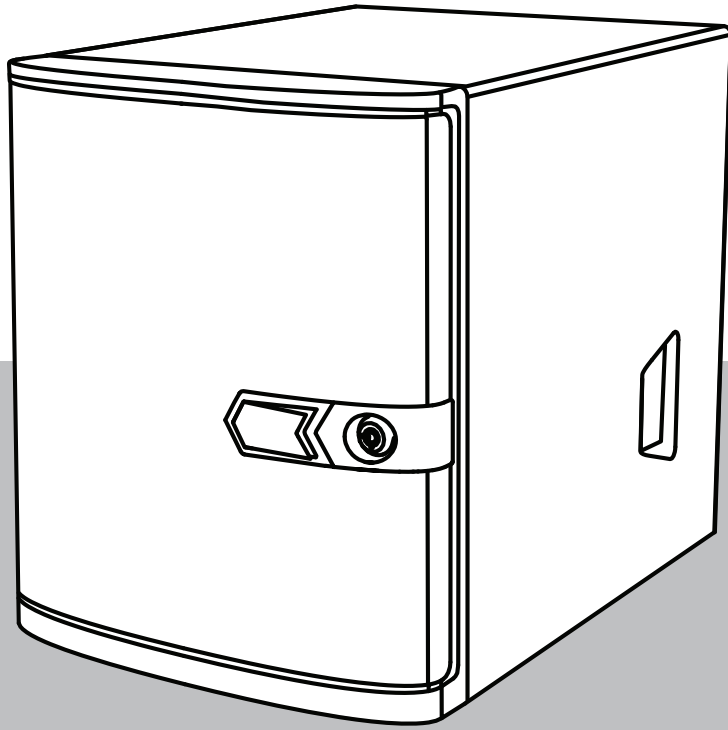




BOSCH

DIVAR IP all-in-one 4000

DIP-4420IG-00N | DIP-4424IG-2HD | DIP-4428IG-2HD |
DIP-442IIG-2HD



İçindekiler

1	Güvenlik	4
1.1	Çalışma önlemleri	4
1.2	Siber güvenlik önlemleri	5
1.3	Yazılım önlemleri	6
1.3.1	En güncel yazılımı kullanın	6
1.3.2	OSS bilgileri	6
2	Giriş	7
3	Sisteme genel bakış	8
4	Sistem ayarı	9
4.1	Varsayılan ayarlar	9
4.2	Ön koşullar	9
4.3	İlk oturum açma ve ilk sistem kurulumu	9
4.3.1	Çalışma modu olarak BVMS'in seçilmesi	11
4.3.2	Çalışma modu olarak VRM'in seçilmesi	11
4.3.3	Çalışma modu olarak iSCSI Veri Depolama'nın seçilmesi	12
5	Yazılımı yükseltme	13
5.1	DIVAR IP System Manager'ı yükseltme	13
5.2	Yazılımın DIVAR IP System Manager kullanarak yükseltilmesi	13
6	Sisteme uzaktan bağlantı	16
6.1	Sistemi yetkisiz erişime karşı koruma	16
6.2	Port yönlendirmeyi ayarlama	16
6.3	Uygun bir istemci seçme	16
6.3.1	BVMS Operator Client ile uzaktan bağlantı	16
6.3.2	Video Security Uygulaması ile uzaktan bağlantı	17
6.4	Enterprise Management Server'a bağlanma	17
6.5	Remote Portal'a bağlanma	17
6.5.1	Remote Portal hesabı oluşturma	17
6.5.2	DIVAR IP all-in-one cihazlarını Remote Portal'a kaydetme	18
6.5.3	DIVAR IP all-in-one cihazlarının kaydını Remote Portal'dan silme	18
7	Bakım	19
7.1	Yönetici hesabında oturum açma	19
7.2	Sistemin izlenmesi	19
7.3	Arızalı sabit disk sürücüyü değiştirme ve yeni bir sabit disk sürücüyü yapılandırma	19
7.3.1	Arızalı sabit disk sürücüyü değiştirme	20
7.3.2	Yeni bir sabit disk sürücü yapılandırma	20
7.4	DIVAR IP System Manager günlük dosyalarının alınması	22
7.5	Birimi eski haline getirme	22
8	Ek bilgiler	24
8.1	Ek belgeler ve istemci yazılımı	24
8.2	Destek hizmetleri ve Bosch Akademisi	24

1 Güvenlik

Bu bölümdeki güvenlik önlemlerine uyun.

1.1 Çalışma önlemleri

**Uyarı!**

Kullanım amacı

Bu ürün sadece profesyonel kullanıma yöneliktir. Genel olarak erişilebilen kamuya açık bir alana monte edilmemelidir.

**Uyarı!**

Bu ürünü nemli veya ıslak bir yerde kullanmayın.

**Uyarı!**

Cihazı elektrik dalgalanmaları ve yıldırım kaynaklı dalgalanmalardan korumak için önlem alın.

**Uyarı!**

Cihazın etrafındaki alanı temiz ve düzenli tutun.

**Uyarı!**

Muhafaza delikleri

Delikleri engellemeyin veya kapatmayın. Muhafazadaki delikler havalandırma amacıyla kullanılır. Bu delikler aşırı ısınmayı önler ve güvenilir bir çalışma sağlar.

**Uyarı!**

Cihaz kapağını açmayın veya çıkarmayın. Kapağı açmak veya çıkarmak sisteme zarar verebilir ve garantiyi geçersiz kılar.

**Uyarı!**

Cihazın üzerine sıvı dökmeyin.

**İkaz!**

Ana kart yakınında servis işlemleri yaparken ve çalışırken dikkatli olun. Sistem çalışırken ana kart üzerinde tehlikeli gerilim veya enerji vardır. Ana karta metal nesnelerle dokunmayın ve ana karta hiçbir şerit kablonun dokunmadığından emin olun.

**Uyarı!**

Ürünü taşımadan önce güç bağlantısını kesin. Ürünü dikkatle taşıyın. Aşırı güç veya darbe, ürüne ve sabit disk sürücülerine zarar verebilir.

**İkaz!**

Bu üründe kullanılan kurşun lehim malzemelerini tutmak California Eyaleti'nde doğum kusurlarına ve diğer üreme zararlarına neden olduğu bilinen kurşuna maruz kalmanıza neden olabilir.

