TOSIBOX® Lock for Container
Kullanım Kılavuzu

V1.4

İçerik

1 Giriş 3
2 Sistem açıklaması 4
3 Docker temelleri 7
4 Bağlantı senaryosu örnekleri 8
5 Lisanslama 11
6 Kurulum ve güncelleme 12
7 Etkinleştirme ve kullanıma alma 13
8 Kullanıcı arayüzü 16
9 Temel yapılandırma 18
10 Rotalar için NAT 20
11 Kurulumu Kaldırma 22
12 Sistem gereksinimleri 22
13 Sorun giderme 23

1 Giriş

Tosibox çözümünü seçtiğiniz için tebrikler!

Tosibox küresel olarak denetlenir, patentlidir ve sektördeki en yüksek güvenlik seviyelerinde performans gösterir. Teknoloji, iki faktörlü kimlik doğrulama, otomatik güvenlik güncellemeleri ve en son şifreleme teknolojisine dayanmaktadır.

Tosibox çözümü, sınırsız genişletilebilirlik ve esneklik sunan modüler bileşenlerden oluşur. Tüm TOSIBOX® ürünleri birbiriyle uyumludur ve internet bağlantısı ve operatörden bağımsızdır. Tosibox, fiziksel cihazlar arasında doğrudan ve güvenli bir VPN tüneli oluşturur. Sadece güvenilen cihazlar ağa erişebilir.

TOSIBOX® Lock for Container, İnternet bağlantısı mevcut olduğunda hem özel hem de genel ağlarda çalışır.

- TOSIBOX® Key ağa erişmek için kullanılan bir istemcidir. TOSIBOX® Key'in kullanıldığı iş istasyonu VPN tünelinin başlangıç noktasıdır
- TOSIBOX® Lock for Container, kurulduğu ana cihaza güvenli uzaktan bağlantı sağlayan VPN tünelinin uç noktasıdır

Bu belge Lock for Container sürüm 1.1 için geçerlidir.

2 Sistem açıklaması

2.1 Kullanım bağlamı

TOSIBOX® Lock for Container, TOSIBOX® Key çalıştıran bir kullanıcı iş istasyonundan, TOSIBOX® Mobile Client çalıştıran bir kullanıcı mobil cihazından veya TOSIBOX® Virtual Central Lock çalıştıran özel bir veri merkezinden başlatılan son derece güvenli bir VPN tünelinin uç noktası olarak hizmet verir. Uçtan uca VPN tüneli, ortada bir bulut olmadan, dünyanın herhangi bir yerinde bulunan Konteyner için İnternet üzerinden Lock'a doğru yönlendirilir.

TOSIBOX® Lock for Container, Docker konteyner teknolojisini destekleyen herhangi bir cihazda çalışabilir. Konteyner için Lock, kurulu olduğu ana cihaza güvenli uzaktan bağlantı ve ana cihaza bağlı LAN tarafındaki cihazlara erişim sağlar.

TOSIBOX® Lock for Container, üst düzey güvenlik ile tamamlanan basit kullanıcı erişim kontrolünün gerekli olduğu endüstriyel OT ağları için idealdir. Lock for Container ayrıca bina otomasyonu ve makine üreticileri için veya denizcilik, taşımacılık ve diğer endüstriler gibi tehlikeli ortamlardaki zorlu uygulamalar için de uygundur. Bu senaryolarda Lock for Container, zorlu gereksinimleri karşılamak üzere tasarlanmış donanım cihazlarına güvenli bağlantı sağlar.

2.2 Kısaca TOSIBOX® Lock for Container

TOSIBOX® Lock for Container, Docker teknolojisine dayanan yalnızca yazılımsal bir çözümdür. Kullanıcıların IPC'ler, HMI'lar, PLC'ler ve kontrolörler, endüstriyel makineler, bulut sistemleri, veri merkezleri gibi ağ cihazlarını Tosibox ekosistemlerine entegre etmelerini sağlar.

Ana bilgisayarda veya yapılandırılmışsa LAN cihazlarında çalışan Uzak Masaüstü Bağlantısı (RDP), web hizmetleri (WWW), Dosya Aktarım Protokolü (FTP) veya Güvenli Kabuk (SSH) gibi herhangi bir hizmete VPN tüneli üzerinden erişilebilir. Bunun çalışması için LAN tarafı erişiminin ana cihazda desteklenmesi ve etkinleştirilmesi gerekir.

Kurulumdan sonra kullanıcı girişi gerekmez, Lock for Container sistem arka planında sessizce çalışır. Lock for Container, TOSIBOX® Lock donanımıyla karşılaştırılabilir, yalnızca yazılıma dayalı bir çözümdür.

2.3 Ana Özellikler

Neredeyse tüm cihazlara güvenli bağlantı

Patentli Tosibox bağlantı yöntemi artık sanal olarak her cihazda kullanılabilir. TOSIBOX® Sanal Merkezi Kilidiniz ile tüm cihazlarınızı tanıdık Tosibox kullanıcı deneyimi ile entegre edebilir ve yönetebilirsiniz. TOSIBOX® Lock for Container, TOSIBOX® Sanal Merkezi Kilit erişim gruplarına eklenebilir ve TOSIBOX® Key yazılımından erişilebilir. TOSIBOX® Mobil İstemci ile birlikte kullanılması hareket halindeyken rahat kullanım sağlar.

Uçtan uca yüksek güvenlikli VPN tünelleri oluşturun

TOSIBOX® ağlarının son derece güvenli olduğu, ancak birçok farklı ortam ve kullanıma uyacak şekilde esnek olduğu bilinmektedir. TOSIBOX® Lock for Container, TOSIBOX® Key ve TOSIBOX® Lock for Container arasında tek yönlü, Katman 3 VPN tünellerini veya TOSIBOX® Virtual Central Lock ve Lock for Container arasında iki yönlü, Katman 3 VPN tünellerini, arada üçüncü taraf bir bulut olmadan destekler.

Ağınızda çalışan tüm hizmetleri yönetin

TOSIBOX® Lock for Container, yönetmeniz gereken hizmet veya cihaz sayısını sınırlamaz. Herhangi bir cihaz arasında herhangi bir protokol üzerinden herhangi bir hizmeti bağlayabilirsiniz. Lock for Container, ana cihaz tarafından destekleniyorsa ve etkinleştirildiyse sınırsız erişim sağlar.

