

TOSIBOX[®]

Bedienungsanleitung v2.10

Copyright © Tosibox Oy 2014

Inhaltsverzeichnis

Tosibox Übersicht	3
Lock-Verbindungen	4
Tosibox Glossar	5
Tosibox Produkte und Zubehör	6
Key-Benutzeroberfläche	7
Lock-Benutzeroberfläche	8
Personalisierung von Tosibox Key und Lock	9
Lock verwenden	11
Key verwenden	15
Geräte umbenennen und verwenden	17
Mehrere Keys	18
Personalisierung von zusätzlichen	21
Keys aus der Ferne	
Einen Backup-Key erstellen	22
Verwenden des Mobile Clients	24
Locks verbinden	28
Am Lock anmelden	30
Software aktualisieren	32
3G-Modem für den Lock	32
Key-Verbindungseinstellungen für den Lock	32
Industrieeinstellungen für den Lock	33
Drahtloseinstellungen für den Lock	34
Prioritäten der Internetverbindungen	35
PUK-Code für den Key	36
Problemlösung	37
Wartungsanweisungen	38
Technische Daten für den Lock	39
Technische Daten für den Key	40
Tosibox Lizenzen	41
Konformitätserklärung	42

Tosibox Übersicht

Tosibox bietet eine neue, automatisierte Möglichkeit zur einfachen, schnellen und sicheren Herstellung einer Fernverbindung. Tosibox ist weltweit die einzige Fernwartungslösung mit Plug & Go Technologie. Zur Verwendung benötigen Sie lediglich eine Steckdose und eine Internetverbindung. Die Arbeitsweise von Tosibox ähnelt der eines physikalischen Schlosses und Schlüssels.

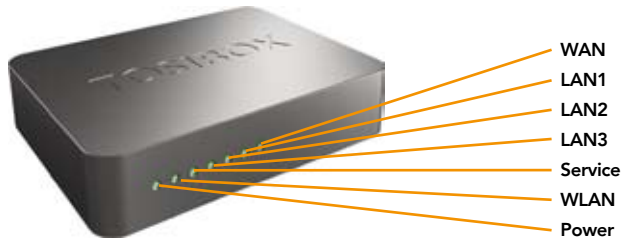
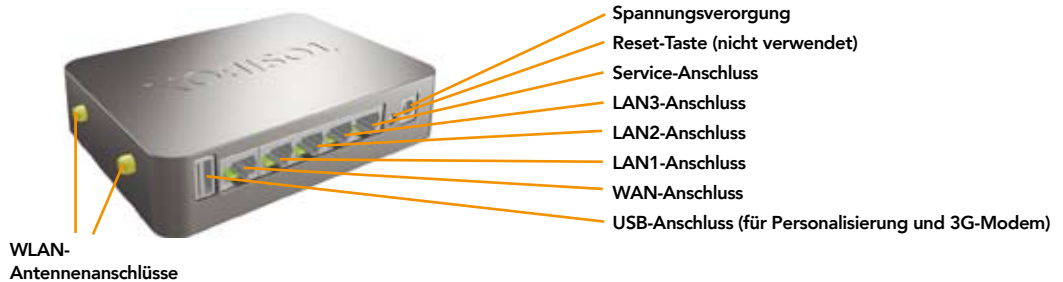
Die Tosibox Lösung besteht aus einem Schlüsselgerät (Key) und einem Schlossgerät (Lock). Die Lösung funktioniert durch physikalische Personalisierung des Keys über den USB-Anschluss des Locks. Zwischen einem Lock und seinen personalisierten Key(s) wird eine verschlüsselte Verbindung hergestellt und dem Nutzer Ansicht und Steuerung der mit dem Lock verbundenen Geräte ermöglicht.

Tosibox Locks und Keys, die miteinander personalisiert wurden, finden sich gegenseitig über das Internet und in separaten lokalen Netzwerken – unabhängig davon, wie sie mit dem Internet verbunden sind. Dies ermöglicht die Steuerung von Netzwerkgeräten im LAN-Netzwerk des Locks.

Diese Bedienungsanleitung gilt für die Lock-Softwareversion 2.11 und die Key-Softwareversion 2.11. Falls neuere Softwareversionen verwendet werden, laden Sie die aktuellste Bedienungsanleitung von der nachstehenden Tosibox Website herunter:

www.tosibox.com/manual

Lock-Verbindungen



Tosibox Glossar

Key = Ein intelligentes USB-basierendes Gerät, das einen sicheren Kryptoprozessor enthält. Der Key kann zum Herstellen einer sicheren Verbindung mit dem Lock verwendet werden.

Sub Key = Ein zusätzlicher Key mit beschränkten Zugangsrechten.

Backup Key = Ein Duplikat des Haupt-Keys. Alle Personalisierungen und Rechte werden automatisch zwischen dem Original- und dem Backup-Key synchronisiert.

Lock = Ein Gerät, das externe Verbindungen von personalisierten Keys akzeptiert und privaten und sicheren Zugriff auf verbundene Netzwerkgeräte schafft. Die Netzwerkgeräte, die mit den LAN-Anschlüsse des Locks verbunden sind, werden automatisch gefunden. Der Lock kann automatisch IP-Adressen für die mit dem LAN-Anschluss des Locks verbundenen Keys, Sub-Keys und Netzwerkgeräte verteilen. Der Lock kann zudem Netzwerkgeräte mit festen IP-Adressen steuern.

Sub Lock = Ein Lock, das in den Sub-Lock-Betriebsmodus gesetzt wurde. Wenn Sie zwei Locks miteinander verbinden, muss sich eines davon im Sub-Lock-Betriebsmodus befinden.

DHCP-Server = Ein Netzwerkgerät oder Software, die IP-Adressen an andere Geräte in einem Netzwerk verteilt.

Tosibox Produkte und Zubehör



Tosibox Lock



Tosibox Key



USB Kabel



Ethernet Kabel



AC Adapter



Antennen (2)

Key-Benutzeroberfläche

Ein intelligentes USB-basierendes Gerät, das einen sicheren Kryptoprozessor enthält. Der Key dient dem Herstellen einer Verbindung mit dem Lock.

*Key-Benutzeroberfläche (vom Key installiert). Im Bild rechts sehen Sie Tosibox Locks, die für den Tosibox Key personalisiert sind, sowie die mit diesem verbundenen Netzwerkgeräte. Klicken Sie zur Anzeige weiterer Optionen auf das Einstellungen-Symbol.



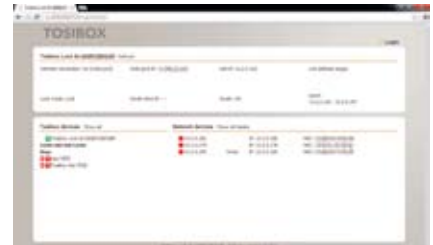
Web-Benutzeroberfläche für den Key*

Lock-Benutzeroberfläche

Ein Tosibox Lock ist ein Gerät, das externe Verbindungen von personalisierten Keys akzeptiert und Zugriff auf verbundene Netzwerkgeräte bereitstellt.