**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**Siber güvenlik önlemleri**

Siber güvenlik nedeniyle aşağıdakilere uyun:

- Sisteme fiziksel erişimin sadece yetkili personelle kısıtlandığından emin olun. Sistemde fiziksel değişiklik yapılmasını önlemek için sistemi kartlı geçişle korunan bir alana yerleştirin.
 - Sabit sürücülerin yetkisiz olarak çıkarılmasını engellemek için ön çerçeveyi kilitleyin. Anahtarı mutlaka kilitlenmiş tutun.
 - Ek olarak cihazı sabitlemek için arka kasa kelepçesini veya Kensington yuvasını kullanın.
 - İşletim sistemi, yazılım görüntüsünün oluşturulduğu zamanda sunulan en son Windows güvenlik yamalarını içerir. İşletim sistemi güvenlik güncellemelerini düzenli olarak yüklemek için Windows çevrimiçi güncelleme işlevi veya çevrimdışı yükleme için ilgili aylık toplama yamalarını kullanın.
 - Windows Defender ve Windows güvenlik duvarını kapatmayın ve her zaman güncelleyin.
 - Virüsten korunma için ek yazılım yüklemeyin.
 - Yetkisinden emin olmadığınız sürece tanımadığınız kişilere sistem bilgilerini ve hassas verileri vermeyin.
 - Web sitesinin güvenliğini kontrol etmeden hassas bilgileri internet üzerinden göndermeyin.
 - Yerel ağ erişimini yalnızca güvenilir cihazlarla sınırlayın. Ayrıntılar, çevrimiçi ürün kataloğunda bulunan aşağıdaki belgelerde açıklanmıştır:
 - *Ağ Kimlik Denetimi 802.1X*
 - *Bosch IP video ürünleri için siber güvenlik kılavuzu*
 - Genel ağlar aracılığıyla erişim için yalnızca güvenli (şifreli) iletişim kanalları kullanın.
 - Yönetici hesabı, tam yönetici ayrıcalıkları ve sisteme sınırsız erişim sağlar. Yönetici hakları, kullanıcıların, yazılımı yüklemesine, güncellemesine veya kaldırmasına ve yapılandırma ayarlarını değiştirmesine imkan verir. Ayrıca yönetici hakları, kullanıcıların, merkezi yönetim ve güvenlik ayarlarına doğrudan erişmesini, kayıt anahtarlarını değiştirmesini ve bununla merkezi yönetim ile güvenlik ayarlarını atlamasını sağlar. Yönetici hesabıyla oturum açan kullanıcılar, güvenlik duvarlarını aşabilir ve virüsten koruma yazılımını kaldırarak sistemi virüslere ve siber saldırılara açık hale getirebilir. Bu, sistem ve veri güvenliği açısından ciddi bir risk oluşturabilir.
- Siber güvenlik risklerini en aza indirmek için aşağıdakilere dikkat edin:
- Yönetici hesabının, şifre ilkesine uygun olarak karmaşık bir şifreyle korunduğundan emin olun.
 - Yalnızca sınırlı sayıda güvenilir kullanıcının yönetici hesabına erişimi olduğundan emin olun.

- Çalışma gereksinimleri nedeniyle sistem sürücüsü şifrelenmemelidir. Şifreleme olmadan, bu sürücüde saklanan veriler kolayca erişilip kaldırılabilir. Veri çalınması veya verilerin kazara kaybını önlemek üzere yalnızca yetkili kişilerin sisteme ve yönetici hesabına erişebildiğinden emin olun.
- Yazılımın yüklenmesi ve güncellenmesinin yanı sıra sistemin kurtarılması için USB cihazlarının kullanılması gerekebilir. Bu nedenle, sisteminizin USB portları devre dışı bırakılamaz. Ancak USB cihazlarının sisteme bağlanması kötü amaçlı yazılım bulaşması riski oluşturur. Kötü amaçlı yazılım saldırılarını önlemek için sisteme virüs bulaşmış USB cihazı bağlanmadığından emin olun.

1.3

Yazılım önlemleri

1.3.1

En güncel yazılımı kullanın

Cihazı ilk kez çalıştırmadan önce, yazılım sürümünüzün en güncel sürümünü yüklediğinizden emin olun. Tutarlı işlevsellik, uyumluluk, performans ve güvenlik için cihazın kullanım ömrü boyunca yazılımı düzenli olarak güncelleyin. Yazılım güncellemeleriyle ilgili ürün belgelerinde yer alan talimatları izleyin.

Aşağıdaki bağlantılar daha fazla bilgi sağlar:

- Genel bilgiler: <https://www.boschsecurity.com/xc/en/support/product-security/>
- Tespit edilen güvenlik açıkları ve önerilen çözümler listesi içeren güvenlik danışma önerileri: <https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html>

Bosch, ürünlerinin yeni yazılım bileşenleriyle işletimi nedeniyle meydana gelen herhangi bir hasar için herhangi bir yükümlülüğü kabul etmez.

En güncel yazılımı ve mevcut yükseltme paketlerini Bosch Security and Safety Systems indirme mağazasında bulabilirsiniz:

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

1.3.2

OSS bilgileri

Bosch, DIVAR IP all-in-one ürünlerinde açık kaynak yazılımlar kullanır.

Kullanılan açık kaynak yazılım bileşenlerinin lisanslarını sistem sürücüsünde şu dizinde bulabilirsiniz:

C:\license txt\

Sisteminize yüklenen herhangi bir başka yazılımda kullanılan Açık Kaynak Yazılım bileşenlerinin lisansları, aşağıdakiler gibi ilgili yazılımın kurulum klasöründe saklanır:

C:\Program Files\Bosch\SysMgmService\apps\sysmgm-commander\[version]\License

veya şu klasörlerde saklanır:

C:\Program Files\Bosch\SysMgmService\apps\sysmgm-executor\[version]\License

2

Giriş

DIVAR IP all-in-one 4000, 32 kanala kadar (8 kanal önceden lisanslıdır) IP video gözetim sistemleri için uygun maliyetli ve kullanımı kolay, hepsi bir arada kayıt, görüntüleme ve yönetim çözümüdür.

DIVAR IP all-in-one 4000, BT odaklı müşteriler için gelişmiş Bosch Video Management System özelliklerini ve modern kayıt yönetimini uygun maliyetli, kurulumu ve çalıştırması kolay tek bir IP kayıt cihazında birleştiren, 2 disk yuvalı mini dikey kasalı cihazdır.

DIVAR IP all-in-one 4000 cihazları dahili tasarım ve temel bileşenler kullanır ve Microsoft Windows Server IoT 2022 for Storage Workgroup işletim sistemi temel alınmıştır.

DIVAR IP all-in-one 4000 cihazları 36 TB'a kadar brüt veri depolama kapasitesi sunan, "kurumsal sınıf" önden değiştirilebilir SATA sabit disk sürücülere sahiptir.

3 Sisteme genel bakış

İşletim sistemi

Microsoft Windows Server IoT 2022 for Storage Workgroup işletim 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 2022 for Storage Workgroup işletim sistemi, veri depolama yönetim senaryolarında önemli iyileştirmelerin yanı sıra veri depolama cihazı yönetim bileşenleri ve işlevlerinin entegrasyonunu sağlar.

DIVAR IP System Manager

DIVAR IP System Manager uygulaması, kolay sistem kurulumu, yapılandırma ve yazılım yükseltmesi sunan merkezi kullanıcı arayüzüdür.

