





# İçindekiler

<b>1</b>	<b>Güvenlik</b>	<b>4</b>
<b>1.1</b>	Çalışma önlemleri	<b>4</b>
<b>1.2</b>	Veri güvenliği önlemleri	<b>4</b>
<b>2</b>	<b>Giriş</b>	<b>5</b>
<b>3</b>	<b>Sisteme genel bakış</b>	<b>6</b>
<b>4</b>	<b>İlk oturum açma ve sistem kurulumu</b>	<b>7</b>
<b>4.1</b>	Çalışma modunu seçme	<b>8</b>
<b>4.1.1</b>	Tam video kaydı ve yönetim sistemi olarak çalışma	<b>8</b>
<b>4.1.2</b>	Saf video kayıt sistemi olarak çalıştırma	<b>9</b>
<b>4.1.3</b>	iSCSI veri depolama alanı genişletmesi olarak çalıştırma	<b>9</b>
<b>5</b>	<b>Yazılımı yükseltme ve güncelleştirme</b>	<b>11</b>
<b>6</b>	<b>Sisteme uzaktan bağlantı</b>	<b>12</b>
<b>6.1</b>	Sistemi yetkisiz erişime karşı koruma	<b>12</b>
<b>6.2</b>	Port yönlendirmeyi ayarlama	<b>12</b>
<b>6.3</b>	Uygun bir istemci seçme	<b>12</b>
<b>6.3.1</b>	Operator Client ile uzaktan bağlantı	<b>12</b>
<b>6.3.2</b>	Video Security Uygulaması ile uzaktan bağlantı	<b>12</b>
<b>6.4</b>	Enterprise Management Server kurma	<b>13</b>
<b>7</b>	<b>Bakım</b>	<b>14</b>
<b>7.1</b>	Sistemin izlenmesi	<b>14</b>
<b>7.2</b>	Birimi eski haline getirme	<b>14</b>
<b>8</b>	<b>Ek bilgiler</b>	<b>15</b>
<b>8.1</b>	Ek belgeler ve istemci yazılımı	<b>15</b>
<b>8.2</b>	Destek hizmetleri ve Bosch Akademisi	<b>15</b>

# 1 Güvenlik

Bu bölümdeki güvenlik önlemlerine uyun.

## 1.1 Çalışma önlemleri

Cihaz yalnızca profesyonel kurulumla yöneliktir. Cihazlar, kişisel veya evde kullanım amaçlı değildir. Güvenlik bilgilerinde belirtilenler hariç olmak üzere cihazın ticari ve endüstriyel alanlarda kullanımında sınırlama yoktur.



### Uyarı!

Bu bir **sınıf A** üründür. Bir ev ortamında bu ürün radyo parazitine neden olabilir; bu durumda kullanıcının yeterli önlemleri alması gerekebilir.



### Uyarı!

Video kaybı dijital video kaydı için normaldir; bu nedenle Bosch Security Systems, eksik video bilgilerinden kaynaklanan herhangi bir zarardan sorumlu tutulamaz.

Kayıp bilgi riskini en aza indirmek için, çoklu, yedeklemeli kayıt sistemlerinin kullanılmasını ve tüm analog ve dijital bilgilerin yedeklenmesi prosedürünü öneririz.

## 1.2 Veri güvenliği önlemleri

Veri güvenliği nedeniyle aşağıdakilere uyun:

- Sisteme fiziksel erişim sadece yetkili personelle kısıtlanmalıdır. Sistemde fiziksel değişiklik yapılmasını önlemek için sistemin giriş kontrol korumalı bir alana yerleştirilmesi kesinlikle önerilir.
- İşletim sistemi güvenlik güncellemelerini yüklemek için Windows çevrimiçi güncelleme işlevi veya çevrimdışı yükleme için ilgili aylık toplama yamaları kullanılabilir.
- Yerel ağ erişimini güvenilir cihazlarla sınırlandırmak kesinlikle önerilir. Ayrıntılar Ağ Kimlik Denetimi 802.1X teknik notunda ve çevrimiçi ürün kataloğunda yer alan Bosch IP Video ve Veri Güvenlik Kılavuzu'nda açıklanmıştır.
- Genel ağlar üzerinden erişim için yalnızca güvenli (şifreli) iletişim kanalları kullanın.