*Web-Benutzeroberfläche des Locks. Die Lock-Einstellungen lassen sich ändern via:

- Service-Anschluss
- Verschlüsselte Tosibox VPN-Verbindung
- Lokales Netzwerk



Web-Benutzeroberfläche für den Lock*

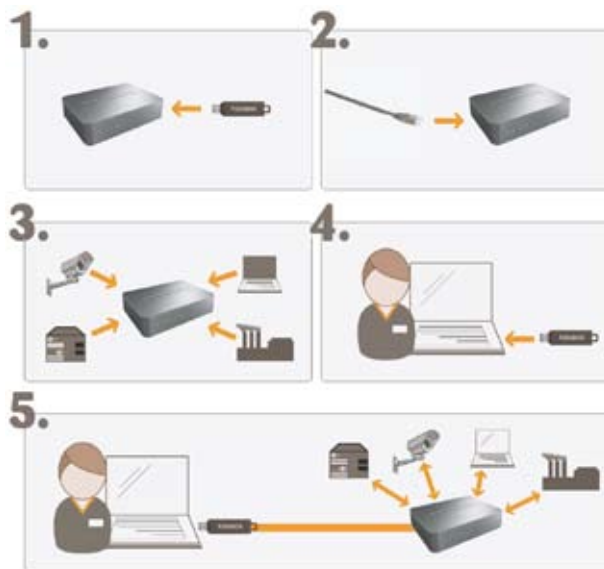
Personalisierung von Tosibox Key und Lock

Die nachstehenden Anweisungen werden durch das beiliegende Diagramm auf der folgenden Seite näher erläutert.

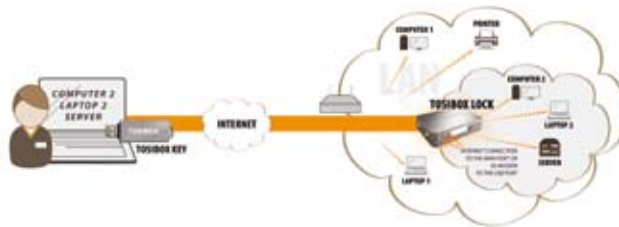
1. Verbinden Sie das Tosibox Netzteil mit dem Lock, warten Sie 2 Minuten. Personalisieren Sie den Key mit dem Lock, indem Sie den Key in den USB-Anschluss des Locks stecken. Wenn die LED am Key aufhört zu blinken, ist die Personalisierung abgeschlossen (dies dauert etwa 10 Sekunden). Entfernen Sie den Key vom Lock. Sie können zudem weitere Locks mit demselben Key personalisieren. Nachdem der erste Key mit dem Lock personalisiert wurde, werden die nachfolgenden Locks (Sub-Locks) mit einem Computer personalisiert. Beachten Sie den Abschnitt "Mehrere Keys" (S. 20). Bitte sehen Sie sich das beigefügte Bild auf der nächsten Seite an.
- 2-3. Verbinden Sie den Lock entsprechend Ihrem Anwendungsfall mit Ihrem Netzwerk. Beachten Sie den Abschnitt "Lock verwenden" (S. 11). Stellen Sie unbedingt sicher, dass der Lock über eine funktionierende Internetverbindung verfügt.

4. Verbinden Sie den Key mit Ihrem Computer und installieren Sie die Key-Software. Befolgen Sie die Anweisungen im Abschnitt "Key verwenden".
5. Nun kann die Tosibox Verbindung zum Steuern und Überwachen externer Geräte genutzt werden.

Personalisierung von Tosibox Key und Lock



Tosibox Lock



Lock verwenden

Gemäß seinen werkseitigen Standardeinstellungen stellt der Lock über seinen WAN-Anschluss oder ein 3G/4G-Modem, das am USB-Anschluss des Locks angeschlossen werden kann, eine Verbindung zum Internet her. In diesem Modus erstellt der Lock sein eigenes geschütztes lokales Netzwerk für die verbundenen Geräte. Nur Geräte, die per Kabel oder per WLAN mit dem Lock verbunden wurden, sind mit dem Key zugänglich.

Hinweise:

- Beachten Sie zum Verbinden eines 3G- oder 4G-Modems mit dem USB-Anschluss des Locks "3G-Modem für den Lock" (S. 31).
- Falls der Lock über einen seiner LAN-Anschlüsse (LAN1, LAN2 oder LAN3) mit einem Netzwerk mit aktivierter DHCP-Funktion verbunden wird, geht die LAN-Funktionalität des Locks verloren und ein Fehler tritt auf. Die LAN-Funktionalität kann wiederhergestellt werden, indem Sie jegliche DHCP-Konflikte durch Entfernen ungeeigneter LAN-Verbindungen mit dem Lock lösen.

Netzwerkgeräte mit dem Lock verbinden

A) Netzwerkgeräte mit dynamischen IP-Adressen verbinden (DHCP):

Netzwerkgeräte mit einem aktivierten DHCP-Client verbinden sich automatisch mit dem Lock. Einfach anschließen und loslegen.

B) Netzwerkgeräte mit statischen IP-Adressen verbinden:

1. Weisen Sie Geräten statische IP-Adressen zu (innerhalb des statischen IP-Bereichs des Locks).
2. Rufen Sie Network > LAN auf und notieren Sie die IP-Adresse des Locks bei "IPv4-Adresse". Stellen Sie außerdem sicher, dass die Netzwerkmaste in "IPv4-Netzmaske" auf 255.255.255.192 eingestellt ist.
3. Rufen Sie die Einstellungen des Netzwerkgerätes auf. Geben Sie eine nicht verwendete IP-Adresse in das Gerät ein, die in den statischen IP-Bereich des Locks fällt; diesen finden Sie auf der Statusseite (Front) der Web-Benutzeroberfläche des Locks.
4. Rufen Sie die Web-Benutzeroberfläche des Locks auf und klicken auf "Scan for LAN Devices". Der Lock lokalisiert automatisch alle Geräte, die mit dem IP-Bereich des Locks übereinstimmen.

C) Statische IP-Adresse eines Locks in Übereinstimmung mit einem bestehenden Netzwerk konfigurieren

1. Notieren Sie IP-Adresse und Netzmaske des/der gesteuerten Netzwerkgeräte(s).
2. Wählen Sie eine nicht verwendete Adresse, die in den von den Netzwerkgeräten verwendeten IP-Adressbereich fällt. Rufen Sie die Einstellungen des Locks auf, indem Sie Network > LAN anklicken. Stellen Sie das IP-Adressfeld des Locks auf "IPv4-Adresse" und das Netzmaskenfeld auf "IPv4-Netzmaske" ein, lassen Sie das Gateway-Broadcast-Feld leer.
3. Wählen Sie Network > DHCP und stellen den "Start"-Wert so ein, dass er höher ist als alle verwendeten statischen Adressen. Legen Sie das Limit so fest, dass es die restlichen nicht verwendeten Adressen im LAN-Bereich abdeckt. Beispiel: Der Bereich 192.168.5.50 – 192.168.5.254 enthält 205 Adressen, sodass das Limit 205 wäre.