Çalışma modları

DIVAR IP all-in-one 4000 cihazları üç farklı modda çalışabilir:

- BVMS ve Video Recording Manager temel bileşenleri ve hizmetleri kullanılan tam video kayıt ve yönetim sistemi.
Bu mod, IP ağı üzerinden sorunsuz bir şekilde dijital video, ses ve veri yönetimi sağlayan gelişmiş bir IP video güvenlik çözümü sunar. IP kameralar ile video kodlayıcıları sorunsuz şekilde birleştirir, sistem genelinde olay ve alarm yönetimine, sistem durumu takibine, kullanıcı ve öncelik yönetimine olanak tanır. Bu mod, Bosch kameraların ve kayıt çözümlerinin benzersiz özelliklerinden yararlanarak Bosch video gözetim cihazlarıyla uyumlu en iyi video yönetim sistemini sunar. Üçüncü taraf kameraları entegre etmek için Video Streaming Gateway bileşenleri içerir.
- Video Recording Manager temel bileşenleri ve hizmetlerini kullanan, Bosch kameralarının ve kayıt çözümlerinin benzersiz özelliklerinden yararlanan bir BVMS sistemi için gelişmiş video kayıt çözümü. DIVAR IP all-in-one cihazında çalışan bir BVMS sistemine iki adede kadar Video Recording Manager sunucusu eklenebilir.
- Farklı bir donanımda çalışan bir BVMS sistemi için iSCSI veri depolama alanı genişletmesi. DIVAR IP all-in-one 4000 cihazında çalışan BVMS sistemine bu iSCSI genişletmelerinden en fazla iki adet eklenebilir.

DIVAR IP System Manager uygulamasında sisteminizi kurarken, sistemi yapılandırmak için istenen çalışma modunu seçmeniz gerekir.

Ayrıca DIVAR IP System Manager uygulaması ile yüklü yazılımı güncelleyebilir ve yükseltebilirsiniz.

En güncel yazılımı ve mevcut yükseltme paketlerini Bosch Security and Safety Systems indirme mağazasında bulabilirsiniz:

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



Uyarı!

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

4

Sistem ayarı

4.1

Varsayılan ayarlar

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 adı: **BVRAdmin**
- Şifre: İlk oturumda şifre belirlenir.
Şifre gereklilikleri:
 - En az 14 karakter.
 - En az bir büyük harf.
 - En az bir küçük harf.
 - En az bir rakam.

4.2

Ön koşullar

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.

4.3

İlk oturum açma ve ilk sistem kurulumu



Uyarı!

İşletim sistemi ayarlarını değiştirmeyin. 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 birimini ve kameraları ağa bağlayın.
2. Birimi açın.
Microsoft Windows Server IoT 2022 for Storage Workgroup 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 yazılım lisans koşulları 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. Yönetici hesabı **BVRAdmin** için yeni bir şifre belirleyin ve onaylayın.
Şifre gereklilikleri:
 - En az 14 karakter.
 - En az bir büyük harf.
 - En az bir küçük harf.
 - En az bir rakam.
 Ardından, Enter tuşu düğmesine basın.
Software Selection sayfası görüntülenir.
6. Sistem, DIVAR IP System Manager kurulum dosyası olan ve `Drive root\BoschAppliance\` yapısına sahip bir klasörde bulunan **SystemManager_x64_[software version].exe** dosyası için yerel sürücüyü ve bağlı harici depolama ortamını otomatik olarak tarar.
Tarama biraz zaman alabilir. Tamamlanmasını bekleyin.
7. Sistem yükleme dosyasını bulduktan sonra yükleme dosyası, **Software Selection** sayfasında görüntülenir. Kurulumu başlatmak için kurulum dosyasını görüntüleyen çubuğa tıklayın.
Uyarı: DIVAR IP System Manager'ın en son sürümünün kurulu olduğundan emin olun. En güncel yazılımı ve mevcut yükseltme paketlerini Bosch Security and Safety Systems indirme mağazasında bulabilirsiniz: <https://downloadstore.boschsecurity.com/>.
8. Tarama işlemi sırasında yükleme dosyası bulunamadıysa aşağıdaki işlemleri yapın:
 - <https://downloadstore.boschsecurity.com/> adresine gidin.
 - **Software** sekmesinin altında, listeden **BVMS Appliances** 'ı seçin ve ardından **Select** seçeneğine tıklayın.
Kullanılabilir tüm yazılım paketlerinin bir listesi görüntülenir.
 - **SystemManager_[software version].zip** ZIP dosyasını bulun ve USB bellek gibi bir veri depolama cihazına kaydedin.
 - Veri depolama ortamındaki ZIP dosyasını açın ve **BoschAppliance** klasörünün veri depolama ortamının kök dizinine yerleştirildiğinden emin olun.
 - Veri depolama ortamını sisteminize DIVAR IP all-in-one sisteminize bağlayın.
Sistem, kurulum dosyası için veri depolama ortamını otomatik olarak tarar.
Tarama biraz zaman alabilir. Tamamlanmasını bekleyin.
 - Yükleme dosyası bulunduğunda, **Software Selection** sayfasında görüntülenir.
Yükleme işlemini başlatmak için yükleme dosyasını gösteren çubuğa tıklayın.
Not: Otomatik olarak algılanması için kurulum dosyasının şu yapıya sahip bir klasörde olması gerekir: `Drive root\BoschAppliance\` (örneğin, `F:\BoschAppliance\`).
Kurulum dosyası önceden tanımlanan klasör yapısıyla eşleşmeyen başka bir konumda bulunuyorsa, ilgili konuma gitmek için  düğmesine tıklayın. Daha sonra yükleme işlemini başlatmak için yükleme dosyasına tıklayın.
9. Yükleme işlemi başlamadan önce **End User License Agreement (EULA)** iletişim kutusu görüntülenir. Lisans koşullarını okuyun ve devam etmek için **Accept** ögesine tıklayın.
Yükleme işlemi başlar.
10. Yükleme işlemi tamamlandıktan sonra sistem yeniden başlatılır ve Windows oturum açma sayfasına yönlendirilirsiniz. Yönetici hesabıyla oturum açın.

11. Microsoft Edge tarayıcısı açılır ve **DIVAR IP - Sistem kurulum** sayfası görüntülenir. Sayfada cihaz tipi ve cihazın seri numarasının yanı sıra, üç çalışma modu ve her çalışma modu için kullanılabilir yazılım sürümleri görüntülenir. DIVAR IP all-in-one sisteminizi yapılandırmak için istediğiniz çalışma modunu ve istediğiniz yazılım sürümünü seçmeniz gerekir.

Not: İlgili çalışma modu için istenen yazılım sürümü yerel bir sürücüde değilse, aşağıdaki şekilde devam edin:

 - <https://downloadstore.boschsecurity.com/> adresine gidin.
 - **Software** sekmesinin altında, listeden **BVMS Appliances** 'ı seçin ve ardından **Select** seçeneğine tıklayın. Kullanılabilir tüm yazılım paketlerinin bir listesi görüntülenir.
 - Örneğin, **BVMS_[BVMS version]_SystemManager_package_[package version].zip** gibi istenen yazılım paketlerinin ZIP dosyalarını bulun ve USB bellek gibi bir depolama ortamına kaydedin.
 - Veri depolama ortamındaki ZIP dosyasını açın. Sıkıştırılmış dosyaların klasör yapısını değiştirmeyin.
 - Depolama ortamını DIVAR IP all-in-one sisteminize bağlayın.



Uyarı!

