



TOSIBOX® Lock for Container User Manual

Content

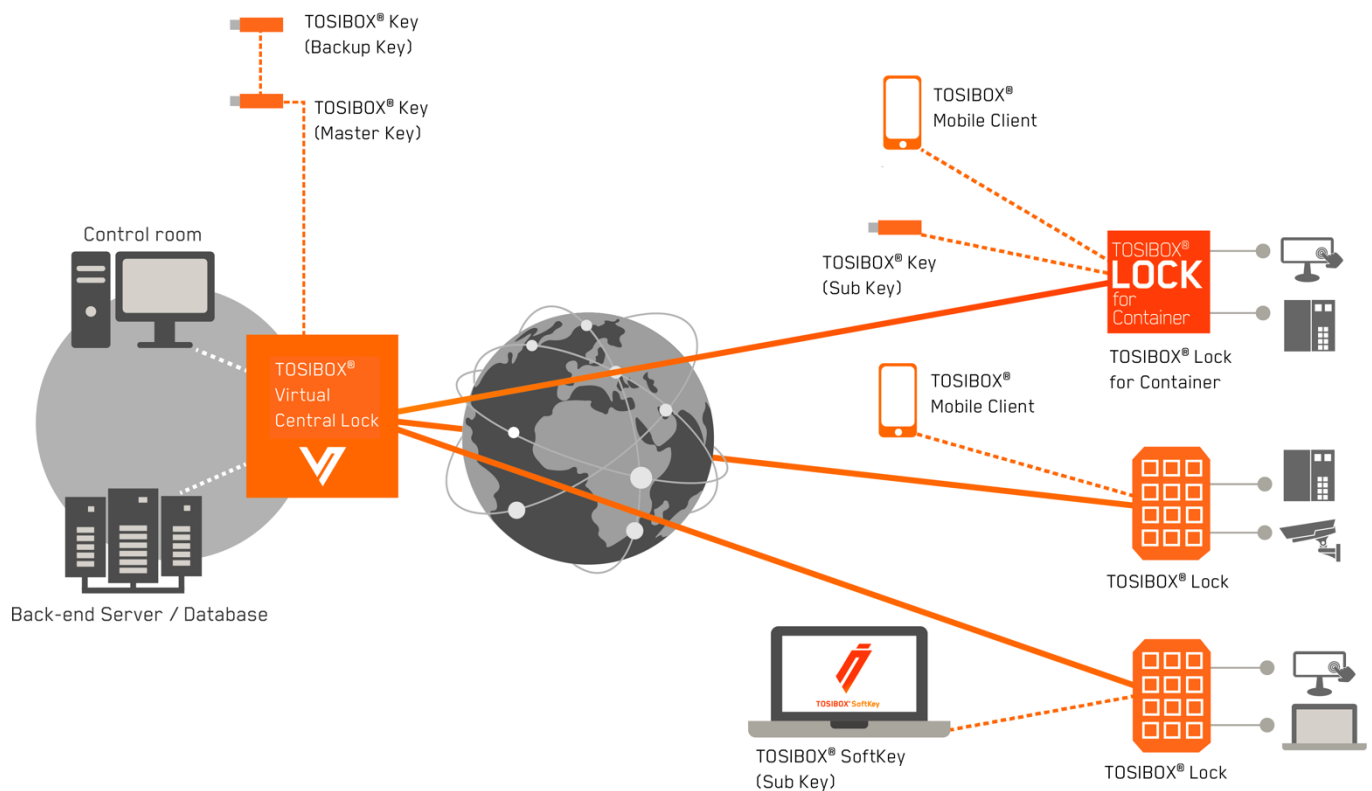
| | | |
|----|--------------------------------------|----|
| 1 | Introduction..... | 3 |
| 2 | System description..... | 5 |
| 3 | Docker fundamentals | 8 |
| 4 | Connectivity scenario examples | 9 |
| 5 | User interface | 12 |
| 6 | Licensing..... | 14 |
| 7 | Installation..... | 15 |
| 8 | Activation..... | 17 |
| 9 | Basic configuration..... | 20 |
| 10 | Uninstallation | 22 |
| 11 | System requirements..... | 22 |
| 12 | Troubleshooting | 23 |

1 Introduction

Congratulations for choosing the TOSIBOX® solution!