Etkinleştirmeden kurun veya anında erişim için etkinleştirin

TOSIBOX® Lock for Container etkinleştirilmeden kurulabilir, yazılımı hazır tutar ve etkinleştirilmeyi bekler. Etkinleştirildikten sonra Lock for Container Tosibox ekosistemine bağlanır ve üretim kullanımına alınmaya hazırdır. Lock for Container kullanıcı lisansı bir cihazdan diğerine aktarılabilir.

Sistem arka planında sessizce çalışır

TOSIBOX® Lock for Container sistem arka planında sessizce çalışır. İşletim sistemi düzeyindeki işlemlere veya ara katman yazılımlarına müdahale etmez. Lock for Container, Tosibox bağlantı uygulamasını sistem yazılımından ayıran Docker platformunun üzerine temiz bir şekilde yüklenir. Lock for Container sistem dosyalarına erişime ihtiyaç duymaz ve sistem seviyesi ayarlarını değiştirmez.

2.4 TOSIBOX® Lock ve Lock for Container Karşılaştırması

Aşağıdaki tabloda fiziksel bir TOSIBOX® Node cihazı ile Lock for Container arasındaki farklar vurgulanmaktadır.

Özellik	TOSIBOX® Node	TOSIBOX® Lock for Container
Çalışma ortamı	Donanım cihazı	Docker platformunda çalışan yazılım
Dağıtım	Plug & Go™ bağlantı cihazı	Docker Hub'da ve iyi donanımlı pazar yerlerinde mevcuttur
SW otomatik güncelleme	✓	Docker Hub üzerinden güncelleme
İnternet bağlantısı	4G, WiFi, Ethernet	-
Katman 3	✓	✓
Katman 2 (Alt Lock)	✓	-
NAT	1:1 NAT	Rotalar için NAT
LAN erişimi	✓	✓
LAN cihaz tarayıcısı	LAN ağı için	Docker ağı için
Eşleştirme	Fiziksel ve uzaktan	Uzaktan
İnternetten güvenlik duvarı portlarını açın	-	-
Uçtan uca VPN	✓	✓
Kullanıcı erişim yönetimi	TOSIBOX® Key İstemcisinden veya TOSIBOX® Sanal Merkezi Lock	TOSIBOX® Key İstemcisinden veya TOSIBOX® Sanal Merkezi Lock

3 Docker temelleri

3.1 Docker konteynerlerini Anlama

Bir yazılım konteyneri, uygulamaları dağıtmanın modern yoludur. Docker konteyneri, Docker platformunun üzerinde çalışan, altta yatan işletim sisteminden ve diğer uygulamalardan güvenli ve emniyetli bir şekilde izole edilmiş bir yazılım paketidir. Konteyner, kodu ve tüm bağımlılıklarını paketleyerek uygulamanın hızlı ve güvenilir bir şekilde çalışmasını sağlar.

Docker, taşınabilirliği ve sağlamlığı sayesinde sektörde büyük ilgi görüyor. Uygulamalar, çok çeşitli cihazlara güvenli ve kolay bir şekilde kurulabilen bir konteyner içinde çalışacak şekilde tasarlanabilir. Uygulama hakkında endişelenmenize gerek yok Sistem yazılımına veya mevcut uygulamalara müdahale edebilmek. Docker aynı ana bilgisayarda birden fazla konteyner çalıştırmayı da destekler.

Docker ve konteyner teknolojisi hakkında daha fazla bilgi için www.docker.com adresine bakın.

3.2 Docker'a Giriş

Docker platformunun birçok çeşidi vardır. Docker, güçlü sunuculardan küçük taşınabilir cihazlara kadar çok sayıda sisteme kurulabilir. TOSIBOX® Lock for Container, Docker platformunun kurulu olduğu herhangi bir cihazda çalışabilir.

TOSIBOX® Lock for Container'ın nasıl kurulacağını anlamak için Docker'ın nasıl çalıştığını ve ağları nasıl yönettiğini bilmek önemlidir.

Docker, altta yatan cihazı tahmin eder ve yüklü konteynerler için yalnızca ana bilgisayara özel bir ağ oluşturur. Lock for Container, ana bilgisayarı Docker ağı üzerinden görür ve yönetilen bir ağ cihazı olarak değerlendirir. Aynı durum aynı ana bilgisayarda çalışan diğer konteynerler için de geçerlidir. Tüm konteynerler Lock for Container ile ilgili ağ cihazlarıdır.

Docker çok sayıda farklı ağ moduna sahiptir; bridge, host, overlay, macvlan veya none. Lock for Container, farklı bağlantı senaryolarına bağlı olarak çoğu mod için yapılandırılabilir. Docker, ana cihaz içinde bir ağ oluşturur. Temel ağ yapılandırması kullanıldığında LAN tipik olarak Lock for Container üzerinde statik yönlendirme gerektiren farklı bir alt ağ üzerindedir.

4 Bağlantı senaryosu örnekleri

4.1 Key Client'tan Lock for Container'a

TOSIBOX® Key Client'tan fiziksel ana cihaz ağına veya TOSIBOX® Lock for Container çalıştıran ana cihazdaki Docker ağına bağlantı, desteklenen en basit kullanım durumudur. Bağlantı, ana cihazda sonlanan TOSIBOX® Key Client'tan başlatılır.

Bu seçenek, ana cihazın veya ana cihazdaki Docker konteynerlerinin uzaktan yönetimi için çok uygundur.

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

4.2 Lock for Container aracılığıyla Key İstemci veya Mobil İstemciden ana cihaz LAN'ına

TOSIBOX® Key İstemcisinden ana bilgisayara bağlı cihazlara bağlantı, önceki kullanım durumunun bir uzantısıdır. Tipik olarak en basit kurulum, ana cihazın aynı zamanda anahtarlama ve İnternet erişimini koruyan cihazlar için ağ geçidi olması durumunda elde edilir. Statik yönlendirme erişiminin yapılandırılması LAN ağ cihazlarına genişletilebilir.