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

4.3.1

Çalışma modu olarak BVMS'in seçilmesi

DIVAR IP all-in-one sistemini tam bir video kaydı ve yönetim sistemi olarak çalıştırmak için:

1. Sayfada **DIVAR IP - Sistem kurulum** çalışma modunu **BVMS** olarak seçin ve kurmak istediğiniz BVMS sürümü seçin, ardından **Sonraki**'e tıklayın. Lisans BVMS sözleşmesi görüntülenir.
2. Lisans sözleşmesini okuyun ve kabul edin, ardından devam etmek için **Kur**'a tıklayın. Yüklemeye başlar ve yükleme iletişim kutusu ilerlemeyi gösterir. Yüklemeye başlarken sisteminizi kapatmayın ve veri depolama ortamını çıkartmayın.
3. Tüm yazılım paketleri başarıyla yüklendikten sonra sistem yeniden başlatılır. Yeniden başlattıktan sonra BVMS masaüstüne yönlendirilirsiniz.
4. BVMS masaüstünde, sisteminizi yapılandırmak için istediğiniz uygulamaya tıklayın.



Uyarı!

Daha ayrıntılı bilgi için ilgili web tabanlı DIVAR IP all-in-one eğitime ve BVMS belgelerine başvurun.

Eğitimi www.boschsecurity.com/x/en/support/training/ adresinde bulabilirsiniz

4.3.2

Çalışma modu olarak VRM'in seçilmesi

DIVAR IP all-in-one sistemini sadece video kayıt sistemi olarak çalıştırmak için:

1. **DIVAR IP - Sistem kurulum** sayfasından çalışma modunu **VRM** olarak seçin ve kurmak istediğiniz VRM sürümü seçin, ardından **Sonraki**'e tıklayın. Lisans VRM sözleşmesi görüntülenir.
2. Lisans sözleşmesini okuyun ve kabul edin, ardından devam etmek için **Kur**'a tıklayın. Yüklemeye başlar ve yükleme iletişim kutusu ilerlemeyi gösterir. Yüklemeye başlarken sisteminizi kapatmayın ve veri depolama ortamını çıkartmayın.
3. Tüm yazılım paketleri başarıyla yüklendikten sonra sistem yeniden başlatılır. Yeniden başlattıktan sonra, Windows oturum açma ekranına yönlendirilirsiniz.

**Uyarı!**

Daha fazla ayrıntı için VRM belgelerine bakın.

4.3.3**Çalışma modu olarak iSCSI Veri Depolama'nın seçilmesi**

DIVAR IP all-in-one sistemini iSCSI saklama genişletmesi olarak çalıştırmak için:

1. **DIVAR IP - Sistem kurulum** sayfasından **iSCSI veri depolama** çalışma modunu ve kurmak istediğiniz iSCSI veri depolama sürümünü seçin, ardından **Sonraki**'ye tıklayın. Yükleme iletişim kutusu görüntülenir.
2. Yükleme iletişim kutusunda, devam etmek için **Kur**'ye tıklayın. Yükleme işlemi başlar ve yükleme iletişim kutusu ilerlemeyi gösterir. Yükleme işlemi sırasında sistemi kapatmayın ve veri depolama aracını çıkartmayın.
3. Tüm yazılım paketleri başarıyla yüklendikten sonra sistem yeniden başlatılır. Yeniden başlattıktan sonra, Windows oturum açma ekranına yönlendirilirsiniz.
4. 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

DIVAR IP System Manager'ı en son sürüme yükselttiğinizden emin olun.

5.1 DIVAR IP System Manager'ı yükseltme

1. <https://downloadstore.boschsecurity.com/> adresine gidin.
2. **Software** sekmesinin altında, listeden **BVMS Appliances** 'ı seçin ve ardından **Select** seçeneğine tıklayın.
Kullanılabilir tüm yazılım paketlerinin bir listesi görüntülenir.
3. **SystemManager_[software version 2.0.0 or higher].zip** dosyasını bulun ve USB çubuğu gibi bir depolama ortamına kaydedin.
4. Veri depolama ortamındaki ZIP dosyasını açın.
5. Depolama ortamını DIVAR IP all-in-one cihazınıza bağlayın.
6. DIVAR IP System Manager uygulamasını başlatın:
 - Windows uygulamasında **BVRAdmin** yönetici hesabıyla oturum açtıysanız, Windows masaüstündeki DIVAR IP System Manager simgesine çift tıklayın.
DIVAR IP System Manager başlar.
 - Sisteminiz BVMS çalışma modunda çalışıyorsa, BVMS masaüstündeki DIVAR IP System Manager simgesine tıklayın ve BVRAdmin yönetici hesabında oturum açın.
DIVAR IP System Manager tam ekran iletişim kutusunda açılır (Alt+ F4 tuşlarına basarak iletişim kutusundan çıkabilirsiniz).
7. **Yazılım paketleri** sayfası görüntülenir. Yazılım paketi **DIVAR IP System Manager Commander**'ı seçin ve ardından, devam etmek için **Sonraki** seçeneğine tıklayın.
Kurulum iletişim kutusu görüntülenir.
8. Kurulum iletişim kutusunda, devam etmek için **Kur** seçeneğine tıklayın.
Kurulum başlar ve kullanıcı arayüzü güncellenir. Bu işlem birkaç dakika sürebilir. Sistemi kapatmayın ve bellek cihazını çıkarmayın.
Sayfanın üst kısmında görüntülenen uyarılara dikkat edin. Yeniden bağlantı başarısız olursa sayfayı yeniden yükleyin.
9. Kurulum başarıyla tamamlandıktan sonra, **Yazılım paketleri** sayfasında yazılım paketi **DIVAR IP System Manager Executor**'ı seçin ve ardından, devam etmek için **Sonraki** seçeneğine tıklayın.
Kurulum iletişim kutusu görüntülenir.
10. Kurulum iletişim kutusunda, devam etmek için **Kur** seçeneğine tıklayın.
Kurulum başlar.
Kurulum işlemi birkaç dakika sürebilir. Sistemi kapatmayın ve kurulum işlemi boyunca bellek cihazını çıkarmayın.
Sayfanın üst kısmında görüntülenen bildirimlere dikkat edin.

5.2 Yazılımın DIVAR IP System Manager kullanarak yükseltilmesi

DIVAR IP System Manager uygulaması ile sisteminizde yüklü olan yazılımı yükseltebilirsiniz. En güncel yazılımı ve mevcut yükseltme paketlerini Bosch Security and Safety Systems indirme mağazasında bulabilirsiniz:

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



Uyarı!

Kurulu yazılımı daha önceki bir sürüme düşürme desteklenmiyor.

