentals

3.1 Understanding Docker containers



A software container is the modern way of distributing applications. A Docker container is a software package that runs on top of the Docker platform, safely and securely isolated from the underlying operating system and other applications. The container packages up code and all its dependencies so the application runs quickly and reliably.

Docker is getting a lot of traction in the industry thanks to its portability and robustness. Applications can be designed to run in a container that can be installed on a wide variety of devices safely and easily. You don't need to worry about the application being able to interfere with the system software or existing applications. Docker also supports running multiple containers on the same host.

For more information about Docker and container technology, see www.docker.com.

3.2 Introduction to Docker

The Docker platform comes in many flavors. Docker can be installed on a multitude of systems ranging from powerful servers to tiny portable devices. TOSIBOX® Lock for Container can run on any device where Docker platform is installed.

To understand how to set up TOSIBOX® Lock for Container, it's important to know how Docker operates and manages networking.

Docker extrapolates the underlaying device and creates a host-only network for the installed containers. Lock for Container sees the host through the Docker network and treats it as a managed network device. The same applies to other containers running on the same host. All containers are network devices in respective to Lock for Container.

Docker has a multitude of different network modes; bridge, host, overlay, macvlan or none. Lock for Container can be configured for most modes depending on different connectivity scenarios. Docker creates a network within the host device. Using basic network configuration LAN is typically on a different subnetwork requiring static routing on Lock for Container.

4 Connectivity scenario examples

4.1 From Key Client to Lock for Container

Connectivity from TOSIBOX® Key Client to the physical host device network or to the Docker network on the host device running TOSIBOX® Lock for Container is the simplest supported use case. Connectivity is initiated from the TOSIBOX® Key Client terminating at the host device.

This option is well suited for remote management of the host device or the Docker containers on the host device.

Figure 1: Connectivity from TOSIBOX® Key Client to the host device or the Docker network within the host device

4.2 From Key Client or Mobile Client to the host device LAN via Lock for Container

Connectivity from TOSIBOX® Key Client to the devices connected to the host is an extension to the previous use case. Typically, the simplest setup is achieved if the host device is also the gateway for the devices providing switching and guarding the Internet access. Configuring static routing access can be extended to the LAN network devices.

This option is well suited for remote management of the host device itself and the local network. It also suits well for the mobile workforce.

Figure 2: Connectivity from TOSIBOX® Key Client to devices behind TOSIBOX® Lock for Container

4.3 From Virtual Central Lock to the host device LAN via Lock for Container

The most flexible configuration is achieved when TOSIBOX® Virtual Central Lock is added to the network. Network access can be configured per device basis on the TOSIBOX® Virtual Central Lock. Users connect to the network from their TOSIBOX® Key Clients.

This option is targeted for continuous data collection and centralized access management, especially in large and complex environments. The VPN tunnel from TOSIBOX® Virtual Central Lock to TOSIBOX® Lock for Container is a two-way connection allowing scalable machine-to-machine communication.