Ein Lock mit aktiviertem Client-Modus mit einem bestehenden Netzwerk verbinden

Der Client-Modus kann zur Verbindung eines Locks mit einem bestehenden Netzwerk (z. B. einem Büronetzwerk) genutzt werden. In diesem Modus tritt der Lock wie jedes andere Gerät (z. B. ein PC) dem Netzwerk bei und bietet externen Nutzern den Zugriff auf andere Geräte in demselben Netzwerk. Der Lock bezieht seine Adresse per DHCP, weshalb das lokale Netzwerk einen funktionierenden DHCP-Server

erfordert, der IP-Adressen zuweist.

Lock auf Client-Modus einstellen:

1. Melden Sie sich als Administrator an der Web-Benutzeroberfläche des Locks an und öffnen Sie die LAN-Einstellungen durch Klicken auf Network > LAN .
2. Ändern Sie das LAN-Schnittstellenprotokollfeld in "DHCP-client". Klicken Sie auf die Schaltfläche "Switch protocol" und dann auf "Save".
3. Verbinden Sie ein Kabel vom lokalen Netzwerk mit einem der LAN-Anschlüsse am Lock (z. B. LAN3).

Hinweis im Client-Modus:

- Stellen Sie keine Internetverbindung mit dem WAN-Anschluss des Locks her und schließen sie kein 3G-Modem am USB-Anschluss an. Andernfalls wird der Client-Modus automatisch aktiviert und die LAN-Einstellungen des Locks auf den werkseitigen Standard zurückgesetzt.
- Verbinden Sie den LAN-Anschluss nicht direkt mit dem Internet.
- Verbinden Sie die gesteuerten Geräte nicht mit den LAN-Anschlüssen des Locks.
- Der Lock durchsucht das gesamte LAN-Netzwerk nach verbundenen Geräten und gewährt jedem Nutzer mit einem personalisierten Key einen Gerätezugriff. Bitte bedenken Sie dies in Anbetracht von Netzwerk- und Informationssicherheit.
- Falls Zugangsrechte beschränkt werden müssen, aktivieren Sie den MAC/IP-Filter (unter Industry settings) oder richten Sie den Lock in seiner werkseitigen Standardkonfiguration ein.
- In diesem Modus schützt die integrierte Firewall des Locks nicht die Geräte im LAN-Netzwerk.

1. Key verwenden



2. Festlegen des Passworts



3. Key-Benutzeroberfläche



Key verwenden

1. Verbinden Sie den personalisierten Key mit dem USB-Anschluss Ihres Computers. Auf dem Desktop sollte sich automatisch ein Fenster öffnen. Wenn dies nicht der Fall ist, doppelklicken Sie die ausführbare Datei (Setup_Tosibox.exe) im Ordner des Keys. Falls Ihr Computer fragt, ob Tosibox Änderungen an Ihrem Computer durchführen darf, klicken Sie auf "ja".
2. Optional können Sie in der Key-Benutzeroberfläche ein Passwort festlegen (wird empfohlen). Mit einem Passwort können Sie eine unberechtigte Nutzung des Keys verhindern. Bewahren Sie das Passwort sicher auf.
3. Die Key-Benutzeroberfläche öffnet ein Fenster, das die personalisierten Locks für diesen Key anzeigt. Verbinden Sie den Key mit dem gewünschten Lock, indem Sie auf die entsprechende "Connect" Schaltfläche klicken.
4. Der Info-Dialog zeigt den Status der Verbindung zwischen dem Key und dem Lock an.

Der Key kann jetzt verwendet werden

Das Lock-Symbol erscheint je nach Betriebszustand des Locks in einer bestimmten Farbe:

- Rot = Lock ist nicht mit dem Internet verbunden
- Gelb = Lock und Key sind mit dem Internet verbunden, eine Verbindung kann hergestellt werden
- Grün = Zwischen Lock und Key wurde eine verschlüsselte Verbindung hergestellt

Auch das Key-Symbol in der Taskleiste erscheint je nach Betriebszustand des Keys in einer bestimmten Farbe:

- Rot = Der Key ist nicht mit dem Internet verbunden
- Gelb = Der Key ist mit dem Internet verbunden, hat aber keine Verbindung zu einem Lock
- Grün = Der Key ist mit mindestens einem Lock verbunden

Key-Benutzeroberfläche

Abbildung 1.

Doppelklick zum öffnen der Lock Benutzeroberfläche

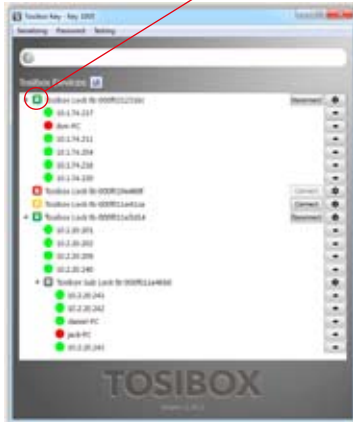


Abbildung 2.

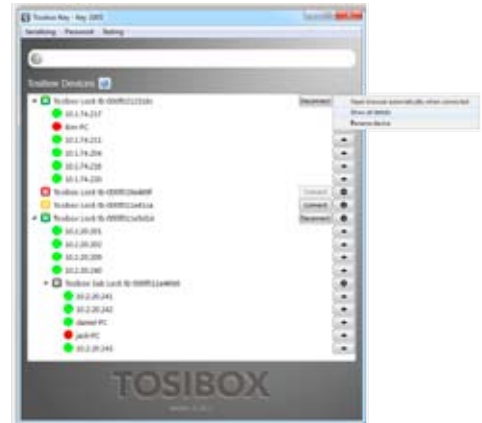


Abbildung 3.




Geräte umbenennen und verwenden

Abbildung 1.

Startfenster der Key-Benutzeroberfläche. Um die Lock-Benutzeroberfläche zu öffnen, doppelklicken Sie auf das Lock-Symbol in der linken Seite des Fensters.

Abbildung 2.

Durch Klicken auf  öffnet sich ein Extra-Menü.

1. Klicken Sie auf "Open browser automatically when connected", um die Lock-Benutzeroberfläche automatisch zu starten, wenn der Key sich mit dem Lock verbindet
2. Mit "Show all details" können Sie alle Informationen über das verbundene Gerät anzeigen
3. Klicken Sie auf "Rename device", um das ausgewählte Gerät umbenennen. Die Benennung der Locks ist abhängig vom Key. Namensänderungen gelten nur für den Key, mit dem die Änderung durchgeführt wurde.

Abbildung 3.

1. In "Open with browser (http)" können Sie die Web-Benutzeroberfläche des gesteuerten Gerätes öffnen
2. In "Open windows network share" können Sie Netzlaufwerke einbinden
3. In "Open Remote Desktop Connection (RDP), if available" können Sie eine Remotedesktopverbindung herstellen
4. In Check if host available (PING) können Sie die Verfügbarkeit des Gerätes mit dem PING-Befehl überprüfen

Mehrere Keys

Abbildung 1.

