CENTRAL LOCK & VIRTUAL CENTRAL LOCK

Table of contents

1. Introduction

The purpose of this document is to illustrate the deployment of TOSIBOX® Central Lock and TOSIBOX® Virtual Central Lock with their most important properties. The administration of Keys and the user interface for Central Lock and Virtual Central Lock are also covered.

Please note that this document concentrates only on the properties of Central Lock and Virtual Central Lock. The basics of Key and Lock products are explained in the Key and Lock user manual. The reader is expected to be familiar with the basics of the Lock and the Key, including the matching of the devices and operational principles.

Unless otherwise stated, any guidance or Central Lock later in this document applies also to Virtual Central Lock.

1.1. Central Lock in brief

The Central Lock operates on the same basic properties as the Lock, but has higher throughput and encryption capacity. This allows the building of large-scale systems that provide simultaneous access to thousands of Locks and Keys and the devices connected to them.

The Central Lock also has additional features not found in the Lock, but are usually needed in more complex network systems. These include:

- Collecting audit log data
- Monitoring and alert services to detect and notify the user about connection problems
- Support for VLANs (virtual LANs)
- Improved access rights management by using access groups

1.2. Virtual Central Lock in brief

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 an arbitrary number of 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.

TOSIBOX® Virtual Central Lock

2. System description

2.1. Overview

The Central Lock makes it possible to build a system consisting of large number of TOSIBOX® Locks and Keys. TOSIBOX® Central Lock is used when the number of users and remote locations is in their hundreds or thousands or when a centralised server software needs to communicate with the remote locations. Central Lock allows connecting up to 4000 serialized Locks and Keys simultaneously.

TOSIBOX® 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. With Virtual Central Lock 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. Main features

1. **Audit log data collection and connection monitoring.**
   The Central Lock collects log data about the events of connected Locks. This feature logs the events of the Central Lock itself and also the events of any connected Locks and Sub Locks. Log collection and monitoring can be enabled from the ***Settings → Advanced settings*** menu of both the Central Lock and the Locks that are expected to report events. Only Locks from which log data is desired should have the logging enabled.
2. **Connection monitoring and alerts.**
   The Central Lock can be set to send email alerts for connections being established and closed. The alerts can be set for any or all serialized Locks. Activating alerts does not require any additional services and can be done from the ***Settings → Alerts*** view.
3. **Virtual LANs (VLANs).**
   Central Lock can be configured to connect to existing VLANs via any of the physical LAN ports. Configuration is available from ***Network → VLANs*** tab.
4. **Access Groups.**
   Access groups allows the administrator to define access rights between the connected devices and networks. Configuration is done via ***Access Groups*** menu.

2.3. System components

The complete system consists of TOSIBOX® Locks and Keys that are matched to the Central Lock in a way that the system owner decides. The matching process for Locks and Keys is presented in the Key and Lock User Manual. Connecting a Lock to the Central Lock is carried out in the same way as when connecting two Locks together, except during the process the connection type is defined either as Layer 2 or Layer 3. The Layer 2 connection type is bridged one, which means that the Lock is essentially in the same network with the Central Lock's LAN port or VLAN that it is bridged to. A Layer 3 creates a routed connection where the Lock and the Central Lock have their own IP networks.

Every matched Key uses either a bridged (Layer 2) or a routed (Layer 3) connection type. 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 Central Lock is Layer 3. Additional Keys can be matched to the Central Lock the same way as they are to a Lock.

3. Web user interface

3.1. Login

You can log in to the product's web user interface with an Internet browser in the following ways:

- By using address http://172.17.17.17 when directly plugged into the service port (Central Lock only)
- Using the virtual machine's graphical console (Virtual Central Lock only)
- 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 (see about access groups later). 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 access level, admin, and the default password has been delivered or defined during the installation of the product.

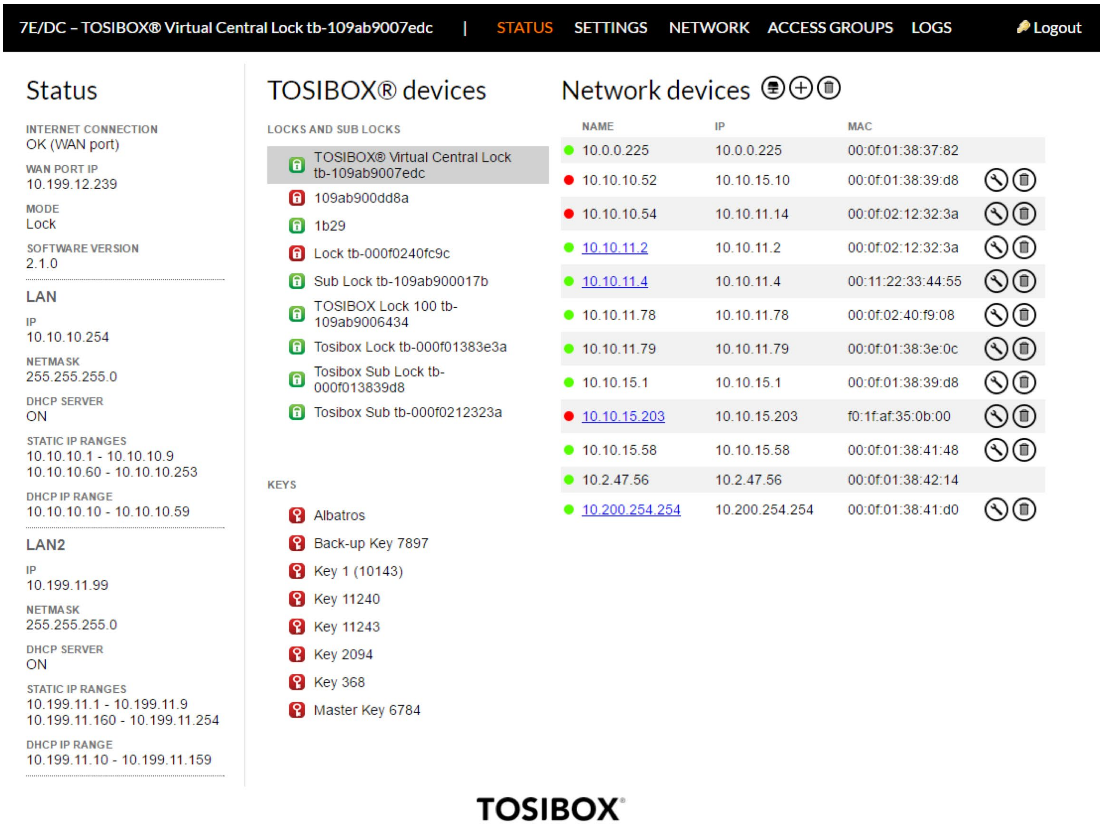
3.2. Status view

The Status view presents basic information about the network configuration, all matched Locks & Keys, and network devices.

