

FORTILOGGER

Kurulum Dökümanı *

V1.4.3

9.11.2017

* Bu döküman FortiLogger 3.1.7 versiyonu için hazırlanmıştır.

Ön Gereksinimler

FortiLogger'ı bilgisayarınıza kurmak için aşağıdaki ön gereksinimlere ihtiyaç duyulmaktadır:

1. Min. 8 GB Bellek, çift çekirdek işlemci, cihaz başına min. 100 GB disk alanı
(**Not:** Disk alanı log tutma ihtiyacınıza göre değişiklik gösterebilir)
2. 64 bit destekli Windows 7 ve üzeri masaüstü veya 64 bit destekli Windows 2008 R2 ve üzeri sunucu işletim sistemleri (32 bit işletim sistemi desteklenmemektedir)
3. Kritik uygulamalarınızın bulunduğu (Muhasebe, ERP, CRM, Active Directory, IP Santral vb.) aynı işletim sistemi üzerine kurulmaması (**Not:** Sanallaştırma platformlarına da kurulum yapılabilir)
4. Windows güncelleştirmelerinin yapılması
5. İnternet bağlantısı
6. Bölge ayarları olarak Türkiye'nin seçilmesi
7. Tarih ve saat ayarlarının güncel olması
(**Not:** Windows güncellemesi ile saat ayarları UTC+03:00 olarak güncellenebilir. Alternatif olarak UTC+03:00 olan bir bölge seçilerek internet üzerinden saat güncelleme seçeneği kapatılabilir)
8. 5651 sayılı kanun kapsamında logların imzalanarak yedeklenmesi işlemi FortiGate cihazının zamanını dikkate almaktadır. Lütfen FortiGate cihaz tarih ve saatinin doğru olduğundan emin olunuz.
9. FortiLogger Yazılımı FortiOS 5.2.6 ve üzeri FortiGate Firmware versiyonlarını desteklemektedir. Gelişkin özellikleri çalıştırabilmek için FortiOS 5.4.0 ve üzeri firmware versiyonları önerilmektedir.
10. FortiLogger Yazılımının internet erişiminde 53 UDP/DNS, 80 TCP/HTTP, 123 UDP/NTP, 443 TCP/HTTPS, 465 TCP/SMTS ve 587 TCP/SMTP portlarının açık olması gerekmektedir.