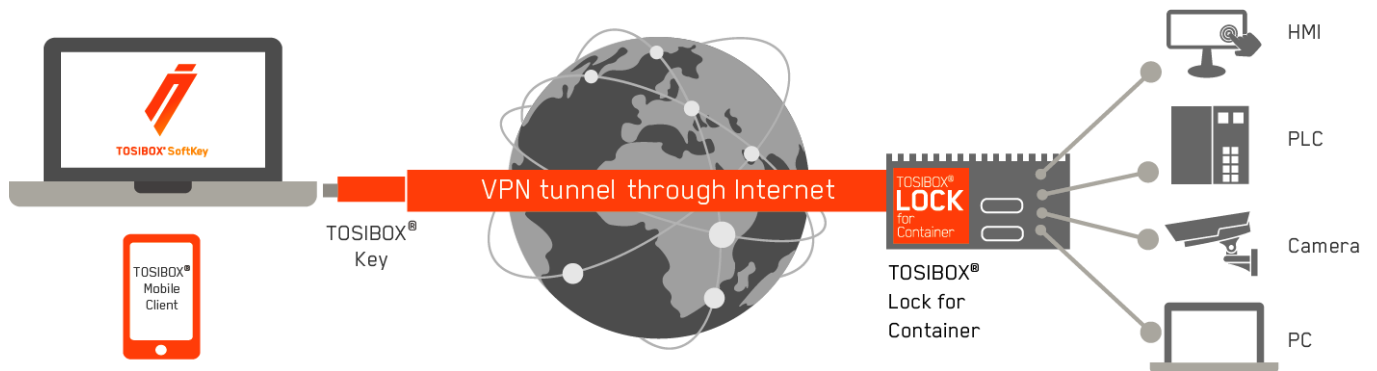
TOSIBOX® is globally audited, patented and performs at the highest security levels in the industry. The technology is based on two-factor authentication, automatic security updates and the latest encryption technology.

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 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



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 TOSIBOX® Lock for Container residing anywhere in the world, without a cloud in the middle.

TOSIBOX® Lock for Container can run on any IPC, HMI, PLC, controller or other device supporting Docker container technology. TOSIBOX® Lock for Container provides a 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 suitable for demanding and hazardous applications such as medical, marine, transport and oil industries. In these scenarios TOSIBOX® Lock for Container brings secure connectivity to hardware devices designed to meet demanding requirements.

TOSIBOX® Lock for Container is ideal for industrial IoT use cases where easy user access control complemented with ultimate security is needed.

2.2 TOSIBOX® Lock for Container in brief

TOSIBOX® Lock for Container is a software-only solution comparable to TOSIBOX® Lock hardware. It enables users to integrate IPCs, HMIs, PLCs, controllers or other devices 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, TOSIBOX® Lock for Container runs silently in the system background.

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 TOSIBOX® 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. TOSIBOX® 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, TOSIBOX® Lock for Container connects to the TOSIBOX® ecosystem and is ready to be taken in production use. TOSIBOX® Lock for Container user license can be transferred from one device to another. Transfer requires inactivating the license on a readily activated device and renewing the activation code.

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. TOSIBOX® Lock for Container installs cleanly on top of the Docker platform separating TOSIBOX® connectivity application from system software. TOSIBOX® 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 TOSIBOX® Lock for Container

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

| Feature | TOSIBOX® Lock (hardware) | TOSIBOX® Lock for Container |
|-----------------------------------|--|---|
| Operating environment | Hardware device | Software running on Docker |
| Internet connectivity | 4G, WLAN, ethernet | - |
| Layer 3 | ✓ | ✓ |
| Layer 2 (Sub Lock) | ✓ | - |
| 1:1 NAT | ✓ | - |
| LAN access | LAN access and device scanner for LAN network | LAN access, device scanner for Docker network |
| Matching | Physical and remote | Remote |
| Open firewall ports from internet | - | - |
| End-to-end VPN | ✓ | ✓ |
| SW auto-update | ✓ | ✓ |
| User access management | From TOSIBOX® Key Client or TOSIBOX® Virtual Central Lock software | Via TOSIBOX® Key Client or TOSIBOX® Virtual Central Lock software |

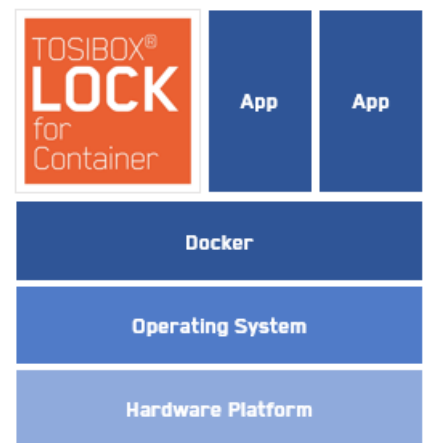
3 Docker fundamentals

3.1 Understanding Docker containers

A software container is the modern way of distributing applications. A container is a software package that runs on top of a 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 a 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 underlying device and creates a host-only network for the installed containers. TOSIBOX® 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 to TOSIBOX® Lock for Container.