Yüklenmiş olan yazılımı yükseltmek için:

1. <https://downloadstore.boschsecurity.com/> adresine gidin.
2. **Software** sekmesinin altında, listeden **BVMS Appliances** 'ı seçin ve ardından **Select** seçeneğine tıklayın.
Kullanılabilir tüm yazılım paketlerinin bir listesi görüntülenir.
3. Örneğin, **BVMS_[BVMS version]_SystemManager_package_[package version].zip** gibi istenen yazılım paketlerinin ZIP dosyalarını bulun ve USB bellek gibi bir depolama ortamına kaydedin.
4. Veri depolama ortamındaki ZIP dosyasını açın. Sıkıştırılmış dosyaların klasör yapısını değiştirmeyin.
5. DIVAR IP System Manager uygulamasını başlatın:
 - Windows uygulamasında **BVRAdmin** yönetici hesabıyla oturum açtıysanız, Windows masaüstündeki DIVAR IP System Manager simgesine çift tıklayın.
DIVAR IP System Manager başlar.
 - Sisteminiz BVMS çalışma modunda çalışıyorsa, BVMS masaüstündeki DIVAR IP System Manager simgesine tıklayın ve BVRAdmin yönetici hesabında oturum açın.
DIVAR IP System Manager tam ekran iletişim kutusunda açılır (Alt+ F4 tuşlarına basarak iletişim kutusundan çıkabilirsiniz).
6. **Yazılım paketleri** sayfası görüntülendiğinde, sayfanın üst kısmında cihaz türünü ve cihazın seri numarasını gösterecek şekilde görüntülenir.
 - **İsim** sütununda, zaten yüklü olan tüm DIVAR IP System Manager yazılım uygulamalarının yanı sıra, sistem tarafından algılanan DIVAR IP System Manager yazılım uygulamalarını (**Images** sürücüsünde veya depolama ortamında) görebilirsiniz.
 - **Kurulu versiyon** sütununda, o anda sisteminize yüklü olan yazılım uygulaması sürümünü görürsünüz.
 - **Durum** sütununda ilgili yazılım uygulamasının durumu görüntülenir:
 -  simgesi, **Images** sürücüsünde veya depolama ortamında sistem tarafından kurulu yazılım uygulamasının daha yeni bir sürümünün tespit edilemediğini belirtir.
Not: En güncel yazılım sürümünü kullanmak istediğinizden emin olmak için, <https://downloadstore.boschsecurity.com/> adresindeki yükleme mağazasından Bosch Security and Safety Systems için mevcut yazılım sürümlerini tekrar kontrol edin:
 -  simgesi, sistem tarafından **Images** sürücüsünde veya depolama ortamında kurulu yazılım uygulamasının daha yeni bir sürümünün tespit edilemediğini belirtir.
Simge, sistem henüz sisteminize kurulu olmayan bir yazılım uygulaması algıladığında da görüntülenir.
 - **Mevcut versiyon** sütununda kurulu yazılım uygulamalarının daha güncel sürümlerini görürsünüz. Bu sürümler, sistem tarafından **Images** sürücüsünde veya depolama ortamında algılanmıştır.
Sütun ayrıca, algılanan ve sisteminize henüz yüklenmemiş olan yazılım uygulamalarının kullanılabilir sürümlerini de görüntüler.
Not: Sadece kurulu yazılım uygulamalarının güncel sürümleri görüntülenir. Yazılım uygulamasını daha önceki bir sürüme düşürme desteklenmiyor.
7. Güncellemek veya yüklemek istediğiniz yazılım uygulamasını seçmek için, **İsim** sütununda ilgili seçeneğin düğmesine tıklayın.
8. **Mevcut versiyon** sütunundan, yazılım uygulamanızı yükseltmek istediğiniz veya yüklemek istediğiniz sürümü belirleyin ve ardından **Sonraki** öğesine tıklayın. Varsa, bir lisans anlaşması iletişim kutusu görüntülenir.

9. Lisans anlaşmasını okuyun ve kabul edin, ardından devam etmek için **Kur** öğesine tıklayın. Kurulum başlar ve kurulum iletişim kutusu, kurulumun ilerlemesini gösterir. Yükleme işlemi sırasında sistemi kapatmayın ve veri depolama ortamını çıkartmayın.
10. Tüm yazılım paketleri başarıyla yüklendikten sonra sayfanın üst kısmından **Kurulum başarıyla tamamlandı.** mesajını alırsınız.
11. Kurulum başarısız olursa **Kurulum başarısız oldu.** mesajı alırsınız ve  simgesi görüntülenir. Bu durumda, F5'e basarak **Yazılım paketleri** sayfasına geri dönün. İlgili yazılım paketlerini tekrar indirin ve tekrar deneyin. Sorun devam ederse, teknik destek servisiyle iletişim kurun.

6 Sisteme uzaktan bağlantı

DIVAR IP all-in-one sistemine uzaktan bağlanabilir ve internet üzerinden erişebilirsiniz. Uzaktan bağlanmak için, aşağıdakileri uygulamanız gerekir:

1. *Sistemi yetkisiz erişime karşı koruma, sayfa 16.*
2. *Port yönlendirmeyi ayarlama, sayfa 16.*
3. *Uygun bir istemci seçme, sayfa 16.*

DIVAR IP all-in-one cihazınıza Bosch Remote Portal aracılığıyla da bağlanabilir ve mevcut ve gelecekteki özelliklerden Remote Portal aracılığıyla yararlanabilirsiniz. Daha fazla bilgi için bkz. Remote Portal'a bağlanma.

6.1 Sistemi yetkisiz erişime karşı koruma

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

6.2 Port yönlendirmeyi ayarlama

Bir DIVAR IP all-in-one sistemine internet üzerinden NAT/PAT özellikli bir yönlendirici (Router) ile bağlanmak için DIVAR IP all-in-one sisteminde ve yönlendiricide port yönlendirmeyi yapılandırmanız gerekir.

Port yönlendirmeyi ayarlamak için:

- İnternet yönlendiricinizin port yönlendirme ayarlarında aşağıdaki port kurallarını girin:
 - BVMS Operator Client kullanarak SSH tüneli erişimi için port 5322.
Not: Bu bağlantı yalnızca BVMS çalışma modu için geçerlidir.
 - VRM'e Video Security Client veya Video Security App kullanarak HTTPS erişimi için port 443.
Not: Bu bağlantı yalnızca BVMS veya VRM çalışma modu için geçerlidir.
- Artık DIVAR IP all-in-one cihazınıza internet üzerinden erişilebilir.

6.3 Uygun bir istemci seçme

DIVAR IP all-in-one sistemi ile uzaktan bağlantı kurmak için iki seçenek bulunur:

- *BVMS Operator Client ile uzaktan bağlantı, sayfa 16*
- *Video Security Uygulaması ile uzaktan bağlantı, sayfa 17.*



Uyarı!

BVMS Operator Client veya Video Security App sürümlerinin uyumluluğu, BVMS veya VRM DIVAR IP yazılımlarının sürümleriyle belirlenir. Ayrıntılı bilgi için ilgili yazılım belgelerine ve eğitim gereçlerine göz atın.

6.3.1 BVMS Operator Client ile uzaktan bağlantı



Uyarı!

Bu bağlantı yalnızca BVMS çalışma modu için geçerlidir.

BVMS Operator Client ile uzaktan bağlantı kurmak için:

1. İstemci iş istasyonuna BVMS Operator Client yükleyin.
2. Yükleme işlemini başarıyla tamamlandıktan sonra masaüstü kısayolunu  kullanarak Operator Client'ı başlatın.