New network devices can be added either

1. automatically by clicking the network icon 🖧 ("Scan for LAN devices"), which searches for all the devices within the LAN networks of the product
2. manually by clicking the plus icon ⊕ ("Add network device") and filling in the required details on the page that opens.

The network device list can be cleared by clicking trash can icon 🗑 ("Clear network device list").


7E/DC – TOSIBOX® Virtual Central Lock tb-109ab9007edc | STATUS SETTINGS NETWORK ACCESS GROUPS LOGS
Logout
TOSIBOX

Status

INTERNET CONNECTION
OK (WAN port)

WAN PORT IP
10.199.12.239

MODE
Lock

SOFTWARE VERSION
2.1.0

LAN

IP
10.10.10.254

NETMASK
255.255.255.0

DHCP SERVER
ON

STATIC IP RANGES
10.10.10.1 - 10.10.10.9
10.10.10.60 - 10.10.10.253

DHCP IP RANGE
10.10.10.10 - 10.10.10.59

LAN2

IP
10.199.11.99

NETMASK
255.255.255.0

DHCP SERVER
ON

STATIC IP RANGES
10.199.11.1 - 10.199.11.9
10.199.11.160 - 10.199.11.254

DHCP IP RANGE
10.199.11.10 - 10.199.11.159

TOSIBOX® devices

LOCKS AND SUB LOCKS

- TOSIBOX® Virtual Central Lock tb-109ab9007edc
- 109ab900dd8a
- 1b29
- Lock tb-000f0240fc9c
- Sub Lock tb-109ab900017b
- TOSIBOX Lock 100 tb-109ab9006434
- Tosibox Lock tb-000f01383e3a
- Tosibox Sub Lock tb-000f013839d8
- Tosibox Sub tb-000f0212323a

KEYS

- Albatros
- Back-up Key 7897
- Key 1 (10143)
- Key 11240
- Key 11243
- Key 2094
- Key 368
- Master Key 6784

Network devices 🖧 ⊕ 🗑

	NAME	IP	MAC
●	10.0.0.225	10.0.0.225	00:0f:01:38:37:82
●	10.10.10.52	10.10.15.10	00:0f:01:38:39:d8
●	10.10.10.54	10.10.11.14	00:0f:02:12:32:3a
●	10.10.11.2	10.10.11.2	00:0f:02:12:32:3a
●	10.10.11.4	10.10.11.4	00:11:22:33:44:55
●	10.10.11.78	10.10.11.78	00:0f:02:40:f9:08
●	10.10.11.79	10.10.11.79	00:0f:01:38:3e:0c
●	10.10.15.1	10.10.15.1	00:0f:01:38:39:d8
●	10.10.15.203	10.10.15.203	f0:1f:af:35:0b:00
●	10.10.15.58	10.10.15.58	00:0f:01:38:41:48
●	10.2.47.56	10.2.47.56	00:0f:01:38:42:14
●	10.200.254.254	10.200.254.254	00:0f:01:38:41:d0

3.3. Settings view

The *Settings* menu makes it possible to change properties for Keys and Locks, change the password of the admin account, restart the Central Lock, remove all matched Keys and Locks from the Central Lock, change the advanced settings, set email alerts and update the software.

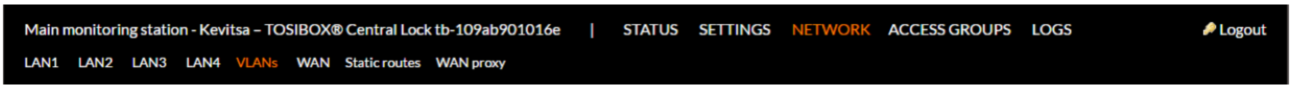
The advanced settings page allows the administrator to control

- automatic discovery of the LAN devices
- remote support access from Tosibox Technical Support
- logging settings
- VPN access from the Mobile Clients
- Force computers using the Key to route all Internet traffic through the Central Lock
- NTP service on Central Lock
- Cipher settings
- Central Lock timezone

3.4. Network view

The product's network settings can be edited in the *Network* menu. When using Central Lock, select the interface LAN1 to LAN4 or WAN to edit from the menu. A view will open that allows to set the IP address settings and DHCP settings for the interface in question. In Virtual Central Lock, all LAN and WAN interfaces are shown and can be edited from the *Interfaces* sub-menu. The *Static routes* view shows all active routes on the Central Lock and allows adding more static routes if necessary.

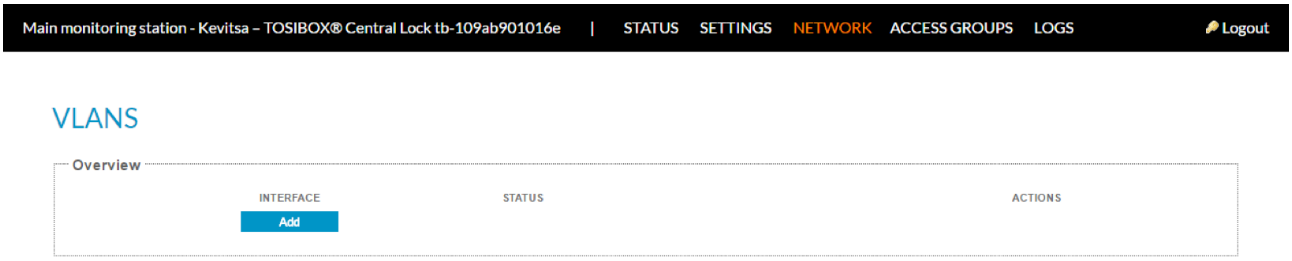
The *VLANs* sub-menu is used to manage virtual LANs. VLANs can be added to any of the product's LAN interfaces.



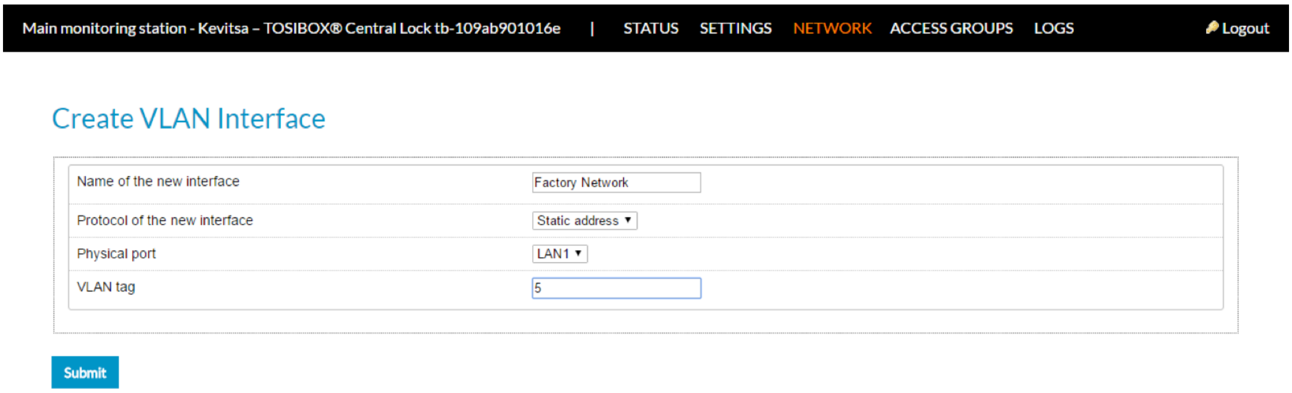
Adding a new virtual LAN

When the install location has different VLAN networks in use, this setting can be used to connect the Central Lock with these VLAN networks. Each VLAN is configured to work over one of the product's LAN interfaces – physical ethernet ports in case of Central Lock and virtual network adapters in case of Virtual Central Lock.