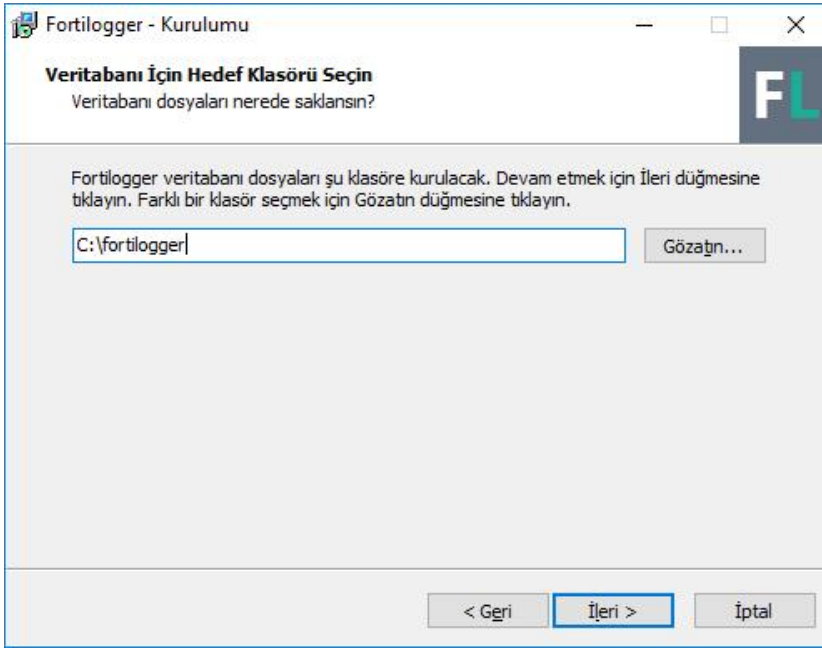
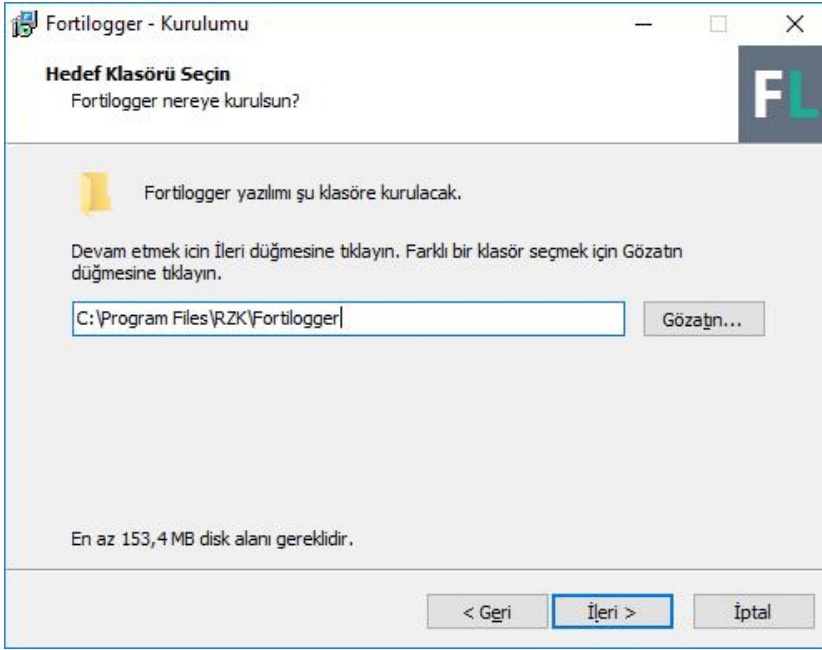
İndirme ve Kurulum

İndirme öncesi işlemler:

1. Cihaz entegrasyonu ve lisanslama işlemlerinizi kullanmanız için [FortiLogger Portal](https://www.fortilogger.com/login) (<https://www.fortilogger.com/login>) üzerinde yeni kullanıcı hesabı oluşturun.
2. Email adresinize gönderilen doğrulama linkine tıklayarak hesabınıza kayıtlı email adresini doğrulayın.
3. **Önemli uyarı:** FortiLogger'i kuracağınız bilgisayarın hassas bilgi ve uygulamaları içermediğinden emin olunuz.

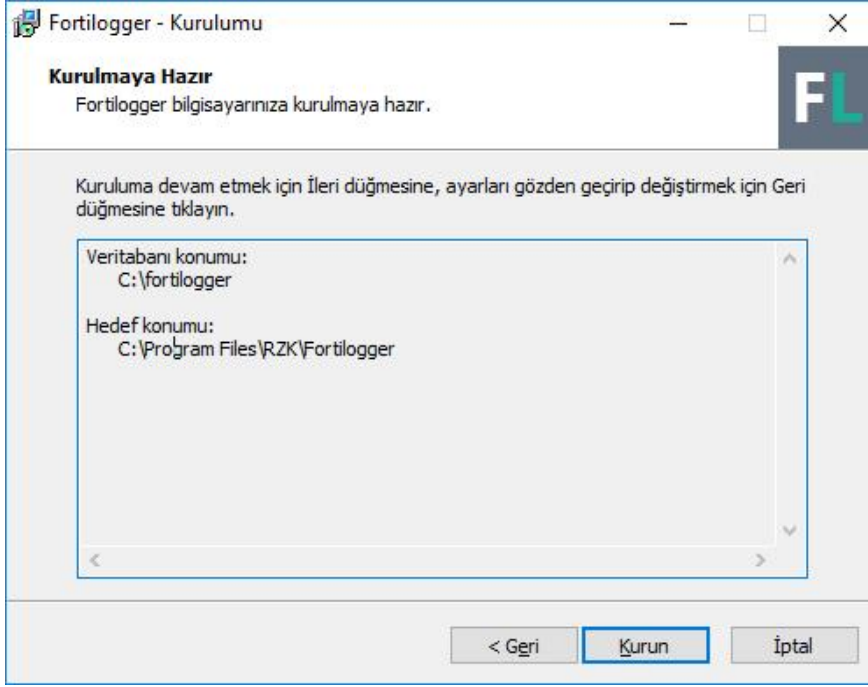
FortiLogger'i bilgisayarınıza kurmak için:

4. Yükleyici dosyasını indirin. (İndirme adresi: <https://www.fortilogger.com/download>)
5. İndirmiş olduğunuz yükleyici dosyasını başlatın.
6. Uygulamanın ve veritabanının kurulacağı yolu seçin
Önemli uyarı: Uygulama ve veritabanı yolu için local disk kullanınız. Network üzerinden diskler ve bilgisayara map edilmiş diskler üzerinden kurulum desteklenmemektedir. ISCSI bağlantılı diskler uzun vadede sağlıklı çalışmadıkları için tavsiye edilmez.
Uygulama ve veritabanı yolu tanımlarken Türkçe karakter ve Boşluk (Space) karakteri kullanmayınız.

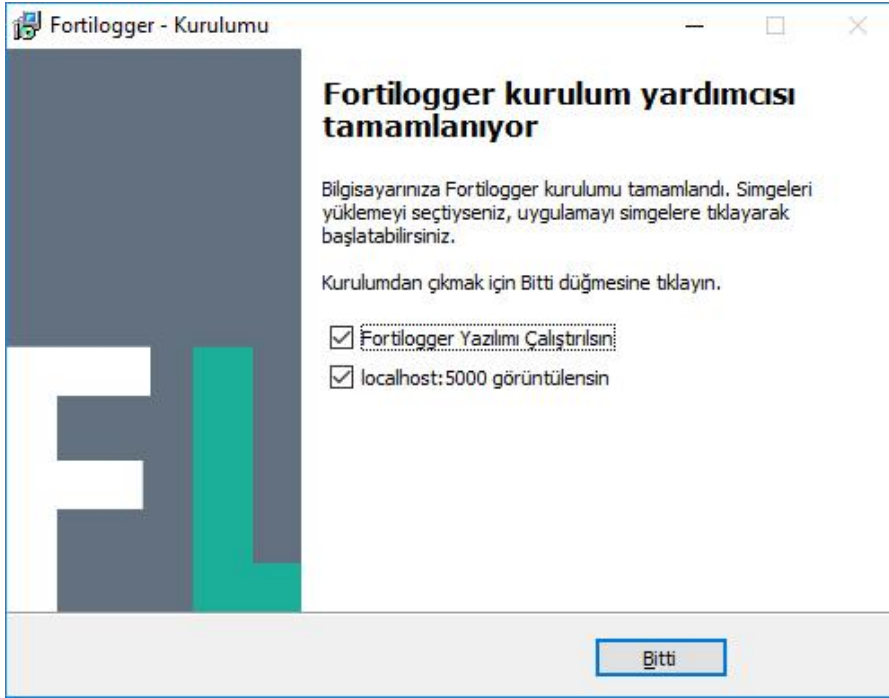