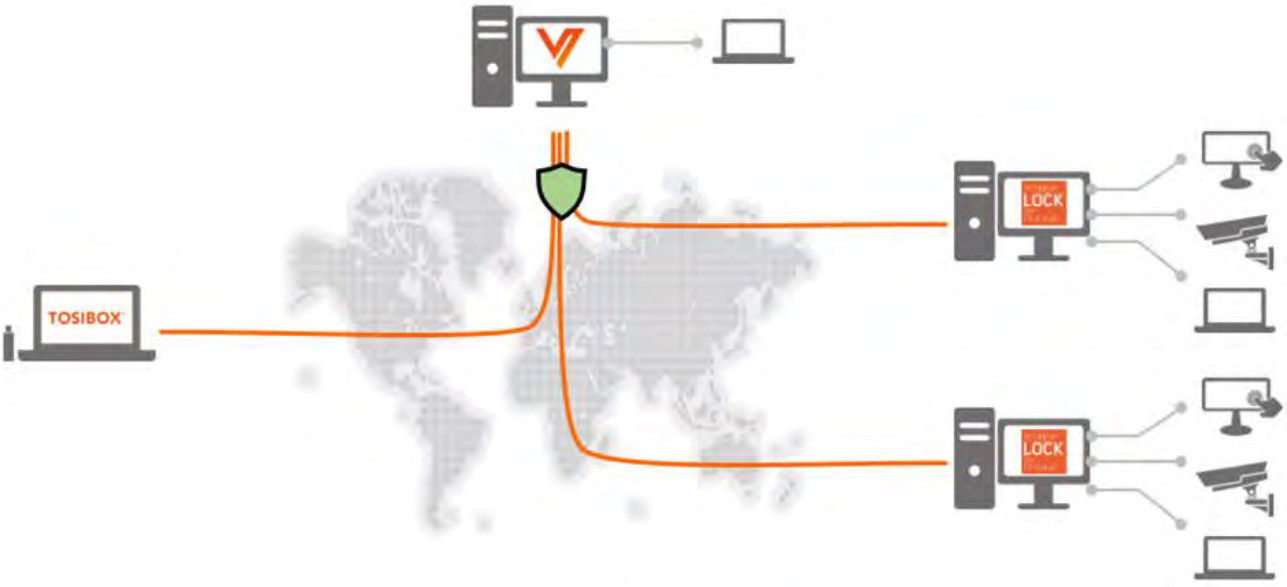
Bu seçenek, ana cihazın kendisinin ve yerel ağın uzaktan yönetimi için çok uygundur. Ayrıca mobil iş gücü için de uygundur.

Şekil 2: TOSIBOX® Key Client'tan TOSIBOX® Lock for Container arkasındaki cihazlara bağlantı

4.3 Lock for Container aracılığıyla Sanal Merkezi Lock'tan Ana cihaz LAN'ına

TOSIBOX® Sanal Merkezi Lock ağa eklendiğinde en esnek yapılandırma elde edilir. Ağ erişimi TOSIBOX® Sanal Merkezi Lock üzerinde cihaz bazında yapılandırılabilir. Kullanıcılar ağa TOSIBOX® Key İstemcilerinden bağlanırlar.

Bu seçenek, özellikle büyük ve karmaşık ortamlarda sürekli veri toplama ve merkezi erişim yönetimi için hedeflenmiştir. TOSIBOX® Virtual Central Lock'tan TOSIBOX® Lock for Container'a VPN tüneli, ölçeklenebilir makineler arası iletişime izin veren iki yönlü bir bağlantıdır.

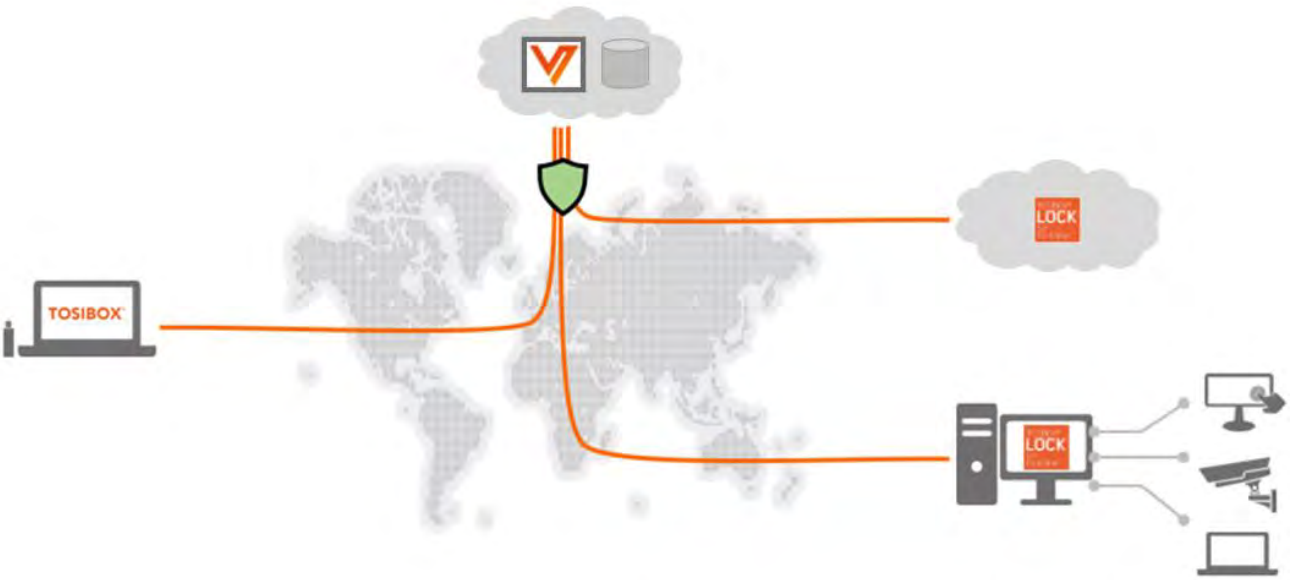


Şekil 3: TOSIBOX® Key İstemcisinden TOSIBOX® Sanal Merkezi Lock aracılığıylaTOSIBOX® Lock for Container arkasındaki cihazlara bağlantı

4.4 Bulutta çalışan Sanal Merkezi Lok'tan Lock for Container aracılığıyla başka bir bulut örneğine

Lock for Container mükemmel bir bulut bağlayıcısıdır, iki farklı bulutu veya aynı bulut içindeki bulut örneklerini güvenli bir şekilde bağlayabilir. Bunun için ana bulutta kurulu Virtual Central Lock ile istemci bulut sistem(ler)inde kurulu Lock for Container gerekir.

Bu seçenek fiziksel sistemleri buluta veya ayrı bulut sistemlerini birbirine bağlamayı hedefler. TOSIBOX® Virtual Central Lock'tan TOSIBOX® Lock for Container'a VPN tüneli, ölçeklenebilir buluttan buluta iletişim sağlayan iki yönlü bir bağlantıdır.