To add a new VLAN interface, open the *Network → VLANs* page and click *Add*



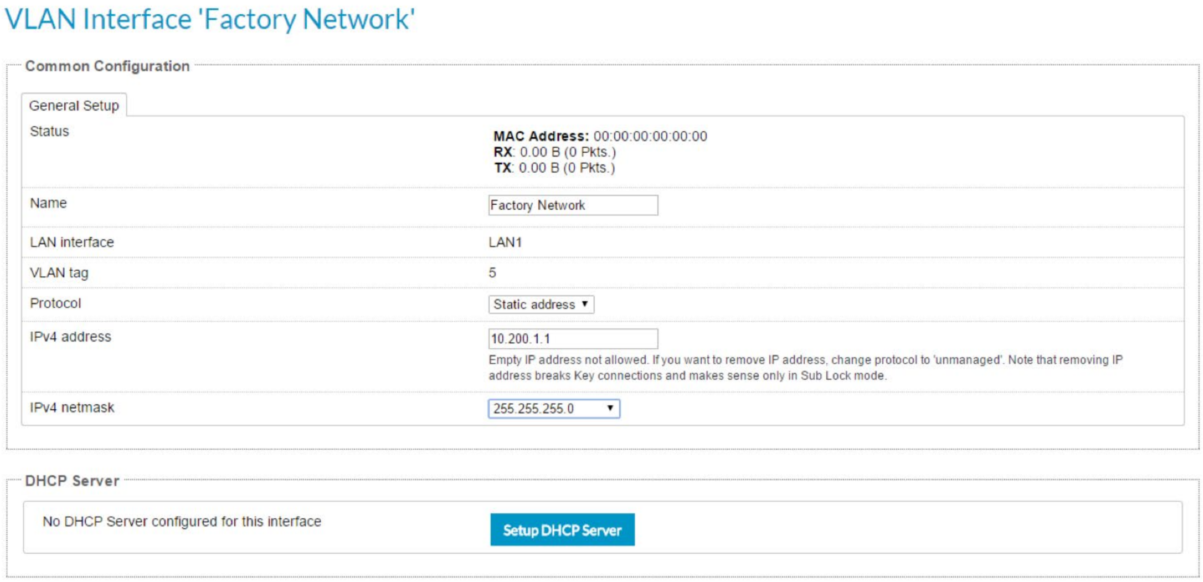
Then, set the interface name, select the physical LAN port and VLAN tag (an integer between 1 and 4094).


Main monitoring station - Kevitsa – TOSIBOX® Central Lock tb-109ab901016e
STATUS
SETTINGS
NETWORK
ACCESS GROUPS
LOGS
Logout
Create VLAN Interface

Name of the new interface	Factory Network
Protocol of the new interface	Static address ▾
Physical port	LAN1 ▾
VLAN tag	5

Finally, click *Submit*.

Next, set the IP address and netmask used by the Central Lock in this VLAN and define DHCP settings if needed.



VLAN Interface 'Factory Network'

Common Configuration

General Setup

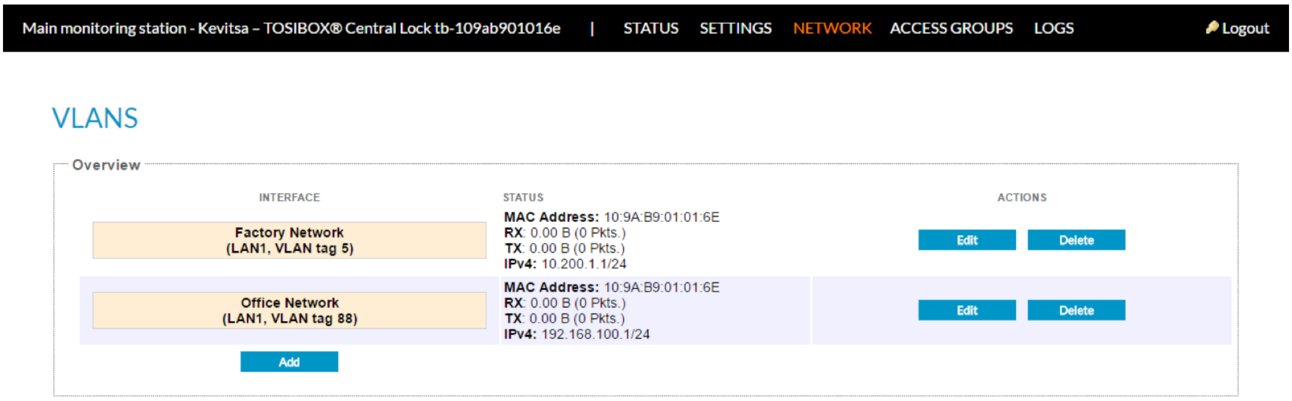
Status	**MAC Address:** 00:00:00:00:00:00 **RX**: 0.00 B (0 Pkts.) **TX**: 0.00 B (0 Pkts.)
Name	Factory Network
LAN interface	LAN1
VLAN tag	5
Protocol	Static address ▾
IPv4 address	10.200.1.1 Empty IP address not allowed. If you want to remove IP address, change protocol to 'unmanaged'. Note that removing IP address breaks Key connections and makes sense only in Sub Lock mode.
IPv4 netmask	255.255.255.0 ▾

DHCP Server

No DHCP Server configured for this interface

Finally, accept the settings by clicking on *Save* button down the page.

Now the *Network → VLANs* page summarizes the configured VLAN interfaces and their settings.