7. Yükleyici penceresini takip ederek kurulum işlemi tamamlayın.

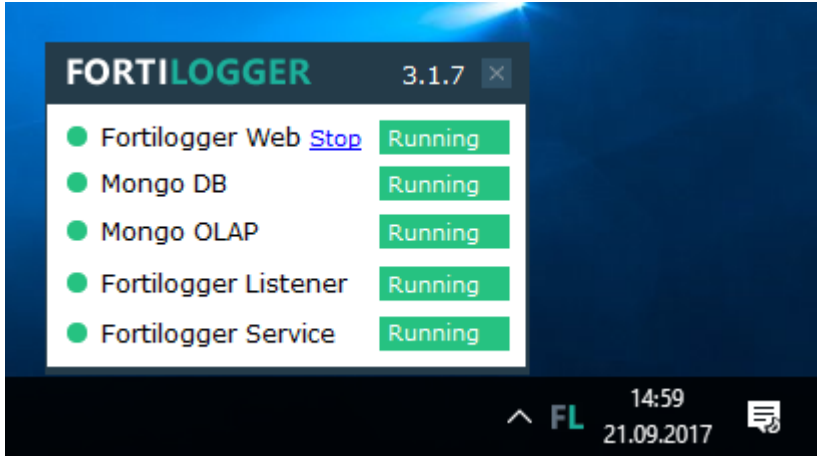
Not: İlk kez kurulum yapıyorsanız bilgisayarınızda bulunmaması halinde **MongoDB 3.2.1, IIS Express 10 ve .Net Framework 4.5** uygulamaları otomatik olarak indirilecek ve kurulacaktır.



8. Kurulum işlemi tamamlandığında "Bitti" butonuna basarak FortiLogger web arayüzünü (http://local_ip_adresiniz:5000) açabilirsiniz.



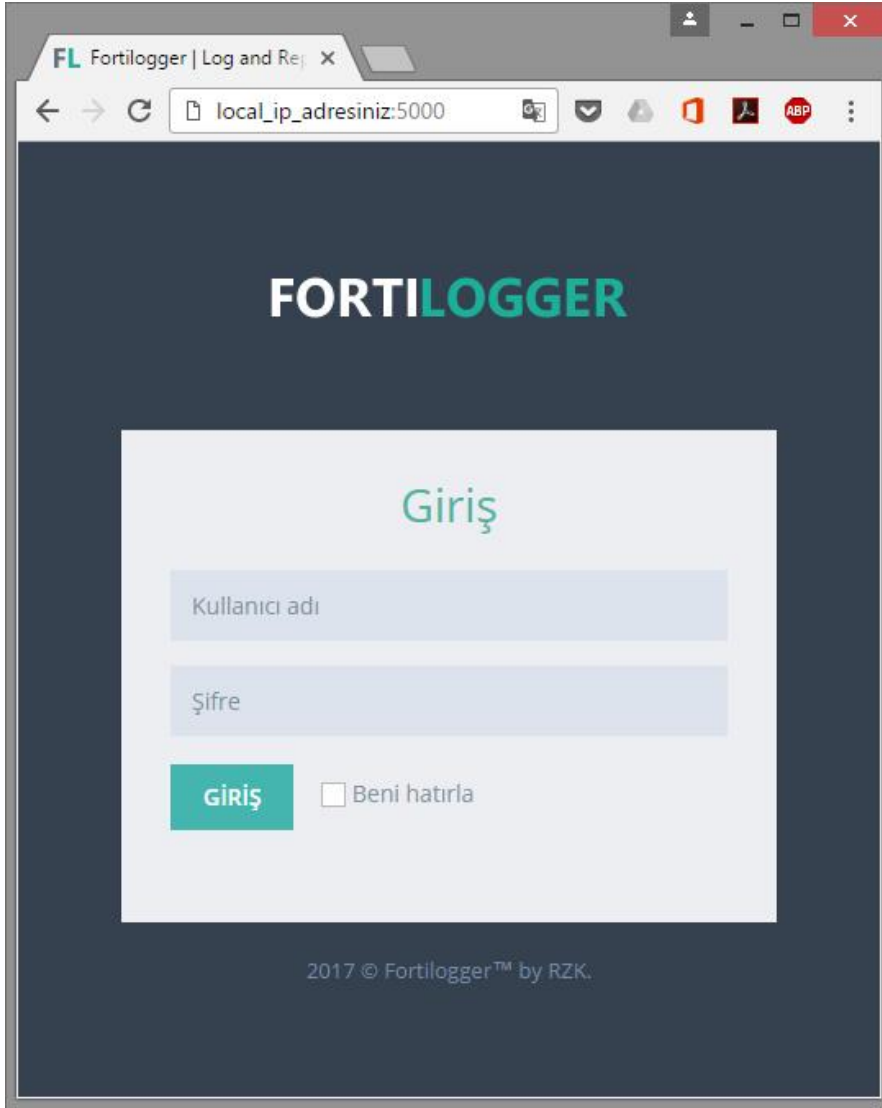
9. Dilerseniz kurulum işleminden sonra tray üzerinde servis ve web uygulaması durumlarını takip edebilirsiniz.