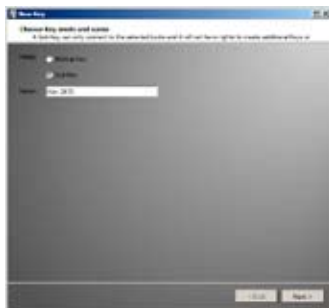


Abbildung 2.

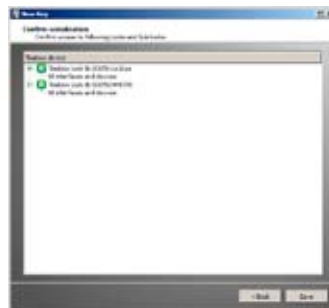


Abbildung 3.

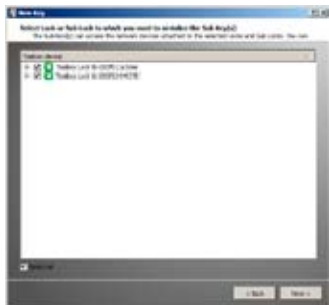


Abbildung 4.

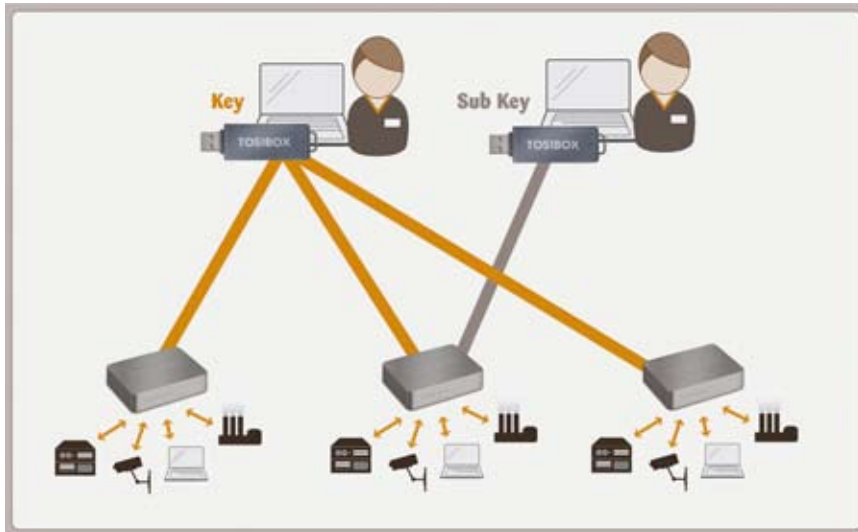


Mehrere Keys

Für einen Lock können zusätzliche Keys personalisiert werden.

1. Verbinden Sie einen bereits personalisierten Key mit dem USB-Anschluss des Computers.
2. Verbinden Sie einen neuen Key mit einem anderen USB-Anschluss des Computers. Abbildung 1.
3. Warten Sie bis sich das Fenster "New Key" öffnet. Abbildung 1.
4. Wenn der neue Key ein Sub-Key werden soll, wählen Sie "Sub-Key", geben Sie einen aussagekräftigen Namen ein und klicken Sie auf "Next". Ein Sub-Key kann zu ausgewählten Locks eine Verbindung herstellen. Mit einem Sub-Key können aber keine neuen Keys personalisiert werden. Abbildung 2.
5. Wählen Sie die Lock(s) / Sub-Lock(s) für die Sie den zusätzlichen Key personalisieren möchten und wählen Sie "Next". Abbildung 3.
6. Bestätigen Sie die Auswahl durch Klicken auf "Save". Die Personalisierung für den zusätzlichen Key ist nun abgeschlossen. Abbildung 4.
7. Die Personalisierung zusätzlicher Keys kann wieder entfernt werden, indem Sie in der Lock-Benutzeroberfläche auf "Edit Tosibox devices" klicken (nur mit Administratorrechten).

Anwendungsfall zusätzlicher Key



Personalisierung von zusätzlichen Keys aus der Ferne

Diese Funktion ist nur für Keys verfügbar, die bereits lokal personalisiert wurden.

1. Verbinden Sie den Key mit dem USB-Anschluss des Computers und warten Sie bis die Tosibox Key-Software gestartet ist.
2. Wählen Sie in der Benutzeroberfläche "Manage Keys" im Menü "Devices" und öffnen Sie die Registerkarte "Sub-Keys".
3. Wählen Sie die zusätzlichen Keys für die Sie neue Locks personalisieren möchten und klicken Sie auf die Schaltfläche "Serialize..." .
4. Wählen Sie die Locks für die Sie die zusätzlichen Keys personalisieren möchten und klicken Sie auf die Schaltfläche "Next".
5. Eine Liste mit den Ziel-Locks wird angezeigt. Bestätigen Sie die Personalisierung und klicken Sie auf "Save".
6. Die Personalisierung der zusätzlichen Keys ist nun abgeschlossen. Klicken Sie die Schaltfläche "Finish", um den Assistenten zu verlassen.

Erstellen eines Backup-Keys

Abbildung 1.

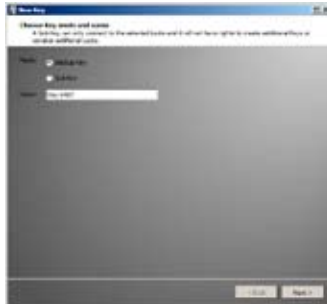


Abbildung 2.

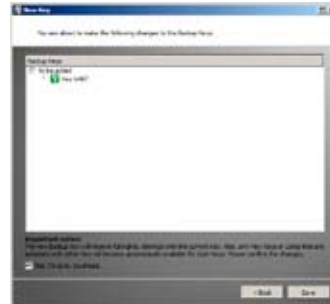


Abbildung 3.



Abbildung 4.



Einen Backup-Key erstellen

Sie können von einem personalisierten Key ein Duplikat machen. Dieses Duplikat kann zum Beispiel als Backup-Key verwendet werden.

1. Verbinden Sie den Key mit dem USB-Anschluss des Computers.
2. Verbinden Sie den neuen Key mit einem anderen USB-Anschluss des Computers.
3. Warten Sie bis sich das Fenster "New Key" öffnet. Abbildung 1.
4. Wählen Sie "Backup-Key" und klicken Sie auf "Next". Alle Personalisierungen und Benutzerrechte werden automatisch zwischen den Backup-Keys synchronisiert. Abbildung 2.
5. Bestätigen Sie durch Klicken auf "Save". Abbildung 3.
6. Der Backup-Key wird nun erstellt. Klicken Sie auf die Schaltfläche "Finish", um die Funktion zu verlassen. Abbildung 4.
7. Die Backup-Keys können später in der Key-Benutzeroberfläche unter "Manage Keys" verwaltet werden. Wichtig: Diese Funktion erstellt einen Backup-Key mit gleichen Benutzerrechten. Wenn die neuen Standorte später mit dem anderen Key verwendet werden, werden die Zugriffsrechte automatisch auf beide Keys kopiert.