Main monitoring station - Kevitsa – TOSIBOX® Central Lock tb-109ab901016e

VLANS

Overview

INTERFACE	STATUS	ACTIONS
Factory Network (LAN1, VLAN tag 5)	**MAC Address:** 10:9A:B9:01:01:6E **RX**: 0.00 B (0 Pkts.) **TX**: 0.00 B (0 Pkts.) **IPv4:** 10.200.1.1/24	Edit Delete
Office Network (LAN1, VLAN tag 88)	**MAC Address:** 10:9A:B9:01:01:6E **RX**: 0.00 B (0 Pkts.) **TX**: 0.00 B (0 Pkts.) **IPv4:** 192.168.100.1/24	Edit Delete

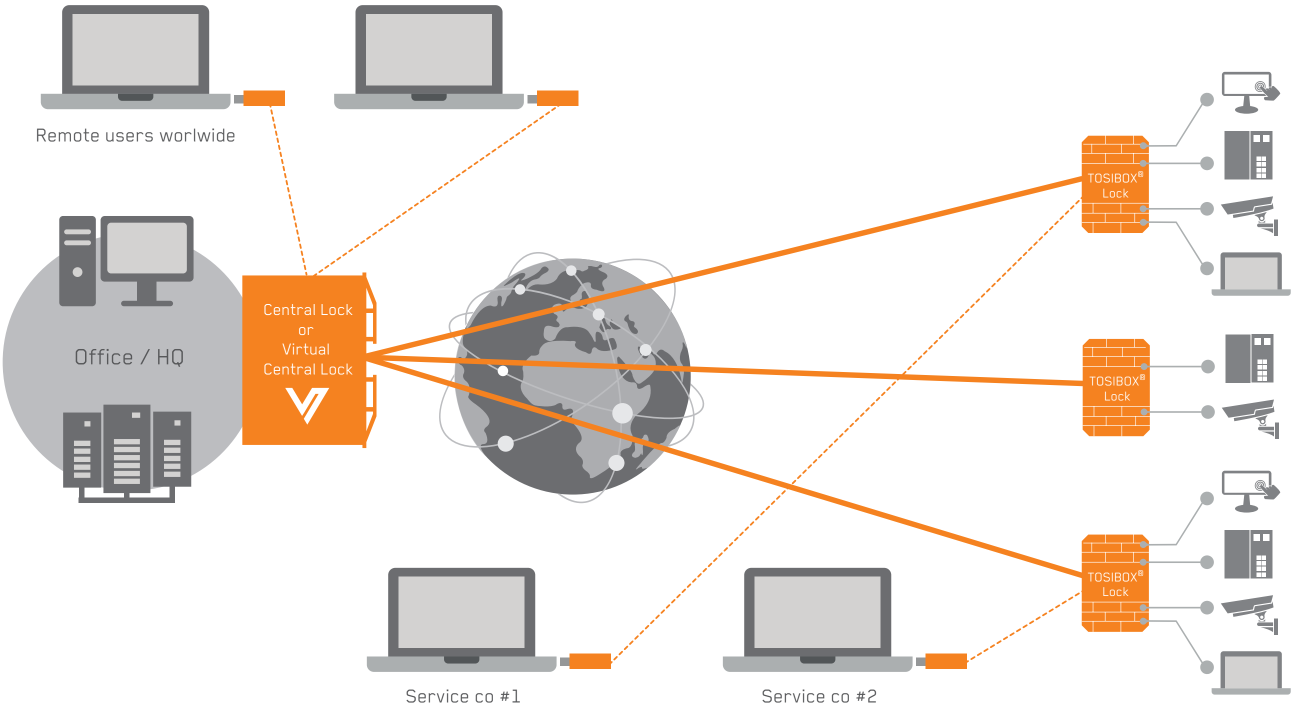
3.5. Access groups view

Access Groups menu allows the administrator to define access control between Keys and Locks already matched with the Central Lock, the Central Lock LANs or VLANs, IP address ranges or single IP address even on port and protocol level. See chapter 5 for detailed instructions on how to configure access groups in different scenarios.

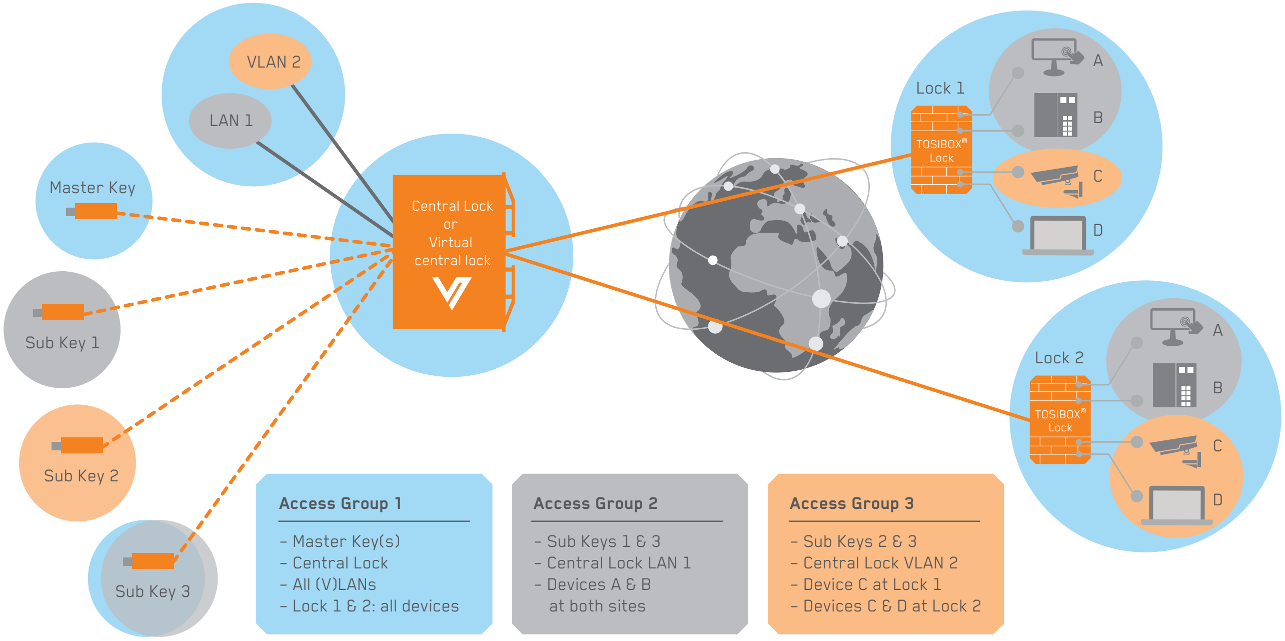
3.6. Logs view

Logs menu contains the log events from the Central Lock and Locks matched with it. Log events can be filtered by event type, text match and date. Logging is configured via Central Lock's *Settings → Advanced* settings view and from the same view of the matched Locks.