10. http://local_ip_adresiniz:5000 adresinde açılan web arayüzüne giriş yapabilirsiniz.

Varsayılan kullanıcı adı: **admin**

Varsayılan şifre: **admin**



Cihaz Entegrasyon

FortiLogger Yazılımı FortiOS 5.2.6 ve üzeri FortiGate Firmware versiyonlarını desteklemektedir. Gelişkin özellikleri çalıştırabilmek için FortiOS 5.4.0 ve üzeri firmware versiyonları önerilmektedir.

5651 sayılı kanun kapsamında logların imzalanarak yedeklenmesi işlemi FortiGate cihazının zamanını dikkate almaktadır. Lütfen FortiGate cihaz tarih ve saatinin doğru olduğundan emin olunuz.

FortiGate Syslog yönlendirme işlemi (1.yöntem):

FortiOS Firmware güncel versiyonlar için Log & Report > Log Settings sayfasından aşağıdaki gibi FortiLogger'in kurulu olduğu bilgisayarın IP ADRES bilgisini girebilirsiniz.

Remote Logging and Archiving

Send Logs to FortiAnalyzer/FortiManager

Send Logs to FortiCloud

Send Logs to Syslog

IP Address/FQDN:

FortiGate Syslog yönlendirme işlemi (2.yöntem):

FortiOS Firmware düşük versiyonlar için ise console üzerinden aşağıdaki komutları girebilirsiniz.
Dashboard > CLI Console

```
config log syslogd setting
set status enable
set server FortiLogger_ip_adresi
end
```

CLI Console

Detach   

```
Connected

FortiGate# config log syslogd setting
FortiGate(setting)# set status enable
FortiGate(setting)# set server fortilogger_ip_adresi
FortiGate(setting)# end
FortiGate#
```

FortiLogger Cihaz Entegrasyonu

FortiGate üzerinde yönlendirme işlemi tamamlandıktan sonra aşağıdaki adımları izleyiniz:

1. http://local_ip_adresiniz:5000 adresinde açılan web arayüzüne giriş yapınız
2. **Cihaz > Cihaz Ayarları** sayfasını açınız

3. **Kayıtsız Cihazlar** sekmesi altında yönlendirdiğiniz cihaz görünecektir.

Not: cihazın **Kayıtsız Cihazlar** sekmesi altında görüntülenmesi yönlendirme işleminden sonra 1 ila 5 dakika arası sürmektedir. Bu süre zarfında cihaz görüntülenmez ise syslog yönlendirme ayarlarınızı ve FortiGate log gönderimini kontrol ediniz.

Cihaz / Açıklama	Cihaz Id	Ayrılmış Disk Kotası	Disk Kullanımı	Yazma Seçeneği	Yazma Durumu	Lisans
FGT80E Kaydet	FGT80E (172.16.40.128)	% 5 (195.89 MB)	0%	Üzerine yaz	Down	Unlicensed

4. **Kaydet** butonuna bastıktan sonra sol tarafta cihaz bilgilerini girerek tekrar **"Cihazı Kaydet"** butonuna tıklayınız.