Docker has a multitude of different network modes; bridge, host, overlay, macvlan or none. TOSIBOX® Lock for Container uses these modes for different connectivity scenarios.

4 Connectivity scenario examples

4.1 From TOSIBOX® Key Client to TOSIBOX® Lock for Container

Connectivity from TOSIBOX® Key Client to 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.



Figure 1: Connectivity from TOSIBOX® Key Client to the host device

4.2 From TOSIBOX® Key Client to the host device LAN via TOSIBOX® Lock for Container

Connectivity from TOSIBOX® Key Client to the IoT 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 IoT 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.



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

4.3 From TOSIBOX® Mobile Client to TOSIBOX® Lock for Container

Connectivity from TOSIBOX® Mobile Client to the host and the IoT devices connected to the host is a use case similar to the previous one. Connectivity between TOSIBOX® Mobile Client and TOSIBOX® Lock for Container allows to access all the host device services as long as the mobile device itself can support those.

This option is well suited for remote management of the host device and the LAN side for the mobile workforce.



Figure 3: Connectivity from TOSIBOX® Mobile Client to IoT devices behind TOSIBOX® Lock for Container

4.4 From TOSIBOX® Virtual Central Lock to the host device LAN via TOSIBOX® Lock for Container

The most flexible configuration is achieved when TOSIBOX® Virtual Central Lock is added in 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.

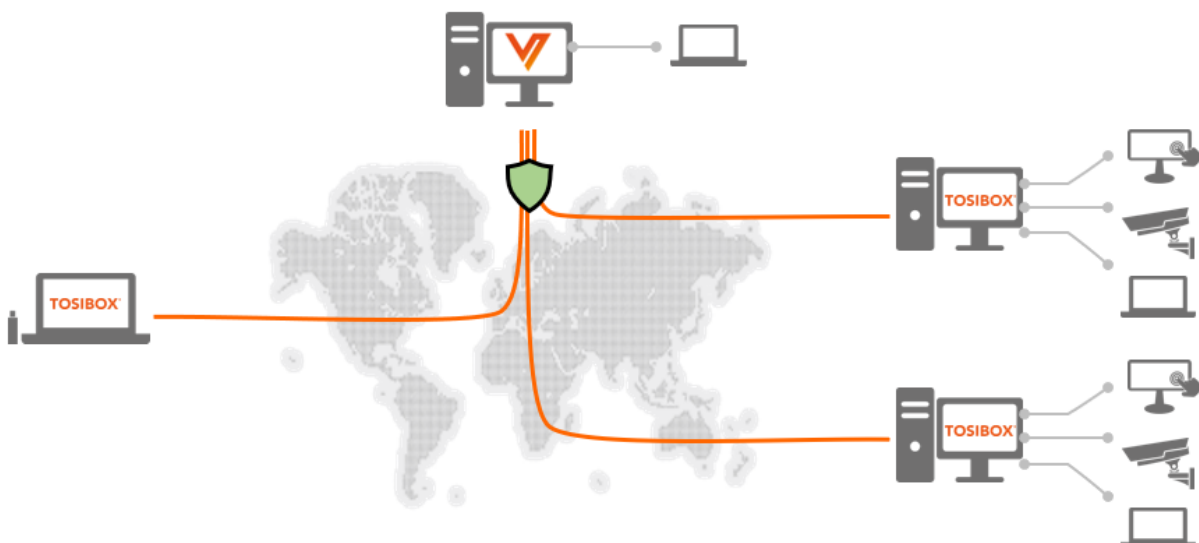


Figure 4: Connectivity from TOSIBOX® Key Client to IoT devices behind TOSIBOX® Lock for Container via TOSIBOX® Virtual Central Lock

4.5 From TOSIBOX® Key Client to Docker network on the host device

Connectivity from TOSIBOX® Key Client to the Docker network on the host device running TOSIBOX® Lock for Container is also possible. This connectivity scenario has the fundamental distinction that there is no connection to the actual device itself, just to the host-only Docker network where a large number of other Docker containers can exist.