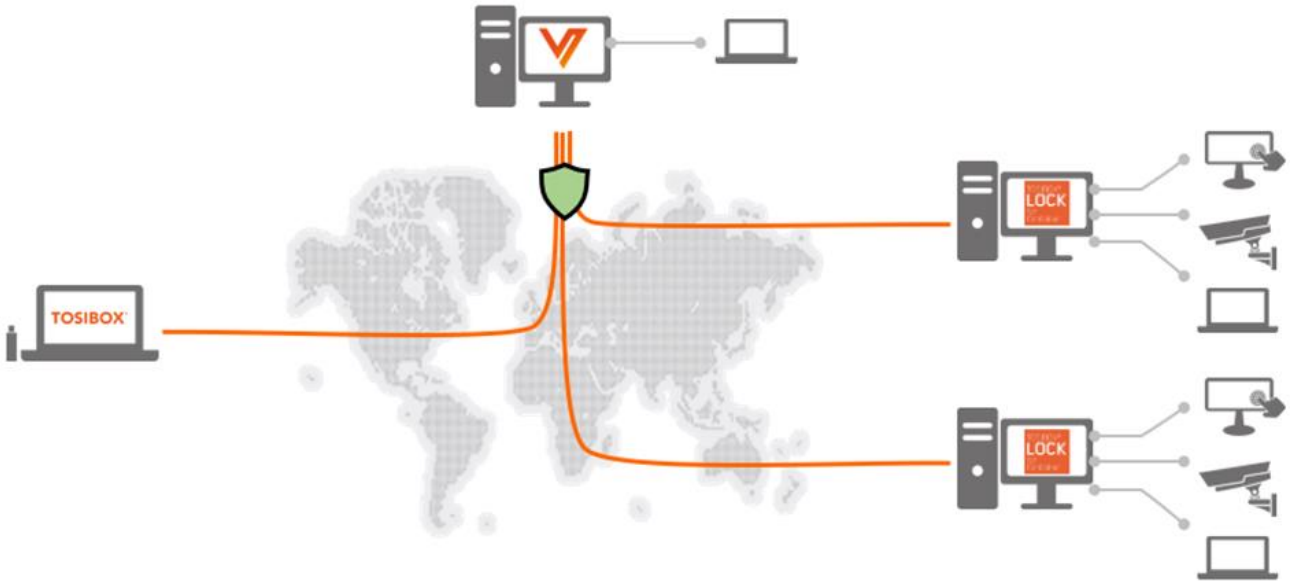


Figure 3: Connectivity from TOSIBOX® Key Client to devices behind TOSIBOX® Lock for Container via TOSIBOX® Virtual Central Lock

4.4 From Virtual Central Lock running in cloud to another cloud instance via Lock for Container

Lock for Container is the perfect cloud connector, it can connect securely two different clouds or cloud instances within the same cloud. This requires Virtual Central Lock installed on the master cloud with Lock for Container installed on the client cloud system(s).

This option is targeted for connecting physical systems to cloud or separate cloud systems together. The VPN tunnel from TOSIBOX® Virtual Central Lock to TOSIBOX® Lock for Container is a two-way connection allowing scalable cloud-to-cloud communication.

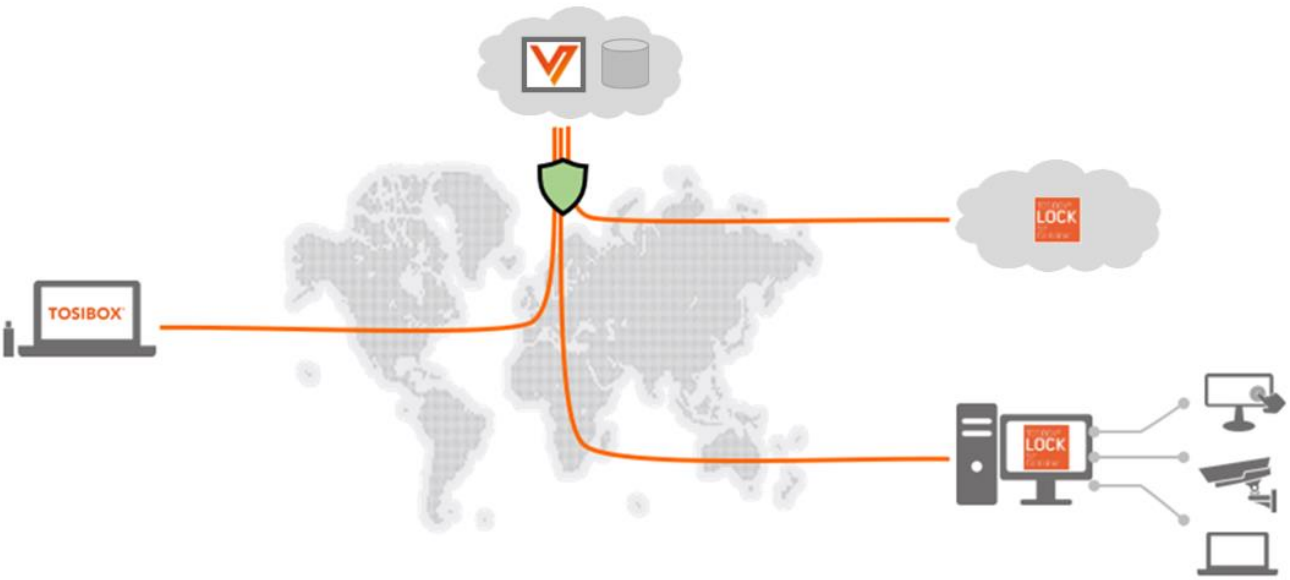


Figure 4: Connectivity from TOSIBOX® Key Client to cloud with TOSIBOX® Lock for Container via TOSIBOX® Virtual Central Lock

5 Licensing

5.1 Introduction

TOSIBOX® Lock for Container can be pre-installed on a device without being activated. An inactive Lock for Container cannot communicate or form secure connections. Activation enables the Lock for Container to connect to the TOSIBOX® ecosystem and start serving VPN connections. To activate the Lock for Container, you need an Activation Code. You can request Activation Code from Tosibox sales. (https://www.tosibox.com/company-contact-us)

The installation of Lock for Container is somewhat dependent on the device where the software is taken in use and can vary case by case. If you have difficulties, browse Tosibox Global Support for assistance (www.tosibox.com/support).