Cihaz Ekle / Güncelle

* Adı

Şirket Güvenlik Duvarı

Açıklama

Birincil Güvenlik Duvarı

Cihaz Id

FGXXXXXXXXXXXXXXXX

Cihaz Rengi

#3598DC

Şehir

Şehir

* Ayrılmış Disk Kotası

Ayrılmış disk alanı dolduğunda

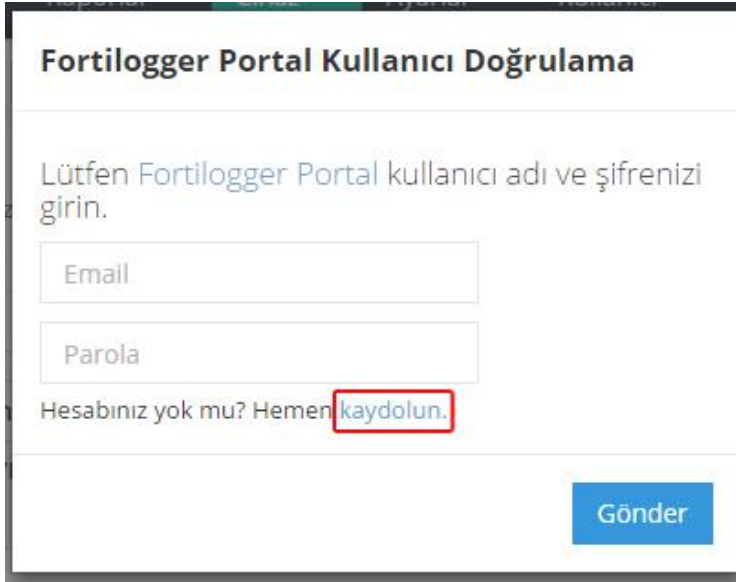
Üzerine yaz

Loglamayı durdur

Cihazı Güncelle

İptal

5. Bu aşamada [FortiLogger Portal \(https://www.fortilogger.com\)](https://www.fortilogger.com) üzerinden oluşturduğunuz üyelik bilgileri ile giriş yapmanız gerekmektedir. Eğer daha önce kayıt yapmadıysanız **"kaydolun"** butonu ile yapabilirsiniz.



Fortilogger Portal Kullanıcı Doğrulama

Lütfen Fortilogger Portal kullanıcı adı ve şifrenizi girin.

Email

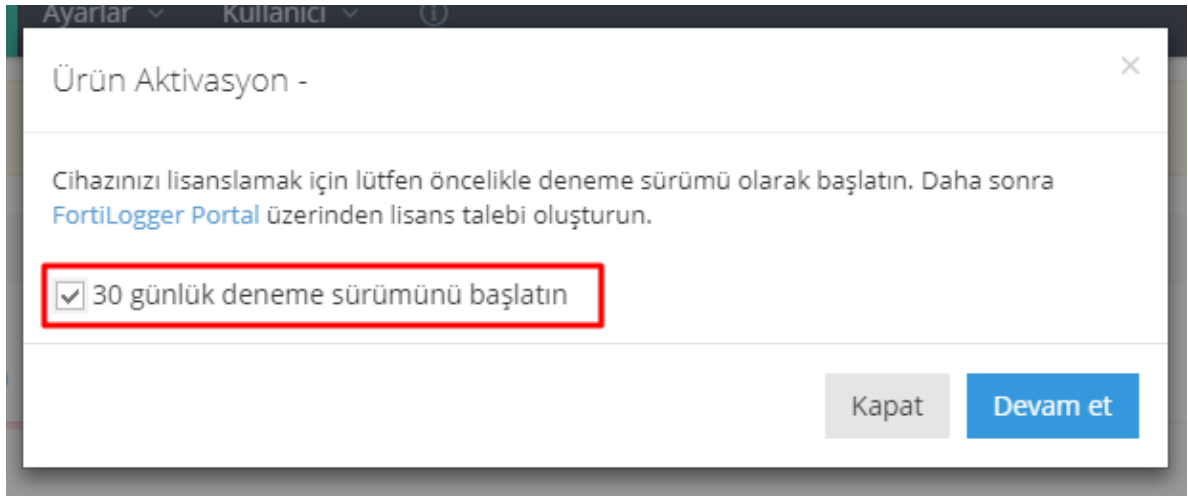
Parola

Hesabınız yok mu? Hemen **kaydolun.**

Gönder

6. Cihazınız için lisans anahtarınız bulunmuyorsa 30 gün deneme sürümünü başlattıktan sonra [FortiLogger Portal \(https://www.fortilogger.com/devices\)](https://www.fortilogger.com/devices) üzerinden cihazınız için lisans talebi oluşturabilirsiniz.

