Visitor Management V5.5

Dahil Mobile Access

tr Kullanıcı kılavuzu

İçindekiler

1 Güvenlik

En güncel yazılımı kullanın

Cihazı ilk kez çalıştırmadan önce, yazılımınızın en son geçerli 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 bağlantılardan daha fazla bilgiye erişebilirsiniz:

– Genel bilgiler: https://www.boschsecurity.com/xc/en/support/product-security/
– Belirlenen güvenlik açıkları ve önerilen çözümlerin listesi olan güvenlik duyuruları: https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html

Bosch, ürünlerinin güncel olmayan yazılım bileşenleri ile çalıştırılmasından kaynaklanan herhangi bir hasar için hiçbir yükümlülük kabul etmez.

2 Giriş

2.1 Bosch Visitor Management Hakkında

Visitor Management, bundan sonra Bosch giriş kontrolü sistemleriyle birlikte çalışan tarayıcı tabanlı bir yazılım aracı olan VisMgmt olarak anılacaktır. Bu araç; ziyaretlerin planlaması, ziyaretçinin profesyonel verileri, ilişkili belgeler ve sözleşmeler, geçici kimlik bilgilerinin atanması dahil olmak üzere giriş kontrollü bir siteye yapılan ziyaretleri yönetir.
Kullanıcı arayüzü özelleştirilebilir ve herhangi bir kullanıcı oturumu kapatmadan kendi dilini anında değiştirebilir.
Birincil kullanıcılar ve bunların kullanım durumları şunlardır:

Kullanıcı türü	Kullanım örnekleri
Danışma görevlisi	Yeni ziyaretleri ve ziyaretçileri kaydetme Ziyaretleri onaylama ve reddetme Ziyaretçileri kara listeye alma Ziyaretçi kartlarını atama ve atamayı kaldırma İlişkili belgeleri yönetme Binadaki ziyaretçi sayısını izleme
Ziyaretçi	Kendi kendine kayıt ve ön kayıt Ziyaretçi profili oluşturma ve sürdürme Belgeleri imzalama
Ziyaret edilen kişi	Ziyaretlerin ve ziyaretçilerin programlarını ve listelerini yönetme Ziyaretlerin ön kaydını yapma
Yönetici	Genel ayarlar yapma Aracın davranışını ve kullanıcı arayüzünü özelleştirme Ayrıca: Tüm Resepsiyonist kullanım senaryoları

2.2 Mobil Erişim Hakkında

Mobile Access, kişinin akıllı telefonu gibi mobil bir cihazda depolanan sanal kimlik bilgilerini kullanan kişilerin giriş kontrolüdür. Sanal kimlik bilgileri, birincil erişim kontrol sisteminde veya ACS'de saklanır.

- ACS'nin operatörleri bu sanal bilgileri birlikte çalışan bir web uygulaması aracılığıyla oluşturur, atar ve kişilere gönderir.
- Mobil kimlik bilgilerinin sahipleri, mobil cihazlarındaki bir Mobile Access uygulamasından Bluetooth aracılığıyla giriş kontrol okuyucularını çalıştırır.
- Mobile Access sistemlerinin teknisyenleri, mobil cihazlarındaki özel bir kurulum uygulamasından Bluetooth aracılığıyla giriş kontrol okuyucularını yapılandırır.
- Sistem mobil cihazlarda kişisel veri depolamaz.

