FORTILOGGER

Kurulum Dokümanı *

v1.5.3

15.02.2021

* Bu doküman FortiLogger 5.2.0 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 Türkiyenin 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 özelliklerinin kullanımı için FortiOS 6.0.0 ve üzeri FortiGate Firmware versiyonları önerilmektedir.
10. FortiLogger Yazılımının internet erişiminde 53 UDP/DNS, 80 TCP/HTTP, 123 UDP/NTP, 443 TCP/HTTPS, 465 TCP/SMTPS ve 587 TCP/SMTP portlarının açık olması gerekmektedir.

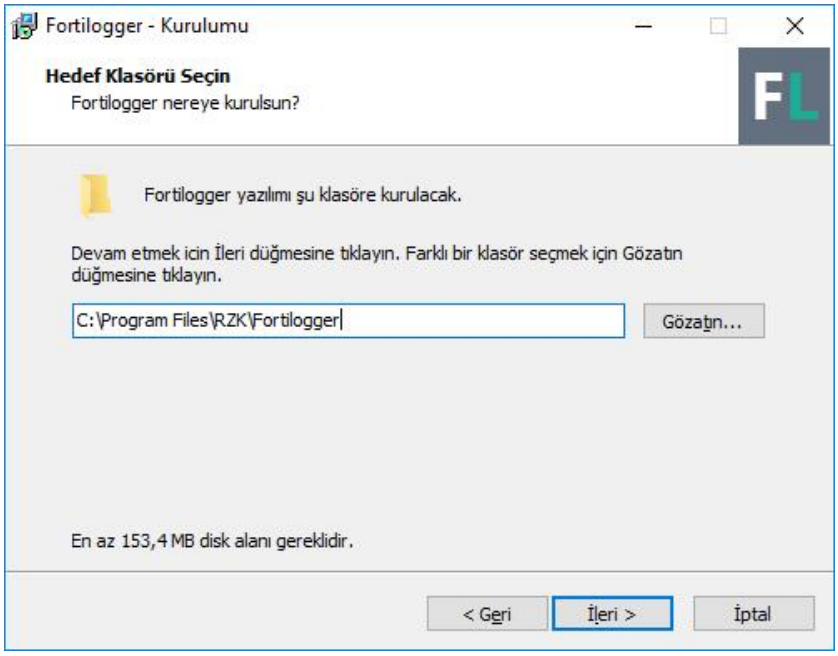
İndirme ve Kurulum

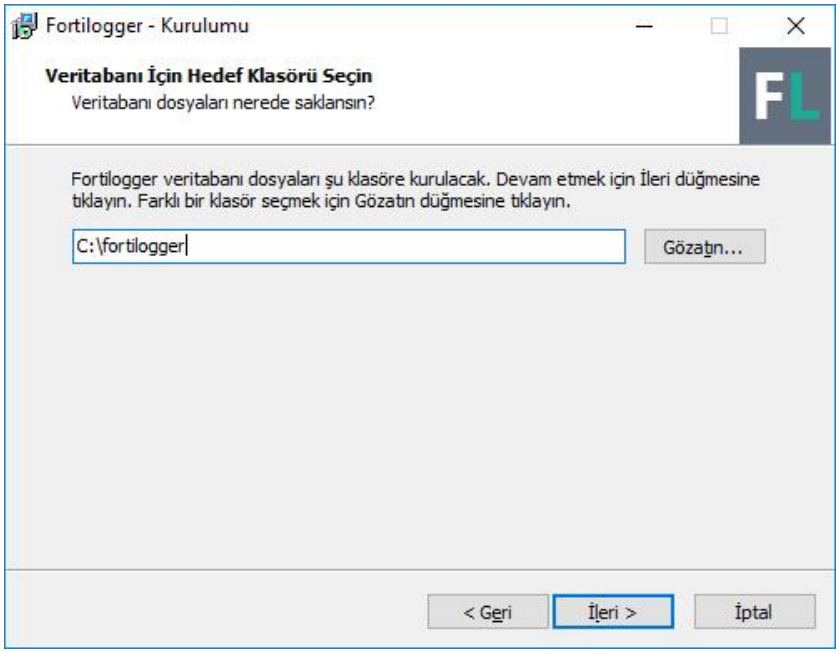
İndirme öncesi işlemler:

1. Cihaz entegrasyonu ve lisanslama işlemlerinizde kullanmanız için FortiLogger Portal (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.