Önemli not: Cihazınızı lisanslamak için öncelikle deneme sürümü olarak kaydetmeniz daha sonra ise [FortiLogger Portal \(https://www.fortilogger.com/devices\)](https://www.fortilogger.com/devices) üzerinden lisans talebi oluşturmanız gerekmektedir.



Ürün Aktivasyon -

Cihazınızı lisanslamak için lütfen öncelikle deneme sürümü olarak başlatın. Daha sonra [FortiLogger Portal](https://www.fortilogger.com/devices) üzerinden lisans talebi oluşturun.

30 günlük deneme sürümünü başlatın

Kapat Devam et

7. Bu aşamadan sonra FortiLogger'in tüm özelliklerini belirtilen deneme süresi boyunca kullanabilirsiniz.

Not: Raporlar cihaz entegrasyonundan en az bir saat sonra oluşmaya başlayacaktır.

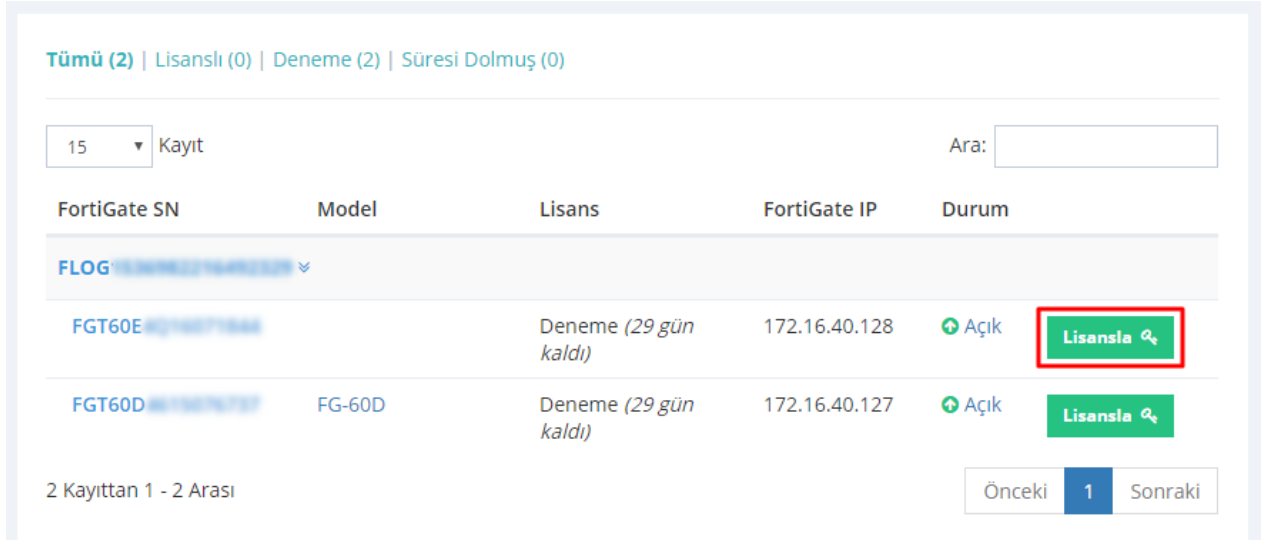
Lisanslama

Fortilogger belirli şartlar altında bedelsiz kullanım aboneliği hakkı sunmaktadır. Bedelsiz kullanım aboneliği şartları aşağıdaki gibidir:

1. FortiGate cihazı RZK tarafından satılmış olmalı
2. Üzerinde RZK çıkışlı devam eden lisans bulunmalı
3. FortiGate-100 serisi ve alt modellerden biri olmalı

FortiLogger Lisanslama işlemi [FortiLogger Portal \(https://www.fortilogger.com\)](https://www.fortilogger.com) üzerinden yapılmaktadır. Lisanslama işlemi için aşağıdaki adımları izleyiniz:

1. [FortiLogger Portal'a \(https://www.fortilogger.com\)](https://www.fortilogger.com) giriş yapınız.
2. [Tüm Cihazlar \(https://FortiLogger.com/devices\)](https://FortiLogger.com/devices) sayfasında aktif cihazlarınız görünecektir.
3. Lisanslamak istediğiniz cihaz için "Lisansla" butonu ile bedelsiz kullanım aboneliği lisansı talebi oluşturabilir veya satınalma yapabilirsiniz.
4. Bedelsiz kullanım aboneliği lisans taleplerinizin sonuçlarını mail yolu ile veya FortiLogger Portal üzerinden takip edebilirsiniz.
5. Lisans satınalmayı tercih etmeniz durumunda kredi kartı ile [FortiLogger Portal \(https://www.fortilogger.com\)](https://www.fortilogger.com) üzerinden ödeme yapabilirsiniz. Bu işlem sonuçlandığında abonelik lisansı otomatik olarak aktive edilecektir.



The screenshot shows the FortiLogger Portal interface. At the top, there are filters: "Tümü (2) | Lisanslı (0) | Deneme (2) | Süresi Dolmuş (0)". Below this is a search bar with "15" and "Kayıt" options, and an "Ara:" field. The main table has columns: FortiGate SN, Model, Lisans, FortiGate IP, and Durum. There are two rows of devices. The first row has FortiGate SN "FGT60E", Model "FG-60D", Lisans "Deneme (29 gün kaldı)", FortiGate IP "172.16.40.128", and Durum "Açık". A red box highlights the "Lisansla" button in the "Durum" column. The second row has FortiGate SN "FGT60D", Model "FG-60D", Lisans "Deneme (29 gün kaldı)", FortiGate IP "172.16.40.127", and Durum "Açık". At the bottom, there is a pagination bar showing "2 Kayıttan 1 - 2 Arası" and buttons for "Önceki", "1", and "Sonraki".

FortiGate SN	Model	Lisans	FortiGate IP	Durum
FGT60E	FG-60D	Deneme (29 gün kaldı)	172.16.40.128	Açık
FGT60D	FG-60D	Deneme (29 gün kaldı)	172.16.40.127	Açık

6. Lisans talebiniz onaylandıktan sonra cihazın altında "Görüntüle" butonuna tıklayarak cihaz ve lisans bilgilerinizi görüntüleyebilirsiniz.

Tümü (2) | Lisanslı (0) | Deneme (2) | Süresi Dolmuş (0)

15 Kayıt

FortiGate SN	Model	Lisans Durumu
FLOG		
FGT60E		Deneme
Görüntüle		kal
FGT60D	FG-60D	Deneme
		kal

2 Kayıttan 1 - 2 Arası

7. FortiLogger arayüzünde **Cihaz > Cihaz Ayarları > Kayıtlı Cihazlar** sekmesi altında **"Lisansı Kontrol Et"** butonuna tıklayarak cihazınızı lisanslı hale getirebilirsiniz. (Not: FortiLogger lisans bilgilerini belirli aralıklarla güncellemektedir. Cihazınız otomatik olarak lisanslı duruma geçebilir.)

Kayıtlı Cihazlar 2 Kayıtsız Cihazlar 4

15 kayıt Ara:

Cihaz / Açıklama	Cihaz Id	Ayrılmış Disk Kotası	Disk Kullanımı	Yazma Seçeneği	Yazma Durumu	Lisans
FGT60E-Mock	FGT60E (172.16.40.128)	% 30 (2.27 GB)	49%	Üzerine yaz	Up	Trial 29 gün kaldı Lisansı kontrol et
FGT60D-Mock	FGT60D (172.16.40.127)	% 30 (2.27 GB)	50%	Üzerine yaz	Up	Trial 29 gün kaldı Lisansı kontrol et

2 kayıttan 1 - 2 arasındaki kayıtlar gösteriliyor

<< < 1 > >>