- Aşağıdakileri girin, ardından **Tamam**'a tıklayın.
Kullanıcı adı: admin (yapılandırıldıysa başka kullanıcı)
Şifre: Kullanıcı şifresi
Bağlantı: ssh://[DIVAR-IP_all-in-one_dış_IP_adresi]:5322

6.3.2 Video Security Uygulaması ile uzaktan bağlantı



Uyarı!

Bu bağlantı yalnızca BVMS veya VRM çalışma modu için geçerlidir.

Video Security App ile uzaktan bağlantı kurmak için:

- Apple App Store'da BoschVideo Security ifadesini arayın.
- Video Security uygulamasını iOS cihazınıza yükleyin.
- Video Security uygulamasını başlatın.
- Ekle**'yi seçin.
- Genel IP adresini veya dynDNS adını girin.
- Güvenli Bağlantı'nın (SSL) açık olduğundan emin olun.
- Ekle**'yi seçin.
- Aşağıdakileri girin:
Kullanıcı adı: admin (yapılandırıldıysa başka bir kullanıcı)
Şifre: Kullanıcı şifresi

6.4 Enterprise Management Server'a bağlanma

BVMS çalışma modunda birden fazla DIVAR IP all-in-one sisteminin merkezi yönetimi için ayrı bir sunucuya kurulu BVMS Enterprise Management Server uygulamasını kullanabilirsiniz. BVMS Enterprise System yapılandırması ve kullanımı hakkında BVMS belgelerine ve eğitim gereçlerine göz atın.

6.5 Remote Portal'a bağlanma

Ön koşullar

Remote Portal bağlantısı

DIVAR IP all-in-one cihazları Remote Portal'a bağlamak için aşağıdaki ön koşulların sağlandığından emin olun:

- Cihazda DIVAR IP System Manager 2.0 (veya üzeri) yüklü olmalıdır.
- Remote Portal hesabı oluşturulmalıdır.

Remote Portal iletişimi

Remote Portal iletişimi için bağlantı gereksinimleri.

Uyarı: Tüm bağlantılar çıkıştır.

HTTPS (Port 443)

- <https://api.remote.boschsecurity.com/rest/iot/devices>
- <https://sw-repo-remote.s3.eu-central-1.amazonaws.com>

MQTTS (Port 8883)

- [mqtt://mqtt.bosch-iot-hub.com:8883](https://mqtt.bosch-iot-hub.com:8883)

6.5.1 Remote Portal hesabı oluşturma

Remote Portal hesabı oluşturmak için:

- <https://remote.boschsecurity.com/login> adresine gidin.
- Devam etmek için **Sign up**.

3. Firma adınızı ve e-postanızı girin.
4. Firmanızın bölgesini seçin.
5. Hüküm ve koşulları ve veri koruma uyarısını okuyun ve ardından kabul etmek için onay kutularını seçin.
6. Devam etmek için Hesap oluşturmak için **Sign up** yapın.

6.5.2

DIVAR IP all-in-one cihazlarını Remote Portal'a kaydetme

DIVAR IP all-in-one cihazını Remote Portal'a kaydetmek için:

1. DIVAR IP System Manager uygulamasını başlatın.
2. **Remote Portal connection** sekmesine tıklayın.
3. Zaten bir Remote Portal hesabınız varsa e-postanızı ve şifrenizi girin ve ardından DIVAR IP all-in-one cihazınızı Remote Portal'a kaydetmek için seçeneğine tıklayın.

Uyarı!



SingleKey ID

Bosch, tüm Bosch uygulamaları, hizmetleri ve platformlarında merkezi olarak oturum açılması için SingleKey ID'yi kimlik sağlayıcı (IdP) olarak kullanıma sundu.

Cihazı SingleKey ID kullanarak Remote Portal'a bağlamak için ekranda gösterilen talimatları uygulayın.

Uyarı!

Default commissioning company uyarı

E-postanız birden çok şirket hesabına atanmışsa, DIVAR IP all-in-one cihazınızı doğru şirket hesabına kaydettiğinizden emin olun.

- Remote Portal hesabınızda oturum açın.

- **User settings > My companies** seçeneğine gidin, istenen hesabı seçin ve ardından seçeneği belirleyin **Default commissioning company**.

Not: Default commissioning company ayarının süresi 12 saat sonra otomatik olarak sona erer.



4. Henüz bir Remote Portal hesabınız yoksa Remote Portal hesabı oluşturmak için önce seçeneğine tıklayın. Bkz. .

6.5.3

DIVAR IP all-in-one cihazlarının kaydını Remote Portal'dan silme

Bir DIVAR IP all-in-one cihazının kaydını Remote Portal'dan silmek için:

1. DIVAR IP System Manager'ı başlatın.
2. **Remote Portal connection** sekmesine tıklayın.
3. DIVAR IP all-in-one cihazınızın kaydını Remote Portal'dan silmek için **Kaydı Sil** seçeneğine tıklayın.

Not: Cihazın kaydının Remote Portal'dan silinmesi Remote Portal'daki cihaz yapılandırmasını silmez. Cihaz yapılandırmasını silmek için ilgili Remote Portal şirket hesabıyla oturum açın.

7

Bakım

7.1

Yönetici hesabında oturum açma

BVMS çalışma modunda yönetici hesabında oturum açma

BVMS çalışma modunda yönetici hesabında oturum açmak için:

1. BVMS masaüstünde Ctrl+Alt+Del'e basın.
2. **Kullanıcı Değiştir** düğmesine tıkladıktan hemen sonra sol Shift tuşunu basılı tutun.
3. Tekrar Ctrl+Alt+Del'e basın.
4. Sistem kurulumu sırasında ayarlanmış şifreyi kullanarak **BVRAdmin** kullanıcılarını seçin ve giriş yapın. Ardından, Enter tuşu düğmesine basın.

Not: BVMS masaüstüne geri dönmek için Ctrl+Alt+Del'e basın ve **Kullanıcı değiştir** veya **Oturumu kapat** düğmesine tıklayın. Sistem yeniden başlatılmadan otomatik olarak BVMS masaüstüne geri döner.

VRM veya iSCSI çalışma modunda yönetici hesabında oturum açma

VRM veya iSCSI çalışma modunda yönetici hesabında oturum açmak için:

- Windows oturum açma ekranında Ctrl+Alt+Del'e basın ve **BVRAdmin** parolasını girin.

7.2

Sistemin izlenmesi

DIVAR IP all-in-one sistemleri, sisteminizi izlemek için önceden kurulu **SuperDoctor** uygulamasıyla birlikte gelir.

İzleme işlevselliğini etkinleştirme

İzleme işlevselliğini etkinleştirmek için:

1. Yönetici hesabında oturum açın (bkz. *Yönetici hesabında oturum açma, sayfa 19*).
2. Masaüstündeki **Tools** klasöründe **startSD5Service** komut dosyasına sağ tıklayın ve ardından **Run with PowerShell** öğesine tıklayın.
3. Masaüstündeki **SuperDoctor 5 Web** simgesine çift tıklayın.
4. Aşağıdaki varsayılan kimlik bilgilerini kullanarak web arayüzünde oturum açma:
 - Kullanıcı adı: **admin**
 - Parola: **DivaripSD5**
5. **Configuration** sekmesine tıklayın ve ardından **Account Setting** öğesine tıklayarak varsayılan şifreyi değiştirin.