## 2

## Giriş

### Çalışma modları

DIVAR IP all-in-one sistemleri üç farklı modda çalışabilir:

- BVMS ve VRM temel bileşenleri ve hizmetleri kullanılan tam video kayıt ve yönetim sistemi: Bu mod, olay ve alarm yönetimi gibi gelişmiş video yönetim özelliklerine imkan verir.
- VRM temel bileşenleri ve hizmetleri kullanılan saf video kayıt sistem.
- Farklı bir donanımda çalışan bir BVMS veya VRM sistemi için iSCSI depolama alanı genişletmesi.



### Uyarı!

Kayıtlı video akışları sistemin maksimum bant genişliği (BVMS/VRM temel sistem ve iSCSI veri depolama genişletmeleri) aşılmayacak şekilde yapılandırılmalıdır.

### DIVAR IP Software Center

DIVAR IP Software Center yazılım kurulumu, yükseltme ve çalışma modu seçimi için kullanılan merkezi kullanıcı arayüzüdür.

DIVAR IP Software Center yüklendikten sonra sisteminizi yapılandırmak için istediğiniz işlem modunu seçmeniz gerekir.

Ayrıca DIVAR IP Software Center ile yüklü yazılımı güncelleyebilir ve yükseltebilirsiniz.

En güncel yazılımı ve mevcut yükseltme paketlerini Bosch Security and Safety Systems **İndirme Alanı**'nda bulabilirsiniz:

<https://downloadstore.boschsecurity.com/>

### 3 Sisteme genel bakış

DIVAR IP all-in-one 7000 sistemler Microsoft Windows Server IoT 2019 for Storage Standard işletim sistemini temel alır. İşletim sistemi, ilk sunucu yapılandırması, birleşik depolama cihaz yönetimi, basitleştirilmiş kurulum ve depolama yönetimi ile Microsoft iSCSI Yazılım Hedefi desteği için kullanıcı arayüzü sağlar.

Ağa bağlı veri depolama için optimum performans sağlamak amacıyla özel olarak ayarlanır. Microsoft Windows Server IoT 2019 for Storage Standard işletim sistemi, veri depolama yönetim senaryolarında önemli iyileştirmelerin yanı sıra veri depolama cihazı yönetim bileşenleri ve işlevlerinin entegrasyonunu sağlar.



#### Uyarı!

Bu bölüm, önceden takılmış sabit sürücülerle sunulan DIVAR IP all-in-one 7000 modelleri için geçerlidir.

Üçüncü taraf sabit sürücülerle yüklenen boş birimlerin işletim sistemi normal olarak başlar, ancak eklenen sabit sürücüler başlangıç yazılımı ayarından önce RAID yardımcı programıyla yapılandırılmalıdır.

Daha fazla ayrıntı için kurulum kılavuzuna bakın.

DIVAR IP sistemler fabrikadan önceden yüklenmiş Yapılandırma Sihirbazı ile birlikte gönderilir. Tüm DIVAR IP sistemleri varsayılan bir IP adresi ve varsayılan iSCSI ayarlarıyla önceden yapılandırılmıştır:

- IP Adresi: Otomatik olarak DHCP tarafından atanır (geri dönüş IP adresi: 192.168.0.200).
- Alt ağ maskesi: Otomatik olarak DHCP tarafından atanır (geri dönüş alt ağ maskesi: 255.255.255.0).

#### Yönetici hesabı için varsayılan kullanıcı ayarları

- Kullanıcı: BVRAdmin
- Şifre: İlk oturumda ayarlanacak.