Şekil 4: TOSIBOX® Sanal Merkezi Lock aracılığıyla TOSIBOX® Lock for Container ile TOSIBOX® Keyr İstemcisinden buluta bağlantı

5 Lisanslama

5.1 Giriş

TOSIBOX® Lock for Container etkinleştirilmeden bir cihaza önceden yüklenebilir. Etkin olmayan bir Lock for Container iletişim kuramaz veya güvenli bağlantılar oluşturamaz. Etkinleştirme, Lock for Container'ın TOSIBOX® ekosistemine bağlanmasını ve VPN bağlantıları sunmaya başlamasını sağlar. Lock for Container'ı etkinleştirmek için bir Aktivasyon Koduna ihtiyacınız vardır. Aktivasyon Kodunu Tosibox satıştan talep edebilirsiniz. (https://www.tosibox.com/company-contact-us)

Lock for Container'ın kurulumu bir şekilde yazılımın kullanıldığı cihaza bağlıdır ve duruma göre değişebilir. Zorluk yaşarsanız,

yardım için Tosibox Global Destek'e göz atın (www.tosibox.com/support).

Üçüncü taraf pazar yerlerinden kurulum yaparken bu yönergeler geçerli olmayabilir, üretici tarafından sağlanan talimatları izleyin.

Lock for Container'ı etkinleştirmek ve çalıştırmak için bir İnternet bağlantısına ihtiyacınız olduğunu unutmayın.

5.2 Kullanılacak lisansın taşınması

TOSIBOX® Lock for Container kullanıcı lisansı, Aktivasyon Kodunun kullanıldığı cihaza bağlıdır. Her Lock for Container Aktivasyon Kodu yalnızca bir kerelik kullanım içindir. Etkinleştirme ile ilgili sorun yaşarsanız Tosibox Destek ile iletişime geçin.

6 Kurulum ve güncelleme

TOSIBOX® Lock for Container, Docker Compose kullanılarak veya komutlar manuel olarak girilerek yüklenir. Lock for Container kurulmadan önce Docker kurulmalıdır.

Kurulum adımları

1. Docker'ı ücretsiz olarak indirin ve kurun, bkz. www.docker.com.
2. Konteyner için Kilidi Docker Hub'dan hedef ana cihaza çekin

---

Üçüncü taraf pazarlardan yükleme yaparken bu yönergeler geçerli olmayabilir, cihaz üreticisi tarafından sağlanan talimatları izlemelisiniz.

6.1 Docker'ı indirin ve yükleyin

Docker çok çeşitli işletim sistemleri ve cihazlar için kullanılabilir. Cihazınıza indirmek ve kurmak için www.docker.com adresine bakın

6.2 Docker Hub'dan Konteyner için Kilidi Çekin

https://hub.docker.com/r/tosibox/lock-for-container adresindeki Tosibox Docker Hub deposunu ziyaret edin. Orada verilen kurulum talimatlarını izleyin.

Docker Compose dosyası, uygun konteyner yapılandırması için sağlanmıştır. Komut dosyasını çalıştırın veya gerekli komutları komut satırına manuel olarak yazın. Komut dosyasını gerektiği gibi değiştirebilirsiniz.

7 Etkinleştirme ve kullanıma alma

Güvenli uzak bağlantılar oluşturabilmeniz için TOSIBOX® Lock for Container etkinleştirilmeli ve Tosibox ekosisteminize bağlanmalıdır.

Özet

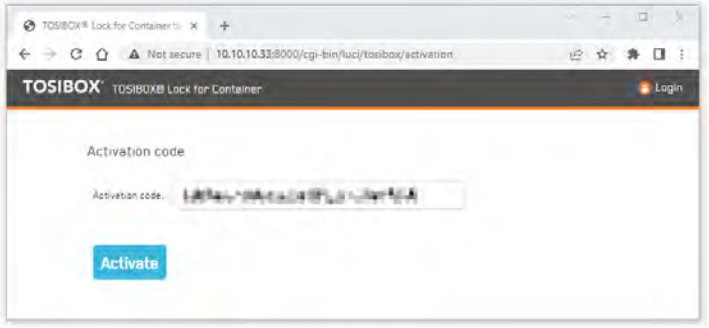
1. Cihazınızda çalışan Lock for Container için web kullanıcı arayüzünü açın.
2. Tosibox tarafından sağlanan Aktivasyon Kodu ile Konteyner için Kilidi etkinleştirin.
3. Varsayılan kimlik bilgileriyle web kullanıcı arayüzünde oturum açın.
4. Uzaktan Eşleştirme Kodunu oluşturun.
5. Konteyner Kilidini TOSIBOX® ağınıza eklemek için TOSIBOX® Key İstemcisi üzerindeki Uzaktan Eşleştirme işlevini kullanın.
6. Erişim hakları verin.
7. Bir HUB'a Bağlanma (Sanal Merkezi Kilit)

7.1 Lock for Container web kullanıcı arayüzünü açın

TOSIBOX® Lock for Container web kullanıcı arayüzünü açmak için, ana bilgisayarda herhangi bir web tarayıcısını başlatın ve http://localhost:8000 adresini yazın (Lock for Container'ın 8000 numaralı bağlantı noktasını dinlemek için varsayılan ayarlarla yüklendiğini varsayarak)

7.2 Lock for Container Etkinleştir

1. Web kullanıcı arayüzünde soldaki Durum alanında "Activation required" mesajını arayın.
2. Aktivasyon sayfasını açmak için "Activation required" bağlantısına tıklayın.
3. Etkinleştirme Kodunu kopyalayarak veya yazarak Konteyner Kilidini etkinleştirin ve Etkinleştir düğmesine tıklayın.



Şekil 5: TOSIBOX® Lock for Container etkinleştirme sayfası

4. Ek yazılım bileşenleri indirilir ve ekranda "Activation completed" mesajı görüntülenir. Lock for Container artık kullanıma hazırdır.

Etkinleştirme başarısız olursa, Etkinleştirme Kodunu iki kez kontrol edin, olası hataları düzeltin ve tekrar deneyin.

7.3 Web kullanıcı arayüzünde oturum açın

TOSIBOX® Lock for Container etkinleştirildikten sonra web kullanıcı arayüzüne giriş yapabilirsiniz. Menü çubuğundaki Oturum Aç bağlantısını tıklayın.