Not: Bosch, **SuperDoctor** uygulamasında ilk oturum açmadan hemen sonra varsayılan şifreyi değiştirmenizi önerir.

6. **Configuration** sekmesinin altından **Alert Configuration** öğesine tıklayın.
7. **SNMP Trap** özelliğini etkinleştirin ve SNMP trap alıcısının IP adresini belirtin.

İzleme işlevselliğini devre dışı bırakma

İzleme işlevselliğini devre dışı bırakmak için:

1. Yönetici hesabında oturum açın (bkz. *Yönetici hesabında oturum açma, sayfa 19*).
2. Masaüstündeki **Tools** klasöründe **stopSD5Service** komut dosyasına sağ tıklayın ve ardından **Run with PowerShell** öğesine tıklayın.

7.3

Arızalı sabit disk sürücüyü değiştirme ve yeni bir sabit disk sürücüyü yapılandırma

DIVAR IP all-in-one sisteminizde kurulu bir sabit disk sürücü arızalı ve artık kullanılamaz durumdaysa aşağıdaki adımları uygulamanız gerekir:

1. *Arızalı sabit disk sürücüyü değiştirme, sayfa 20.*
2. *Yeni bir sabit disk sürücüyü yapılandırma, sayfa 20.*



Uyarı!

Bosch, kendi sağlamadığı sabit sürücülerle donatılmış birimlerdeki herhangi bir veri kaybı veya hasarından ya da sistem arızalarından sorumlu değildir. Sorunun nedeninin Bosch tarafından sağlanmayan sabit sürücüler olduğu değerlendirilirse Bosch destek veremez. Bosch, olası donanım sorunlarını gidermek için kendi sağladığı sabit sürücülerin takılmasını zorunlu tutar.

7.3.1

Arızalı sabit disk sürücüyü değiştirme

Arızalı sabit disk sürücüyü değiştirmek için:

1. DIVAR IP all-in-one cihazını kapatın.
2. Arızalı sabit disk sürücüyü cihazdan çıkarın ve yeni sabit disk sürücüyü takın.
Kurulum kılavuzundaki *SATA sabit disk sürücüsü kurulumu* bölümüne bakın.

7.3.2

Yeni bir sabit disk sürücü yapılandırma

Yeni bir sabit disk sürücü yapılandırmak için aşağıdakileri uygulamanız gerekir:

1. *Yeni disk bölümü ve birimi oluşturma, sayfa 20*
2. *Sunucu hizmetini etkinleştirme, sayfa 21.*
3. *LUN'ların oluşturulması (iSCSI sanal diskler), sayfa 21.*
4. *Sunucu hizmetini devre dışı bırakma, sayfa 22.*
5. *LUN'leri biçimlendirme, sayfa 22.*

Yeni disk bölümü ve birimi oluşturma

Yeni disk bölümü ve birimi oluşturmak için:

1. Windows **Başlat** menüsünden **Server Manager** seçeneğini seçin ve ardından **File and Storage Services > Volumes > Disks** yoluna gidin.
Sisteminize kurulu tüm disk sürücülerini görüntülenir.
2. Yüklediğiniz yeni disk sürücüyü sağ tıklayın ve ardından **New Volume...** ögesine tıklayın
New Volume Wizard iletişim kutusu görüntülenir.
3. Devam etmek için **Next** 'ye tıklayın.
Server and Disk iletişim kutusu görüntülenir.
4. İlgili sunucu ve diski seçin ve devam etmek için **Next** seçeneğine tıklayın.
Size iletişim kutusu görüntülenir.
5. **Volume size:** alanına, kullanmak istediğiniz birim boyutunu girin. Maksimum birim boyutunu kullanmak için seçili olan değeri değiştirmeden bırakın. Ardından, devam etmek için **Next** seçeneğine tıklayın.
Drive Letter or Folder iletişim kutusu görüntülenir.
6. **Drive letter:** listesinden sürücüyü atanacak sürücü harfini seçin ve devam etmek için **Next** seçeneğine tıklayın.
File System Settings iletişim kutusu görüntülenir.
7. Şu adımları uygulayın:
 - **File system:** NTFS
 - **Allocation unit size:** Default
 - **Volume label:** Değiştirilmiş arızalı disklerden biriyle (**Data** veya **Data2**) aynı birim etiketini girin.
8. Devam etmek için **Next**'ye tıklayın.
Confirmation iletişim kutusu görüntülenir.
9. Tüm ayarların doğru olduğundan emin olun ve ardından **Create** seçeneğine tıklayın.
Sistem, yeni disk bölümü ve birim oluşturma işlemini başlatır.
Oluşturma işlemi tamamlandıktan sonra **Results** iletişim kutusu görüntülenir.
10. Devam etmek için **Next** seçeneğine tıklayın.
Yeni disk bölümü ve birimi başarıyla oluşturulur ve tüm depolama alanı tahsis edilir.

Sunucu hizmetini etkinleştirme

1. Windows **Başlat** menüsünden **Services** seçeneğini belirleyin.
Services iletişim kutusu görüntülenir.
2. **Server** listesinden hizmeti bulun ve çift tıklayın.
Server Properties iletişim kutusu görüntülenir.
3. **General** sekmesinin altındaki **Startup type:** listesinden **Manual** seçeneğini belirleyip **Apply** ögesine tıklayın.
4. Hizmeti başlatmak için **Service status:** ögesinin altından **Start** ögesine ve ardından değişiklikleri uygulamak için **OK** ögesine tıklayın. Ardından **Services** iletişim kutusunu kapatın.

LUN'ların oluşturulması (iSCSI sanal diskler)

1. Windows **Başlat** menüsünden **Server Manager** seçeneğini tercih edip ardından **File and Storage Services > iSCSI** ögesini seçin.
Sisteminizdeki tüm iSCSI sanal diskler görüntülenir.
2. Değiştirilen sabit sürücünün **Error durumundaki LUN'ına (iSCSI sanal disk) sağ tıklayın**, ardından **Remove iSCSI Virtual Disk** seçeneğine tıklayın.
Remove iSCSI Virtual Disk iletişim kutusu görüntülenir.
3. LUN'un kaldırılmasını onaylamak için **OK** seçeneğine tıklayın.
4. **Error** durumundaki tüm LUN'lar için bu adımları tekrarlayın.
5. **iSCSI VIRTUAL DISKS** iletişim kutusunda boş bir alana sağ tıklayın ve ardından **New iSCSI Virtual Disk...** seçeneğine tıklayın.
iSCSI Virtual Disk Location iletişim kutusu görüntülenir.
6. **Server** ögesinin altındaki **Storage location:** seçeneğinden ilgili sunucuyu seçin ve ardından **Type a custom path** ögesini seçerek yeni sabit sürücüye atadığınız harfi yazın (bkz. *Yeni disk bölümü ve birimi oluşturma, sayfa 20*). Ardından, devam etmek için **Next** seçeneğine tıklayın.
iSCSI Virtual Disk Name iletişim kutusu görüntülenir.
7. **Name:** alanına LUN adını girin. Ardından, devam etmek için **Next** seçeneğine tıklayın.
iSCSI Virtual Disk Size iletişim kutusu görüntülenir.
8. **Size** alanına 2000 yazın ve boyut birimini **GB** olarak değiştirin.
2000 GB'den az alan varsa LUN boyutunu mevcut GB alandan 50 MB eksik olacak şekilde ayarlayın.
9. **Fixed size:** ögesinin altındaki **Clear the virtual disk on allocation** onay kutusu işaretini kaldırın. Ardından, devam etmek için **Next** seçeneğine tıklayın.
iSCSI Target iletişim kutusu görüntülenir.
10. **Existing iSCSI target:** ögesinin altından **TG0** seçeneğini belirleyin. Ardından, devam etmek için **Next** seçeneğine tıklayın.
Confirmation iletişim kutusu görüntülenir.
11. Tüm ayarların doğru olup olmadığını kontrol edin ve ardından **Create** seçeneğine tıklayın.
Sistem, yeni iSCSI sanal disk oluşturma işlemi başlatır.
Oluşturma işlemi tamamlandıktan sonra **Results** iletişim kutusu görüntülenir.
12. İletişim kutusunu kapatmak için **Close** seçeneğine tıklayın.
13. Mevcut tüm alanı kullanarak daha fazla LUN oluşturmak için bu adımları tekrarlayın.
14. Tüm LUN'lar oluşturulduktan sonra **iSCSI VIRTUAL DISKS** listesinde görünür.