4. Use case examples



4.1 Basic access rights model



Access Group 1

- Master Key(s)
- Central Lock
- All (V)LANs
- Lock 1 & 2: all devices

Access Group 2

- Sub Keys 1 & 3
- Central Lock LAN 1
- Devices A & B at both sites

Access Group 3

- Sub Keys 2 & 3
- Central Lock VLAN 2
- Device C at Lock 1
- Devices C & D at Lock 2

4.2 Centralized access rights model

5. Access rights management

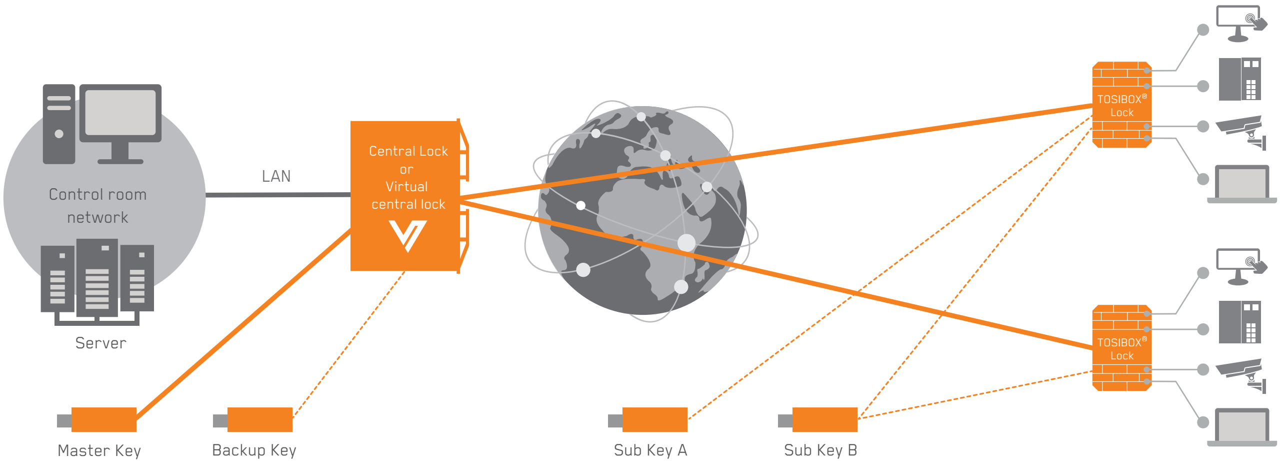
There are two different principal models for managing the access rights of a TOSIBOX® Central Lock and connected Locks, and those are called ***basic model*** and ***centralized model***.

In the basic model, the Sub Keys have direct access to Locks at remote locations. As a result, these connections are not routed via the Central Lock. When using direct Sub Key connections to Locks, the access rights are defined primarily at the level of individual Locks and this happens at the master Key user interface. If there is a need to define access rights to individual network devices behind a Lock, this is done on each Lock individually.

The centralized model enables an easy to use and versatile deployment of access rights management in one place. Access groups define access rights between group members which can be Keys, Locks, IP addresses or network ranges, or MAC addresses. Members of an access group can communicate freely, and members can belong to several different access groups. In this model the Sub Keys have access to the remote locations via the Central Lock and direct access to the Locks is not granted. For an example, please see the second figure in chapter 4.

5.1. Basic model

In the basic access rights model, the Central Lock can operate for instance as a data collection point, connection status log recorder or a connection supervisor. The Central Lock creates an always-on, bidirectional protected connection that enables for instance data collection and real-time direct service connections to the devices installed in the field.



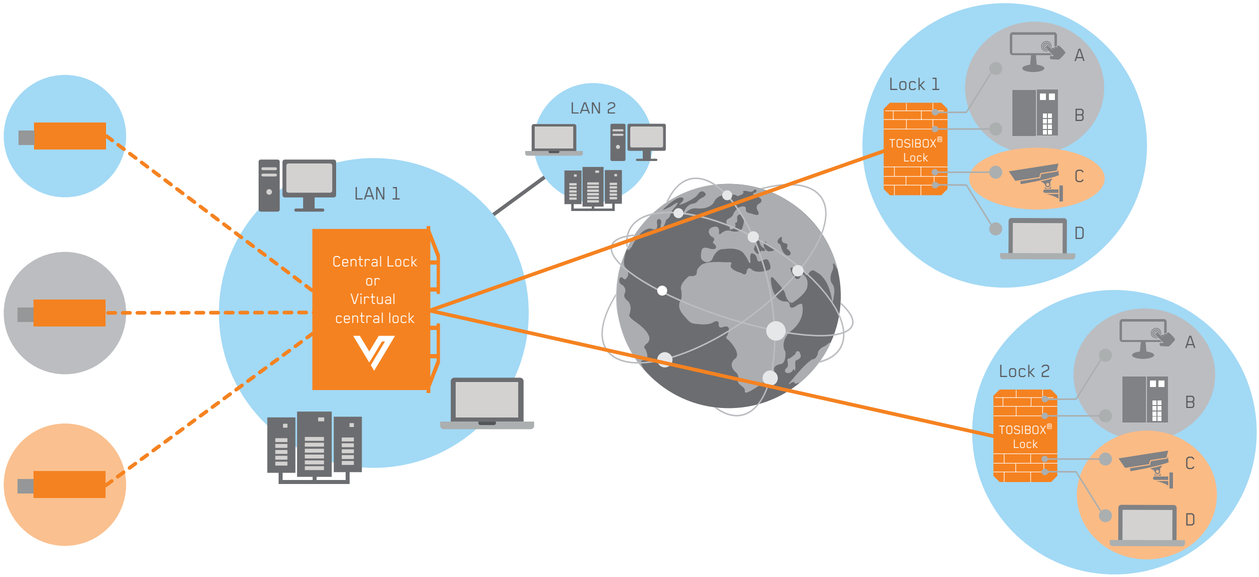
In the example above:

- The administrator has access to all remote locations via the company's local area network (LAN / Control room network)
- Master and Backup Key users have similar access rights with the administrator to the remote locations with their own Keys
- User of Sub Key A has access to one location and user of Sub Key B has access to two locations
- The server is connected to Central Lock via the internal network and protected from the Internet
- The server has access to the remote locations through the Central Lock and the encrypted VPN tunnels

5.2. Centralized model

In the Centralized model the Central Lock operates similarly to the basic access rights model with the addition that access groups are managed on the Central Lock and used to define access rights between group members. While providing the centralized access management this also means all connections to the remote locations are routed via the Central Lock and care must be taken to ensure an adequate bandwidth for the Internet connection.

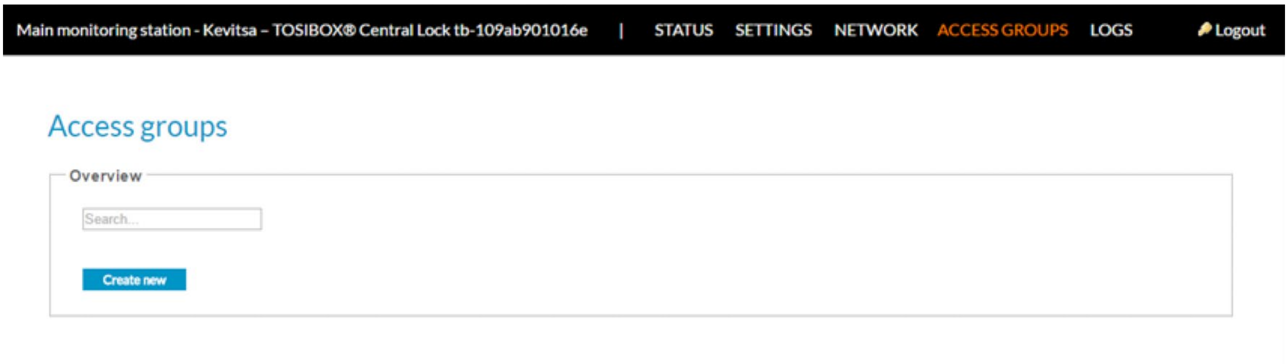
Access can be granted to Locks (Lock's LAN network), devices (IP addresses or ranges on Lock's network or on Central Lock LANs / VLANs) or devices with port and protocol restrictions, allowing protected, customer specific "server / field device / remote user" networks to be created, all of which are separated from each other.