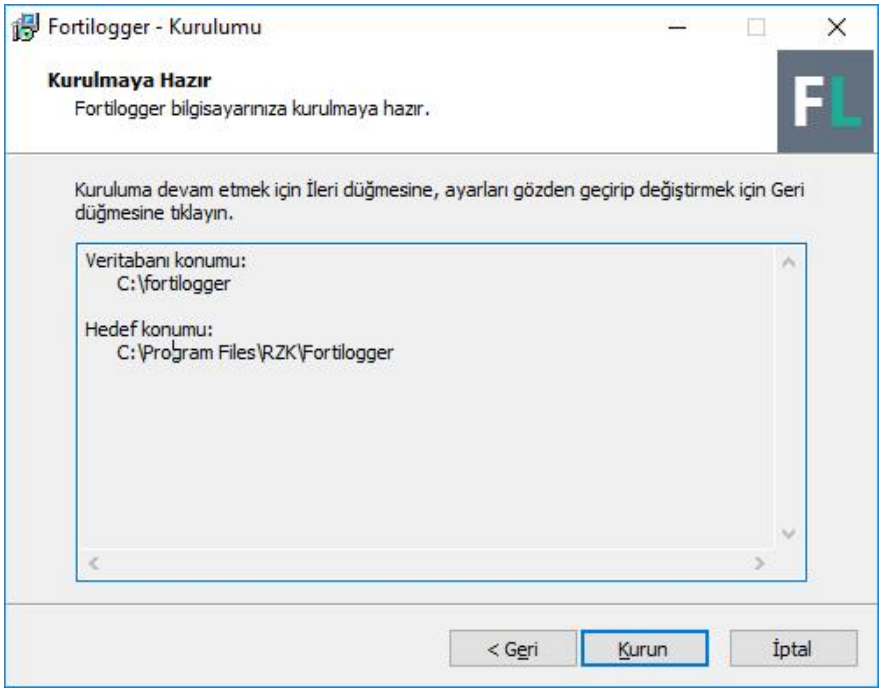
FortiLogger'i bilgisayarınıza kurmak için:

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.

