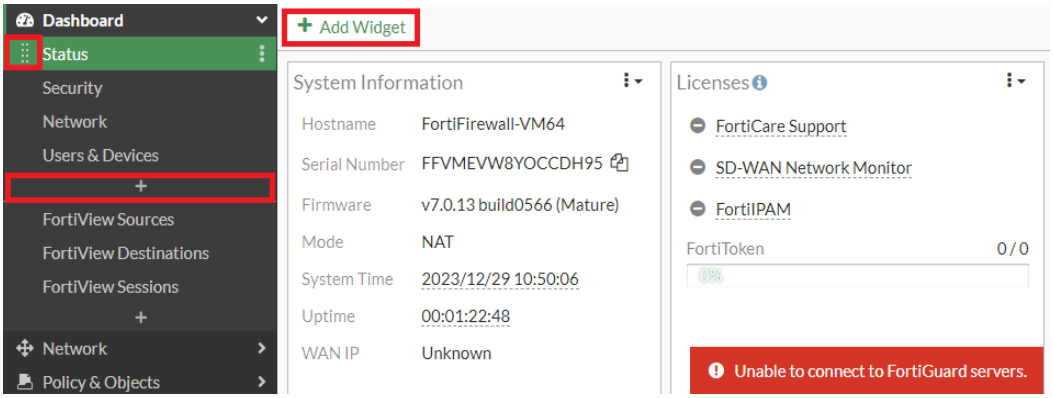
İlk Konfigürasyon

İlk konfigürasyona başlamadan önce Fortigate FW'un arayüzünde oturum açıldığında karşılaşılan sekmelerin kullanım alanlarına kabaca bakılırsa;

- **Dashboard**, Fortigate cihazın arayüzüne bağlanıp oturum açıldığında kullanıcıyı karşılayan sekmedir (Status sekmesi). Bu sekmede cihazın genel durumu hakkında/istatistiksel bilgiler sağlayan Widget'lar bulunuyor. Mouse ile Widget'ların köşelerinden sürükleyerek yer değişikliği yapılabildiği gibi ekleme/çıkarma işlemleriyle özelleştirmeler de yapılabiliyor. Benzer şekilde Dashboard sekmesi altındaki sekmeler üzerinde de yer değişikliği veya ekleme çıkarma işlemleri yapılabiliyor



- **Network**, cihaz üzerindeki arayüz konfigürasyonları, yönlendirme işlemleri gibi network tabanlı ayarlamaların yapıldığı sekmedir.
- **Policy & Objects**, trafik şekillendirme, güvenlik duvarı politikaları tanımlama gibi işlemlerin gerçekleştirildiği sekmedir.
- **VPN**, IPsec ve SSL VPN ayarlamalarının yapıldığı sekmedir.
- **User & Authentication**, cihaz üzerindeki kullanıcı hesapları üzerinde ayarlamalar yapmak için kullanılan sekmedr. Güvenlik duvarı üzerinde local kullanıcı oluşturulabildiği gibi Active Directory veya Radius gibi uzak bir kimlik doğrulama sunucusundan da kimlik doğrulama işlemi yapılabiliyor.
- **System**, sistem genelinde ayarlamaların yapıldığı sekmedir.
- **Secırity Fabric**, çeşitli network cihazlarıyla entegre çalışabilmek için ayarlamaların yapıldığı sekmedir. Network üzerindeki FortiGate, FortiAnalyzer, FortiClient, FortiSandbox, FortiAP, FortiSwitch ve FortiClient Enterprise Management Server (EMS) dahil olmak üzere farklı Fortinet ürünlerinin davranışını koordine etmek için kulanılabilyor
- **Log & Report,** VPN, Wifi veya sistem hakkındaki loğları ve raporları görüntüleyebilmek için kullanılan sekmedir