When installing from 3rd party marketplaces these guidelines may not apply, follow instructions provided by the manufacturer.

Note that you need an Internet connection to activate and operate the Lock for Container.

5.2 Migrating the license to use

TOSIBOX® Lock for Container user license is tied to the device where the Activation Code is used. Each Lock for Container Activation Code is for one-time use only. Contact Tosibox Support if you have issues with the activation.

6 Installation and update

TOSIBOX® Lock for Container is installed using Docker Compose or by entering the commands manually. Docker must be installed prior to installing Lock for Container.

Installation steps

1. Download and install Docker free of charge, see www.docker.com.
2. Pull the Lock for Container from Docker Hub on to the target host device

---

When installing from 3rd party marketplaces these guidelines may not apply, you should follow instructions provided by the device manufacturer.

6.1 Download and install Docker

Docker is available for a wide variety of operating systems and devices. See www.docker.com for downloading and installing on your device.

6.2 Pull the Lock for Container from Docker Hub

Visit the Tosibox Docker Hub repository at https://hub.docker.com/r/tosibox/lock-for-container. Follow the installation instructions provided there.

Docker Compose file is provided for convenient container configuration. Run the script or type the needed commands manually on the command line. You can modify the script as required.

7 Activation and taking in use

TOSIBOX® Lock for Container must be activated and connected to your Tosibox ecosystem before you can create secure remote connections.

Summary

1. Open the web user interface to the Lock for Container running on your device.
2. Activate Lock for Container with the Activation Code provided by Tosibox.
3. Log in to the web user interface with the default credentials.
4. Create the Remote Matching Code.
5. Use the Remote Matching functionality on the TOSIBOX® Key Client to add the Lock for Container to your TOSIBOX® network.
6. Grant access rights.
7. Connecting to a HUB (Virtual Central Lock)

7.1 Open the Lock for Container web user interface

To open TOSIBOX® Lock for Container web user interface, launch any web browser on the host and type in the address http://localhost:8000 (presuming Lock for Container has been installed with default settings to listen on port 8000)

7.2 Activate Lock for Container

1. Look for the “Activation required” message on the Status area on the left in the web user interface.
2. Click the “Activation required” link to open the activation page.
3. Activate the Lock for Container by copying or typing in the Activation Code and click the Activate button.

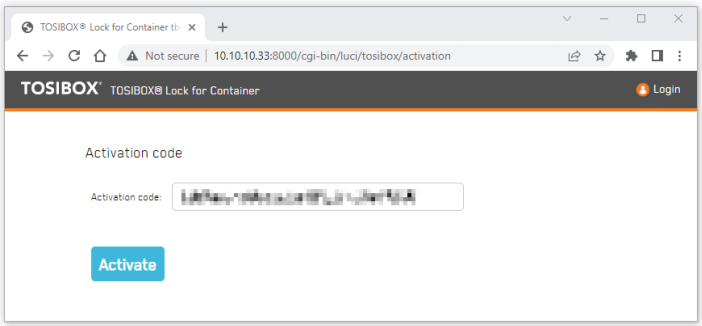


Figure 5: TOSIBOX® Lock for Container activation page

4. Additional software components are downloaded and “Activation completed” appears on the screen. The Lock for Container is now ready for use.

If activation fails, double-check the Activation Code, correct possible errors and try again.

7.3 Log in to the web user interface

Once TOSIBOX® Lock for Container is activated you can login to the web user interface. Click the Login link on the menu bar.

Log in with the default credentials:

- Username: admin
- Password: admin

After logging in, Status, Settings and Network menus become visible.

You must accept EULA before you can use Lock for Container.

7.4 Create Remote Matching code

1. Log in to the TOSIBOX® Lock for Container and go to *Settings > Keys and Locks*. Scroll down to the bottom of the page to find Remote Matching.