Varsayılan kimlik bilgileriyle oturum açın:

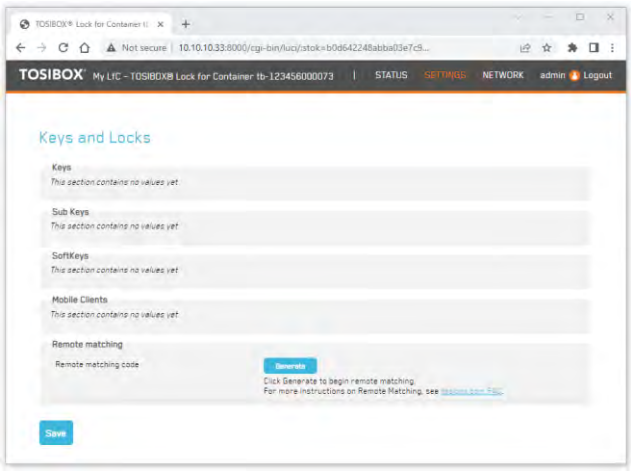
- Username: admin
- Password: admin

Oturum açtıktan sonra Durum, Ayarlar ve Ağ menüleri görünür hale gelir.

Lock for Container'ı kullanabilmeniz için EULA'yı kabul etmeniz gerekir.

7.4 Uzaktan Eşleştirme kodu oluşturma

1. TOSIBOX® Lock for Container'da oturum açın ve *Settings* > *Keys Locks* 'a gidin ve sayfanın en altına inerek Remote Matching 'i bulun.



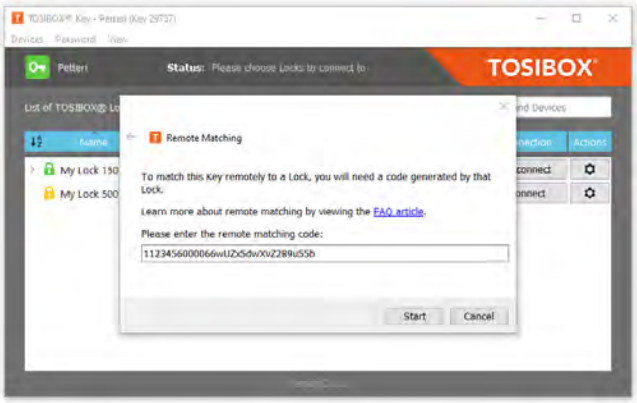
Şekil 6: Remote Matching Kodu oluşturma sayfası

2. Uzaktan Eşleştirme Kodunu oluşturmak için Create düğmesine tıklayın.
3. Kodu kopyalayın ve ağ için Master Key 'e sahip olan ağ yöneticisine gönderin. Yalnızca ağ yöneticisi Konteyner Kilidini ağa ekleyebilir.

7.5 Uzaktan Eşleştirme

TOSIBOX® Anahtarını iş istasyonunuza yerleştirin ve TOSIBOX® Anahtar İstemcisi açılır. Eğer TOSIBOX® Key Client yüklü değilse, daha fazla bilgi için www.tosibox.com adresine göz atın. Ağınız için Ana Anahtarı kullanmanız gerektiğini unutmayın

Kimlik bilgilerinizle giriş yapın ve şu adrese gidin *Devices > Remote Matching*.



Şekil 7: TOSIBOX® Key İstemcisinde Uzaktan Eşleştirme

Uzak Eşleştirme kodunu metin alanına yapıştırın ve Start'a tıklayın. Key İstemcisi TOSIBOX® altyapısına bağlanacaktır. Ekranda "Remote Matching completed successfully" yazısı belirdiğinde, Konteyner Kilidi ağınıza eklenmiş demektir. Key İstemci arayüzünde hemen görebilirsiniz.

7.6 Erişim hakları verin

Siz ek izinler verene kadar TOSIBOX® Lock for Container'a erişimi olan tek kullanıcı sizsiniz. Erişim hakları vermek için TOSIBOX® Key Client'ı açın ve *Devices* > *Manage Keys*'e gidin. Erişim haklarını gerektiği gibi değiştirin.

7.7 Sanal Merkezi Lock'a Bağlanma

Ağınızda TOSIBOX® Virtual Central Lock kuruluysa, her zaman açık, güvenli VPN bağlantısı için Lock for Container'ı bağlayabilirsiniz.

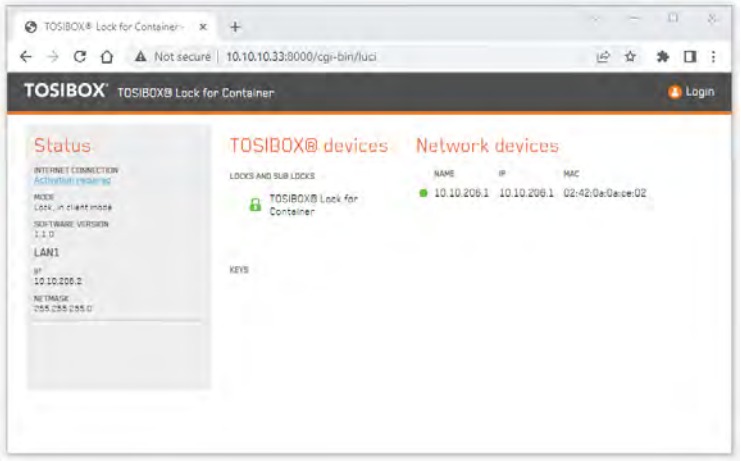
1. TOSIBOX® Key Client'ı açın ve şu adrese gidin *Devices > Connect Locks*.
2. Yeni yüklenen Konteyner Kilidini ve Sanal Merkezi Kilidi işaretleyin ve Next 'e tıklayın.
3. Bağlantı Türü Seç için her zaman Katman 3'ü seçin (Katman 2 desteklenmez), Next 'e tıklayın.
4. Onay iletişim kutusu görüntülenir, Save 'e tıklayın ve VPN tüneli oluşturulur.

Artık Virtual Central Lock'a bağlanabilir ve Erişim Grubu ayarlarını gerektiği gibi atayabilirsiniz.

8 Kullanıcı arayüzü

TOSIBOX® web kullanıcı arayüzü ekranı dört bölüme ayrılmıştır:

A. Menu bar – Ürün adı, menü komutları ve Giriş/Çıkış komutu
B. Status area – Sisteme genel bakış ve genel durum
C. TOSIBOX® devices – Lock for Container ile ilgili Lock ‘lar ve Key ‘ler
D. Network devices – Ağ taraması sırasında keşfedilen cihazlar veya diğer Docker kapsayıcıları



Şekil 8: Etkinleştirilmeyi bekleyen Lock for Container

TOSIBOX® Lock for Container etkinleştirilmediğinde, web kullanıcı arayüzü Durum alanında “Activation required” bağlantısını görüntüler. Bağlantıya tıklamak sizi aktivasyon sayfasına götürür. Etkinleştirme için Tosibox'tan bir etkinleştirme Kodu gereklidir. Etkin olmayan bir Lock for Container İnternet ile iletişim kurmaz, bu nedenle Lock for Container etkinleştirilene kadar İnternet Bağlantısı durumu BAŞARISIZ olarak görüntülenir.