2.3 Hedef kitleler

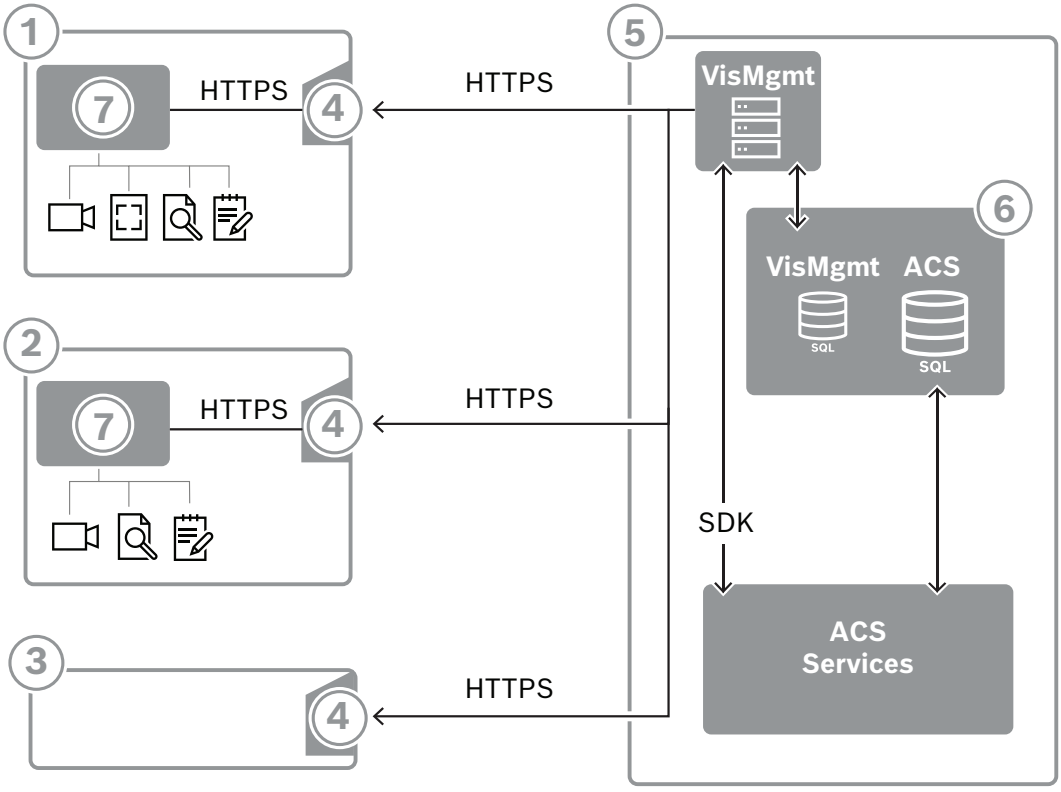
- Yükleyiciler ve yöneticiler Visitor Management
- Visitor Management'ın ana kullanıcı türleri

2.4 Bu belgeleri kullanma

- İlgili içeriği bulmak için yardım görüntüleyicinizdeki **Arama** işlevini kullanın.

- **Sisteme genel bakış, kurulum** ve **yapılandırma** bölümleri birincil olarak sistem yöneticilerini ilgilendirir
- **Çalışma** bölümleri öncelikle sistem kullanıcılarını ilgilendirir.

3 Sisteme genel bakış ve topoloji



Etiket	Açıklama
1	**Danışma görevlisi** iş istasyonu. Bu iş istasyonu; kayıt okuyucu, web kamerası ve imzalar ve belgeler için tarayıcılar gibi isteğe bağlı çevre donanımları içerebilir.
2	Hizmet bankosu modunda desteklenen tarayıcıyla birlikte **Ziyaretçi** hizmet bankosu iş istasyonu. Bu iş istasyonu, web kamerası ve imzalar ve belgeler için tarayıcılar gibi isteğe bağlı çevre donanımları içerebilir.
3	**Ziyaret edilen kişi** iş istasyonu, yani ziyaretçiyi alan çalışanın iş istasyonu.
4	VisMgmt web sitesiyle desteklenen tarayıcı
5	ACS sunucusu (BIS veya AMS)
6	ACS sunucusunun veritabanı örneği (Bu, ayrı bir bilgisayarda olabilir).
7	Tarayıcı ve çevre donanımı arasındaki iletişimi yöneten, isteğe bağlı **Bosch Çevresel Cihazlar eklentisi**.

Önerilen sistem topolojisi, ana giriş kontrolü sistemiyle aynı bilgisayarda VisMgmt sunucusuna ve aynı veritabanı örneğinde veritabanına sahiptir.
Bosch Çevresel Cihazlar eklentisi yalnızca çevresel cihazlara erişmesi gereken iş istasyonlarına kurulur.
Ziyaret edilen kişi iş istasyonu genellikle VisMgmt sunucusuna, yalnızca tarayıcı erişimi gerektirir.

4 Yükleme ve kaldırma

4.1 Yazılım ve donanım gereksinimleri

VisMgmt sunucusunu, ana giriş kontrol sistemiyle aynı bilgisayara yükleyin. Bu durumda, aynı yazılım ve donanım gereksinimleri geçerli olur.
Ana giriş kontrol sistemi henüz kurulu değilse Visitor Management'ı kurmadan önce onu kurduğunuzdan emin olun.
İlk kurulum veya güncellemeler için kurulum sırası aşağıdaki şekilde olmalıdır:

1. Ana giriş kontrolü sistemi - Access Management System
2. Credential Management ve/veya Visitor Management.
3. Mobile Access.