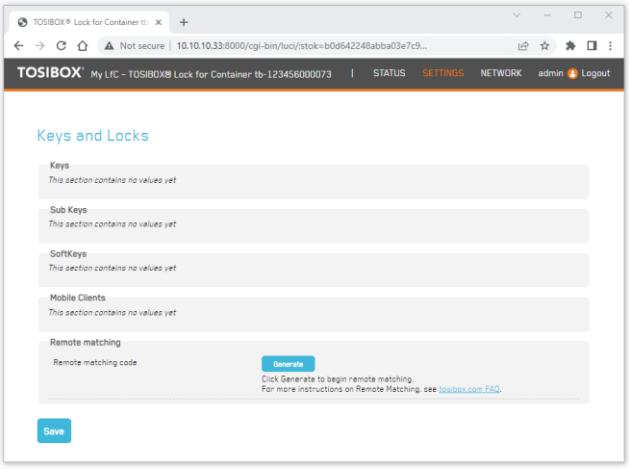


Figure 6: Remote Matching Code generation page

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 Lock for Container to the network.

7.5 Remote Matching

Insert TOSIBOX® Key in your workstation and TOSIBOX® Key Client opens. If TOSIBOX® Key Client 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*.

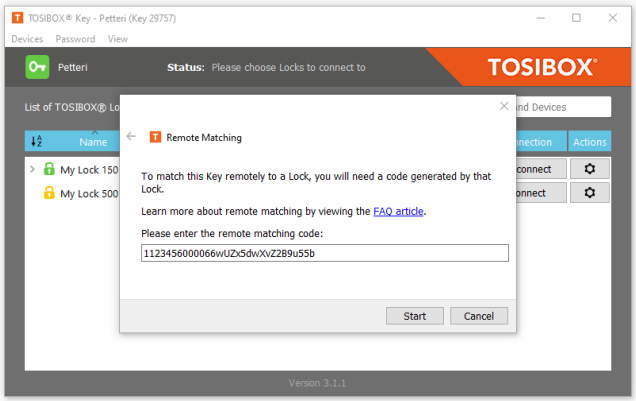


Figure 7: Remote Matching on TOSIBOX® Key Client

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

7.6 Grant access rights

You are the only user with access to the TOSIBOX® Lock for Container until you grant additional permissions. To grant access rights, open TOSIBOX® Key Client and go to *Devices > Manage Keys*. Change access rights as needed.

7.7 Connecting to a Virtual Central Lock

If you have TOSIBOX® Virtual Central Lock installed in your network you can connect Lock for Container for always-on, secure VPN connectivity.

1. Open TOSIBOX® Key Client and go to *Devices > Connect Locks*.
2. Tick the newly installed Lock for Container and the Virtual Central Lock and click Next.
3. For Select Connection Type choose Layer 3 always (Layer 2 is not supported), click Next.
4. Confirmation dialog is displayed, click Save and the VPN tunnel is created.

You can now connect to Virtual Central Lock and assign Access Group settings as needed.

8 User interface

The TOSIBOX® web user interface screen is dived 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 – Locks and Keys related to the Lock for Container
D. Network devices – Devices or other Docker containers discovered during network scan

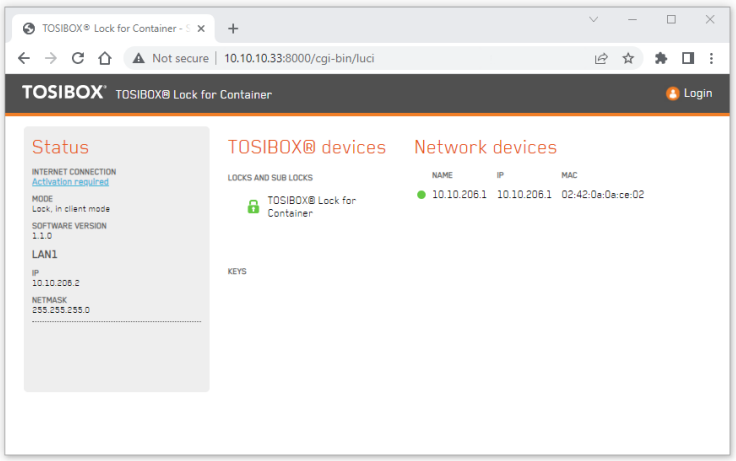


Figure 8: Lock for Container waiting for activation

When TOSIBOX® Lock for Container is not activated, the web user interface displays “Activation required” link on the Status area. Clicking the link takes you to the activation page. An activation Code from Tosibox is required for activation. An inactive Lock for Container does not communicate to the Internet, so Internet Connection status displays FAIL until the Lock for Container is activated.