Ekranınızın ayarlara ve ağınıza bağlı olarak farklı görünebileceğini unutmayın.

8.1 Kullanıcı arayüzünde gezinme

Status menü

Status menü komutu, ağ yapılandırması, eşleşen tüm TOSIBOX® Lock'ları ve TOSIBOX® Key'leri ve olası LAN cihazları veya TOSIBOX® Lock for Container'ın keşfettiği diğer konteynerler hakkında temel bilgileri içeren Durum görünümünü açar.

TOSIBOX® Lock for Container kurulum sırasında bağlı olduğu ağ arayüzünü tarar. Varsayılan ayarlarla Lock for Container yalnızca ana bilgisayar Docker ağını tarar ve keşfedilen tüm konteynerleri listeler. LAN ağ taraması, gelişmiş Docker ağ ayarları ile fiziksel LAN cihazlarını keşfetmek için yapılandırılabilir.

Settings menü

Ayarlar menüsü, TOSIBOX® Lock'lar ve TOSIBOX® key'ler için özellikleri değiştirmeyi, bir Lock'un adını değiştirmeyi, yönetici hesabının şifresini değiştirmeyi, Lock for Container ile eşleşen tüm Key'leri kaldırmayı ve gelişmiş ayarları değiştirmeyi mümkün kılar.

Network menü

TOSIBOX® Lock for Container'ın ağ LAN bağlantısı için statik rotalar Ağ menüsünde düzenlenebilir. Statik rotalar görünümü Lock for Container üzerindeki tüm aktif rotaları gösterir ve gerekirse daha fazlasını eklemeye izin verir.

Statik rota görünümü, rota için LAN IP adresi değiştirilemediğinde veya düzenlenmek istenmediğinde yapılandırılabilen rotalar için özel bir NAT alanı içerir. NAT, LAN IP adresini maskeler ve verilen NAT adresiyle değiştirir. Bunun etkisi, artık gerçek LAN IP adresi yerine NAT IP adresinin TOSIBOX® Key'e bildirilmesidir. NAT IP adresi boş bir IP adresi aralığından seçilirse, bu, aynı LAN IP aralığının birden fazla ana cihazda kullanılması durumunda ortaya çıkabilecek olası IP çakışmalarını çözer.

9 Temel yapılandırma

9.1 Uzaktan Eşleştirme kodu oluşturma

Uzaktan eşleştirme kodunun oluşturulması ve uzaktan eşleştirme süreci 7.4 - 7.5 bölümlerinde açıklanmıştır.

9.2 Admin şifresini değiştirme

TOSIBOX® Lock for Container web kullanıcı arayüzünde oturum açın ve şifreyi değiştirmek için *Settings* > *Change admin password* 'e gidin. Web kullanıcı arayüzüne Master Key(ler)den bir VPN bağlantısı üzerinden uzaktan da erişebilirsiniz. Web kullanıcı arayüzüne diğer Key'lerden veya ağlardan erişme ihtiyacı varsa, erişim haklarına açıkça izin verilebilir.

9.3 LAN erişimi

Varsayılan olarak, TOSIBOX® Lock for Container ana cihaza veya ana cihazla aynı ağda bulunan LAN cihazlarına erişime sahip değildir.

Konteyner için Kilit üzerinde statik rota yapılandırarak LAN tarafına erişebilirsiniz. Yönetici olarak oturum açın ve Network > Static routes 'a gidin. Statik IPv4 Rotaları listesinde alt ağa erişmek için bir kural ekleyebilirsiniz.

- Interface: LAN
- Hedef: Alt ağ IP adresi (örn. 10.10.10.33)
- IPv4 Netmask: Alt ağa göre maske (örn. 255.255.255.255)
- IPv4 Ağ Geçidi: LAN ağına giden ağ geçidinin IP adresi
- NAT: Fiziksel adresi maskelemek için kullanılan IP adresi (opsiyonel)
  Metrik ve MTU varsayılan olarak bırakılabilir.

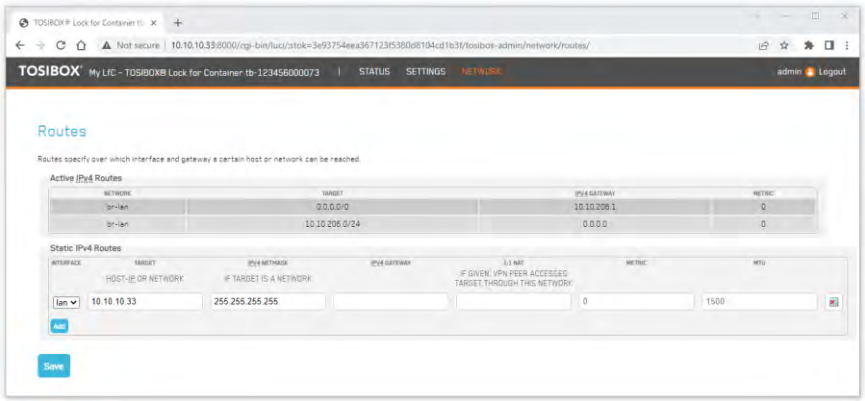


Figure 9: Static routes

9.4 Lock'un adını değiştirme

TOSIBOX® Lock for Container web kullanıcı arayüzünü açın ve admin olarak oturum açın. "Settings > Lock name" kısmına gidin ve yeni adı yazın. Save 'e basın ve yeni isim ayarlanır. Bu aynı zamanda TOSIBOX® Key İstemcisinde görülen adı da etkileyecektir.

9.5 TOSIBOX® uzaktan destek erişimini etkinleştirme

TOSIBOX® Lock for Container web kullanıcı arayüzünü açın ve admin olarak oturum açın. " Settings > Advanced settings " kısmına gidin ve Remote Support checkbox ‘ı işaretleyin. Save 'e tıklayın. Tosibox desteği artık cihaza erişebilir.

9.6 TOSIBOX® SoftKey veya TOSIBOX® Mobil İstemci erişimini etkinleştirme

TOSIBOX® Key İstemcisini kullanarak yeni kullanıcılara erişim ekleyebilirsiniz.
Kullanım kılavuzu için www.tosibox.com/support adresine bakın.