Sunucu gereksinimleri

İşletim sistemleri	– Windows 11 Professional ve Enterprise 23H2; – Windows Server 2019 (Version 1809) (64bit, Standard, Datacenter); – Windows Server 2022 (64 bit, Standart, Veri Merkezi)
Veritabanı yönetim sistemleri	– MS SQL Server 2019 and later Her zaman ACS (birincil giriş kontrol sistemi) ile aynı veritabanı örneğini kullanın
Minimum monitör çözünürlük	Tam HD 1920x1080
Desteklenen tarayıcılar	Google Chrome, Mozilla Firefox, Microsoft Edge (Chromium tabanlı) Windows işletim sisteminiz için tarayıcının en son sürümünü kullanın.

Bosch Çevresel Cihazlar eklentisi için gerekenler

Bosch Çevresel Cihazlar eklentisi, tarayıcı ile kayıt okuyucu, web kamerası, imza tarayıcısı ve belge tarayıcısı gibi çevresel cihazlar arasındaki elektronik iletişimi sağlayan programdır. İstemci bilgisayar, çevre donanımına fiziksel olarak bağlı olan bilgisayardır. Ayrıca VisMgmt sunucusuna bağlanan tarayıcıyı da çalıştırır.
Çevresel cihazlar kurulum için sıkı gereksinimlere sahip olmasa da ziyaretçi kaydı sürecinin verimliliğini önemli ölçüde artırdıkları için bunların da acilen temin edilmesi önerilir.

Gereksinim	Açıklama
Minimum monitör çözünürlüğü	Full HD 1920x1080
Desteklenen tarayıcılar	Google Chrome, Mozilla Firefox, Microsoft Edge (Chromium based) Windows işletim sisteminiz için tarayıcının en son sürümünü kullanın.

4.1.1 Ana giriş kontrolü sistemi

Mobil Erişim olmadan

Mobile Access gerekli değilse VisMgmt sürüm 5.5 aşağıdaki Bosch giriş kontrol sistemleriyle çalışır:

– Access Management System (AMS) 5.5 ve sonraki sürümleri

Mobil Erişim ile
Mobile Access ek lisans olarak seçilirse VisMgmt 5.5 sürümü, aşağıdaki Bosch giriş kontrol sistemleriyle çalışır:
– Access Management System (AMS) sürüm 5.5 (Mobile Access uzantısı içerir) ve sonrası

VisMgmt aracının kurulumuna geçmeden önce, kendi kurulum kılavuzuna göre, ana giriş kontrolü sisteminin yüklenmesini tamamlayın.

4.1.2 Ziyaretçi Yöneticisi veritabanını barındırmak için bir veritabanı örneği

Ana giriş kontrol sisteminin kurulumu, VisMgmt veritabanı `dbVisitorManagement`'ı barındırmak için kullanabileceğiniz bir veritabanı örneği oluşturur.
Bu örneğin varsayılan adı ACS'ye bağlı olarak değişir
– AMS için adı `ACE`'dir
– BIS ACE için adı `BIS_ACE`'dir

4.1.3 Yerel veritabanı erişimine ayrılmış bir kullanıcı

Kullanıcı `VMUser`, VisMgmt uygulaması adına Ziyaretçi Yöneticisi veritabanına erişir.
VisMgmt sunucusu kurulum programı, VisMgmt sunucusunda bir Windows kullanıcısı (`VMUser`) oluşturur.

4.1.4 Uzak veritabanı erişimine ayrılmış bir kullanıcı

VisMgmt, uzak bir veritabanı sunucusundaki bir veritabanını kullanacaksa aşağıda açıklandığı gibi, Windows ve SQL Server'da `VMUser` oluşturup yapılandırın.
ÖNEMLİ: Bu prosedürü tamamlamadan önce VisMgmt kurulumunu çalıştırmayın.