Aşağıdakilere uyun:

- Kurulum sırasında DIVAR IP'de etkin ağ bağlantısı olması gerekir. Bağlanmaya çalıştığınız ağ anahtarının açık olduğundan emin olun.
- Varsayılan IP adresi ağdaki başka bir cihaz tarafından kullanılıyor olmamalıdır. Ağdaki mevcut DIVAR IP sistemlerinin varsayılan IP adreslerinin başka bir DIVAR IP eklenmeden önce değiştirildiğinden emin olun.

## 4 İlk oturum açma ve sistem kurulumu



### Uyarı!

İşletim sistemi ayarlarını değiştirmemenizi kesinlikle öneririz. İşletim sistemi ayarlarını değiştirmek, sistemin arızalanmasına neden olabilir.



### Uyarı!

İdari görevleri gerçekleştirmek için yönetici hesabında oturum açmanız gerekir.



### Uyarı!

Şifrenin kaybedilmesi durumunda, kurulum kılavuzunda açıklandığı gibi bir sistem kurtarma işlemi gerçekleştirilmelidir. Yapılandırma en baştan yapılmalıdır veya içe aktarılmalıdır.

Sistemi kurmak için:

1. DIVAR IP all-in-one 7000 birimini ve kameraları ağa bağlayın.
2. Birimi açın.  
Microsoft Windows Server IoT 2019 for Storage Standard kurulum rutinleri gerçekleştirilir. Bu işlem birkaç dakika sürebilir. Sistemi kapatmayın.  
İşlem tamamlandıktan sonra, Windows dil seçim ekranı görüntülenir.
3. Listedeki ülkenizi/bölgenizi, istediğiniz işletim sistemi dilini ve klavye düzenini seçin, ardından **İleri**'ye tıklayın.  
Microsoft Software License Terms ve EULA (Son Kullanıcı Lisans Sözleşmesi) görüntülenir.
4. Lisans koşullarını kabul etmek için **Kabul Et**'e tıklayın ve Windows yeniden başlatılana kadar bekleyin. Bu işlem birkaç dakika sürebilir. Sistemi kapatmayın.  
Yeniden başlatmadan sonra, Windows oturum açma sayfası görüntülenir.
5. **BVRAdmin** yönetici hesabı için yeni bir şifre ayarlayın ve onaylayın (Not: Minimum şifre uzunluğu 14 karakterdir). Ardından ENTER'a basın.  
**Yazılım Seçimi** sayfası görüntülenir.
6. DIVAR IP Software Center yükleme dosyasına tıklayın.  
DIVAR IP Software Center yükleme işlemi başlar. Yükleme tamamlandıktan sonra, Windows yeniden başlatılır ve Windows oturum açma sayfasına yönlendirilirsiniz.  
Not: DIVAR IP Software Center yükleme dosyası yerel bir sürücüde bulunmuyorsa yükleme dosyasıyla birlikte bir depolama ortamı (USB flash sürücü, DVD-ROM) takın.  
Depolama ortamı DIVAR IP Software Center yükleme dosyası için otomatik olarak tanınır ve yükleme dosyası **Yazılım Seçimi** sayfasında görüntülenir.
7. Yönetici hesabında oturum açın.  
Microsoft Edge tarayıcısı otomatik olarak başlatılır.
8. Yönetici kullanıcı adını ve şifresini girerek **Oturum aç**'a tıklayın.  
DIVAR IP Software Center başlatılır ve yazılım paketleri yüklenir.  
Not: İsteddiğiniz çalışma moduna ait ilgili yazılım paketleri yerel bir sürücüde bulunmuyorsa sistem kurulumuna devam etmek için yazılım paketleriyle birlikte bir depolama ortamı takın.