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

8.1 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® Locks and TOSIBOX® Keys and possible LAN devices or other containers the TOSIBOX® Lock for Container has discovered.

The TOSIBOX® Lock for Container scans the network interface it is tied to during installation. With default settings the Lock for Container scans the host-only Docker network and lists all discovered containers. The LAN network scan can be configured to discover physical LAN devices with the advanced Docker networking settings.

Settings menu

The Settings menu makes it possible to change properties for TOSIBOX® Locks and TOSIBOX® Keys, change the name for a Lock, change the password of the admin account, remove all matched Keys from the Lock for Container and change the advanced settings.

Network menu

Static routes for TOSIBOX® Lock for Container's network LAN connectivity can be edited in the Network menu. The Static routes view shows all active routes on the Lock for Container and allows adding more if necessary.

Static route view contains a special NAT for routes field that can be configured when the LAN IP address for the route cannot or is not wanted to be changed or edited. NAT masks the LAN IP address and replaces it with the given NAT address. The effect is that now, instead of the real LAN IP address, the NAT IP address is reported to TOSIBOX® Key. If the NAT IP address is selected from a free IP address range this resolves possible IP conflicts that can emerge if using the same LAN IP range in multiple host devices.

9 Basic configuration

9.1 Generating Remote Matching code

Generating remote matching code and the remote matching process is explained in chapters 7.4 – 7.5.

9.2 Change admin password

Log in to the TOSIBOX® Lock for Container web user interface and go to *Settings > Change admin password* to change the password. You can access the web user interface also remotely over a VPN connection from the 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.

9.3 LAN access

By default, TOSIBOX® Lock for Container does not have access to the host device or to the LAN devices residing in the same network with the host device itself.

You can access the LAN side by configuring static route on the Lock for Container. Log in as admin and go to *Network > Static routes*. On the Static IPv4 Routes list you can add a rule to access the subnetwork.

- Interface: LAN
- Target: Subnetwork IP address (e.g. 10.10.10.33)
- IPv4 Netmask: Mask according to subnetwork (e.g. 255.255.255.255)
- IPv4 Gateway: IP address of the gateway to the LAN network
- NAT: The IP address used to mask the physical address (optional)

Metric and MTU can be left as defaults.

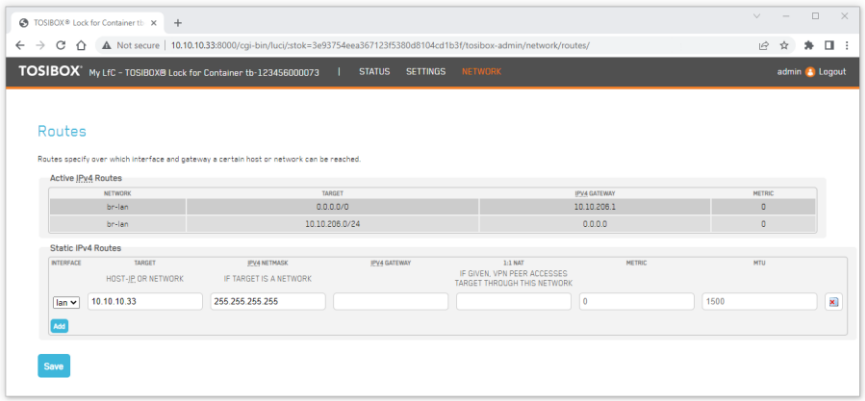


Figure 9: Static routes

9.4 Changing Lock's name

Open the TOSIBOX® Lock for Container web user interface and log in as admin. Go to "Settings > Lock name" and type in the new name. Press Save and the new name is set. This will also affect the name as it's seen on the TOSIBOX® Key Client.

9.5 Enabling TOSIBOX® remote support access

Open the TOSIBOX® Lock for Container web user interface and log in as admin. Go to "Settings > Advanced settings" and tick the Remote Support checkbox. Click Save. Tosibox support can now access the device.