1. Uzak veritabanı sunucusunda aşağıdaki ayarlarla bir Windows kullanıcısını oluşturun:
– **Kullanıcı adı** (büyük küçük harf duyarlı): `VMUser`
– **Şifre**: Şifreyi tüm bilgisayarlarınız için geçerli olan güvenlik ilkelerine göre ayarlayın. VisMgmt kurulumu için gerekli olduğundan dikkatli şekilde not edin.
– **Grup üyesi**: `Administrators`
– **Kullanıcının bir sonraki oturum açışında şifresini değiştirmesi gerekir**: `NO`
– **Kullanıcı şifresini değiştiremez**: `YES`
– **Şifrenin süresi hiçbir zaman dolmaz**: `YES`
– **Hizmet olarak oturum aç**: `YES`
– **Hesap devre dışı bırakıldı**: `NO`

(`VMUser` kullanıcısını uzak SQL Server'a oturum açma sunucusu olarak ekleyin)
1. SQL Management Studio'yu açın
2. Uzak SQL örneğine bağlanın
3. **Güvenlik** > **Oturum Aç**'a gidin
4. `VMUser` kullanıcısını `sysadmin` sunucu rolüyle ekleyin

Daha sonra, VisMgmt sunucusunda VisMgmt kurulumunu yürüttüğünüzde, **uzak veritabanı sunucusu** seçeneğini belirleyerek yukarıda `VMUser` için belirlediğiniz şifreyi gireceksiniz.

4.1.5 Ana giriş kontrolü sisteminde ayrılmış bir kullanıcı

1. Ana giriş kontrolü sisteminde **sınırsız API kullanımı** özelliğine sahip bir kullanıcı oluşturun.
   Ayrıntılı talimatlar için ana giriş kontrolü sisteminin operatör kılavuzundaki **Kullanıcı (operatör) profilleri atama** başlıklı bölüme bakın.
2. BIS ACE kullanılıyorsa şifreyi ayarlamak için BIS Classic veya Smart Client'da bu kullanıcıyla bir kez oturum açın.
3. VisMgmt kurulum sihirbazları tarafından gerekli olacağı için kullanıcı adını ve şifreyi dikkatlice not alın.

4.2 Sunucu kurulumu

Tüm yazılım gereksinimlerini sağlayana kadar kurulum programını başlatmayın.
Kurumsal bir ağ ortamında AMS, Visitor Management, Credential Management, Mobile Access çalıştırılırken kurumsal CA (Sertifika Yetkilisi) tarafından verilen sertifikaların kullanılması önerilir. Sertifikaların düzenlenmesi, arka uç sistemlerden herhangi birinin kurulumundan önce yapılmalıdır. Lütfen AMS kurulum kılavuzundaki *Özel sertifikalar kullanma* bölümüne bakın.

4.2.1 Sunucu kurulum programını çalıştırma

1. İstenen VisMgmt sunucusunda Yönetici olarak `BoschVisitorManagementServer.exe` dosyasını çalıştırın.
2. Varsayılan kurulum paketini kabul etmek için **İleri**'ye tıklayın.
3. Son Kullanıcı Lisans Sözleşmesi'ni (EULA) kabul ediyorsanız bunu belirtin ve **İleri**'ye tıklayın.
4. Kurulum için hedef klasörü seçin. Varsayılan klasör önerilir.

– **SQL Server yapılandırması** ekranında

5. Veritabanını, VisMgmt sunucusundaki veritabanı örneği olan yerel SQL Server örneğinde mi yoksa uzak bir veritabanı sunucusu bilgisayarında mı oluşturmak istediğinizi seçin.
   – **Not:** Uzak veritabanı sunucusu seçerseniz kurulum programı `VMUser` kullanıcısının şifresini ister. Bu kullanıcı, uzak veritabanı sunucusunda (Yazılım gereksinimleri bölümüne bakın) kurduğunuz yönetici kullanıcısıdır.
6. Aşağıdakileri kontrol edin ve gerekirse aşağıdaki parametrelerin değerlerini değiştirin:

SQL sunucusu	Veritabanı sunucusu bilgisayarının adı
SQL örneği	Ana ACS veritabanı örneğinin adı. Burada, ziyaretçi veritabanı oluşturulur. AMS için adı `ACE`'dir BIS ACE için adı `BIS_ACE`'dir
SQL kullanıcı adı	Örneğin yönetici kullanıcısının adı, genellikle `sa` şeklindedir
SQL şifresi	Bu yönetici kullanıcının şifresi.