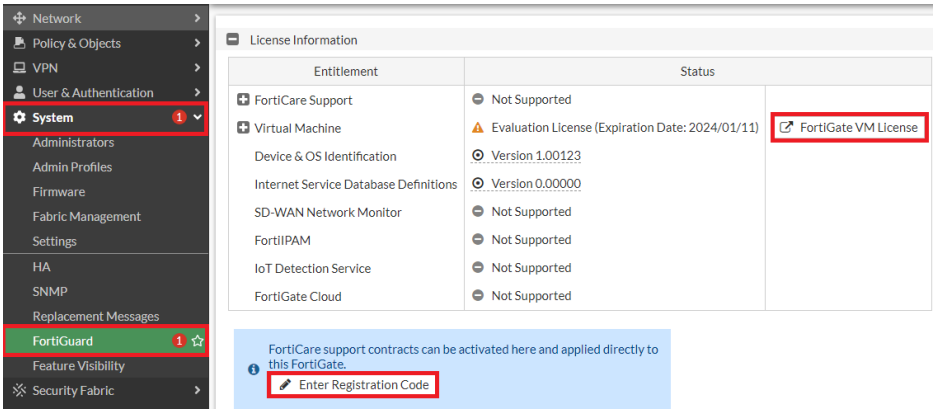
İlk Konfigürasyon

Fortigate güvenlik duvarını kullanımaya başlamadan önce cihaz üzerinde birkaç ayarlamanın yapılması gerekiyor. Bu ayarlamalar;

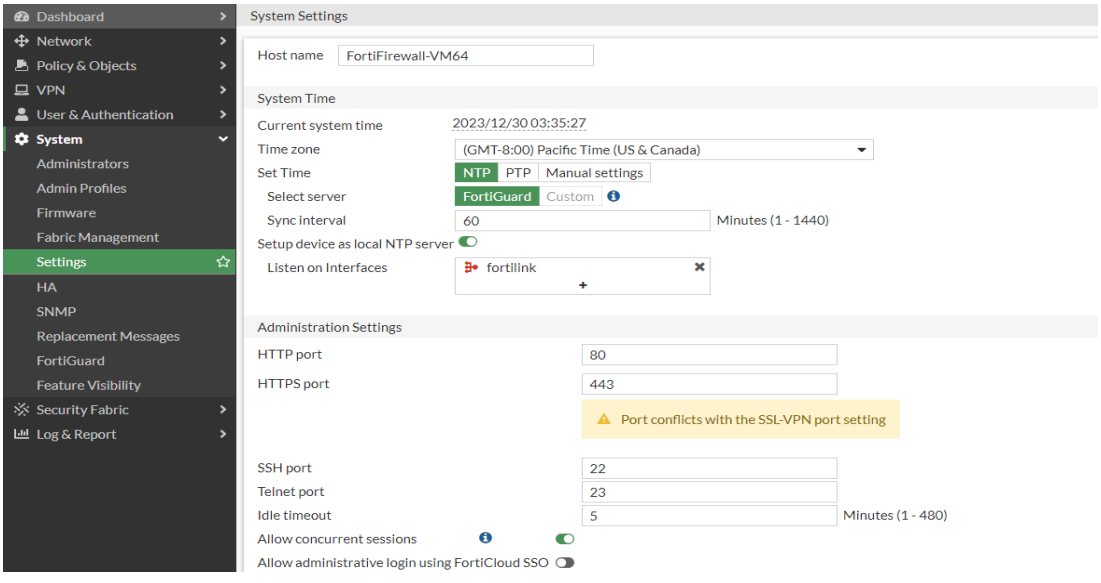
- Fortigate lisansını aktive etmek gerekiyor. Bunun için **System-> Fortiguard** yolu takip edilerek lisans detayları ve desteklenen özellikler görüntülenebilir. Lisans dosyasını yüklemek için "Fortihate VM Licanse" kısmı kullanabileceği gibi "Enter the Licanse Code" kısmında verilen

lisans numarası girilerek de cihaz lisansı devreye alınabiliyor (Fiziksel cihazlarda arayüze bağlanıp ilk kez oturum açıldığında kayıt işlemleri için bir ekranı çıkıyor. Burada daha önce kayıt olduysanız oturum açabilir, kayıt olmadıysanız yeni kayıt oluşturabilirsiniz).