The access rights are managed in the Central Lock web user interface from ***Access Groups*** menu. TOSIBOX® Keys and Locks, Central Lock LANs and VLANs or IP addresses are simply added to or removed from the desired access groups and the correct access rights to destinations are instantly deployed.

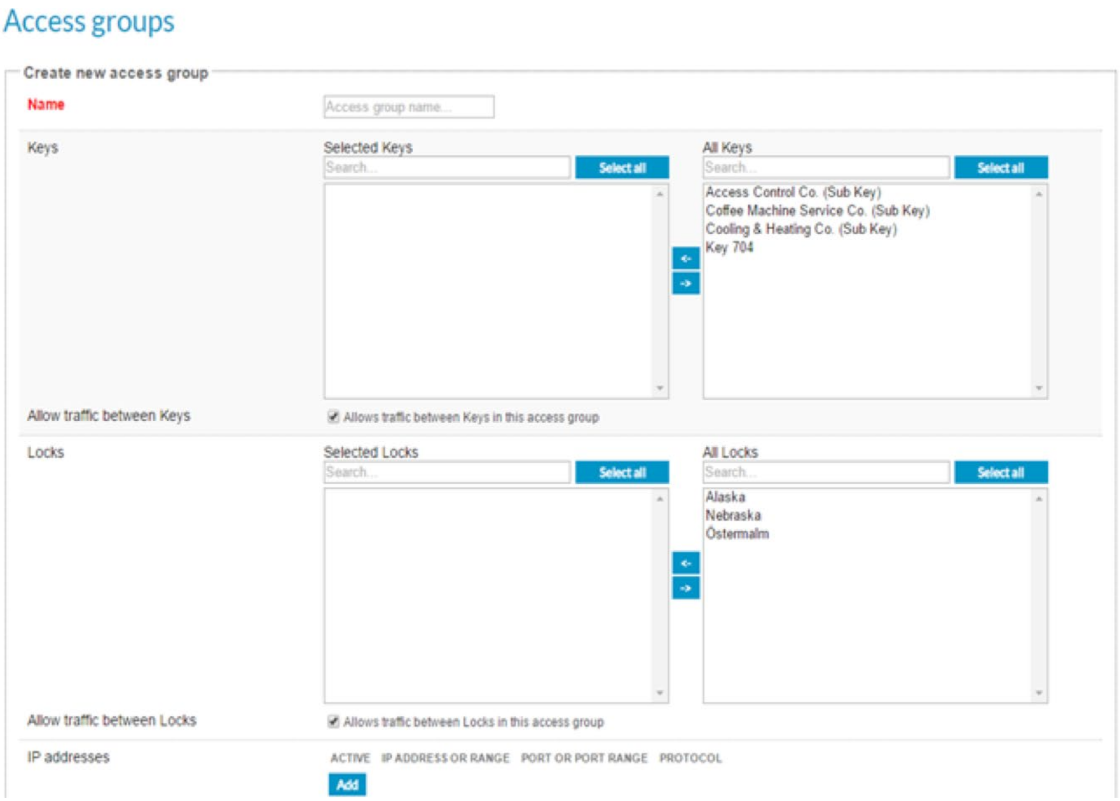
Adding an access group

Log in to the Central Lock using the admin credentials. Click on "Access Groups" on the menu bar.


Main monitoring station - Kevitsa – TOSIBOX® Central Lock tb-109ab901016e | STATUS SETTINGS NETWORK ACCESS GROUPS LOGS Logout
Access groups
Overview
Search...
Create new

Start creating an access group by clicking on "Create new".

The access group definition page is displayed. The selection boxes on the right hand side show all TOSIBOX® Keys and TOSIBOX® Locks that have already been matched with the Central Lock and thus available for adding to the access group.



Access groups

Create new access group

Name: Access group name...

Keys

Selected Keys

All Keys

Access Control Co. (Sub Key)
Coffee Machine Service Co. (Sub Key)
Cooling & Heating Co. (Sub Key)
Key 704

Allow traffic between Keys: ☑ Allows traffic between Keys in this access group

Locks

Selected Locks

All Locks

Alaska
Nebraska
Östermalm

Allow traffic between Locks: ☑ Allows traffic between Locks in this access group

IP addresses

ACTIVE	IP ADDRESS OR RANGE	PORT OR PORT RANGE	PROTOCOL

1. Give the access group a name.

2. Select the relevant TOSIBOX® Keys for this access group from the right hand side "All Keys" and move them to the box on the left hand side with the arrow button. You can also have access groups that do not involve any Keys.

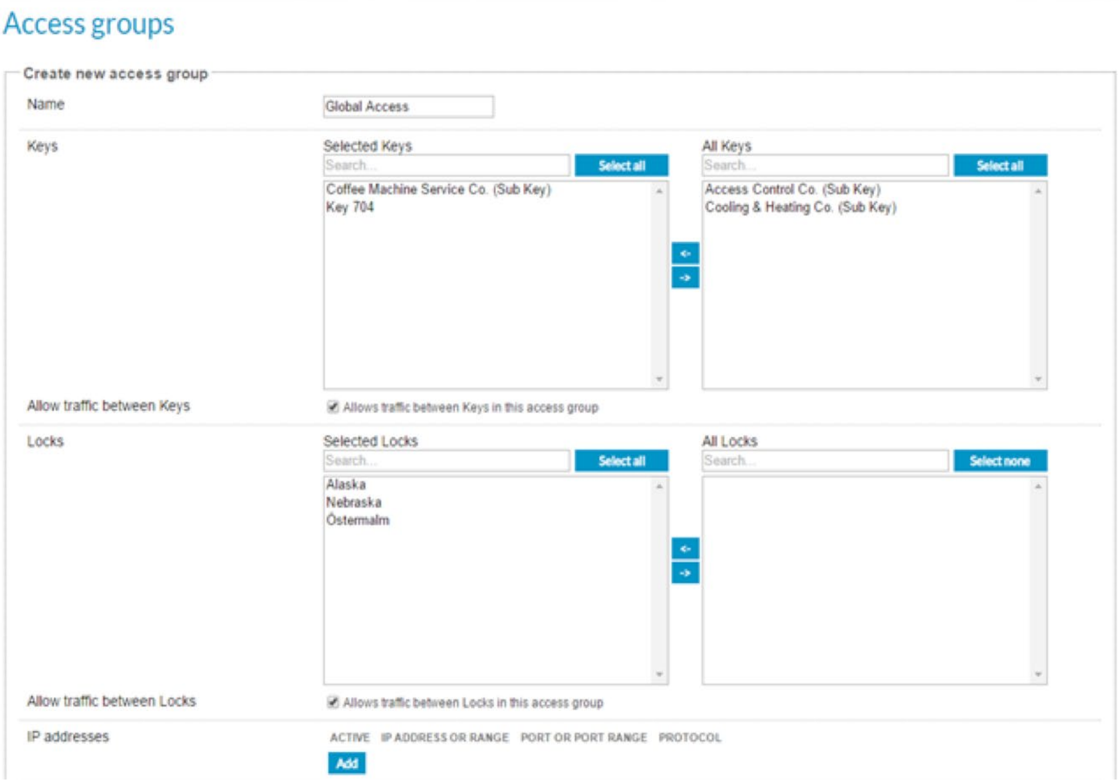
3. Select the relevant TOSIBOX® Locks for this access group from the right hand side "All Locks" box and move them to the left hand side box with the arrow button. This will grant access to all devices on selected Locks' networks. You can also have access groups that do not involve any Locks.