7. Girdiğiniz parametre değerlerini kullanarak veritabanı kopyasına ulaşılıp ulaşılmayacağını test etmek için **Test bağlantısı**'na tıklayın. Test başarısız olursa parametreleri yeniden kontrol edin.
8. Devam etmek için **İleri**'ye tıklayın

– **ACS giriş yapılandırması** ekranında (ACS; ana giriş kontrolü sistemi olan AMS veya ACE anlamına gelir)

9. Aşağıdaki parametrelerin değerlerini girin:

ACS ziyaret edilen kişi adı	ACS'nin çalıştığı bilgisayarın adı
ACS kullanıcı adı	Sınırsız API kullanımı olan ACS'nin ayrılmış kullanıcısının adı. Yazılım gereksinimleri bölümüne bakın.
ACS şifresi	Bu ayrılmış ACS kullanıcısının şifresidir.

10. Devam etmek için **İleri**'ye tıklayın
– **Kimlik sunucusu yapılandırma** ekranında
11. İlgili ACS kimlik sunucusunun URI'sini girin:
   – AMS: `HTTPS://<ACSsunucusununAdı>:44333`
   – BIS: `HTTPS://<ACSsunucusununAdı>/BisIdServer`
12. Kimlik sunucusunun ulaşılabilir olup olmadığını test etmek için **Bağlantıyı test et**'e tıklayın.
13. Özet ekranı için **İleri**'ye tıklayın ve ardından VisMgmt sunucusunun kurulumunu başlatmak için **Yükle**'ye tıklayın.
14. Yüklemeden sonra bilgisayarı yeniden başlatın.

4.2.2 Appsettings JSON dosyası

VisMgmt sunucusuna ilişkin bir dizi yapılandırma parametresi aşağıdaki `.JSON` dosyasında saklanır:

`<installation drive>:\Program Files (x86)\Bosch Sicherheitssysteme\Bosch Visitor Management\appsettings.json`

Genellikle varsayılan değerleri değiştirmenize gerek yoktur ancak dosyanın **Ayarlar** bölümündeki aşağıdaki parametreleri ayarlamanız yararlı olabilir. Parametreleri ayarlarsanız ilk önce dosyanın yedek kopyasını oluşturun. Değişikliklerinizi arızaya neden olursa yedek dosya, değişiklikleri hızlı bir şekilde geri döndürmenize yardımcı olur.

Değişikliklerinizi kaydedin ve değiştirilen parametreleri uygulamaya koymak için VisMgmt Windows hizmetini yeniden başlatın. Hizmetin adı, `Bosch Visitor Management` şeklindedir.

Parametre adı	Varsayılan değer	Açıklama
`PageSizeNumberOfVisit`	`20`	Ekranda bir defada görüntülenen maksimum ziyaret kaydı sayısı. Kullanıcı sayfayı kaydırdığında her yeni sayfa, veritabanından yüklenen bu sayıda kayıtla doldurulur.
`MaximumUploadFileSizeBytes`	`31457289`	Karşıya yüklenen bir dosyanın içerebileceği en fazla bayt sayısı.
`StartoverTimeoutAskSeconds`	`300`	Kullanıcı oturum açma bilgileri girişi sırasında durakladığında, uygulama bu kadar saniye bekler ve ardından giriş sorar.
`StartoverTimeoutResetSeconds`	`60`	Sorulduktan sonra, uygulama oturum ekranını sıfırlamadan önce bu kadar saniye bekler.

4.3 VisMgmt istemci bilgisayarını kurma

Bosch Çevresel Cihazlar eklentisi, sunucu bilgisayara yüklenebilir ancak genellikle aynı ağdaki bir istemci bilgisayara yüklenir. Bu durumda, ACS sunucusundan HTTPS sertifikasını kopyalayın ve istemci bilgisayara da yükleyin. Talimatlar için aşağıdaki *Güvenli iletişim için sertifikalar, sayfa 14* bölümüne bakın.
Bosch Çevresel Cihazlar eklentisi, kayıt okuyucular ve tarayıcılar gibi cihazlar için bağlantı yazılımıdır. Böyle bir cihaz gerekmiyorsa (örneğin, ziyaret edilen kişi kullanıcısı için) tarayıcı erişiminin oturum açması ve VisMgmt uygulamasını çalıştırması yeterlidir.

Aşağıdaki kayıt okuyucuları ve kart biçimleri desteklenir.