<https://downloadstore.boschsecurity.com/> adresindeki Bosch Security and Safety Systems **İndirme Alanı**'nda en güncel yazılımları ve mevcut yükseltme paketlerini bulabilirsiniz

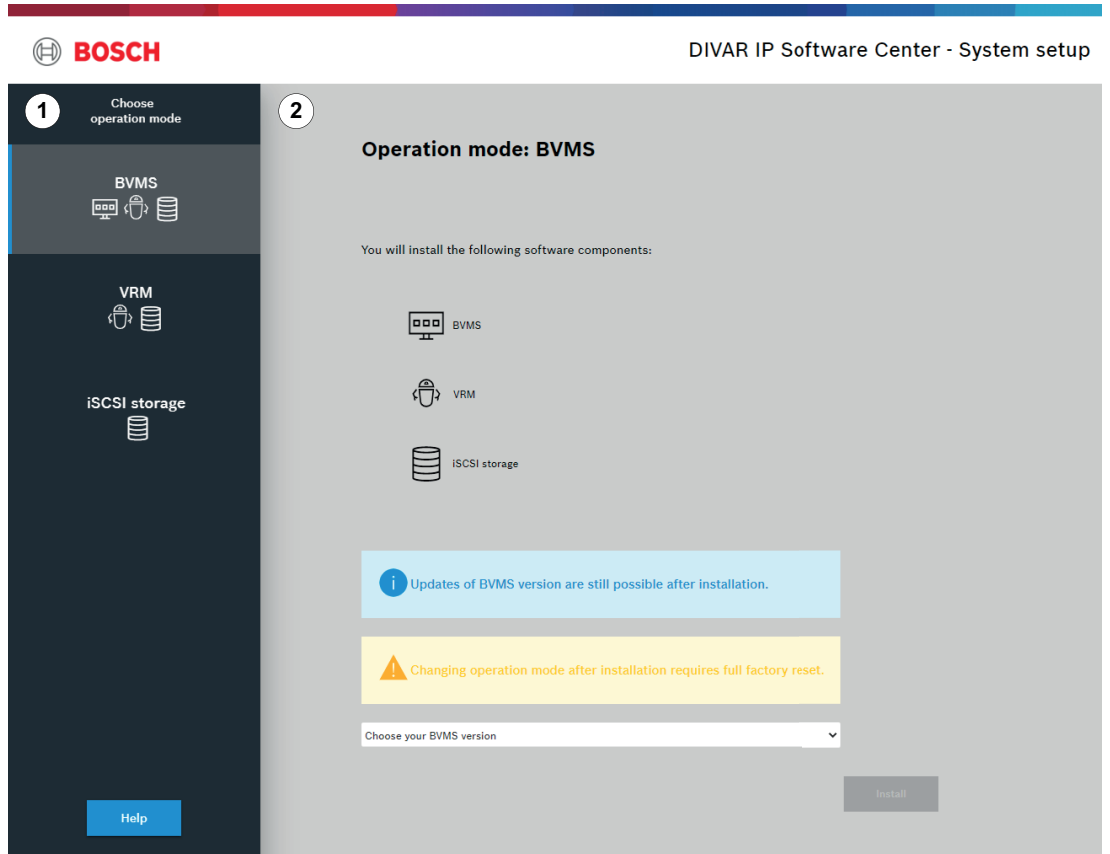
## 4.1 Çalışma modunu seçme

DIVAR IP Software Center uygulamasında DIVAR IP all-in-one 7000 sisteminizi yapılandırmak için istediğiniz çalışma modunu seçmeniz gerekir.



### Uyarı!

Yükleme işleminden sonra çalışma modunu değiştirmek için tam fabrika ayarları sıfırlaması gerekir.



1	Seçim penceresi
2	Ana pencere

### Bkz.

– Çalışma modları, sayfa 5

### 4.1.1

#### Tam video kaydı ve yönetim sistemi olarak çalışma

DIVAR IP sisteminizi tam video kaydı ve yönetim sistemi olarak çalıştırmak için:

- Seçim penceresinde **BVMS**'ye tıklayın. Yüklenilecek yazılım bileşenleri ana pencerede görüntülenir.
- Listeden istediğiniz BVMS sürümünü seçin ve ardından **Install**'e tıklayın. Yüklenilecek yazılım paketlerini gösteren **BVMS installation** iletişim kutusu görüntülenir.