9.6 Enabling TOSIBOX® SoftKey or TOSIBOX® Mobile Client access

You can add access to new users using the TOSIBOX® Key Client. See www.tosibox.com/support for the user manual.

10 NAT for routes

NAT for routes provides the ability to define 1:1 NAT'ing for routes, i.e. allows Key and HUB to access the device through another network than the device has internally. NAT for routes is similar to 1:1 NAT available in Node firmware for LAN networks.

NAT for routes can be used for example in situations where several Lock for Containers can potentially have identical internal, non-LAN, networks. When having this internal network as a route (e.g. 10.10.10.0/24) Key can access it fine but if Key is connected to two different Lock for Containers that have the same internal networking, routes will overlap.

Due to practical constraints, it can be that the internal networks cannot be changed. To connect to both systems at the same time NAT for routes can be utilized.

Use case example

For example, if a route that gets advertised to Key or HUB is 10.10.10.33/24, this address can be translated to any other wanted address, for example to 10.20.20.33/24 by having netmapping 10.20.20.0.

Constraints:

- Both Lock for Containers can have the 10.10.10.0/24 internal network defined
- Configure 1:1 NAT for either of the Lock for Containers so it will advertise a different network resolving network conflict issues at Key and HUB
- Add the host device on the Status page with the "Add network device" functionality using the NAT'ed address

This way devices can have the same internal, non-LAN, networks while being accessible from the Key user interface without having overlapping routes for clients.

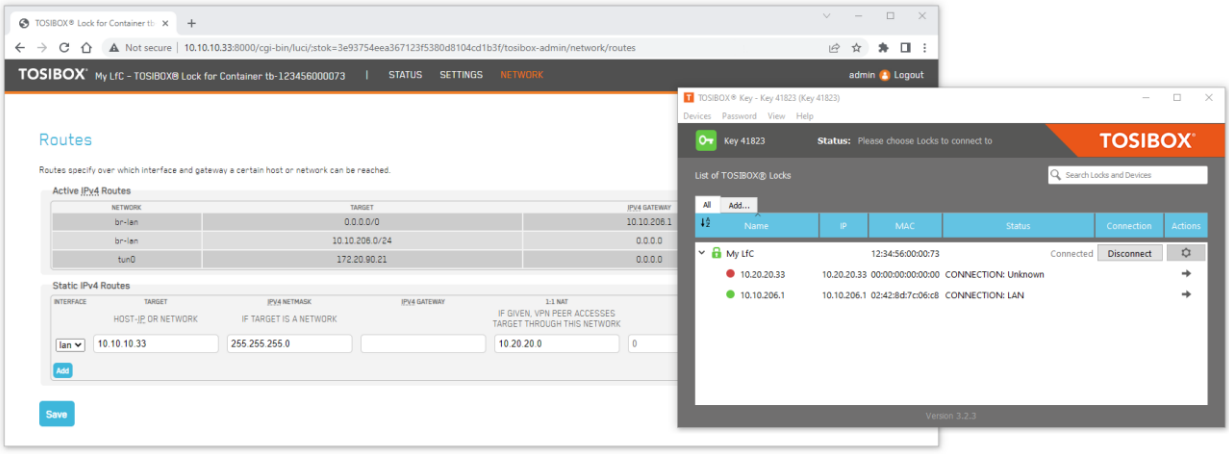


Figure 10: 1:1 NAT configured on Lock for Container

Manually added device will appear in red as if it is not reachable but this due to LAN scan not being able to traverse the LAN subnet. LAN scan can only discover containers on the Docker network, not manually added LAN devices.

Note that after 1:1 NAT is configured on the Lock for Container user interface the device can be reached through the configured NAT IP address. In this example the working address is 10.20.20.33, not 10.10.10.33.

NAT for routes is a new feature introduced in TOSIBOX® Lock for Container version 1.1. NAT for routes requires kernel support from the host device.

---

11 Uninstallation

Uninstallation steps

1. Remove all Key serializations using the TOSIBOX® Lock for Container web user interface.
2. Uninstall TOSIBOX® Lock for Container using Docker commands.
3. Uninstall Docker if needed.
4. If you intend to install the Lock for Container on another device, please contact Tosibox Support for license migration.

12 System requirements

The following recommendations are well suited for general purpose. However, requirements can vary between environments and uses.