	MIFARE DESFire EV1 Bosch Kodu	MIFARE DESFire EV1 CSN	MIFARE Classic CSN	HID Prox 26 bit	iCLASS 26 bit	iCLASS 35 bit	iCLASS 37 bit	iCLASS 48 bit	EM 26 bit
LECTUS enroll ARD-EDMCV002-USB	X								
OMNIKEY 5427 CK		X	X	X	X	X	X	X	X

Bkz.
– *Güvenli iletişim için sertifikalar, sayfa 14*

4.3.1 Çevresel Cihazlar eklentisini kurma

Çevresel Cihazlar eklentisi yalnızca kayıt okuyucularına, tarayıcılara veya diğer çevre cihazlarına bağlanan istemci bilgisayarlarda gereklidir. Bu gereksinime sahip her istemci bilgisayarda aşağıdaki prosedürü tekrarlayın.

1. İstenen istemci bilgisayarında, kurulum ortamından `BoschPeripheralDeviceAddon.exe` dosyasını yönetici olarak çalıştırın.
   – Ana bileşenler, yani istemci yazılımı ve her zamanki çevresel cihazların yazılımı belirtilir. Şu anda donanıma sahip olmasanız bile listelenen tüm bileşenleri yüklemenizi öneririz.
2. Varsayılan kurulum paketlerini kabul etmek için **İleri**'ye tıklayın.
3. **İstemci yapılandırması** ekranında

– **Kurulum dizini:** Varsayılanı kabul edin (önerilir) veya gerektiği şekilde değiştirin.
– **COM portu:**
  – LECTUS kayıt okuyucusu kullanılıyorsa kayıt okuyucusunun bağlı olduğu COM portunun numarasını (örneğin `COM3`) girin. Bu değeri Windows cihaz yöneticisinde doğrulayın.
  – HID OMNIKEY okuyucusu kullanılıyorsa bu alanı boş bırakın.
  – Kamera, Signopad ve belge tarayıcısı "tak ve kullan" özelliğine sahiptir ve COM portu gerektirmez. Tarayıcı bağlanmak için izin istediğinde, **İzin Ver**'e tıklayın.
– **Sunucu adresi** ve **Port:**

- Tüm sunucu bilgisayarların adını, varsayılan olarak en azından birincil ACS sunucusu bilgisayarını ve çevre cihazlarını kontrol etmesi gereken arka uç hizmetlerinin port numaralarını girin.
  Her durumda **Test Bağlantısı**'na tıklayın ve onay bekleyin.
  Daha fazla sunucu eklemek için **Ekle**'ye tıklayın.
  Sunucuları kaldırmak için **Sil**'e tıklayın.
- Olağan arka uç hizmetleri için varsayılan bağlantı noktaları şunlardır: CredMgmt için
  5806 , VisMgmt için
  5706

4. Yüklenecek bileşenlerin özeti için **İleri**'ye tıklayın.
5. Yüklemeyi başlatmak için **Yükle**'ye tıklayın.
6. Kurulumu bitirmek için **Finish**'e (Bitir) tıklayın.
7. Yüklemeden sonra bilgisayarı yeniden başlatın.

4.3.2 Güvenli iletişim için sertifikalar

İstemci makinesindeki tarayıcı ve ACS sunucusu arasında güvenli bir iletişim için aşağıdaki sertifikayı ACS sunucusundan istemci bilgisayarlara kopyalayın. Yüklemek için Windows yönetici haklarına sahip bir hesap kullanın.
Sertifikanın her zamanki yolu:

- <kurulum sürücüsü>:
  `\Bosch Sicherheitssysteme\Access Management System\Certificates\Bosch Security System Internal CA - BISAMS.cer`

Not: Sertifikanın kullanıma sunulmasından sonra Mobile Access arka ucu veya Bosch Credential Management hizmetini ve Bosch Visitor Management hizmetini yeniden başlatın.

Sertifika aktarma işlemlerine genel bakış

Nereye? → Nereden? ↓	**ACS**	**MA** Mobile Access arka ucu	**DB** Veritabanı	**S** Kurulum uygulaması	**M** Kart sahibi giriş uygulaması	**R** Okuyucu
ACS	/	Kurulum sihirbazı ile aktarıldı (cert aracı aracılığıyla)	/	/	/	/
MA Mobile Access arka ucu	MA kurulum sihirbazı ile aktarıldı	/	/	QR kodu kaydı ile aktarıldı Anında ileti bildirimi aracılığıyla güncellendi	QR kodu kaydı ile aktarıldı Anında ileti bildirimi aracılığıyla güncellendi	/
DB Veritabanı	/	/	/	/	/	/

S Kurulum uygulaması	/	QR kodu kaydı ile aktarıldı	/	/	/	/
M Kart sahibi giriş uygulaması	/	QR kodu kaydı ile aktarıldı	/	/	/	/

4.3.2.1 Firefox tarayıcısı için sertifikalar

Firefox tarayıcısı kullanmıyorsanız bu bölümü yok sayabilirsiniz.