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



Figure 5: Connectivity from TOSIBOX® Key Client to the Docker network on the host device

5 User interface

The TOSIBOX® web user interface screen is divided into four sections:

- A. Menu bar – Product name, menu commands and Login/Logout command
- B. Status area – System overview and general status
- C. TOSIBOX® devices – Locks and Keys related to the Lock for Container
- D. Network devices – Devices or other Docker containers discovered during network scan

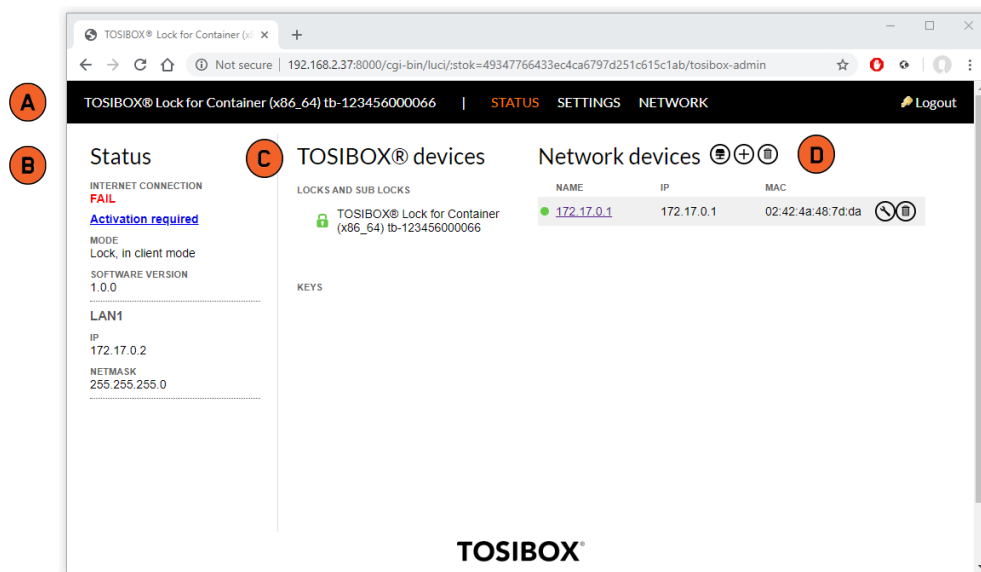


Figure 6: Lock for Container waiting for activation

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.

5.1 Navigating in the user interface

Login on the web user interface

To log in to the TOSIBOX® Lock for Container web user interface

- A) launch any web browser and type in the address `http://172.17.0.2` (presuming Lock for Container has been installed with default settings) or
- B) launch the software from TOSIBOX® Key Client by clicking the Login link on the menu bar and logging in with the default credentials:

- Username: admin
- Password: admin

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

Note: We strongly recommend changing the default password after the first login.

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, update the software 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. None of the settings related to Internet connectivity are available.

6 Licensing

6.1 Introduction

TOSIBOX® Lock for Container is installed on the host device acting as the endpoint for a VPN tunnel. The device can be any single workstation or controller, or for a local area networks, a network gateway. TOSIBOX® Lock for Container can be installed on any device running Docker platform.

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 an Activation Code from Tosibox sales. (www.tosibox.com/contact-us)

The installation of TOSIBOX® 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 Helpdesk for assistance (helpdesk.tosibox.com).

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

6.2 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. Transferring the license from one device to another requires a new license and a new Activation Code. Contact Tosibox Support if you have issues with the activation.

7 Installation

TOSIBOX® Lock for Container is installed with an installation script. The script is a plain text file that needs to be executed on the device where the Lock for Container is hosted. Docker must be installed prior to installing TOSIBOX® Lock for Container.

Installation steps

1. Download and install Docker free of charge, see www.docker.com.
2. Download TOSIBOX® Lock for Container installation script file to your device.
3. Install the Lock for Container by running the installation script.

7.1 Docker installation

Download and install Docker

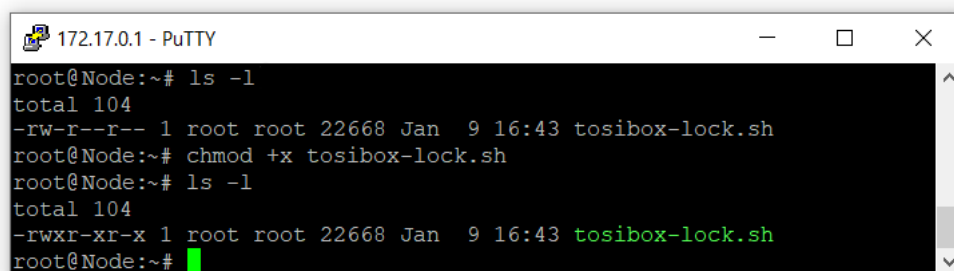
Docker is available for a wide variety of operating systems and devices. See www.docker.com for downloading and installing on your device.