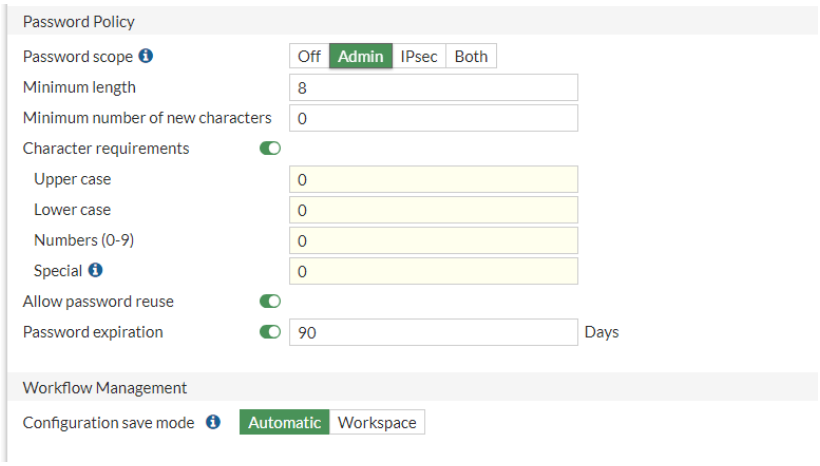
- Normalde bu sayfada lisanslama ile birlikte gelen özelliklerin (Web filtreleme, Antivirüs ve IPS güncellemelerin alınabilmesi gibi daha pek çok özellik) ayarlamaları yapılabiliyor ama deneme sürümünde bu özellikler bulunmadığı için deneme şansımız bulunmuyor.



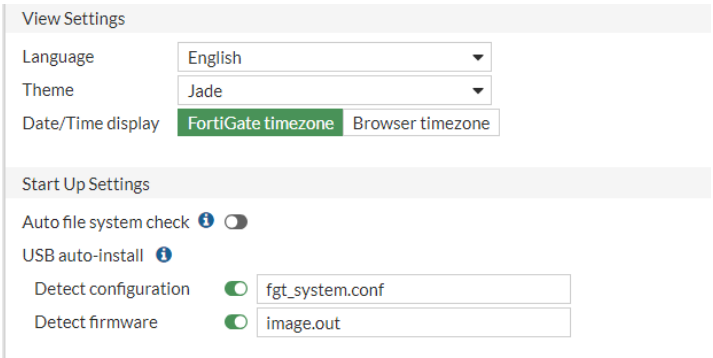
- Lisanslama işlemi sonlandıktan sonra **Syatem-> Settings** sekmesine gelinerek;
  - "**Hostname**" kısmıyla cihaza benzersiz bir isim tanımlanması gerekiyor.
  - System Time alanında, Time Zone seçimi yapıldıktan sonra zaman bilgisinin güncel tutulması için kullanılacağı kaynağın belirtilmesi gerekiyor. Varsayılanda NTP sunucusu olarak FortiGuard üzerinden her 60 saniyede bir senkronize edilecek şekilde geliyor. İsteğe bağlı olarak CLI üzerinde farklı bir NTP tanımı (farklı bir NTP sunucusunun ip adresi) veya PTP tanımı yapılabileceği gibi manuel olarak ayarlanabilir (Loglama ve raporlama sürecinde zaman damgalarının doğru eklenebilmesi adına önemli bir adımdır).
  - Administrative Settings alanında, cihaza erişim için kullanılan protokollerin port bilgileri belirleniyor (Güvenlik nedeniyle varsayılanda gelen portların değiştirilmesi faydalı olacaktır). "**Idle Timeout**" seçeneği ile açılan oturumda kaç dakika işlem yapılmadığı takdirde oturumun sonlanacağı belirleniyor. Allow Concurrent Sessions seçeneği ile admin hesabıyla aynı anda birden fazla oturum açılıp açılamayacağı belirleniyor.