Firefox tarayıcısı kök sertifikalarını farklı şekilde işler: Firefox, güvenilen kök sertifikaları için Windows sertifika deposuna danışmaz. Bunun yerine, her tarayıcı profili kendi kök sertifika deposunu sağlar. Daha fazla ayrıntı için https://support.mozilla.org/en-US/kb/setting-certificate-authorities-firefox sayfasına başvurun
Bu web sayfası, Firefox'un tüm kullanıcıları Windows sertifika deposunu kullanmaya zorlamasına yönelik yönergeler de içerir.
Alternatif olarak, aşağıda açıklandığı gibi varsayılan sertifikaları içe aktarabilirsiniz. Not:
- Her kullanıcı ve Firefox profili için sertifikaları almanız gerekir.
- Aşağıda açıklanan sunucu sertifikası, kurulum işleminde oluşturulan varsayılan sertifikadır. Bir Sertifika Yetkilisinden kendi sertifikanızı satın aldıysanız bunun yerine kendi sertifikanızı kullanabilirsiniz.

Sertifikaları Firefox sertifika deposuna aktarma
İstemci bilgisayardaki Firefox'yan ACS sunucusuna erişmek için aşağıdaki varsayılan sertifikayı sunucudan aktarabilirsiniz:
- <kurulum sürücüsü>:
  `\Bosch Sicherheitssysteme\Access Management System\Certificates\Bosch Security System Internal CA - BISAMS.cer`

Alternatif olarak BIS ACE için sertifikayı web üzerinden de indirebilirsiniz:
- `HTTP://`<Ziyaret edilen kişi adı>`/`<Ziyaret edilen kişi adı>`.cer`

Çevresel cihazlar: Belge veya imza tarayıcısı gibi bir bağlı çevresel cihaza, istemci bilgisayardaki Firefox'tan erişmek için varsayılan sertifikayı kullanabilirsiniz. İstemci bilgisayarında aşağıdaki konumda bulabilirsiniz:
<kurulum sürücüsü>`:\Program Files (x86)\Bosch Sicherheitssysteme\Bosch Peripheral Device Addon\BoschAcePeripheralDeviceAddonHardware CA.cer`

Prosedür (her sertifika ve Firefox profili için tekrarlayın):
Gereken sertifikaları yüklemek için istemci bilgisayarda aşağıdaki prosedürü kullanın:
1. Yüklemek istediğiniz sertifikayı bulun.
2. Firefox tarayıcısını açın ve adres çubuğuna `about:preferences` yazın.
- Bir seçenekler sayfası açılır.
3. **Seçeneklerde Bul** alanına `certificate` yazın
- Sayfada **Sertifikaları Göster** düğmesi görünür.
4. **Sertifikaları Göster** düğmesine tıklayın.
- **Sertifika Yöneticisi** iletişim kutusu birkaç sekmeyle açılır
5. **Yetkililer** sekmesini seçin.

6. **İçe aktar...**'a tıklayın
– Bir sertifika seçici iletişim kutusu açılır.
7. 1. adımda bulduğunuz sertifikayı seçip **Aç**'a tıklayın.
– **Sertifika indiriliyor** iletişim kutusu açılır.
8. **Web sitelerini tanımlamak için bu CA'ya güven**'i seçin ve **Tamam**'a tıklayın.
– **Sertifika indiriliyor** iletişim kutusu kapanır
9. **Sertifika Yöneticisi** iletişim kutusunda **Tamam**'a tıklayın.
– Sertifika içe aktarma prosedürü tamamlanmıştır.