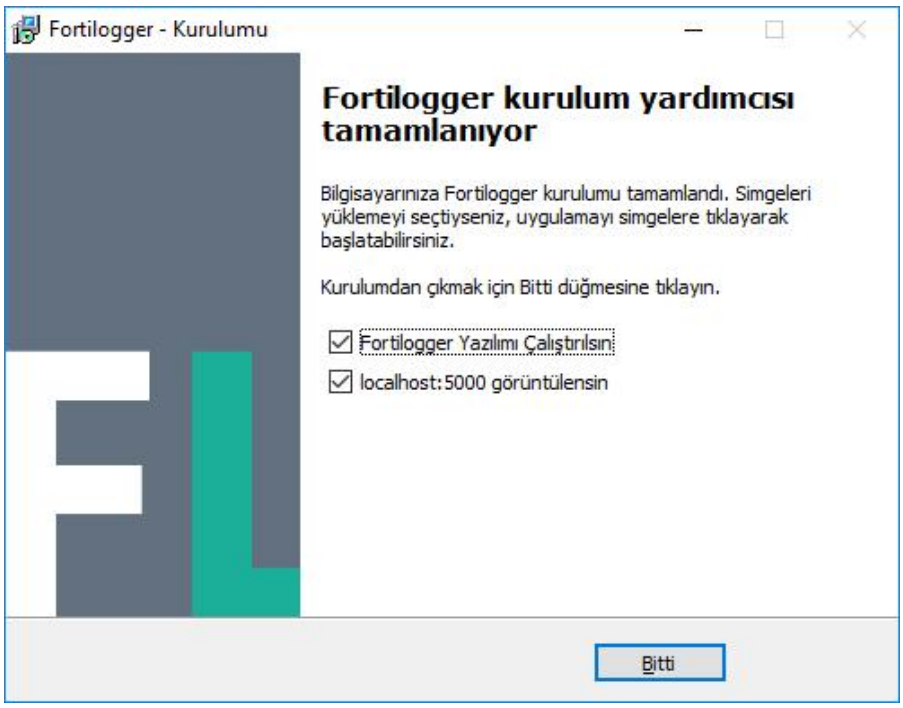




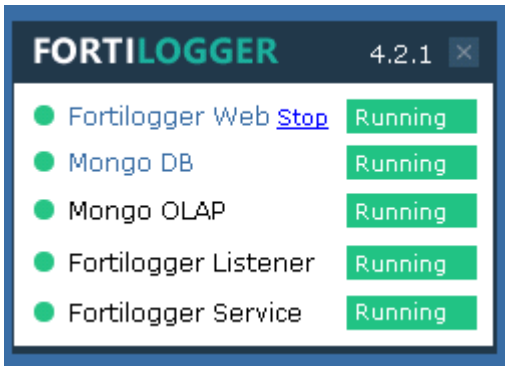
7. Yükleyici penceresini takip ederek kurulum işlemini tamamlayın.
   Not: İlk kez kurulum yapıyorsanız bilgisayarınızda bulunmaması halinde **MongoDB 4.2.2, IIS Express 10 ve .Net Framework 4.7** uygulamaları otomatik olarak indirilecek ve kurulacaktır.


Fortilogger - Kurulumu
Kurulmaya Hazır
Fortilogger bilgisayarınıza kurulmaya hazır.
FL
Kuruluma devam etmek için İleri düğmesine, ayarları gözden geçirip değiştirmek için Geri düğmesine tıklayın.
Veritabanı konumu:
C:\fortilogger
Hedef konumu:
C:\Program Files\RZK\Fortilogger
< Geri
Kurun
İptal

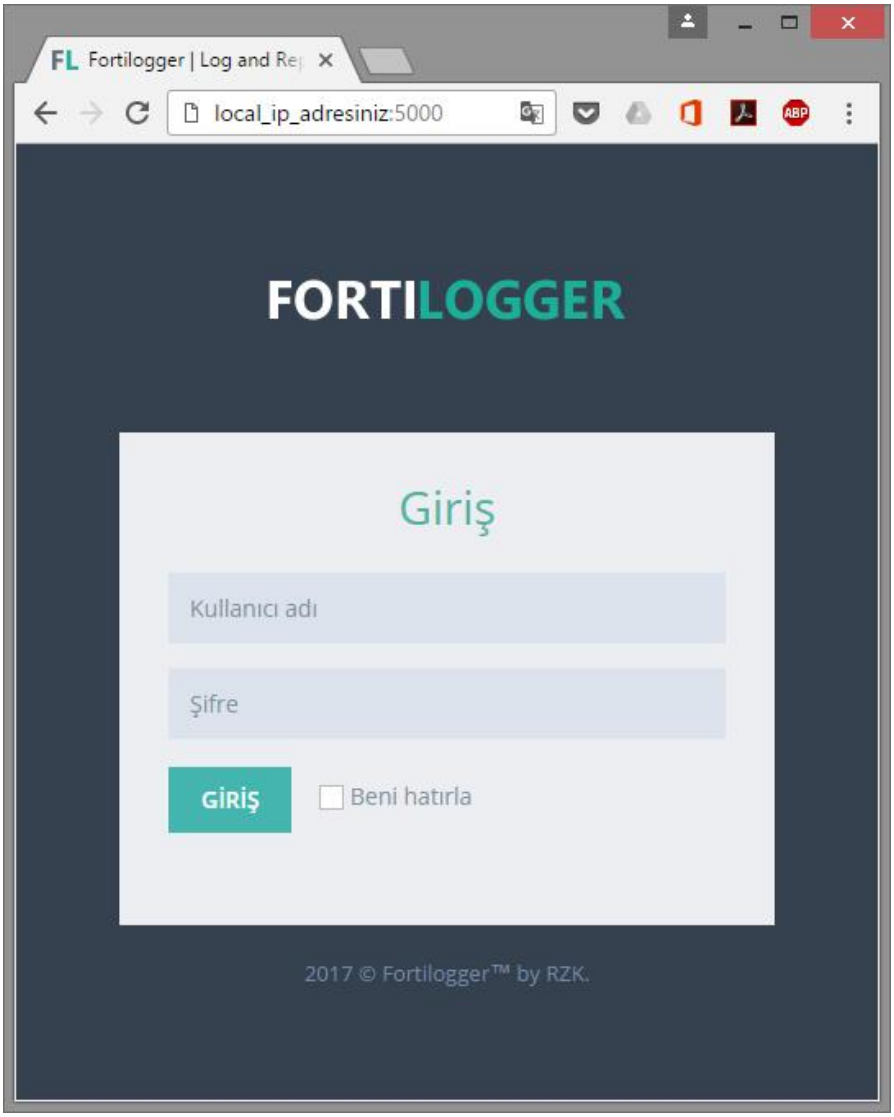
8. Kurulum işlemi tamamlandığında "**Bitti**" butonuna basarak FortiLogger web arayüzünü (http://local_ip_adresiniz:5000) açabilirsiniz.