Verwenden des Mobile Clients



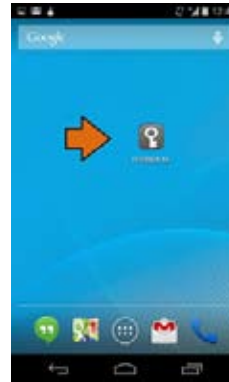
1. Herunterladen und installieren des Tosibox Mobile Client vom Google Play Store.
2. Öffnen der Tosibox Key Benutzeroberfläche durch einstecken eines Personalisierten Keys in den USB-Port des Computers.
3. Im Software Menü unter Devices > Manage Keys
4. Auswählen des Mobile Clients Tabs und auf Add new... klicken



5. Eintragen eines Namens zur Identifikation des Mobilgerätes und auf Next klicken.



6. Auswählen der Locks welche für das Mobilgerät zugänglich gemacht werden sollen und durch Next übernehmen.



7. Öffnen des Tosibox Mobile Clients auf dem Mobilgerätes.



8. Auf den Bildschirm klicken und die Serialisierung durchzuführen.



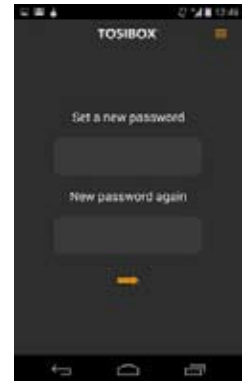
9. Scannen des QR Codes oder manuelle Eingabe des Serialisierungs Codes, welcher auf dem PC angezeigt wird.



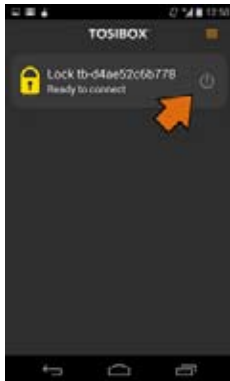
10. Durch Klick auf Finish wird die Serialisierung beendet.



11. Sicherstellen dass das Mobilgerät angezeigt wird und das Key Manager Fenster schließen.



12. Vergeben eines Passwortes zur Nutzung des Mobile Clients.



13. Verbinden mit einem Lock über die Auswahl on/off.



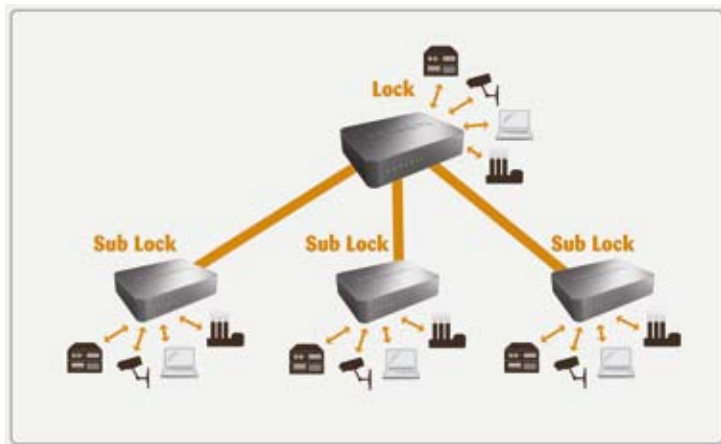
14. Prüfen des Dialoges zur Vertrauensregelung zur App und mit OK bestätigen.



Herzlichen Glückwunsch! Es ist erledigt! Nun ist das Mobilegerät serialisiert und kann mit den angezeigten Locks verbunden werden.

Die Netzwerkgeräte können über den Web Browser (wenn verfügbar) geöffnet werden in dem auf das Symbol des Web Browser geklickt wird. Hinweis: Falls das Netzwerkgerät keine Web Benutzeroberfläche hat (HTTP/HTTPS), ist es möglich eine andere App zum Zugriff zu verwenden. Entsprechende Apps finden sich im Google Play Store. Einfach die Netzwerkadresse des Netzwerkgerätes, durch klicken auf das IP Symbol, kopieren und in der anderen App übernehmen.

Locks verbinden



Locks verbinden

Mit den Tosibox Locks können Sie Maschinen an getrennten Orten verbinden, so dass die Verbindung zwischen ihnen dauerhaft und automatisch hergestellt wird. Ein Beispiel ist eine in Echtzeit gesicherte Verbindung zwischen Zuhause und Büro. Dies erfolgt mit einer Lock / Sub-Lock Lösung (siehe Abbildung). Bis zu 10 Sub-Locks können an einem Lock angeschlossen werden.

Personalisieren Sie zuerst den Key mit allen Locks, wie im Abschnitt "Tosibox Lock und Key Personalisierung" beschrieben.

1. Einfügen eines personalisierten Keys an den USB-Anschluss des Computers
2. Wählen Sie "Devices" aus dem Key Benutzermenü und "Serialize Locks" aus dem Aufklappmenü.
3. Wählen Sie die Locks, die Sie zusammen personalisieren möchten und klicken Sie auf "Next".
4. Wählen Sie den Lock mit dem Sie die Sub-Locks verbinden möchten. Die anderen Locks werden in den Sub-Lock Betriebsmodus umgeschaltet.
5. Bestätigen Sie die Auswahl "Save" Personalisierung ist bereit.

Hinweis: Die Personalisierungen werden erst wirksam, wenn die Locks Zugang zum Internet haben.

Die Sub-Lock Endpunkte der Verbindung im Bild haben keinen eigenen DHCP-Dienst. Wenn die Verbindung zwischen dem Lock und dem Sub-Lock unterbrochen ist, können die Netzwerkgeräte, die mit dem Sub-Lock verbunden sind, sich nicht mehr zum Internet und untereinander verbinden.

Am Lock anmelden

Der Lock hat zwei Benutzerkonten mit unterschiedlichen Zugriffsebenen: Benutzer und Administrator. Die Benutzernamen und Passwörter sind auf der Unterseite des Locks aufgedruckt. Das Benutzerkonto hat nur eingeschränkte Rechte um Änderungen vornehmen. Die Einstellungen des Locks können von der Ferne mit einem personalisierten Key oder lokal durch direkten Anschluss des Computers am Service-Anschluss des Locks über ein Ethernetkabel geändert werden.

Melden Sie sich am Lock mit dem Benutzernamen "admin" oder "user" an. Die Adresse bei der Anmeldung direkt über den Service-Anschluss des Locks ist "http://service.tosibox" oder "http://172.17.17.17". Die Adresse bei der Anmeldung über die LAN-Anschlüsse (1, 2 oder 3) ist "http://service.tosibox" (inaktiv im Client-Modus).