7.2 Download the installation file

1. Open a web browser and navigate to www.tosibox.com/documentation-and-downloads/
2. Scroll down and look for “Download TOSIBOX® Lock for Container”. This is the Linux installation script file you need on your device.
3. Download the file on your desktop.

7.3 Copy the installation file to your device and change the file mode

1. Make sure you have the installation script file readily available. Copy the installation file to your IoT device, for example with SCP, FTP, using wget command or transfer on an SD card.
2. Verify the file: Execute `ls -l` on the command line and see if the file is executable. If the file is missing the executable property (last x in `-rwxr-xr-x`), change it with the `chmod` command.



```
172.17.0.1 - PuTTY
root@Node:~# ls -l
total 104
-rw-r--r-- 1 root root 22668 Jan  9 16:43 tosibox-lock.sh
root@Node:~# chmod +x tosibox-lock.sh
root@Node:~# ls -l
total 104
-rwxr-xr-x 1 root root 22668 Jan  9 16:43 tosibox-lock.sh
root@Node:~#
```

Figure 7: Example of changing file mode to executable on Linux

7.4 Install Lock for Container

TOSIBOX® Lock for Container is installed with the installation script file. The installation process walks through the steps and asks for relevant settings. Execute the script with the install parameter

```
./tosibox-lock-for-container-v1.sh install
```

Note that you will need Internet access during the installation process. The installation will download the needed software components.

8 Activation

TOSIBOX® Lock for Container must be activated before you can create secure remote connections.

8.1 Summary of activation steps

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 Virtual Central Lock

8.2 Open the Lock for Container web user interface

Open a web browser and type in the device IP address followed with port 8000:

http://←address→:8000

If TOSIBOX® Lock for Container is installed on the default IP address, the web user interface is accessible also at <http://172.17.0.2>

8.3 Activate TOSIBOX® 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.

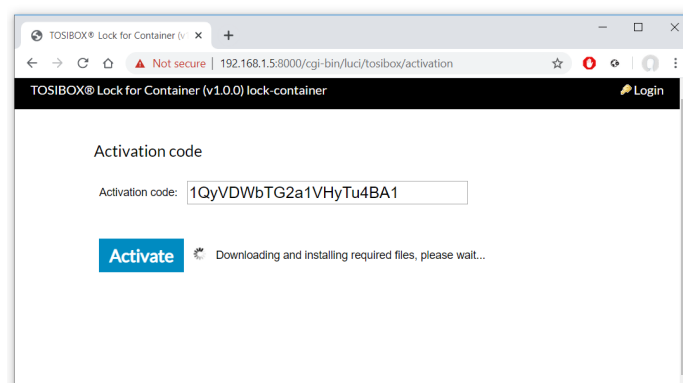


Figure 8: TOSIBOX® Lock for Container activation page

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.

8.4 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. Default credentials are

- Username: admin
- Password: admin

You must accept EULA before you can use TOSIBOX[®] Lock for Container.

8.5 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.

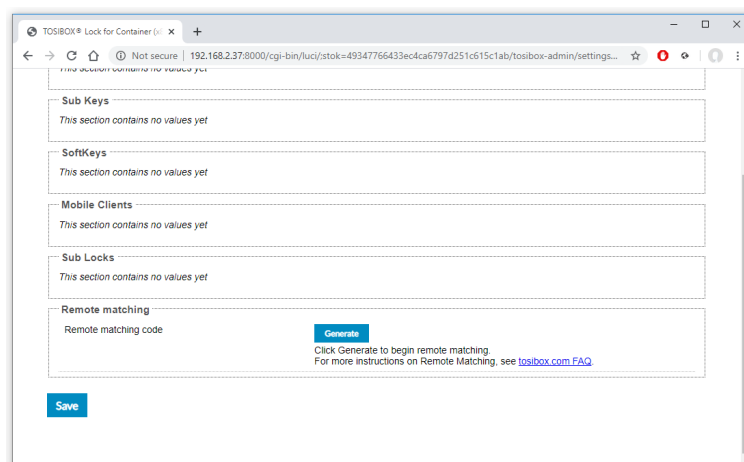


Figure 9: Remote Matching Code generation page

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.