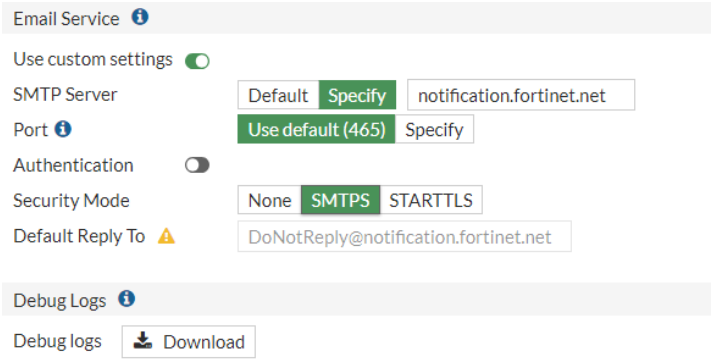
- Password Policy alanında, admin hesapları ve IPsec sürecinde kimlik doğrulama süreci için belirlenecek parolalara yönelik ayrı ayrı veya he ikisi için de geçerli olacak şekilde politika belirlenebiliyor.
  - "**configure system global**" ve "**set admin-lockout threshold <Fail Authentication Count>**" komutları kullanılarak giriş sırasında yanlış denemeler sonucunda kullanıcı hesabının belirli bir süre kitlenmesini ağlamak da mümkün. Hesabın kilitlenme süresini ayarlamak için de "**set admin-lockout duration <Second**>" komutu kullanılıyor.
- Workflow Management alanında, cihaz üzerinde yapılan değişikliklerin otomatik olarak kaydedilip istenip istenmediği belirleniyor.



- Wiev Settings alanında, cihazda kullanılacak dil seçimi ve arayüzde kullanılan renklerin/temasının seçimi belirleniyor.
  - Date/Time Display alanında "**FortiGate Timezone**" seçeneği seçildiğinde System Time alanında seçilen ayarlar geçerli olacaktır. "**Browser Timezone**" seçeneği seçildiğinde ise System Time alanında yapılan ayarlamalar geçersiz sayılarak tarayıcı üzerindeki saat ve tarih bilgisi kullanılacaktır.
  - Varsayılanda cihazlar daylight özelliğiyle yaz saatine otomatize uyum sağlar ayarlamada geliyor. Yaz saati uygulamasına uymayan ülkeler için bu özellik "**config system global**" ve "**set sdt <Disable | Enable>**" komutuyla devreye alınabiliyor veya devre dışı bırakılabiliyor.
- StartUp Settings alanında, güç kesintisi durumunda dosya sistemindeki hataların otomatik olarak kontrol edilmesinin istenip istenmediği ayarlanabildiği gibi cihaz yeniden başlatıldığında bir USB cihaz üzerinden yazılım güncellemelerinin veya konfigürasyon dosyalarının otomatik olarak yüklenebilmesi için ayarlamalar yapılabiliyor.



- Email Service alanında, yöneticileri/kullanıcıları mail hizmetini kullanarak cihaz üzerindeki olaylar hakkında bilgilendirilmesini sağlamak için ayarlamaların yapıldığı alandır. Cihaz üzerinde bir problem yaşanması durumunda hızlı tepki verebilmek adına önemli olacaktır.
- Debug Logs alanında, cihaz üzerinde sorun giderme sürecine yardımcı olacak hata ayıklama kayıtları indirilebilir.

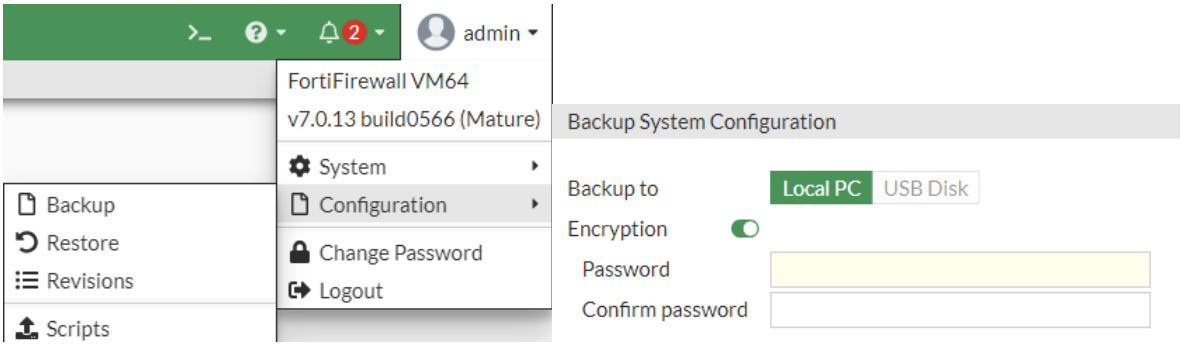


- Bu sekme altındaki alanlar cihaz sürümüne göre değişiklik gösterebiliyor. Konfigürasyon hakkında daha detaylı bilgi için https[:]//docs.fortinet.com/document/fortigate/7.4.1/administration-guide/178518/settings adresinden Fortigate'in kedi dökümanlarını inceleyebilirsiniz.