Das Benutzerkonto hat folgende Rechte:

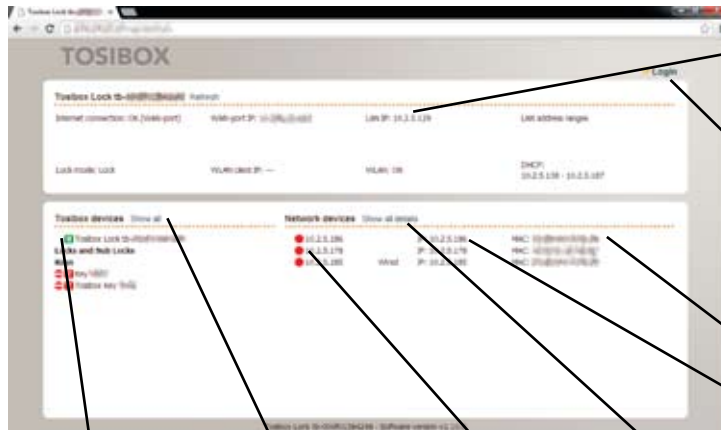
- Hinzufügen von neuen Netzwerkgeräten
- Umbenennung der gesteuerten Geräte
- Entfernen von gesteuerten Geräten
- Download eines Software-Updates
- Neustart

Das Administratorkonto hat folgende Rechte:

- Alle Rechte der Benutzerebene
- Ändern des Admin-Passworts

- Scannen der Netzwerkgeräte
- Umbenennung der Key- und Lock-Verbindungen
- Entfernen der Key- und Lock-Verbindungen
- Entfernen von Personalisierungen
- Automatische Software-Updates erlauben / verbieten
- Änderung des Betriebsmodus (Lock / Sub-Lock)
- Drahtloseinstellungen (WLAN)
- Einstellungen der LAN- und WAN-Verbindungen (zum Beispiel DHCP-Einstellungen, eigene statische IP-Adressen des Locks, statische Routen)
- 3G-Einstellungen
- Industrieereinstellungen
- MAC-Filter
- Prioritätseinstellungen der Internetverbindungen
- Einstellung der Drahtlosklientverbindung

Lock-Benutzeroberfläche



Statusfenster zeigt den Betriebsmodus des Locks an

Locks und Keys
Grün: Verbindung ist bereit
Rot: Lock nicht gefunden

Zusätzliche Informationen über die Keys und Locks

Ferngesteuerte Geräte
Grün: Verbindung ist bereit
Rot: keine Verbindung

Informationen über die ferngesteuerten Geräte

Zusätzliche Informationen über die ferngesteuerten Geräte IP-Adressen und MAC-Adressen

Anmeldung mit dem Benutzer oder Administrator
Passwort, das auf der Unterseite des Locks aufgedruckt ist.

Software aktualisieren

1. Schließen Sie den Computer mit einem Ethernet-Kabel an den Service-Anschluss des Lock an. Prüfen Sie zuerst, dass Sie über den Service-Anschluss Zugang zum Internet haben. Öffnen Sie den Internetbrowser. Geben Sie `http://172.17.17.17` oder `http://service.tosibox` in die Adressleiste ein, um zu der Lock-Benutzerschnittstelle zu gelangen. Geben Sie vor dem `http://` beider Adressen kein `www` ein.

Sie können sich auch entfernt mit der `admin` Benutzer-ID anmelden. Wenn die Verbindung zwischen dem Key und dem Lock aktiv ist, klicken Sie zweimal auf das Lock-Symbol in der Key-Benutzerschnittstelle. Melden Sie sich mit `admin` für die Benutzer-ID an. Das Passwort finden Sie auf der Unterseite des Locks.

2. Wählen Sie `settings` > `software update` > `Start software update`.
3. Warten Sie, bis die Software heruntergeladen wurde. Unterbrechen Sie während des Software-Updates nicht die Stromzufuhr zu dem Lock. Das Update ist abgeschlossen, wenn die Software die Meldung `Software updated successfully` anzeigt.

Automatische Software-Updates werden als Standardeinstellung aktiviert. Sie können den Zeitpunkt für automatische Updates der veröffentlichten Software wählen. Sie können das automatische Software-Update von der Lock-Benutzerschnittstelle aus deaktivieren. Wählen Sie `settings` > `software update` > `uncheck the box auto update enable`.

3G-Modem für den Lock

Sie können den Lock über ein 3G-Modem mit dem Internet verbinden. Informationen zu unterstützten Modems erhalten Sie unter `help.tosibox.fi`.

1. Melden Sie sich als Admin an, wählen Sie `network` > `3G`.
2. Füllen Sie den APN aus und ggf. das PIN-Feld gemäß den SIM-Karteneinstellungen.
3. Wenn Sie den automatischen Zustandswechsel deaktivieren, können Sie erzwingen, dass die Datenbearbeiter-Teilnehmerverbindung im 3G- oder 2G-Modus arbeitet.
4. Bestätigen Sie die Auswahl > `Save`.
5. Schließen Sie ein von Tosibox unterstütztes 3G-Modem an den USB-Anschluss des Locks an.

Key-Verbindungseinstellungen für den Lock

Sie können Verbindungen vom Lock zum Key erlauben: Melden Sie sich als Admin im Lock an, wählen Sie `edit Tosibox devices` > `remove selection Deny access towards client`.

Der Verbindungstyp für den Key kann von Layer 3 routed zu Layer 2 bridged (`Connection type` > `Layer 2-bridged`) geändert werden.

Industrieeinstellungen für den Lock

1. Melden Sie sich als admin an
2. Wählen Sie "settings" > "industry"
3. Wählen Sie die gewünschte Einstellung und bestätigen Sie die Auswahl > Save

Mit Industrieeinstellungen können Sie:

- den Lock so einstellen, dass er automatisch nach Geräten sucht ("Auto Discover Enabled")
- erlauben, dass Tosibox zur Fehlerbehebung Zugang zu Ihrem Lock erhält ("Allow Remote Support")
- Internetzugang für mit dem Lock verbundene Geräte vermeiden
- Internetzugang für einen vorgegebenen Zeitraum erlauben. ("Temporarily allow internet access")
- Internetzugang von mit dem Lock verbundenen Netzwerkgeräten vermeiden ("Prevent internet access from LAN and service port")
- Key- und Lock-Verbindungen vom Internet zum Lock vermeiden ("Prevent VPN access from the Internet")
- Vermeiden, dass Sub-Locks sich über einen Lock miteinander verbinden ("Prevent traffic between sub Locks")
- MAC-Filter: Verbindung über den Lock kann auf spezielle MAC-Adressen beschränkt werden
- Wenn der Key in Ihrem Computer steckt, können Sie den gesamten Internetverkehr durch den Lock am entfernten Standort übertragen ("Relay Tosibox Key user's internet access through Lock")

Drahtloseinstellungen für den Lock

Netzwerkgeräte können mit einer Drahtlosverbindung drahtlos mit dem Lock verbunden werden.

1. Schließen Sie die Antennen (2 Teile) an, indem Sie diese in die Buchsen an der Seite des Lock drehen
2. Melden Sie sich mit der Admin-Benutzer-ID im Lock an
3. Gehen Sie zu "Network" > "Wireless" > "Wireless Overview" > "Edit".
4. Gehen Sie zu "Device Configuration" und wählen Sie "Enable" auf der rechten Seite der Statusnachricht "Drahtlosnetzwerk ist deaktiviert". Die WLAN-Statusnachricht wird zu "Wireless network is enabled" geändert
5. Gehen Sie zu "Interface Configuration" > "Wireless Security" und wählen Sie "WPA2-PSK" als "Verschlüsselung".
6. Legen Sie ein WLAN-Netzwerkpasswort fest und geben Sie es in "Key" ein.
7. Speichern Sie die Einstellungen mit "Save".