Lock for Container is targeted to run on following processor architectures:

- ARMv7 32-bit
- ARMv8 64-bit
- x86 64-bit

Recommended software requirements

- Any 64-bit Linux OS supported by Docker and Docker Engine - Community v20 or later installed and running (www.docker.com)
- Docker Compose
- Linux kernel version 4.9 or later
- Full functionality requires certain kernel modules related to IP tables
- Any 64-bit Windows OS with WSL2 enabled (Windows Subsystem for Linux v2)
- Installation requires sudo or root level user rights

Recommended system requirements

- 50MB RAM
- 50MB hard disk space
- ARM 32-bit or 64-bit processor, Intel or AMD 64-bit dual core processor
- Internet connectivity

Required open firewall ports

- Outbound TCP: 80, 443, 8000, 57051

- Outbound UDP: random, 1-65535
- Inbound: none

13 Troubleshooting

I try to open the host device web UI from TOSIBOX® Key but get another device

Issue: You are opening a device web user interface for example by double-clicking the IP address on your TOSIBOX® Key Client but get the wrong user interface instead.

Solution: Make sure your web browser is not caching web site data. Clear the data to force your web browser to read the page again. It should now display the wanted content.

I try to access the host but get “This site can’t be reached”

Issue: You are opening a device web user interface for example by double-clicking the IP address on your TOSIBOX® Key Client but after a while get ‘This site can’t be reached’ on your web browser.

Solution: Try other means of connection, ping is recommended. If this results in the same error, there might be no route to the host device. See help earlier in this document for how to create static routes.

I have another web service running on the host device, can I run Lock for Container

Issue: You have a web service running on the default port (port 80) and installing another web service on the device will overlap.

Solution: The Lock for Container has a web user interface and thus needs a port from which it can be accessed. Despite all other services, the Lock for Container can be installed on the device but needs to be configured on another port. Just make sure you use a different port than what is used for existing web services. The port can be configured during the installation.

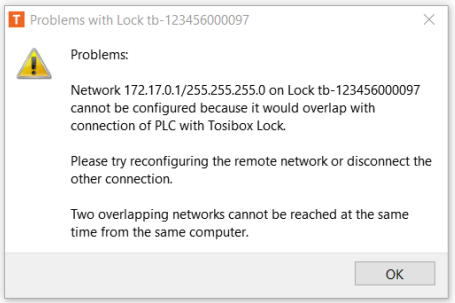
Installation fails with “cannot exec in a stopped state: unknown” error

Issue: You are installing TOSIBOX® Lock for Container but at the end of the installation get an error ”`cannot exec in a stopped state: unknown`” or similar.

Solution: Execute “`docker ps`“ on the command line and verify if the container is running. If the Lock for Container is in a restart loop, i.e. the status field displays something like

"`Restarting (1) 4 seconds ago`", this indicates the container is installed but cannot run successfully. It is possible that the Lock for Container is not compatible with your device, or you used the wrong settings during the installation. Verify if your device has an ARM or Intel processor and use the appropriate installation switch.

I get IP address conflict when opening VPN



Issue: You are opening two concurrent VPN tunnels from your TOSIBOX® Key Client to two Lock for Container instances and receive a warning about overlapping connections.

Solution: Verify if both Lock for Container instances have been configured on the same IP address and either configure NAT for routes or reconfigure the address on either installation. To install a Lock for Container on a custom IP address, use the networking commands during the installation.

VPN throughput is low

Issue: You have a VPN tunnel up but are experiencing low data throughput.

Solution: TOSIBOX® Lock for Container uses device HW resources to encrypt/decrypt VPN data. Verify (1) the processor and memory utilization on your device, for example with Linux *top* command, (2) which VPN cipher you are using from the Lock for Container menu "Settings / Advanced settings", (3) if your Internet access provider is throttling your network speed, (4) possible network congestions along the route, and (5) if outgoing UDP ports are open as suggested for best performance. If nothing else helps, check how much data you are transferring and if it's possible to reduce it.

I get "Your connection is not private" on my web browser

Issue: You tried to open the Lock for Container web user interface but receive "Your connection is not private" message on your Google Chrome browser.

Solution: Google Chrome warns when your network connection is not encrypted. This is useful when operating on the Internet. The Lock for Container in turn transmits data over an extremely secure and highly encrypted VPN tunnel that Chrome cannot identify. When using Chrome with a TOSIBOX® VPN, Chrome's warning can be safely ignored. Click the Advanced button and then "Proceed to" link to continue to the web site.