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**



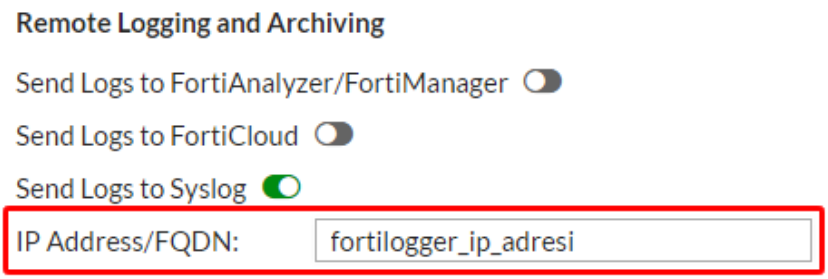
Cihaz Entegrasyon

FortiLogger özelliklerinin kullanımı için FortiOS v6.0.0 ve üzeri FortiGate 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):

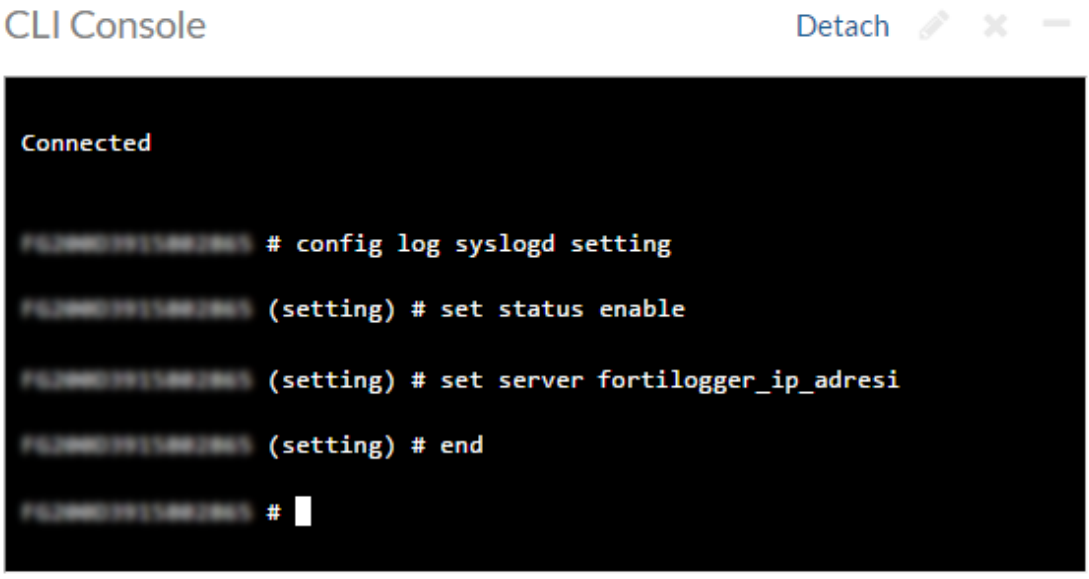
FortiOS Firmware güncel versiyonlar için Log & Report > Log Settings sayfasından aşağıdaki gibi FortiLogger'in kurulu olduğu bilgisayarın IP ADRES bilgisini girebilirsiniz.