WLAN-Klient

Der Lock kann über WLAN mit dem Internet verbunden werden

1. Melden Sie sich mit dem Admin-Benutzernamen in der Lock-Benutzerschnittstelle an
2. Gehen Sie zu "Network" > "Wireless" und wählen Sie "Edit"
3. Wählen Sie "Client" in dem Feld "Mode"
4. Legen Sie den Namen des Netzwerks in dem Feld "ESSID" fest
5. Wenn das Netzwerk eine Verschlüsselung verwendet, wählen Sie dieselbe Verschlüsselung in "Wireless security" > "Encryption"
6. Wenn nötig, geben Sie dem Netzwerk ein Passwort unter "Wireless security" > "Key"

Prioritäten der Internetverbindungen

Der Lock kann mehrere alternative Internetverbindungen nutzen. Eine der verfügbaren Verbindungen kann als Hauptverbindung gewählt werden, weitere Verbindungen können als Ersatz-Verbindungen verwendet werden. Wenn die Hauptverbindung unterbrochen ist, wird die Verbindung automatisch auf die vorgewählten Ersatz-Verbindungen entsprechend der Prioritäteneinstellung verlagert (zum Beispiel WAN-Anschluss --> 3G --> WLAN-Klient).

- "WAN-port maximum allowed latency in milliseconds" = maximale Verzögerung (in Millisekunden) mit einer Kabelverbindung, nach der die Verbindung als nicht funktionierend betrachtet wird
- "WLAN client maximum allowed latency in milliseconds" = maximale Verzögerung (in Millisekunden) für eine WLAN-Verbindung, nach der die Verbindung als nicht funktionierend betrachtet wird
- "3G maximum allowed latency in milliseconds" = maximale Verzögerung (in Millisekunden) für eine 3G-Verbindung, nach der die Verbindung als nicht funktionierend betrachtet wird
- "Interval between the ping packets in milliseconds" = Der Intervall (in Millisekunden) zwischen den Ping-Paketen, mit denen eine Verzögerung erkannt wird
- "Servers to ping" = Server, mit denen die Verzögerung erkannt wird
- "Maximum allowed ping timeouts per connection" = maximale Anzahl an gescheiterten Ping-Paketen pro Verbindung, nach der die Verbindung als nicht funktionierend betrachtet wird

- "Number of times each server is pinged" = Anzahl der zwischen Lock und Server vorgenommenen Verzögerungsmessungen
- "3G connect minimum time for 3G-reset (minutes)" = Dauer der minimalen Wartezeit (in Minuten) für einen 3G-Verbindungsaufbau, nach der die 3G zurückgesetzt wird.
- "3G maximum latency for USB reset (milliseconds)" = maximal erlaubte Verzögerung (in Millisekunden) für eine 3G-Verbindung, nach der die USB-Zurücksetzung aktiviert wird
- "3G maximum allowed ping timeouts for USB reset" = maximal erlaubte gescheiterte Ping-Pakete für eine 3G-Verbindung, nach denen die USB-Zurücksetzung aktiviert wird

Hinweis! Eine Änderung der Prioritäteneinstellungen kann zu Verbindungsproblemen führen. Ändern Sie die Einstellungen nur gemeinsam mit einem Netzwerkspezialisten.

PUK-Code für den Key

1. Wird sechs Mal hintereinander ein falsches Key-Passwort eingegeben, wird der Key gesperrt. Zum Freischalten des Keys ist ein persönlicher Freischaltcode, PUK, nötig. Der PUK-Code wird mit dem Key geliefert. Bewahren Sie ihn sicher auf.
2. Gehen Sie zum "Password"-Menü des Keys und wählen Sie "Change password using PUK code..."
3. Geben Sie den PUK-Code in das Feld "PUK-Code" ein
4. Geben Sie ein neues Passwort in das Feld "New password" ein
5. Bestätigen Sie Ihr Passwort, indem Sie es ein weiteres Mal in das Feld "New password (again)" eingeben
6. Wählen Sie "OK"

Problemlösung

Die Key-Software kann nicht installiert werden:

- Prüfen Sie, dass Ihr Computer über ein Betriebssystem verfügt, das von Tosibox unterstützt wird: Windows XP/SP3, Windows Vista, Windows 7, Windows 8, Mac Leopard 10.5 oder eine neuere Version.
- Starten Sie den Computer neu und schließen Sie den Key wieder an

Das Key-Verbindungsfenster zeigt keine Verbindungen an:

- Der Computer ist nicht mit dem Internet verbunden.
- Der Key ist nicht mit dem Lock personalisiert.
- Der Lock verfügt über keine Internetverbindungen oder ist nicht mit dem Tosibox Netzteil verbunden.

Die Lock-Verbindung in dem Fenster bleibt gelb:

- Der Key hat einen Lock gefunden, aber das VPN wurde noch nicht aufgebaut.

Geräte-Verbindungen oder die Lock-Verbindung in dem Fenster bleibt

- Vergewissern Sie sich, dass die kontrollierten Geräte mit dem Lock verbunden sind.
- Nutzen Sie bei Drahtlosverbindung den Ethernet-Service-Anschluss, um sich im Lock anzumelden. Prüfen Sie, dass die Drahtlosverbindung aktiviert ist und dass der Lock und das kontrollierte Gerät dieselben Passwort- und Verschlüsselungseinstellungen haben.

- Vergewissern Sie sich, dass das kontrollierte Gerät einen DHCP-Service hat. Falls nicht,
- fügen Sie das Gerät der Geräteliste des Locks hinzu und geben Sie die
- IP-Adresse des Gerätes an

Weitere Anleitungen erhalten Sie unter <http://help.tosibox.com>.

Wartungsanweisungen

Tosibox Geräte sollten sorgfältig behandelt werden. Wenn Sie die folgenden Anleitungen beachten, können Sie die maximale Leistung der Geräte nutzen und genießen volle Garantie.

- Halten Sie die Geräte trocken. Schützen Sie die Geräte vor Niederschlägen, Feuchtigkeit und Flüssigkeiten. Ansonsten könnte es zu Korrosion an den elektronischen Schaltungen kommen. Die Geräte sind nur für den Gebrauch im Innenbereich bestimmt. Verwenden Sie sie nicht an nassen Orten oder im Freien.
- Schützen Sie die Geräte vor Schmutz und Staub. Falls nötig, reinigen Sie die Geräte mit einem weichen, trockenen Tuch. Verwenden Sie keine Chemikalien, Lösungsmittel, Reinigungsmittel oder Druckluft.
- Schützen Sie die Geräte vor Hitze. Hohe Temperaturen können die Kunststoffteile beschädigen und die Lebensdauer der Elektronik verkürzen.
- Schützen Sie die Geräte vor Kälte. Niedrige Temperaturen können die Geräte bruchempfindlicher machen. Vergewissern Sie sich, dass die Gerätetemperatur stabil ist, bevor Sie die Geräte im Netzwerk einsetzen.
- Schützen Sie die Geräte vor mechanischen Erschütterungen. Sie sollten die Geräte nicht schütteln, schlagen oder fallen lassen.
- Malen Sie die Geräte nicht an.

