

# Guía Rápida Tosibox Config. Lock modo por defecto o modo cliente



Guía Tosibox

Config. Lock modo  
defecto o modo cliente

Versión manual: 1.1  
Fecha: 8/01/2015

www.elion.es

Servicio Asistencia Técnica  
Farell, 5  
08014 Barcelona  
Tel. 932 982 040  
soporte.tecnico@elion.es

 **elion**<sup>®</sup>

## 1. Alcance

Este documento describe los pasos necesarios a seguir para serializar una key a un Lock.

## 2. Glosario de términos

Se enumeran y describen los términos a los que se hará referencia posteriormente en este documento.

- Key (ver Fig.1)

Llave inteligente (microprocesador) con puerto USB para conectarse, que establece conexión con el Lock.

- Sub Key

Key accesoria que tiene limitados los derechos de usuario.

- Backup Key

Duplicado de la Key original. Todas las serializaciones y derechos de usuario son sincronizados automáticamente entre la *backup key* y la *key original*.

- Lock (ver Fig.2)

Dispositivo principal, con dos modos de funcionamiento. En **modo cliente**, el lock automáticamente busca dispositivos en la misma **red local** dónde está conectado. Es necesario acceder al software para activar este modo.

En **el modo por defecto** solo los dispositivos de red conectados directamente a los **puertos LAN** del Lock son accesibles. El *lock* crea su propia red local, distribuyendo automáticamente las direcciones IP. Admite conexiones mediante un cable de red al puerto WAN, conexión Wireless o insertando un router 3G compatible con tosiobox.

- DHCP-Server

Dispositivo de red que distribuye las direcciones IP a los otros dispositivos de la misma red.

- Serializado

Asignación de un código único para cada *key*.