- Devam etmek için **Install**'ye tıklayın.  
Yazılım paketlerinin yüklenmesi başlar. Bu işlem birkaç dakika sürebilir. Sistemi kapatmayın ve depolama ortamını çıkarmayın.  
Not: Yükleme sırasında hata oluşursa **Finish**'e tıklayın. Bu, sistemi yeniden başlatır.  
Yeniden başlattıktan sonra, ilgili yazılım paketlerini güncelleştirin ve kurulumu devam edin.
- Tüm paketler başarıyla yüklendikten sonra **Finish**'e tıklayın.  
Sistem yeniden başlatılır. Yeniden başlattıktan sonra BVMS masaüstüne yönlendirilirsiniz.
- BVMS masaüstünde, sisteminizi yapılandırmak için istediğiniz uygulamaya tıklayın.

**Uyarı!**

Daha fazla ayrıntı için BVMS belgelerine bakın.

**4.1.2****Saf video kayıt sistemi olarak çalıştırma**

DIVAR IP sistemini sadece video kayıt sistemi olarak çalıştırmak için:

- Seçim penceresinde **VRM**'ye tıklayın.  
Yüklenecek yazılım bileşenleri ana pencerede görüntülenir.
- Listeden istediğiniz VRM sürümünü seçin ve ardından **Install**'ye tıklayın.  
Yüklenecek yazılım paketlerini gösteren **VRM installation** iletişim kutusu görüntülenir.
- Devam etmek için **Install**'ye tıklayın.  
Yazılım paketlerinin yüklenmesi başlar. Bu işlem birkaç dakika sürebilir. Sistemi kapatmayın ve depolama ortamını çıkarmayın.  
Not: Yükleme sırasında hata oluşursa **Finish**'e tıklayın. Bu, sistemi yeniden başlatır.  
Yeniden başlattıktan sonra, ilgili yazılım paketlerini güncelleştirin ve kurulumu devam edin.
- Tüm paketler başarıyla yüklendikten sonra **Finish**'e tıklayın.  
Sistem yeniden başlatılır. Yeniden başlattıktan sonra, Windows oturum açma ekranına yönlendirilirsiniz.

**Uyarı!**

Daha fazla ayrıntı için VRM belgelerine bakın.

**4.1.3****iSCSI veri depolama alanı genişletmesi olarak çalıştırma**

DIVAR IP sistemini iSCSI saklama genişletmesi olarak çalıştırmak için:

- Seçim penceresinde **iSCSI storage**'na tıklayın.  
Yüklenecek yazılım bileşenleri ana pencerede görüntülenir.
- Listeden istediğiniz bileşenleri seçin ve ardından **Install**'ye tıklayın.  
Yüklenecek yazılım paketlerini gösteren **iSCSI storage installation** iletişim kutusu görüntülenir.
- Devam etmek için **Install**'ye tıklayın.  
Yazılım paketlerinin yüklenmesi başlar. Bu işlem birkaç dakika sürebilir. Sistemi kapatmayın ve depolama ortamını çıkarmayın.  
Not: Yükleme sırasında hata oluşursa **Finish**'e tıklayın. Bu, sistemi yeniden başlatır.  
Yeniden başlattıktan sonra, ilgili yazılım paketlerini güncelleştirin ve kurulumu devam edin.
- Tüm paketler başarıyla yüklendikten sonra **Finish**'e tıklayın.  
Sistem yeniden başlatılır. Yeniden başlattıktan sonra, Windows oturum açma ekranına yönlendirilirsiniz.
- Sistemi harici bir BVMS veya VRM sunucusuna BVMS Configuration Client veya Configuration Manager kullanarak iSCSI veri depolama alanı genişletmesi olarak ekleyin.



**Uyarı!**

Daha fazla ayrıntı için BVMS veya Configuration Manager belgelerine bakın.

## 5

# Yazılımı yükseltme ve güncelleştirme

Ayrıca DIVAR IP Software Center ile yüklü yazılımı da güncelleyebilir ve yükseltebilirsiniz.