4. Define the Individual device IP addresses or IP address ranges into the "IP addresses" field. By defining IP addresses or IP address ranges, you only allow access to these IP addresses between the group members. If the IP addresses refer to networks behind a Lock, you do not have to select the Locks in question separately.

5. Add an interface (LAN or VLAN) that the group members have access to. By defining an interface, you will grant access for group members to all devices on that particular interface. See instructions on section 3.4 on adding a virtual LAN. You can also have access groups that do not involve any interface.

6. Save the settings with the "Save" button at the bottom of the page.

In the following image, the Keys "Key 704" and "Coffee Machine Service Co (Sub Key)" have access to all devices connected to TOSIBOX® Locks "Alaska", "Nebraska" and "Östermalm" as well as LAN1 on the Central Lock.



Access groups

Create new access group

Name: Global Access

Keys

Selected Keys: Coffee Machine Service Co. (Sub Key)
Key 704

All Keys: Access Control Co. (Sub Key)
Cooling & Heating Co. (Sub Key)

Allow traffic between Keys: ☑ Allows traffic between Keys in this access group

Locks

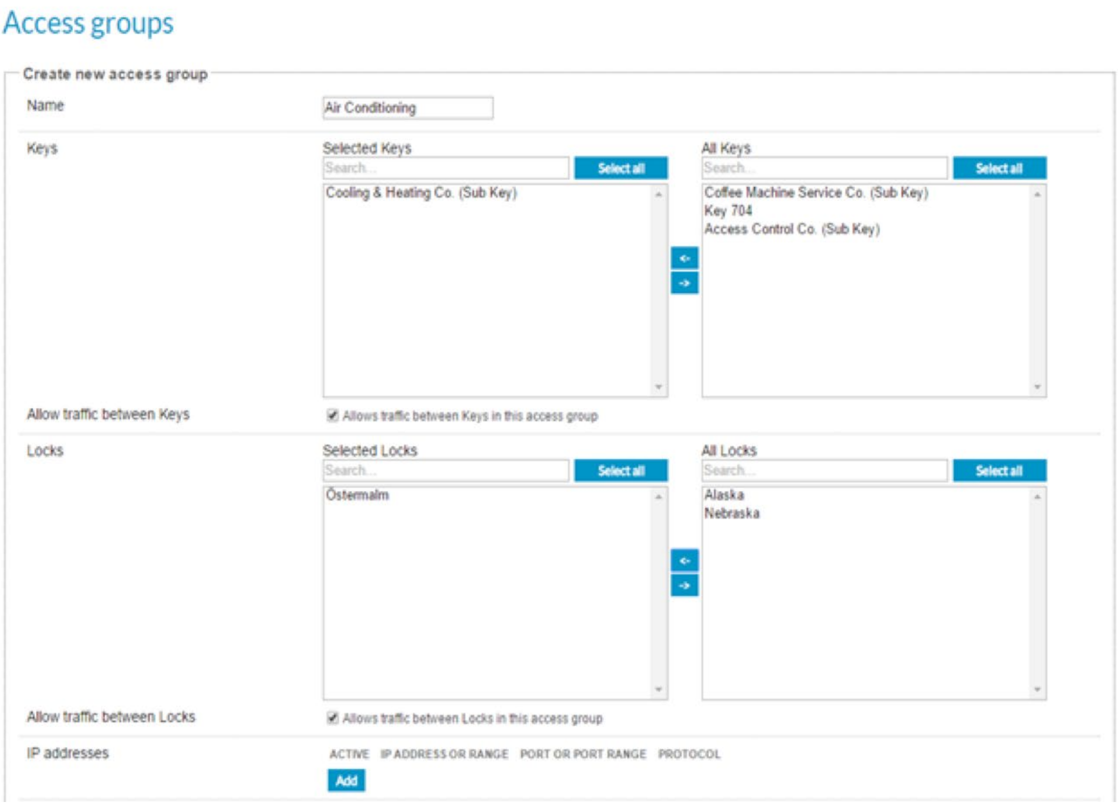
Selected Locks: Alaska
Nebraska
Östermalm

All Locks:

Allow traffic between Locks: ☑ Allows traffic between Locks in this access group

IP addresses: ACTIVE IP ADDRESS OR RANGE PORT OR PORT RANGE PROTOCOL

In the next image the Key "Cooling & Heating Co" has access to all devices connected to TOSIBOX® Lock named as "Östermalm"



Access groups

Create new access group

Name: Air Conditioning

Keys

Selected Keys: Cooling & Heating Co. (Sub Key)

All Keys: Coffee Machine Service Co. (Sub Key)
Key 704
Access Control Co. (Sub Key)

