

## Hızlı Başlangıç Kılavuzu

Bu kılavuz, tipik bir kuruluşa başlamanıza yardımcı olur.

**Ulusal Dil Sürümü:** Hızlı Başlangıç Kılavuzu'nu başka dillerde edinmek için, kuruluş ortamından dile özgü PDF'yi yazdırın.

### Ürüne genel bakış

IBM® QRadar Security Intelligence Platform ürünleri, güvenlik bilgileri ve olay yönetimini (SIEM), günlük yönetimini, olağan dışı durum algılamayı, olay adli tıp verilerini ve yapılandırma ve güvenlik açığı yönetimini bütünleştirmeye yönelik birleşik bir mimari sağlar. Bu Hızlı Başlangıç Kılavuzu, IBM Security QRadar araçlarının kurulmasına ilişkin bilgi sağlar.

### 1 Adım 1: Yazılım ve belgelere erişme



Kurmak istediğiniz QRadar bileşeni için yayın notlarını gözden geçirin.

IBM FIX Central web sitesinden QRadar bileşeniniz için ISO'yu karşıdan yükleyin.

### 2 Adım 2: Ön ve arka panel özelliklerini gözden geçirme

Uygun bağlantı ve işlevselliği onaylamak için araçların ön ve arka panel özelliklerine ilişkin bilgileri gözden geçirin.

Araçların ön ve arka panel özelliklerine ilişkin ek bilgi için bkz. ön ve arka panel özellikleri.

Her araç tipinin arka panelinde seri bağlayıcı ve Ethernet bağlayıcıları, Tümüleşik Yönetim Modülü kullanılarak yönetilebilir. Tümüleşik Yönetim Modülü hakkında daha fazla bilgi için bkz. *Integrated Management Module User's Guide*.

### 3 Adım 3: Kuruluş önkoşulları



Aşağıdaki gereksinimlerin karşılandığından emin olun:

- Gerekli donanım kurulu olmalıdır.
- QRadar araçları için, aracın arkasındaki seri kapısına bir dizüstü bilgisayar takılı ya da bir klavye ve monitör takılı olmalıdır.
- Kök kullanıcı olarak oturum açmış olmalısınız.
- Etkinleştirme anahtarı bulunmalıdır.

IBM® Security QRadar® ürününün kendi aracınıza başarılı şekilde kurulduğundan emin olmak için Red Hat Enterprise Linux işletim sistemini kurmanız gerekir. Aracınızın QRadar devreye alımları için sistem gereksinimlerini karşıladığından emin olun. Daha fazla bilgi için bkz. *QRadar Hardware Guide*.

## 4 Adım 4: Kendi aracınıza QRadar SIEM ürününü kurma



QRadar Risk Manager ve QRadar Incident Forensics için kendi lisansının gerekli olduğunu ve bunların ayrı araçlara kurulması gerektiğini unutmayın. QRadar Risk Manager, yönetilen anasistem olarak kurulmalıdır. QRadar Vulnerability Manager, tümü bir arada konsolda konsolla aynı makineye kurulabilir.

1. Kendi aracınızı kullanıyorsanız QRadar ISO görüntüsünü bağlayın:
  - a. Şu komutu yazarak /media/cdrom dizinini oluşturun:  
mkdir /media/cdrom
  - b. Şu komutu yazarak QRadar ISO görüntüsünü bağlayın:  
mount -o loop <QRadar ISO yolu> /media/cdrom
  - c. Kuruluşa başlamak için şu komutu yazın:  
/media/cdrom/setup
2. Sizden etkinleştirme anahtarı istendiğinde, IBM'den aldığınız, 4 bölümden oluşan 24 basamaklı alfasayısal dizeyi girin. I harfi ve 1 (bir) rakamı aynı olarak değerlendirilir. O harfi ve 0 (sıfır) rakamı da aynı olarak değerlendirilir.
3. Kuruluş tipi için **Normal** seçeneğini belirleyin.
4. IP adresi tipini seçin.
5. Sihirbazda **Anasistem Adı** alanına tam tanımlı etki alanı adını girin.
6. **IP adresi** alanına bir statik IP adresi girin ya da DHCP tarafından atanan IP adresini kullanın.  
IPv6 birincil ya da ikincil anasistemini ayarlama hakkında bilgi için bkz. *IBM Security QRadar High Availability Guide*.
7. E-posta sunucunuz yoksa, **E-posta sunucusu adı** alanına localhost girin.
8. **Son'u** tıklatın.
9. **Kök parola** alanında bir parola oluşturun. Parolalar en az 5 karakter uzunluğunda olmalı, boşluk içermemelidir ve şu özel karakterleri içerebilir: @, #, ^ ve \*.
10. Kuruluşu tamamlamak için kuruluş sihirbazındaki yönergeleri izleyin. Kuruluş işlemi birkaç dakika sürebilir.

## 5 Adım 5: Lisans anahtarınızı uygulama



1. QRadar'da oturum açın:  
https://IP\_Address\_QRadar  
Varsayılan **Kullanıcı adı**: admin. **Parola**, kök kullanıcı hesabının parolasıdır.
2. **Admin** (Yönetim) sekmesini tıklatın.
3. Gezinme bölmesinde **System Configuration** (Sistem Yapılandırması) ögesini tıklatın.
4. **System and License Management** (Sistem ve Lisans Yönetimi) simgesini tıklatın.
5. **Display** (Görüntü) liste kutusundan **Licenses** (Lisanslar) ögesini seçin ve lisans anahtarınızı karşıya yükleyin.
6. Ayrılmamış lisansı seçin ve **Allocate System to License** (Lisansa Sistem Ayır) seçeneğini tıklatın.
7. Lisans listesinden bir lisans seçin ve **Allocate License to System** (Sisteme Lisans Ayır) seçeneğini tıklatın.

## 6 Adım 6: Başlangıç



QRadar bileşenlerinizi kullanmaya başlama hakkında daha fazla bilgi için aşağıdaki kaynaklara bakın:

- IBM Security QRadar SIEM ile çalışmaya başlama
- IBM Security QRadar Risk Manager ile çalışmaya başlama
- IBM Security QRadar Vulnerability Manager ile çalışmaya başlama
- IBM Security QRadar Incident Forensics ile çalışmaya başlama
- IBM Security QRadar Packet Capture ile çalışmaya başlama

## Daha fazla bilgi



Ürün belgelerinin tamamı için, IBM QRadar Security Intelligence Platform Knowledge Center'ı veya Download Document sayfasını ziyaret edin.