En güncel yazılımı ve mevcut yükseltme paketlerini Bosch Security and Safety Systems **İndirme Alanı**'nda bulabilirsiniz:

<https://downloadstore.boschsecurity.com/>

### Yazılımı yükseltme

Yüklenen yazılımı yükseltmek için:

1. İsteddiğiniz yazılım paketlerini **İndirme Alanı**'ndan indirin ve bunları yerel bir sürücüye veya depolama ortamına kaydedin. Ardından depolama ortamını sisteminize bağlayın.
2. DIVAR IP Software Center uygulamasını başlatın.  
**Installed software** sayfası görüntülenir.
3. **Upgrades** bölümünde mevcut sürüm yükseltmeleri görüntülenir. İsteddiğiniz yazılımı yükseltmek **Upgrade**'e tıklayın.  
**Upgrade** iletişim kutusu, yükseltmede yer alan yazılım paketlerini gösterir.  
Not: Sürüm yükseltme tüm ayarlarınızı kaydeder, yazılımı günceller ve sistemi yeniden başlatır.
4. Devam etmek için **Install**'ye tıklayın.  
Yazılım paketlerinin yüklenmesi başlatılır. Bu işlem birkaç dakika sürebilir. Sistemi kapatmayın ve depolama ortamını çıkarmayın.  
Yükleme tamamlandıktan sonra sistem yeniden başlatılır.

### Yazılımı güncelleme

Yüklenen yazılımı güncellemek için:

1. İsteddiğiniz yazılım paketlerini **İndirme Alanı**'ndan indirin ve bunları yerel bir sürücüye veya depolama ortamına kaydedin. Ardından depolama ortamını sisteminize bağlayın.
2. DIVAR IP Software Center uygulamasını başlatın.  
**Installed software** sayfası görüntülenir.
3. **Updates** bölümünde mevcut güncellemeler görüntülenir. Tüm yazılım paketlerini yeni sürüme güncellemek için **Update all**'a tıklayın.  
Güncellenecek olan yazılım paketlerini gösteren **Update** iletişim kutusu görüntülenir.  
Not: Güncelleme tüm ayarlarınızı kaydeder, yazılımı günceller ve sistemi yeniden başlatır.
4. Devam etmek için **Install**'ye tıklayın.  
Yazılım paketlerinin yüklenmesi başlatılır. Bu işlem birkaç dakika sürebilir. Sistemi kapatmayın ve depolama ortamını çıkarmayın.  
Yükleme tamamlandıktan sonra sistem yeniden başlatılır.

## 6 Sisteme uzaktan bağlantı

Bu bölümde, DIVAR IP sistemine internet üzerinden erişmek için gerekli olan adımlar açıklanmaktadır.

### 6.1 Sistemi yetkisiz erişime karşı koruma

Sistemi yetkisiz erişime karşı korumak için sistemi internete bağlamadan önce güçlü şifre kurallarına uymanızı öneririz. Şifreniz ne kadar güçlü olursa sisteminiz yetkisiz kişilerden ve kötü amaçlı yazılımlardan o kadar korunur.

### 6.2 Port yönlendirmeyi ayarlama

Bir DIVAR IP sistemine internet üzerinden NAT/PAT özellikli bir yönlendirici ile bağlanmak için DIVAR IP sisteminde ve yönlendiricide port yönlendirme yapılandırılmış olmalıdır.

#### Port yönlendirmeyi ayarlamak için:

- ▶ İnternet yönlendiricinizin port yönlendirme ayarlarında aşağıdaki port kurallarını girin:
  - BVMS Operator Client kullanarak SSH tüneli erişimi için port 5322.
  - VRM'e Video Security Client veya Video Security App kullanarak HTTPS erişimi için port 443.

DIVAR IP sistemine artık internetten erişebilirsiniz.

### 6.3 Uygun bir istemci seçme

Bu bölümde, bir DIVAR IP sistemine internet üzerinden uzaktan bağlantı sağlayan yollar açıklanmaktadır.