Allow traffic between Keys: ☑ Allows traffic between Keys in this access group

Locks

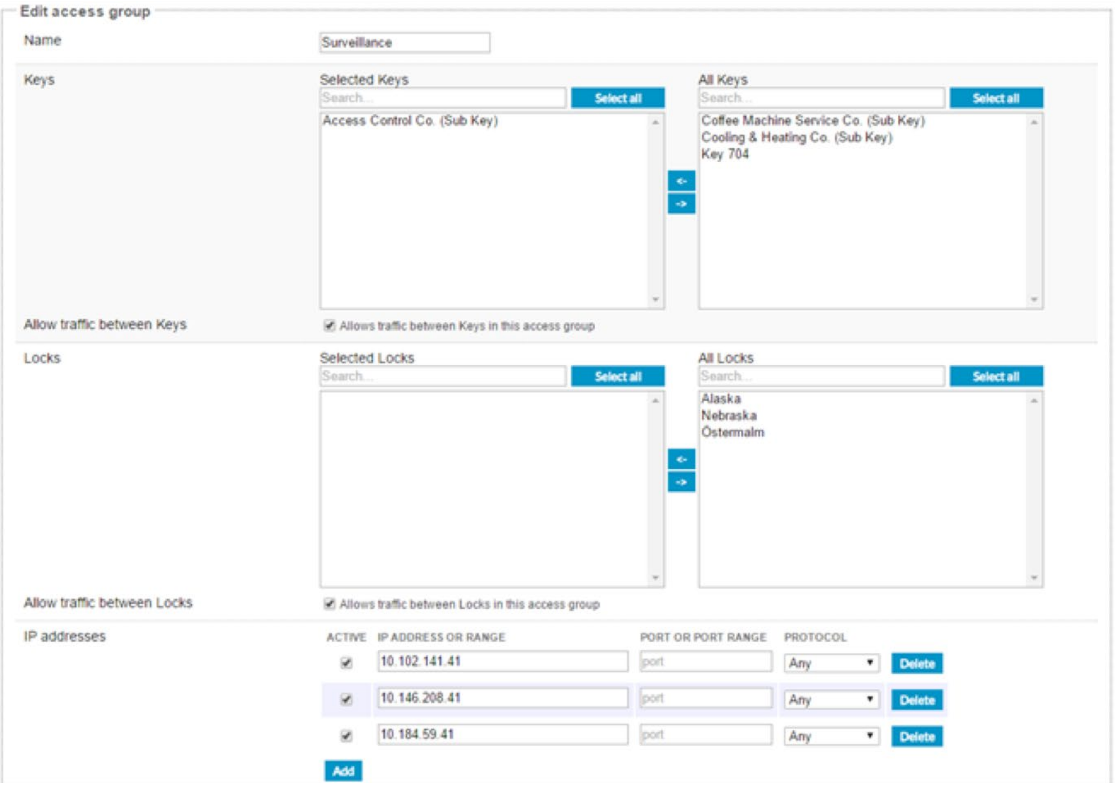
Selected Locks: Östermalm

All Locks: Alaska
Nebraska

Allow traffic between Locks: ☑ Allows traffic between Locks in this access group

IP addresses: ACTIVE IP ADDRESS OR RANGE PORT OR PORT RANGE PROTOCOL

In the next image the Sub Key for "Access Control Co" has access only to devices defined in IP addresses -fields. These devices can be connected to remote TOSIBOX® Locks or LANs or VLANs of the Central Lock.



Edit access group

Name: Surveillance

Keys

Selected Keys	All Keys
Access Control Co. (Sub Key)	Coffee Machine Service Co. (Sub Key) Cooling & Heating Co. (Sub Key) Key 704

Allow traffic between Keys: ☑ Allows traffic between Keys in this access group

Locks

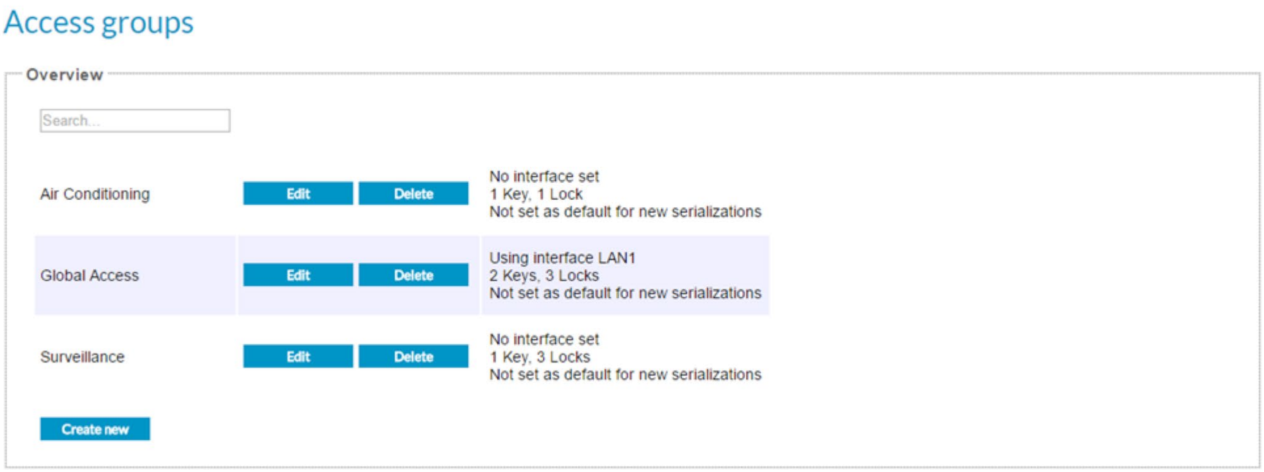
Selected Locks	All Locks
	Alaska Nebraska Östermalm

Allow traffic between Locks: ☑ Allows traffic between Locks in this access group

IP addresses

ACTIVE	IP ADDRESS OR RANGE	PORT OR PORT RANGE	PROTOCOL
☑	10.102.141.41	port	Any
☑	10.146.208.41	port	Any
☑	10.184.59.41	port	Any

After the access groups have been defined, the ***Access groups*** view shows the defined access rights groups and a summary of how many Keys and Locks are connected to them. More detailed information is available by clicking the "Edit" button of an access group.



Access groups

Overview

Air Conditioning	Edit Delete	No interface set 1 Key, 1 Lock Not set as default for new serializations
Global Access	Edit Delete	Using interface LAN1 2 Keys, 3 Locks Not set as default for new serializations
Surveillance	Edit Delete	No interface set 1 Key, 3 Locks Not set as default for new serializations

6. Technical data

6.1. Central Lock

Main features

- One 1 Gbit/s WAN port
- Four 1 Gbit/s LAN ports
- Over 700 Mbit/s encryption throughput
- 1000 concurrent remote connections per LAN network
- Encryption and authentication: PKI, 3072 bit RSA
- Data encryption: TLS, AES-256-CBC / AES-192-CBC / AES-128-CBC / Blowfish-128-CBC
- Mirrored hard disks (RAID 1)

Physical properties

- 1U (rack unit) for 19" rack cabinet (rack rails included)
- Length 570 mm / width 430 mm / height 43 mm
- Weight: 12.0 kg (incl. accessories)

Environmental conditions

- Operational temperature 10˚C … 30˚C
- Humidity 20% … 80% non-condensing
- Power consumption max 250 W
- Input voltage 90 … 264 V AC
- Input frequency 47 … 63 Hz

6.2. Virtual Central Lock

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

Technical requirements

- A supported virtualization platform based on one of the following:
    - VMWare ESXi 5.0 or greater
    - Microsoft Hyper-V
    - Linux KVM
- 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 non-firewalled public IP address
- At least 10/10 Mbit/s Internet connection

7. Legal notices

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 or by mail:
Tosibox Oy, Teknologiantie 12A, FIN-90590 OULU, SUOMI-FINLAND

Finland
sales@tosibox.com
support@tosibox.com
Sales, Finland Tel. +358 447090100
Sales, International Tel. +358 447090200
www.tosibox.com

TOSIBOX®
Plug & Go™ Connectivity