- Bedecken Sie die Geräte nicht und installieren Sie sie nicht aufeinander. Das könnte zu Überhitzung führen. Lassen Sie um die Geräte herum ausreichend Platz, damit die Kühlluft abfließen kann.
- Öffnen Sie die Geräte nicht. In den Geräten befinden sich keine zu wartenden Teile. Wenn die Geräte defekt sind oder gewartet werden müssen, kontaktieren Sie eine autorisierte Servicestelle.

Nachdem die Lebensdauer der Geräte über ist, nicht werfen sie in den Hausmüll. Stattdessen nehmen sie eine genehmigten Abfall Elektronik Sammelstelle.

Technische Daten für den Lock

WLAN:

WEP, WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK gemischt, WPA-EAP, WPA2-EAP

TKIP/AES -Verschlüsselung

Frequenz 2.412 – 2.472 GHz, 13 Kanäle

Ausgangsleistung 20 dBm, max

IEEE 802.11 n/g/b (max. 150 Mbps)

Anschlüsse:

- USB 2.0-Verbindung x 1
- RJ-45, WAN-Verbindung x 1, 10/100 M Auto-Negotiation
- RJ-45, LAN-Verbindung x 3, 10/100 M Auto-Negotiation (MDI/MDIX-Unterstützung)
- RJ-45, Service-Verbindung x 1, 10/100 M Auto-Negotiation (MDI/MDIX-Unterstützung)

Verbindungen:

- 12-24V DC +-20%
- Drahtlose Netzwerkantennenanschlüsse, 2 x RP-SMA (weiblich)
- DIN-Schienenbefestigung (unten)

Zubehör:

- Kabel: RJ45 Cat6, USB-Verlängerungskabel
- WLAN-Antennen x 2, 2 dBi
- Stromquelle: Eingang 100 – 240V AC, Frequenz 47 – 63 Hz,
- Ausgang 12.0V, 0,6A, 7,2W max

Maße/Material:

- 132 mm (L) x 99 mm (W) x 35,5 mm (H)
- Gewicht 365 g
- Aluminium-Gussgehäuse
- Betriebstemperatur -25 °C ... +70 °C
- Lagertemperatur -40 °C ... +70 °C
- Schutzklasse IP20

WAN Verbindungsmerkmale:

- Unabhängig von Betriebssystemen
- funktioniert bei allen Internetverbindungen (benutzerunabhängig) unter folgenden Bedingungen:
- Kein Zwangsproxy-Service in der Internetverbindung
- Keine Passwörter für Internetzugang nötig
- Funktioniert mit dynamischen, statischen und privaten IP-Adressen.
- Firewall, NAT
- 10 gleichzeitige VPN-Verbindungen (max)
- VPN Durchsatz 6 Mbit (BF-CBC 128 bit)

Mobile Verbindungsmerkmale:

- Unterstützte 2G/3G/4G Modems (Huawei): E3276, E392, E372, E3131, E353, E367, E160, E169, E173, E176, E180, E1552 und die neue Industrie Tosibox 3G-Modem. HiLink Versionen von E353 und E3131 werden nicht unterstützt!
- Mehr Informationen und neuesten unterstützten Modem-Modelle finden Sie unter: help.tosibox.com.

Technische Daten für den Key

USB 2.0-Verbindung, unterstützte Betriebssysteme:

Supported operating systems:

Windows 8 (32/64 bit), Windows 7 (32/64 bit), Windows Vista (32/64 bit), Windows XP (SP3)

Mac OS X Leopard 10.5 oder neuere Version (Intel)

Maße und Material:

- 74,8 mm (L) x 23,2 mm (B) x 10,3 mm (H)
- Gewicht 16 g
- ABS-Gehäuse
- Betriebstemperatur 0 °C – 70 °C
- Lagertemperatur -20 °C – 85 °C
- Standard CSP/PKCS#11

Verbindung:

- OpenVPN-Verbindung, Netzwerkverbindung auf Layer 2-Ebene
- Stark verschlüsselte PKI-Methode bei Verbindungsaufbau
- TLS/Blowfish 128-bit Datenverschlüsselung
- Verbindungsauthentifizierung und Austausch des Verschlüsselungsschlüssels verwendet RSA 1024 bit Verschlüsselung
- Ende-zu-Ende Verschlüsselung: Datenverschlüsselung und -entschlüsselung in den Verbindungsendpunkten (Tosibox Geräte)

Tosibox Lizenzen

© 2014 Tosibox Oy. Alle Rechte vorbehalten.

Die Vervielfältigung, Verteilung oder Speicherung eines Teils oder des gesamten Inhalts dieses Dokuments ist ohne vorherige schriftliche Genehmigung durch Tosibox untersagt.

Aufgrund der laufenden Produktentwicklung behält Tosibox sich das Recht vor, jedes hier erwähnte Produkt ohne Vorankündigung zu ändern und zu verbessern.

Tosibox übernimmt keine Verantwortung für Verlust von Informationen oder Einnahmen oder besondere, beiläufige, indirekte Schäden oder Folgeschäden.

Die Inhalte in diesem Dokument werden auf Istbasis zur Verfügung gestellt. Es werden keine Garantien jeglicher Art, weder impliziert noch ausdrücklich, einschließlich, aber nicht begrenzt auf, der implizierten Gewährleistung der Markttauglichkeit und Eignung für einen bestimmten Zweck, hinsichtlich der Genauigkeit, Zuverlässigkeit oder der Inhalte dieses Dokuments gegeben. Tosibox behält sich das Recht vor, dieses Dokument jederzeit ohne Vorankündigung zu überarbeiten oder zurückzuziehen.

Tosibox Produkte enthalten Technologie auf Opensource-Software-Basis. Auf Anfrage des Kunden stellt Tosibox detailliertere Informationen zu den für die Lizenzen erforderlichen Teile zur Verfügung. Quellcode-Anfragen können per E-Mail eingereicht werden an:

sourcecode.request@tosibox.com oder auf dem Postweg:

Tosibox Oy

Elektroniikkatie 10

90590 OULU SUOMI-FINNLAND

Konformitätserklärung

Hiermit erklärt Tosibox Oy, dass Tosibox Lock ist in Übereinstimmung mit den grundlegenden Anforderungen der die europäischen Richtlinien:

- 1999/5/EC, Artikel 3.1 a) 3.1 b) und 3.2; R&TTE / EMC
- 2011/65/EC; RoHS
- 2006/95/EC; Low Voltage
- 2009/125/EC; ErP (Regulation 287/2009/EC)

In Oulu, Finnland am 1.9.2014
Tosibox Oy
Tero Lepistö, Geschäftsführer



HINWEISE

TOSIBOX®

Elektroniikkatie 10
FIN-90590 Oulu
FINNLAND

www.tosibox.com

Version 2.10