Uzaktan bağlantı kurmanın 2 yolu vardır:

- *Operator Client ile uzaktan bağlantı, sayfa 12*
- *Video Security Uygulaması ile uzaktan bağlantı, sayfa 12.*




#### Uyarı!

Yalnızca DIVAR IP ile aynı sürümdeki BVMSOperator Client veya Video Security App'i kullanın. Diğer istemciler veya uygulama yazılımları çalışabilir ancak desteklenmez.

#### 6.3.1 Operator Client ile uzaktan bağlantı

##### BVMSOperator Client ile uzaktan bağlantı kurmak için:

1. İstemci iş istasyonuna BVMSOperator Client yükleyin.
2. Yükleme işlemi başarıyla tamamlandıktan sonra masaüstü kısayolunu  kullanarak Operator Client'ı başlatın.
3. Aşağıdakileri girin, ardından **Tamam**'a tıklayın.
  - Kullanıcı adı:** admin (yapılandırıldıysa başka kullanıcı)
  - Şifre:** Kullanıcı şifresini girin
  - Bağlantı:** ssh://[public-IP-address-of-DIVAR-IP\_all-in-one]:5322

#### 6.3.2 Video Security Uygulaması ile uzaktan bağlantı

##### Video Security App ile uzaktan bağlantı kurmak için:

1. Apple App Store'da BoschVideo Security ifadesini arayın.
2. Video Security uygulamasını iOS cihazınıza yükleyin.
3. Video Security uygulamasını başlatın.
4. **Ekle**'yi seçin.
5. Genel IP adresini veya dynDNS adını girin.

6. Güvenli Bağlantı'nın (SSL) açık olduğundan emin olun.
7. **Ekle**'yi seçin.
8. Aşağıdakileri girin:  
**Kullanıcı adı:** admin (yapılandırıldıysa başka bir kullanıcı)  
**Şifre:** Kullanıcı şifresini girin

## 6.4 Enterprise Management Server kurma

Birden fazla sistemi merkezi olarak yönetmek için ayrı bir sunucuya Bosch VMS Enterprise Management Server kurabilirsiniz.

### **Bosch VMS Enterprise Management Server'ı ayrı bir sunucuya kurmak için:**

1. Ürün sayfasından yükleyiciyi BVMS yükleyicisini indirin.
2. BVMS yükleyicisini Enterprise Management Server olarak görev yapması gereken sunucuya kopyalayın.
3. Yükleyici programına çift tıklayın, ardından güvenlik mesajı kabul edin.
4. **Hoş Geldiniz** iletişim kutusunda, **Enterprise Management Server** ve **Configuration Client** haricindeki tüm onay kutularını temizleyin.
5. Kurulum talimatlarını izleyin.
6. Yükleyici başarıyla tamamlandıktan sonra masaüstü kısayolunu kullanarak Configuration Client'ı başlatın.



### **Uyarı!**

Enterprise Management Server yapılandırması için BVMS belgelerine bakın.

## 7

## Bakım

### 7.1

### Sistemin izlenmesi

Sistem, durum izleme için araçlar sağlar.

İzleme işlevini etkinleştirmek için yönetici hesabında (BVRAdmin) oturum açmanız gerekir.

1. Sistem ekranında (seçilen çalışma moduna bağlı olarak BVMS masaüstü veya Windows oturum açma ekranıdır), CTRL+ALT+DEL tuşlarına basın.
2. SHIFT tuşunu basılı tutun, **Kullanıcı Değiştir**'e tıklayın ve SHIFT tuşunu beş saniye süreyle basılı tutun.
3. Kullanıcı adını ve şifreyi girin.
4. Masaüstündeki **Araçlar** klasöründe **Enable\_SuperDoctor\_5\_Service** komut dosyasına sağ tıklayın ve **Yönetici olarak çalıştır**'a tıklayın.
5. Aynı klasördeki **SuperDoctor 5 Web** simgesine çift tıklayın.
6. Şu varsayılan kimlik bilgilerini kullanarak web arayüzünde oturum açın:  
Kullanıcı adı: admin  
Şifre: DivaripSD5
7. **Yapılandırma** sekmesine ve ardından **Şifre ayarları**'na tıklayın ve varsayılan şifreyi değiştirin.
8. **Yapılandırma** sekmesine ve ardından **Uyarı Yapılandırması**'na tıklayın.
9. **SNMP Trap** özelliğini etkinleştirin ve SNMP trap alıcısının IP adresini belirtin.