10 Rotalar için NAT

Rotalar için NAT, rotalar için 1:1 NAT tanımlama yeteneği sağlar, yani Key ve HUB'ın cihaza cihazın dahili olarak sahip olduğundan başka bir ağ üzerinden erişmesine izin verir. Rotalar için NAT, LAN ağları için Node ürün yazılımında bulunan 1:1 NAT'a benzer.

Rotalar için NAT, örneğin birkaç Lock for Container'ın potansiyel olarak aynı dahili, LAN olmayan ağlara sahip olabileceği durumlarda kullanılabilir. Bu dahili ağ bir rota olarak kullanıldığında (örn. 10.10.10.0/24) Key bu ağa sorunsuz bir şekilde erişebilir ancak Key aynı dahili ağa sahip iki farklı Lock for Container'a bağlıysa rotalar çakışacaktır.

Pratik kısıtlamalar nedeniyle, dahili ağlar değiştirilemeyebilir. Her iki sisteme aynı anda bağlanmak için rotalar için NAT kullanılabilir.

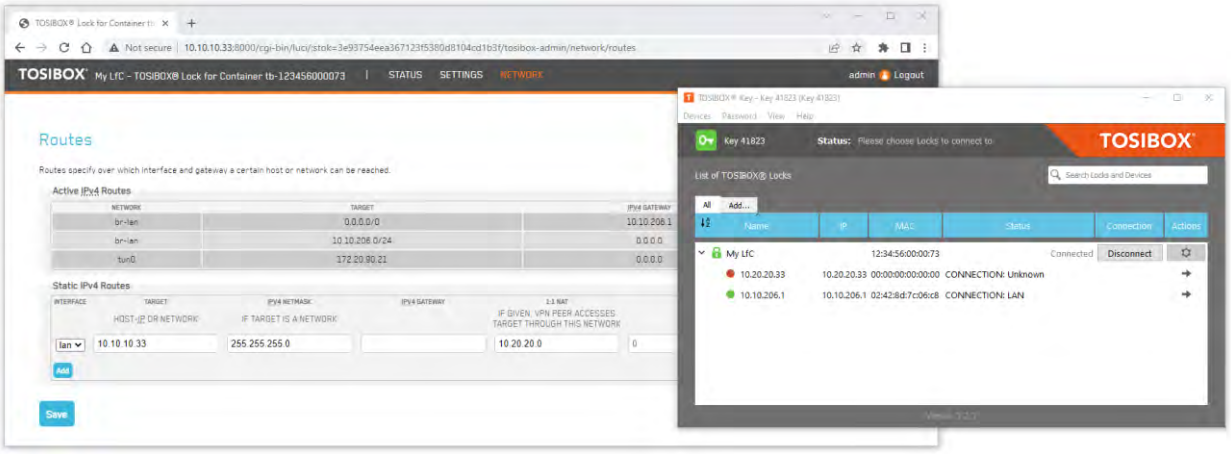
Kullanım örneği

Örneğin, Key veya HUB'a bildirilen bir rota 10.10.10.33/24 ise, bu adres istenen başka bir adrese, örneğin 10.20.20.0 netmapping'ine sahip olarak 10.20.20.33/24'e çevrilebilir.

Kısıtlamalar:

- Her iki Lock for Containers da 10.10.10.0/24 dahili ağ tanımına sahip olabilir
- Lock for Containers'ın herhangi biri için 1:1 NAT yapılandırın, böylece farklı bir ağın reklamını yaparak Key ve HUB'daki ağ çakışması sorunlarını çözecektir
- NAT'lanan adresi kullanarak "Add network device" işleviyle Durum sayfasına ana cihazı ekleyin

Bu şekilde cihazlar, istemciler için çakışan rotalara sahip olmadan Key kullanıcı arayüzünden erişilebilirken aynı dahili, LAN olmayan ağlara sahip olabilir.



Şekil 10: Lock for Container üzerinde yapılandırılmış 1:1 NAT

Manuel olarak eklenen cihaz erişilebilir değilmiş gibi kırmızı renkte görünecektir, ancak bunun nedeni LAN taramasının LAN alt ağını geçememesidir. LAN taraması yalnızca Docker ağındaki kapsayıcıları keşfedebilir, manuel olarak eklenen LAN cihazlarını keşfedemez.

Lock for Container kullanıcı arayüzünde 1:1 NAT yapılandırıldıktan sonra cihaza yapılandırılan NAT IP adresi üzerinden erişilebileceğini unutmayın. Bu örnekte çalışma adresi 10.10.10.33 değil 10.20.20.33 'tür.

Rotalar için NAT, TOSIBOX® Lock for Container sürüm 1.1'de sunulan yeni bir özelliktir. Rotalar için NAT, ana cihazdan çekirdek desteği gerektirir.

---

11 Kurulumu Kaldırma

Kurulumu Kaldırma adımları

1. TOSIBOX® Lock for Container web kullanıcı arayüzünü kullanarak tüm Key serileştirmelerini kaldırın.
2. Docker komutlarını kullanarak TOSIBOX® Lock for Container'ı kaldırın.
3. Gerekirse Docker'ı kaldırın.
4. Lock for Container'ı başka bir cihaza kurmayı düşünüyorsanız, lisans geçişi için lütfen Tosibox Destek ile iletişime geçin.

12 Sistem gereksinimleri

Aşağıdaki öneriler genel amaç için çok uygundur. Ancak, gereksinimler ortamlar ve kullanımlar arasında değişiklik gösterebilir.

Lock for Container'ın aşağıdaki işlemci mimarilerinde çalışması hedeflenmektedir:

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

Önerilen yazılım gereksinimleri

- Docker ve Docker Engine tarafından desteklenen herhangi bir 64 bit Linux işletim sistemi - Community v20 veya üstü yüklü ve çalışıyor(www.docker.com)
- Docker Compose
- Linux kernel sürümü 4.9 veya üstü
- Tam işlevsellik için IP tablolarıyla ilgili belirli çekirdek modülleri gerekir
- WSL2 etkinleştirilmiş herhangi bir 64 bit Windows işletim sistemi (Linux için Windows Alt Sistemi v2)
- Kurulum sudo veya root seviyesinde kullanıcı hakları gerektirir

Önerilen sistem gereksinimleri

- 50MB RAM
- 50MB hard disk alanı
- ARM 32-bit veya 64-bit işlemci, Intel veya AMD 64-bit çift çekirdekli işlemci
- İnternet bağlantısı

Gerekli açık güvenlik duvarı bağlantı noktaları

- Giden TCP: 80, 443, 8000, 57051

- Giden UDP: rastgele, 1-65535
- Gelen: yok

13 Sorun Giderme

TOSIBOX® Key'den ana cihaz web kullanıcı arayüzünü açmaya çalışıyorum ancak başka bir cihaz alıyorum

Sorun: Örneğin TOSIBOX® Key İstemcinizdeki IP adresine çift tıklayarak bir cihaz web kullanıcı arayüzü açıyorsunuz ancak bunun yerine yanlış kullanıcı arayüzünü alıyorsunuz.