Fig.1. Key



Fig.2. Lock

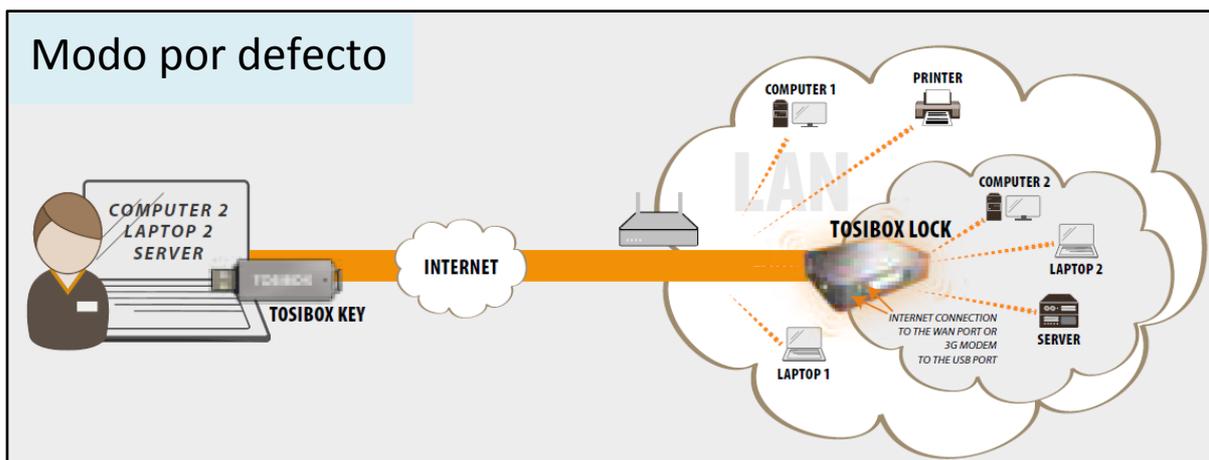


### 3. Modo de trabajo

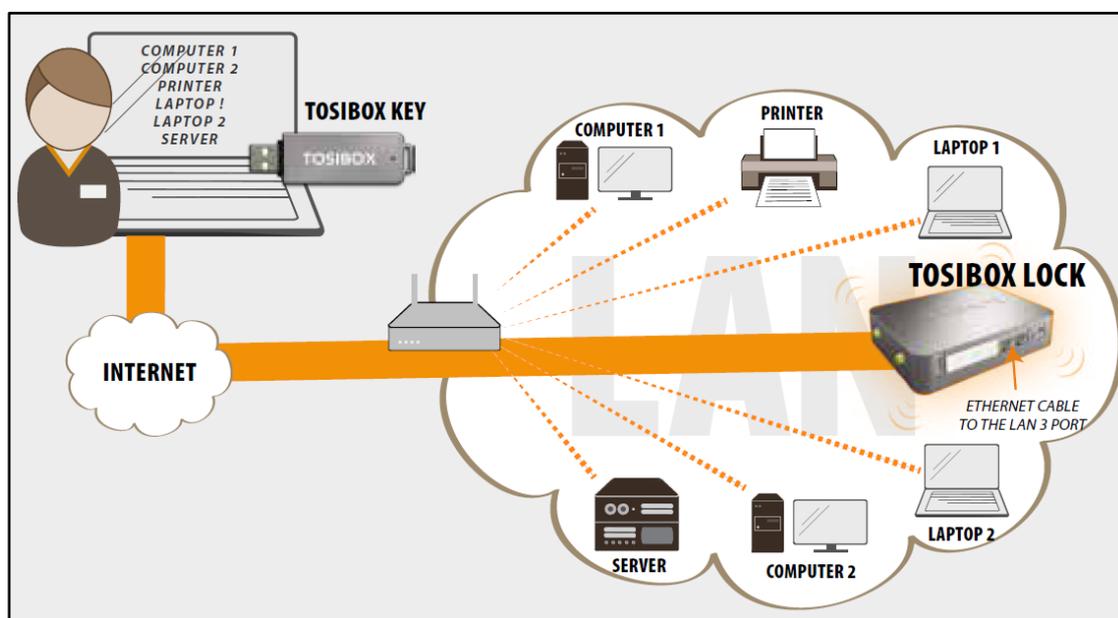
Existen dos modos de trabajo: el modo por defecto, y el modo cliente.

En el modo por defecto, el *lock* crea una red "privada", por lo que únicamente tenemos acceso a los dispositivos conectados al *lock*.

Para cambiar de modo por defecto a modo cliente, se requiere modificar ciertos parámetros en el software (ver punto 4.1).



En el modo cliente, la *key* tiene acceso a toda la red a la que el *lock* está conectada. Este modo de trabajo es denominado Plug&Go debido a la gran facilidad de puesta en marcha del sistema.



#### 4. Configuración del modo de trabajo por defecto

El *lock* creará automáticamente su propia red protegida, con los equipos que tiene conectados o mediante su propia red wireless.

En caso de conectar una red local que tiene su propio servidor DHCP, el *lock* desactivará su propia LAN.

En caso de querer cambiar del modo de trabajo por defecto al modo cliente, deberemos loguearnos como administrador en la interfaz del *Lock* (*ver guía primeros pasos*). El procedimiento se describe con detalle en el punto 5.1 .

##### 1.1 Utilizando equipos con IPs dinámicas

En caso de que todos los equipos tengan IPs dinámicas, se conectarán automáticamente al *lock*. En este caso la red LAN se creará en modo Plug&Go.

##### 1.2 Utilizando equipos con IPs estáticas

Conectar el PC al *lock* a través del puerto *Service*. Conectar con el *lock*. Escribiendo <http://service.tosibox> o "172.17.17.17" en el navegador. El nombre de usuario es *admin* y la contraseña está escrita en la parte inferior del *lock*.

Ir a *Network-> LAN*, y ver la IP del *lock* en el campo "IPv4 adress". Comprobar que la máscara de red está en 255.255.255.192 .

Ajustar la dirección IP de los equipos conectados al *lock* dentro del rango de IPs del *lock*. Por ejemplo, si el *lock* tiene dirección IP 10.25.15.193, asignaremos la IP 10.25.15.194 al primer equipo, 10.25.15.195 al segundo equipo, etc.

En los ajustes del *lock*, hacer click en *new network device* y escribir la dirección IP del equipo conectado (hacerlo por cada equipo conectado). También se puede utilizar la opción *Scan for LAN devices*, para buscar automáticamente otros dispositivos en el rango de IPs definidas por el *lock*.