8.6 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.

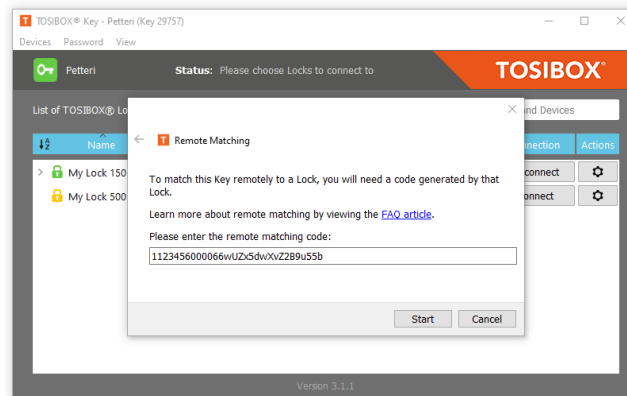


Figure 10: Remote Matching on TOSIBOX® Key Client

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.

8.7 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.

8.8 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.

9 Basic configuration

9.1 Generating Remote Matching code

Open the TOSIBOX® Lock for Container web user interface and log in as admin. Go to “Settings → Keys and Locks” and scroll down the page to find the Remote Matching section. Generate a new Remote Matching code by clicking the Generate button. If the button is not available, the Lock is already matched, and a new code cannot be generated now.

9.2 Change admin password

Open the TOSIBOX® Lock for Container web user interface and log in as admin. 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. 10.4.12.0)
- IPv4 Netmask: Mask according to subnetwork (e.g. 255.255.255.0)
- IPv4 Gateway: IP address of the gateway to the LAN network

Metric and MTU can be left as defaults.

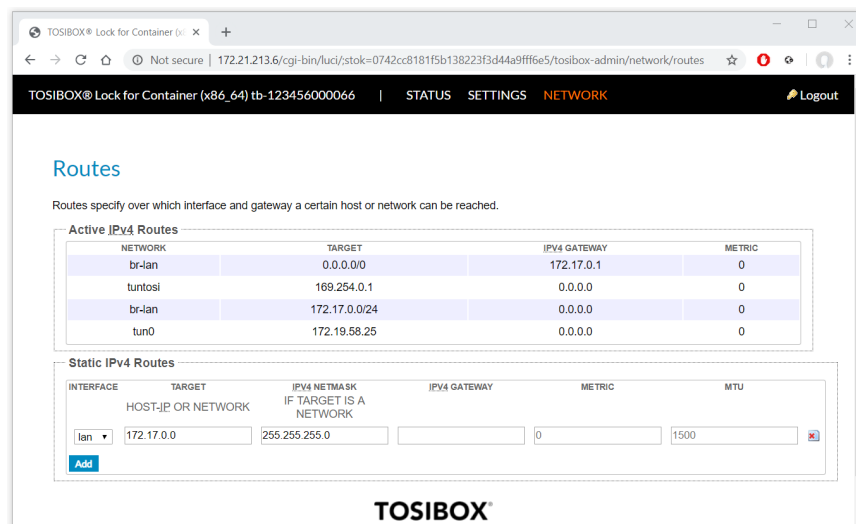


Figure 11: Static route

9.4 Changing a 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 <https://www.tosibox.com/documentation-and-downloads/> for the user manual.

10 Uninstallation

Uninstallation steps

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

11 System requirements

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

Recommended software requirements

- Any 64-bit Linux OS supported by Docker
- Docker Engine - Community v19 or later installed and running (www.docker.com)
- 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

12 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

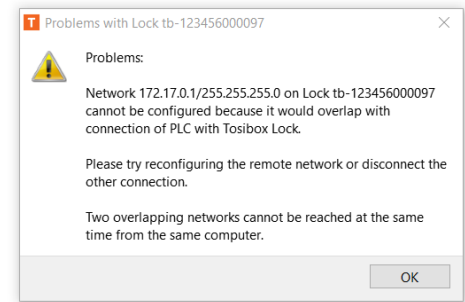
Issue: You are installing TOSIBOX® Lock for Container but at the end of the installation get an error “cannot exec in a stopped state: unknown” or similar.

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, .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 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 of the Lock for Container instances have been configured on the same IP address and reconfigure the address on either installation. To install a Lock for Container on a custom IP address, use the networking commands with the installation script.



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 utilisation 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.