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

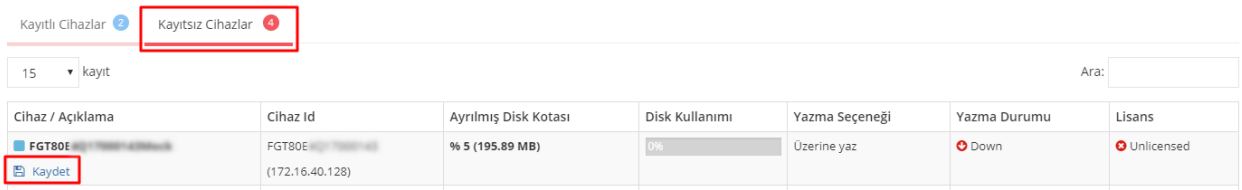


FortiLogger Cihaz Entegrasyonu

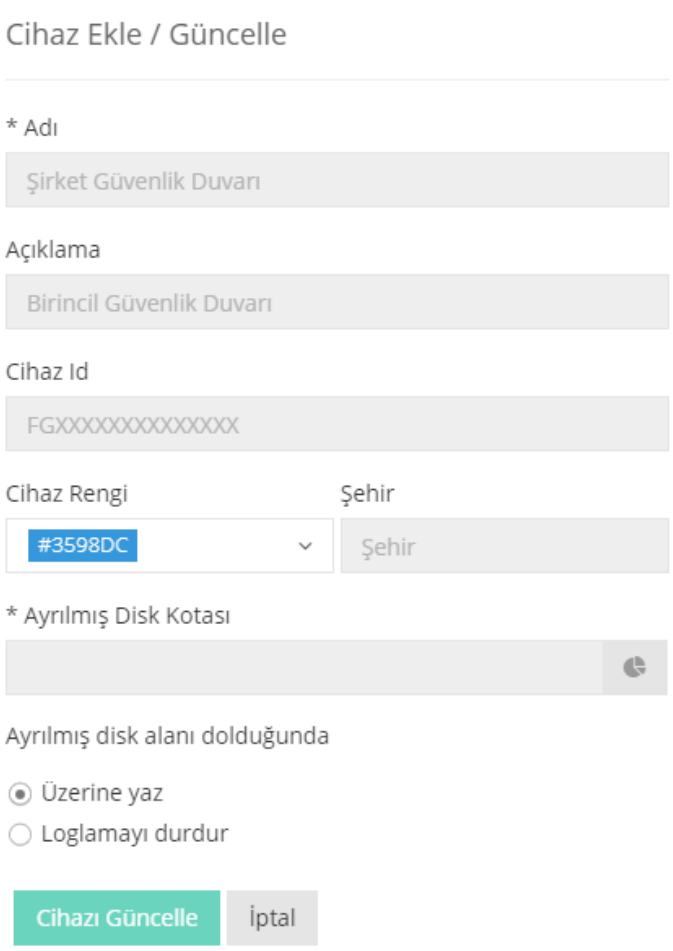
FortiGate üzerinde yönlendirme işlemini tamamladıktan sonra aşağıdaki adımları izleyiniz:

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

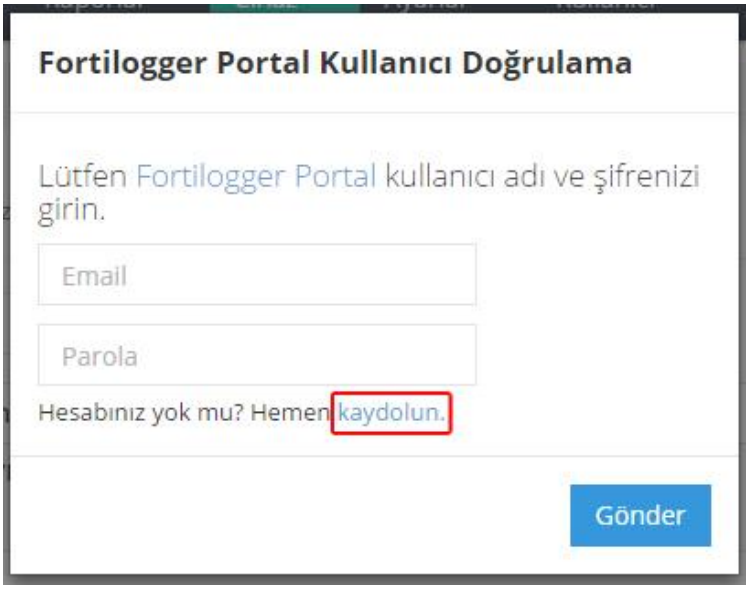
3. **Kayıtsız Cihazlar** sekmesi altında yönlendirdiğiniz cihaz görünecektir.
Not: cihazın **Kayıtsız Cihazlar** sekmesi altında görüntülenmesi yönlendirme işleminden sonra 1 ila 5 dakika arası sürmektedir. Bu süre zarfında cihaz görüntülenmez ise syslog yönlendirme ayarlarınızı ve FortiGate log gönderimini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



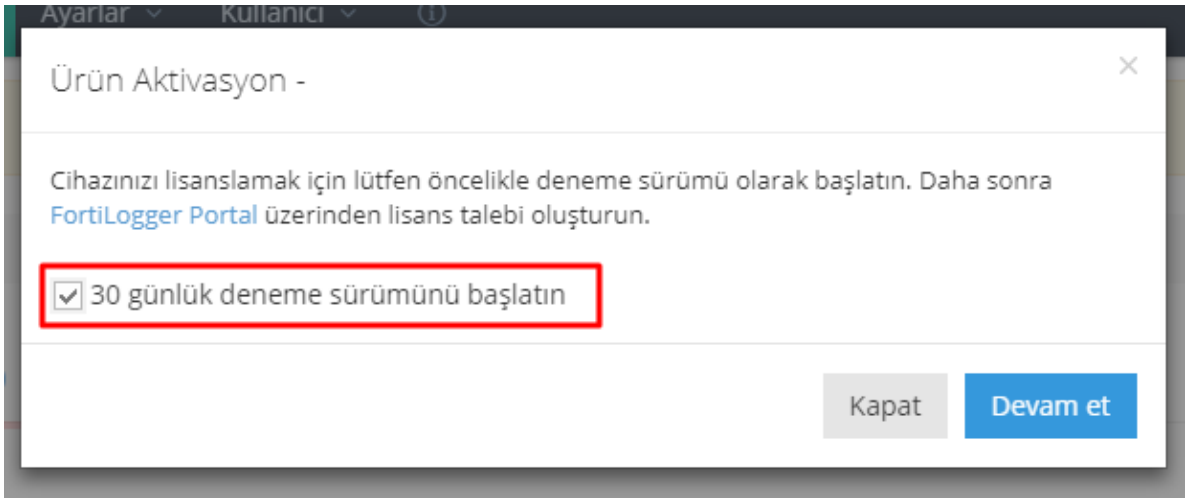
4. **Kaydet** butonuna bastıktan sonra sol tarafta cihaz bilgilerini girerek tekrar "**Cihazı Kaydet**" butonuna tıklayınız.



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



6. Cihazınız için lisans anahtarınız bulunmuyorsa 30 gün deneme sürümünü başlattıktan sonra FortiLogger Portal (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) üzerinden lisans talebi oluşturmanız gerekmektedir.