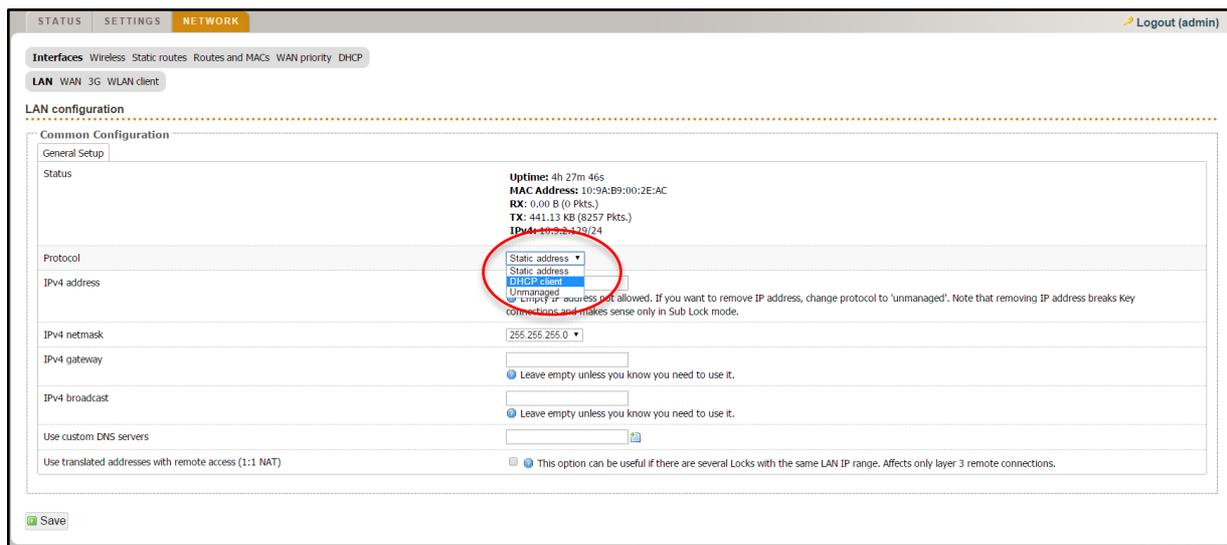


#### 4.1 Conmutar del modo por defecto al modo cliente.

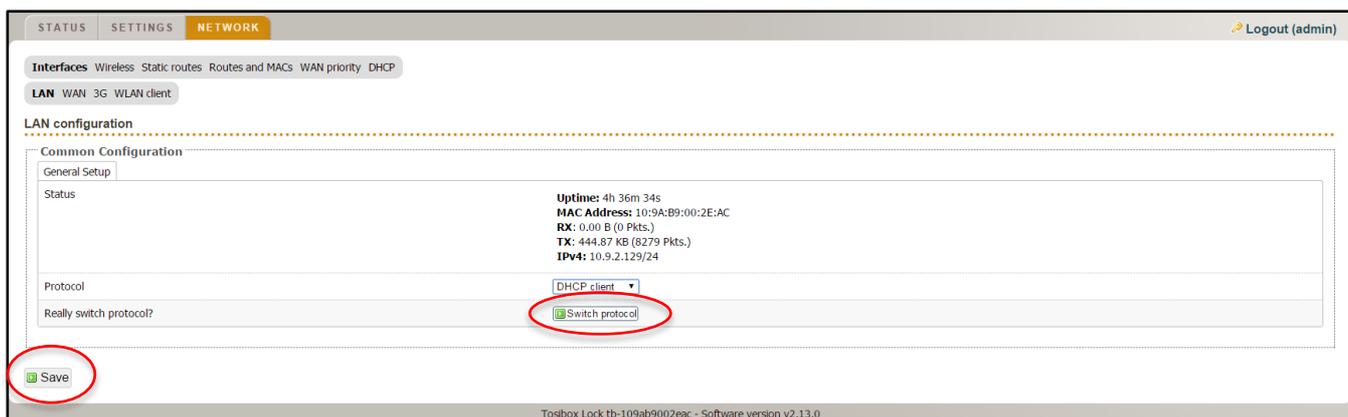
Para conmutar del modo de trabajo por defecto al modo cliente, será necesario abrir la ventana de configuración del *lock*, e identificarse como administrador.

Es **importante** recordar que para poder cambiar de modo de trabajo, el *lock* no podrá recibir conexión a través del puerto WAN ni wireless, ni estar conectado por los puertos LAN1-LAN2 (ya que se conmutaría automáticamente al modo de trabajo por defecto). Se deberá hacer de forma local mediante conexión al puerto *Service*.

Se debe ir a la pestaña *NETWORK*, y hacer click en *LAN*.  
Cambiaremos el protocolo a DHCP-Client



Y se hará click en *Switch protocol*, y posteriormente en *Save*.



Desde este momento el *lock* pasa al modo de trabajo cliente.



## 5. Configuración del modo de trabajo cliente

Con una *key* tendremos acceso a todos los dispositivos conectados a la red donde está conectado el *lock*.

En el *lock* solo se necesita alimentación y un cable ethernet conectado al puerto LAN3. La red local no necesita ser modificada. Este modo necesita un servidor DHCP (típicamente el router de la red) para asignar direcciones IP.

*Avisos:*

- No conectar internet al puerto WAN mediante cable o modem 3G al puerto USB, hacer esto commutará el modo de trabajo al modo B de forma automática.
- No conectar dispositivos al puerto LAN (excepto LAN3).
- El usuario de la *key* tiene acceso a **todos** los dispositivos de la red. Esto podría ser no recomendable si se quieren restringir accesos a dispositivos conectados.
- En caso de necesitar restringir el acceso, se podría hacer mediante filtrado de MACs o mediante el modo de trabajo por defecto.