### 7.2

### Birimi eski haline getirme

Aşağıdaki prosedürde fabrika varsayılan görüntüsünün nasıl geri yükleneceği açıklanmaktadır.

#### Birimi fabrika varsayılan görüntüsüne geri yüklemek için:

1. Birimi başlatın ve BIOS açma otomatik testi sırasında **F7**'ye basın.  
Kurtarma menüsü görüntülenir.
2. Aşağıdakilerden birini seçin:
  - **İlk fabrika ayarı:** Fabrika varsayılan görüntüsünü geri yükler ve HDD'lerdeki tüm verileri siler.  
veya
  - **Sistem Kurtarma (Fabrika Varsayılan Ayarlarına geri dön):** Fabrika varsayılan görüntüsünü geri yükler; HDD'lerdeki veriler silinmez.

#### Not:

**Sistem Kurtarma** seçeneği veri HDD'lerinde saklanan video görüntülerini silmediği halde, varsayılan bir yapılandırma ile işletim sistemi bölümünün tamamını (VMS ayarları dahil) değiştirir. Kurtarmanın ardından mevcut video görüntülerine erişmek için VMS yapılandırmasının Sistem Kurtarma işleminden önce dışa aktarılması ve daha sonra yeniden içe aktarılması gerekir.



#### Uyarı!

İşlem sırasında birimi kapatmayın. Bu, Kurtarma ortamına zarar verir.

3. Birim Kurtarma ortamından başlatılır. Ayar başarılıysa **Evet**'e basarak sistemi yeniden başlatın.
4. Windows işletim sisteminin ilk kurulumunu gerçekleştirin. Windows kurulumu tamamlandıktan sonra birim yeniden başlatılır.
5. Birim yeniden başlatıldıktan sonra fabrika ayarları yüklenir.

## 8 Ek bilgiler

### 8.1 Ek belgeler ve istemci yazılımı

Daha fazla bilgi, yazılım indirmeleri ve belge için [www.boschsecurity.com](http://www.boschsecurity.com) adresini ziyaret edin ve ürün kataloğundaki ilgili ürün sayfasına gidin.

En güncel yazılımı ve mevcut yükseltme paketlerini Bosch Security and Safety Systems **İndirme Alanı**'nda bulabilirsiniz:

<https://downloadstore.boschsecurity.com/>

### 8.2 Destek hizmetleri ve Bosch Akademisi



#### Destek

**Destek hizmetlerimize** [www.boschsecurity.com/xc/en/support/](http://www.boschsecurity.com/xc/en/support/) adresinden erişebilirsiniz.

Bosch Security and Safety Systems şu alanlarda destek sağlar:

- [Uygulamalar ve Araçlar](#)
- [Bina Bilgileri Modelleme](#)
- [Faaliyete Alma](#)
- [Garanti](#)
- [Sorun giderme](#)
- [Onarım ve Değişim](#)
- [Ürün Güvenliği](#)



#### Bosch Building Technologies Akademisi

Bosch Building Technologies Akademisi web sitesini ziyaret edin ve **eğitim kursları, görüntülü eğitimler** ve **belgelere** erişim kazanın: [www.boschsecurity.com/xc/en/support/training/](http://www.boschsecurity.com/xc/en/support/training/)









**Bosch Security Systems B.V.**

Torenallee 49

5617 BA Eindhoven

Netherlands

**[www.boschsecurity.com](http://www.boschsecurity.com)**

© Bosch Security Systems B.V., 2020