Yedekleme ve Yedekten Dönme

Her ne kadar ilk konfigürasyon olsa da belirli sıklıklarda konfigürasyonların yedeklerinin alınması gerekiyor ki bir aksaklık olması durumunda yedeklerden geri dönülmesi mümkün olsun. Bunun için "**Admin -> Configuration –> Backup**" yolu izlenerek bir USB diske veya tarayıcı üzerinden cihazın arayüze bağlanan bilgisayarın local diskine yedek alınmalıdır.

- İsteğe bağlı olarak yedekler şifreli olarak alınabiliyor. Şifreli yedekleme alındığında yedekten geri dönebilmek için şifrenin unutulmaması gerekiyor.
- Yedekten dönmek için ise yine aynı yol üzerindeki "**Restore**" seçeneği kullanılıyor. Bu seçenekten sonra yedek alınan dosya seçilir ve cihaz yeniden başlatılır.



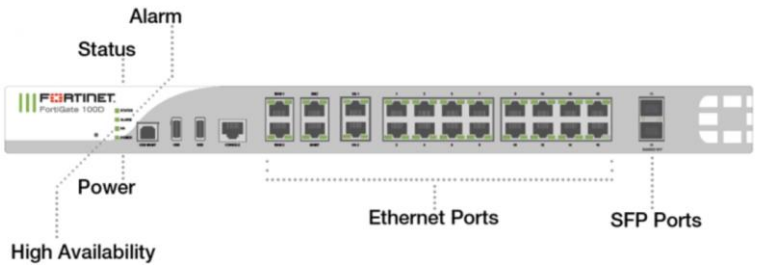
Cihaz Üzerindeki Ledlerin Özellikleri

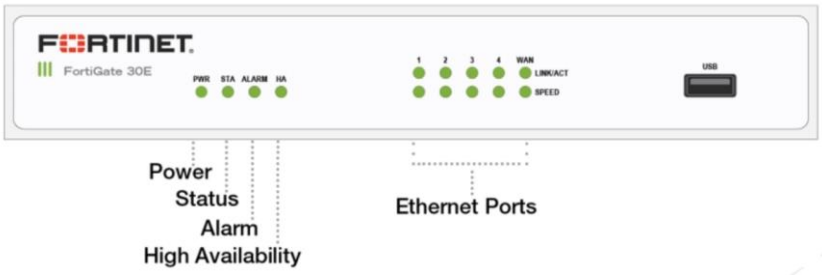
Sahada cihazların durumu hakkında genel bir fikir sahibi olabilmek konusunda cihaz üzerinde bulunan ledler faydalı olabiliyor. Ledleri cihazın genel durumu hakkında bilgilendirmek üzere kullanılan ledler ve portların durumu hakkında bilgilendiren ledler olarak iki başlık altında inceleyebiliriz. Cihazın genel durumu hakkında bilgi veren birkaç ledin anlamlarına bakıldığında;