### 5.1 Filtrado de MACs

Se describe a continuación el procedimiento para realizar un filtrado de MACs.

Dentro de la pestaña *SETTINGS->Industry settings*. En el subgrupo *LAN Access settings*, está ubicada la opción *Limit LAN traffic to certain MAC or IP addresses*.

The screenshot shows the 'Industry settings' page in a web interface. The 'LAN access settings' section is expanded, and the option 'Limit LAN traffic to certain MAC or IP addresses' is highlighted with a red circle. The description for this option is also circled in red: 'Prevents access to all LAN devices, with the following exceptions:'. Other options in the 'LAN access settings' section include 'Prevent traffic between Sub Locks', 'Allow VLAN 0 pass-through', and 'Source NAT IP traffic from L3 Central Locks towards LAN'. The 'Advanced settings' section is also visible at the bottom.

Al hacer click en casilla correspondiente, se abrirá un campo donde se podrá introducir la dirección MAC, así como la dirección IP a las que se quiere permitir el acceso.

LAN access settings	
Prevent traffic between Sub Locks	<input type="checkbox"/> Devices behind a Sub Lock cannot access devices behind other Sub Locks.
Limit LAN traffic to certain MAC or IP addresses	<input checked="" type="checkbox"/> Prevents access to all LAN devices, with the following exceptions.
List of allowed MAC addresses	<input type="text" value="3F-51-4J-36-DF-94"/>
List of allowed IP addresses	<input type="text"/>
Allow VLAN 0 pass-through	<input type="checkbox"/> Some devices require this for proper Layer 2 (Ethernet) communication, e.g. PROFINET messages with Siemens SIMATIC S7.
Source NAT IP traffic from L3 Central Locks towards LAN	<input checked="" type="checkbox"/> Allows return traffic from LAN towards Layer 3 serialized Central Locks to work even if the devices do not have correct default gateway or routes. Usually enabling this setting provides best compatibility.

Una vez se ha introducido la dirección MAC correspondiente, se hará click en **SAVE** para guardar los cambios.

LAN access settings	
Prevent traffic between Sub Locks	<input type="checkbox"/> Devices behind a Sub Lock cannot access devices behind other Sub Locks.
Limit LAN traffic to certain MAC or IP addresses	<input checked="" type="checkbox"/> Prevents access to all LAN devices, with the following exceptions.
List of allowed MAC addresses	<input type="text" value="3F-51-4J-36-DF-94"/>
List of allowed IP addresses	<input type="text"/>
Allow VLAN 0 pass-through	<input type="checkbox"/> Some devices require this for proper Layer 2 (Ethernet) communication, e.g. PROFINET messages with Siemens SIMATIC S7.
Source NAT IP traffic from L3 Central Locks towards LAN	<input checked="" type="checkbox"/> Allows return traffic from LAN towards Layer 3 serialized Central Locks to work even if the devices do not have correct default gateway or routes. Usually enabling this setting provides best compatibility.

Advanced settings	
Relay Tosibox Key users' Internet access through Lock	<input type="checkbox"/> A computer with Tosibox Key will access Internet using the Lock.
IP addresses to be accessible through Lock's WAN, WLAN or 3G connection	<input type="text"/>
<small>For example, if you have a server behind WAN connection, but don't want to relay Internet connection through Lock, you can use this to route only specific hosts through Lock. Only works for Layer 3 Key connections, you need to change Key to Layer 3 mode from Status -&gt; Edit Connections.</small>	

Desde este momento se ha configurado correctamente el filtrado de direcciones MAC, por lo que dispositivos con una MAC distinta a las autorizadas no podrán ser conectados al *lock*.





**ELION, S.A.**

Farell, 5  
08014 Barcelona  
Tel. 932 982 000  
Fax 934 311 800  
elion@elion.es  
www.elion.es

**DELEGACIONES:**

**Cataluña:**

Farell, 5  
08014 Barcelona  
Tel. 932 982 000  
Fax 934 311 800  
elion@elion.es

**Norte:**

Avda. Ategorrieta, 9-4ª Derecha  
20013 San Sebastián  
Tel. 943 292 795  
Fax 934 326 515  
aayala@elion.es

**Centro:**

Avda. Burgos, 28-8ªB  
28033 Madrid  
Tel. 913 835 709  
Fax 913 835 710  
elionmad@elion.es

**Sur:**

Urb. La Cierva, c/ Lince, 14  
41510 Mairena del Alcor - Sevilla  
Tel. 955 943 441  
Fax 955 745 861  
egiraldez@elion.es

**Servicio Asistencia Técnica**

Farell, 5  
08014 Barcelona  
Tel. 932 982 040  
soporte.tecnico@elion.es

**DISTRIBUIDORES EN TODA ESPAÑA**