7. Bu aşamadan sonra Fortilooger'in tüm özelliklerini belirtilen deneme süresi boyunca kullanabilirsiniz.
Not: Raporlar cihaz entegrasyonundan en az bir saat sonra oluşmaya başlayacaktır.

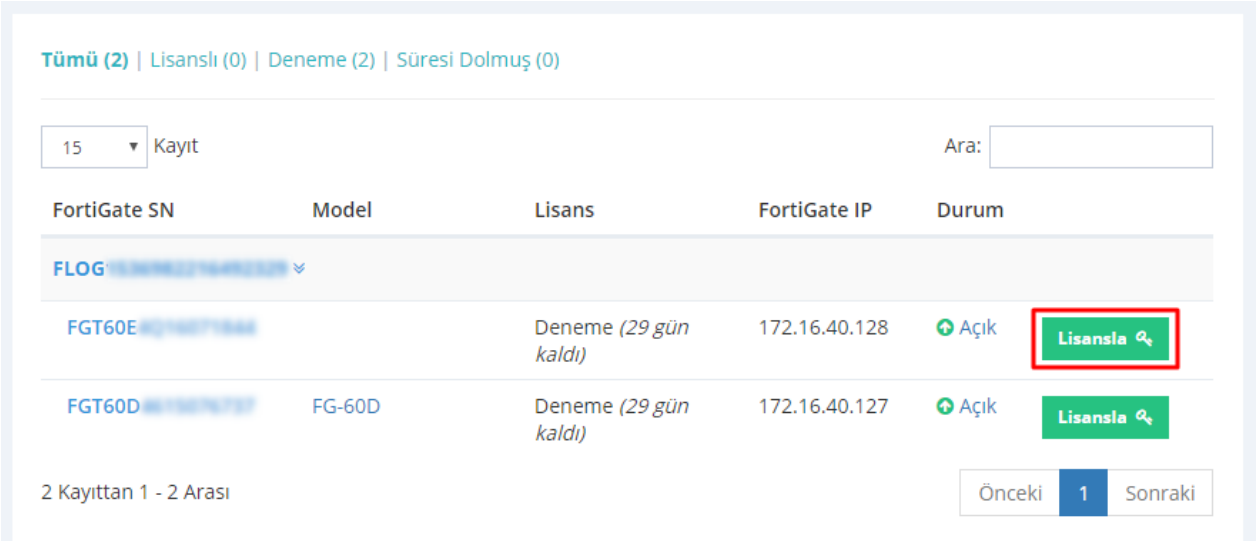
Lisanslama

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

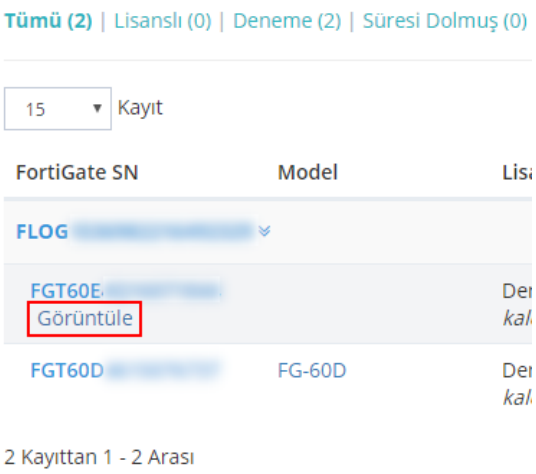
1. FortiGate cihazı RZK tarafından satılmış olmalı
2. Üzerinde RZK çıkışlı devam eden lisans bulunmalı
3. FortiGate-100 serisi ve alt modellerden biri olmalı

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

1. FortiLogger Portal'a (https://www.fortilogger.com) giriş yapınız.
2. Tüm Cihazlar (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) üzerinden ödeme yapabilirsiniz. Bu işlem sonuçlandığında abonelik lisansı otomatik olarak aktive edilecektir.



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



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.)