Çözüm: Web tarayıcınızın web sitesi verilerini önbelleğe almadığından emin olun. Web tarayıcınızı sayfayı tekrar okumaya zorlamak için verileri temizleyin. Şimdi istenen içeriği görüntülemelidir.

Ana bilgisayara erişmeye çalışıyorum ancak "Bu siteye erişilemiyor" mesajı alıyorum

Sorun: Örneğin TOSIBOX® Key İstemcinizdeki IP adresine çift tıklayarak bir cihaz web kullanıcı arayüzünü açıyorsunuz ancak bir süre sonra web tarayıcınızda 'Bu siteye ulaşılamıyor' mesajı alıyorsunuz.

Çözüm: Diğer bağlantı yöntemlerini deneyin, ping önerilir. Bu da aynı hatayla sonuçlanırsa, ana cihaza giden bir rota olmayabilir. Statik rotaların nasıl oluşturulacağını öğrenmek için bu belgenin başındaki yardım bölümüne bakın.

Ana cihazda çalışan başka bir web servisim var, Lock for Container'ı çalıştırabilir miyim

Sorun: Varsayılan bağlantı noktasında (bağlantı noktası 80) çalışan bir web hizmetiniz var ve cihaza başka bir web hizmeti yüklemek çakışacaktır.

Çözüm: Lock for Container bir web kullanıcı arayüzüne sahiptir ve bu nedenle erişilebileceği bir bağlantı noktasına ihtiyaç duyar. Diğer tüm hizmetlere rağmen, Lock for Container cihaza kurulabilir ancak başka bir bağlantı noktasında yapılandırılması gerekir. Mevcut web hizmetleri için kullanılandan farklı bir bağlantı noktası kullandığınızdan emin olun. Bağlantı noktası kurulum sırasında yapılandırılabilir.

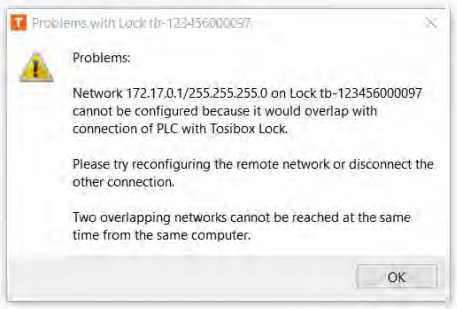
Kurulum "durdurulmuş bir durumda yürütülemiyor: bilinmiyor" hatasıyla başarısız oluyor

Sorun: TOSIBOX® Lock for Container'ı yüklüyorsunuz ancak yüklemenin sonunda ”`cannot exec in a stopped state: unknown`” veya benzeri bir hata alıyorsunuz.

Çözüm: Komut satırında “`docker ps`“ komutunu çalıştırın ve konteynerin çalışıp çalışmadığını doğrulayın. Lock for Container yeniden başlatma döngüsündeyse, yani durum alanında

“Restarting (1) 4 seconds ago”, gibi bir şey görüntüleniyorsa, bu konteynerin kurulu olduğunu ancak başarılı bir şekilde çalışamadığını gösterir. Lock for Container cihazınızla uyumlu olmayabilir ya da kurulum sırasında yanlış ayarları kullanmış olabilirsiniz. Cihazınızın bir ARM veya Intel işlemciye sahip olup olmadığını doğrulayın ve uygun kurulum anahtarını kullanın.

VPN'i açarken IP adresi çakışması alıyorum



Sorun: TOSIBOX® Key Client'ınızdan iki Lock for Container örneğine iki eşzamanlı VPN tüneli açıyorsunuz ve çakışan bağlantılar hakkında bir uyarı alıyorsunuz.

Çözüm: Her iki Lock for Container örneğinin de aynı IP adresinde yapılandırılıp yapılandırılmadığını doğrulayın ve rotalar için NAT'ı yapılandırın ya da her iki yüklemede de adresi yeniden yapılandırın.
Bir Lock for Container'ı özel bir IP adresine yüklemek için yükleme sırasında ağ komutlarını kullanın.

VPN verimi düşük

Sorun: Bir VPN tüneliniz var ancak düşük veri çıkışı yaşıyorsunuz.

Çözüm: TOSIBOX® Lock for Container VPN verilerini şifrelemek/şifresini çözmek için cihazın HW kaynaklarını kullanır. (1) cihazınızdaki işlemci ve bellek kullanımını, örneğin Linux top komutu ile, (2) Lock for Container menüsü "Settings / Advanced settings"dan hangi VPN şifresini kullandığınızı, (3) İnternet erişim sağlayıcınızın ağ hızınızı düşürüp düşürmediğini, (4) rota boyunca olası ağ tıkanıklıklarını ve (5) giden UDP bağlantı noktalarının en iyi performans için önerildiği gibi açık olup olmadığını doğrulayın. Başka hiçbir şey yardımcı olmazsa, ne kadar veri aktardığınızı ve bunu azaltmanın mümkün olup olmadığını kontrol edin.

Web tarayıcımda "Bağlantınız gizli değil" mesajı alıyorum

Sorun: Lock for Container web kullanıcı arayüzünü açmaya çalıştınız ancak Google Chrome tarayıcınızda "Bağlantınız özel değil" mesajı aldınız.

Çözüm: Google Chrome, ağ bağlantınız şifrelenmediğinde uyarı verir. Bu, internette çalışırken kullanışlıdır. Lock for Container, verileri Chrome'un tanımlayamayacağı son derece güvenli ve yüksek derecede şifrelenmiş bir VPN tüneli üzerinden iletir. Chrome'u bir TOSIBOX® VPN ile kullanırken, Chrome'un uyarısı güvenli bir şekilde göz ardı edilebilir. Web sitesine devam etmek için Gelişmiş düğmesine ve ardından "İlerle" bağlantısına tıklayın.