- Power Led
    - Yeşil yanıyorsa, cihazın açık olduğunu gösterir.
    - FortiWifi ünitesinin açık olduğunu gösterir.
    - Yanmıyorsa, cihazın kapalı olduğunu gösterir.
- Status Led
    - Yeşil, sorunsuz çalıştığını gösterir.
    - Yeşil (yanıp/sönen), cihazda önyükleme olduğunu gösteriyor.
    - Turuncu cihazın doğru çalışmadığını, bir hata oluştuğunu gösterir,
    - Kırmızı, cihazın doğru çalışmadığını, kritik bir alarm olduğunu gösterir.
- Alarm Led
    - Kapalıi cihazda alarmlık bir durum olmadığını gösterir.
    - Sarı (Koyu), cihazın büyük bir alarm olduğunu gösterir
    - Kırmızı, cihazın kritik bir alarmı olduğunu gösterir
- High Availability Led
    - Yeşil, HA kmesinde çalıştığını gösterir
    - Turuncu/Kırmızı, yük devretme durumunun oluştuğunu gösterir.
    - Kapalı, HA yapısının yapılandırılmadığını gösterir.
- PoE Led
    - Yeşil, PoE cihazının bağlı olduğunu ve güç aldığını gösterir.
    - Turuncu, bir sorun oluştuğunu gösterir.
    - Kapalı, PoE cihazının bağlı olmadığını veya güç almadığını gösterir.
- Power Supply Led
    - Yeşil, güç sağlayıcının sağlıklı bir şekilde çalıştığını gösterir.
    - Yeşil (yanıp/sönen), güç sağlayıcısının algılandığı ama güç sağlamadığını (bekleme moduna alındığını) gösterir.
    - Turuncu, güç kaynağı hatası olduğunu veya giriş gücünün olmadığını ancak yedek beslemenin açık olduğunu gösterir.
    - Turuncu (yanıp/sönen), güç kaynağı hatası olduğunu ve güç kaynağının değiştirilmesi gerektiğini gösterir.
    - Kırmızı, gücün kesildiğini gösterir.
    - Kırmızı (yanıp/sönen), güç sağlayıcısının uyarı verdiğini gösterir.
    - Kapalı, güç sağlayıcısının tespit edilmediğini gösterir.
- Fan Led
    - Yeşil, fanların normal çalıştığını gösterir.
    - Turuncu, problem olduğunu gösterir.
    - Turuncu (yanıp/sönen), fan değiştirme/başlatma işleminin devam ettiğini gösterir.
    - Kırmızı, dönme hızlarının (RPM) çok yüksek veya çok düşük olduğunu gösterebileceği gibi fan setlerinin en az bir hataya sahip olduklarını gösterir.
    - Kırmızı (yanıp/sönen), bir fan setinde en az bir uyarı olduğunu gösterir.
    - Kapalı, fanların kapalı olduğunu veya hata oluştuğunu gösterir.

Cihaz üzerindeki portlar hakkında bilgi veren birkaç ledin anlamlarına bakıldığında;

- Ethernet Led
    - Yeşil, 1Gbps hızında çalıştığını gösterir (Her renk için yanıp sönüyor olması çalıştığı bant genişliğinde veri iletimi yaptığını gösteriyor).
    - Turuncu, 10/100Mbps hızında çalıştığını gösterir.
    - Kapalı, bağlantı olmadığını gösterir.
- SFP Led
    - Yeşil, 1Gbps hızında çalıştığını gösterir (Her renk için yanıp sönüyor olması çalıştığı bant genişliğinde veri iletimi yaptığını gösteriyor).
    - Kapalı, bağlantı olmadığını gösterir.
- PoE Led
    - Yeşil, PoE cihazının sorunsuz şekilde güç aldığını gösterir.
    - Kırmızı, PoE cihazının bağlı olduğunu ancak güç sağlanamadığını gösterir.
    - Kapalı, PoE gücünün kapalı olduğunu veya güç alacak bağlı cihazın olmadığını gösterir.





Detaylı bilgi ve daha fazlası için Fortigate'in kendi sitesini ziyaret edebilirsiniz (https[:]//docs.fortinet.com/document/fortigate/7.4.1/administration-guide/997251/leds).

NOTLAR:

- PTP (Precision Time Protocol)
- System sekmesi altındaki ayarlamaları CLI ekranından yapılmak istendiğinde komutlar "**config system global**" komutu altında uygulanıyor.
- Kullanılabilecek birkaç faydalı link
    - https[:]//www.fortiguard.com/webfilter - bir web sitesinin kategorisini öğrenmek için kullanılabiliyor.
    - https[:]//www.fortiguard.com/encyclopedia - zararlı yazılımlarla ilgili bilgiler bulunuyor.
    - https[:]//www.fortiguard.com/appcontrol - uygulamaların kategorisini öğrenmek için kullanılabiliyor.