Sunucu hizmetini devre dışı bırakma

1. Windows **Başlat** menüsünden **Services seçeneğini belirleyin.**
Services iletişim kutusu görüntülenir.
2. **Server** listesinden hizmeti bulun ve çift tıklayın.
Server Properties iletişim kutusu görüntülenir.
3. Hizmeti durdurmak için **General** sekmesinin altındaki **Service status:** ögesinin altından **Stop** seçeneğine tıklayın.
4. **Startup type:** listesinden **Disabled** seçeneğini tercih edin ve ardından **Apply** seçeneğine tıklayın.
5. Değişiklikleri uygulamak için **OK** seçeneğine tıklayın ve ardından **Services** iletişim kutusunu kapatın.

LUN'leri biçimlendirme

1. Configuration Client'ı başlatmak için BVMS ögesine tıklayın.
2. **Cihaz Ağacı** ögesinde, hatalı sabit sürücüyü içeren havuza gidin, **TGO** iSCSI hedefine sağ tıklayın ve ardından bu iSCSI hedefindeki kullanılabilir LUN'ların listesini güncelleştirmek için **Hedef Tara** seçeneğine tıklayın.
Bu seçim, arızalı sabit sürücüyle ilişkili LUN'ları kaldırır ve oluşturulan LUN'ları yeni sabit sürücüye ekler.
3. **LUN'lar** iletişim kutusu, kullanılabilir tüm LUN'ları listeler ve durumlarını gösterir (biçimlendirilmiş veya biçimlendirilmemiş).
4. Biçimlendirilmemiş LUN'ları seçin ve **LUN'u Formatla seçeneğine tıklayın.** Ardından, devam etmek için **Tamam** seçeneğine tıklayın.
5. Biçimlendirme sona erdikten sonra bir onay iletişim kutusu görüntülenir. İşlemi sona erdirmek için **Tamam** seçeneğine tıklayın.

7.4

DIVAR IP System Manager günlük dosyalarının alınması

DIVAR IP System Manager uygulaması, günlük dosyası almayı kolaylaştıran özel bir komut içerir.

DIVAR IP System Manager günlük dosyalarını almak için:

1. Yönetici hesabında oturum açın (bkz. *Yönetici hesabında oturum açma, sayfa 19*).
2. Windows **Başlat** menüsünden **Export System Manager Logs** ögesine tıklayın.
Komut dosyası, günlük dosyalarını Documents\Bosch klasörüne aktarır ve şu ad yapısına sahip bir ZIP dosyası oluşturur: SysMgrLogs-[date]_[time].
Ayrıntılı hata açıklamasına eklemek için bu ZIP dosyasını kullanabilirsiniz.

7.5

Birimi eski haline getirme

Birimi eski haline getirmek için:

1. Birimi açın ve Windows PE'ye girmek için BIOS açma otomatik testi sırasında F7'ye basın.
System Management Utility iletişim kutusu görüntülenir.
2. Aşağıdaki seçeneklerden birini seçin:
 - **System factory default:** Bu seçenek, video veri bölümlerini biçimlendirir ve işletim sistemi bölümünü fabrika varsayılan görüntüsüyle geri yükler.
Bu işlem 5 dakika sürebilir.
 - **Full data overwrite and system factory default:** Bu seçenek, mevcut verilerin tamamen üzerine yazarak video veri bölümlerini biçimlendirir ve işletim sistemi bölümünü fabrika varsayılan görüntüsüyle geri yükler.
Bu işlem 48 saat sürebilir.

- **OS system recovery only:** Bu seçenek, işletim sistemi bölümünü fabrika varsayılan görüntüsüyle geri yükler ve mevcut video verisi bölümlerindeki sanal sabit sürücülerini içe aktarır.
Bu işlem 5 dakika sürebilir.

Not:

OS system recovery only, veri sabit disk sürücülerinde saklanan video görüntülerini silmez. Ancak, tüm işletim sistemi bölümünü (video yönetim sistemi ayarları dahil) varsayılan yapılandırma ile değiştirir. Kurtarmanın ardından mevcut video görüntülerine erişmek için video yönetim sistemi yapılandırmasının sistem kurtarma işleminden önce dışa aktarılması ve daha sonra yeniden içe aktarılması gerekir.



Uyarı!

İşlem sırasında cihazı kapatmayın. Bu, kurtarma veri ortamına zarar verir.

3. Belirlenen seçeneği onaylayın.
Sistem, biçimlendirme ve görüntü kurtarma işlemini başlatır.
4. Kurtarma işlemi tamamlandıktan sonra, sistemi yeniden başlatmayı onaylayın.
Sistem yeniden başlatılır ve rutin kurulum işlemleri gerçekleştirilir.
5. İşlem tamamlandıktan sonra Windows dil seçim ekranı görüntülenir.
6. İlk sistem kurulumuna devam edin.

Bkz.

- *İlk oturum açma ve ilk sistem kurulumu, sayfa 9*

8 Ek bilgiler

8.1 Ek belgeler ve istemci yazılımı

Daha fazla bilgi, yazılım indirmeleri ve belge için ürün kataloğundaki ilgili ürün sayfasına gidin: <http://www.boschsecurity.com>

En güncel yazılımı ve mevcut yükseltme paketlerini Bosch Security and Safety Systems indirme mağazasında bulabilirsiniz:

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

8.2 Destek hizmetleri ve Bosch Akademisi



Destek

Destek hizmetlerimize www.boschsecurity.com/xc/en/support/ adresinden erişebilirsiniz.



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/

Bosch Security Systems B.V.

Torenallee 49

5617 BA Eindhoven

Hollanda

www.tr.boschsecurity.com

© Bosch Security Systems B.V., 2023

Building solutions for a better life.

202309021035