4.3.2.2 Chrome tarayıcı sertifikaları

Chrome tarayıcı kullanmıyorsanız bu bölümü yok sayabilirsiniz.
Chrome tarayıcıdaki sertifika işlemlerine ilişkin değişiklikler için lütfen ACS'nizin sürüm notlarına başvurun.
Microsoft Windows'daki Chrome tarayıcıda bir sertifika yüklemek için:

1. Sertifika dosyasını indirin.
2. Chrome ayarları sayfasına (`chrome://settings`) gidin ve **Gelişmiş**'e tıklayın.
3. **Gizlilik ve Güvenlik**'in altındaki **Sertifikaları Yönet**'e tıklayın
4. Sertifika yükleme işlemini başlatmak için **Sertifikalarınız** sekmesinde **İçe aktar**'a tıklayın:
– Bir sertifika içe aktarma sihirbazı görünür.
5. Sertifika dosyasını seçin ve sihirbazı tamamlayın.
6. Yüklenen sertifika **Güvenilir Kök Sertifika Yetkilileri** sekmesinde görüntülenir.

4.3.2.3 Mobil Erişim uygulamalarını yükleme

Giriş

Bosch, Mobile Access için aşağıdaki uygulamaları sağlar
– Bosch Mobile Access: Sanal bilgileri depolamak ve bunları Mobile Access için yapılandırılan okuyuculara Bluetooth aracılığıyla aktarmak için kullanılan bir kart sahibi uygulaması. Böyle bir okuyucu uygulamanın depolanmış kimlik bilgilerinden birinin geçerli olup olmadığına bağlı olarak giriş izni verir veya reddeder.
– Bosch Setup Access: Okuyucuları Bluetooth aracılığıyla taramak ve yapılandırmak için kullanılan bir teknisyen uygulaması.

Visitor Management ve Credential Management'ın yetkili operatörleri hem kart sahibi hem de teknisyen uygulamaları için sanal kimlik bilgileri gönderebilir.

Kart sahibi olan uygulama çalıştığı ve mobil cihazda etkin olduğu sürece, bu kartı fiziksel bir kartmış gibi kullanabilirsiniz. Uygulamadan komut vermeye veya ekranın kilidini açmaya gerek yoktur.

Uyarı!
ÖNEMLİ: Kart sahibi ve teknisyen uygulamalarını eş zamanlı olarak çalıştırmayın
Kart sahibi uygulaması kullanılırken teknisyen uygulamasını kimsenin kullanmadığından ve bunun tersinin geçerli olmadığından emin olun.

Prosedür

Bosch Mobile Access uygulamaları, Google ve Apple uygulama mağazalarından indirilebilir ve normal şekilde yüklenebilir. Uygulama mağazalarındaki adları şunlardır:

– Bosch Mobile Access
– Bosch Setup Access

4.3.3 Appsettings JSON dosyası

VisMgmt istemci bilgisayarına ilişkin bir dizi yapılandırma parametresi aşağıdaki `.JSON` dosyasında saklanır:

<kurulum sürücüsü>:`\Program Files (x86)\Bosch Sicherheitssysteme\Bosch Visitor Management\appsettings.json`

Genellikle varsayılan değerleri değiştirmenize gerek yoktur ancak dosyanın **AppSettings** bölümündeki aşağıdaki parametreleri ayarlamanız yararlı olabilir.

Değişikliklerinizi kaydedin ve değiştirilen parametreleri uygulamaya koymak için VisMgmt Windows hizmetini yeniden başlatın. Hizmetin adı, `Bosch Ace Visitor Management Client` şeklindedir

Parametre adı	Örnek	Açıklama
`CorseOrigins`	`"https://my-vm-server:5706"`	Ziyaretçi Yönetimi sunucusunun adresi ve bağlantı noktası numarası.
`CardReaderPort`	`"com3"`	Bir LECTUS kayıt okuyucunun bağlı olduğu COM port numarası. HID OMNIKEY okuyucular için bu parametre boş olabilir.

4.4 Sunucu yüklemesini doğrulama

Desteklenen tarayıcılardan birini kullanarak aynı ağ içindeki bir bilgisayardan aşağıdaki URL'yi açın:

`https://`<VisMgmt sunucu bilgisayarı>`:5706/main`

Sunucu çalışıyorsa uygulama oturum açma sayfası görüntülenir.

4.5 Mobil Erişimi Yükleme

Giriş

Mobile Access arka uç hizmeti hem Credential Management hem de Visitor Management için mobil erişim işlevi sağlar.

Ana Giriş Kontrolü Sistemi'nin en son sürümünü ve Mobile Access arka ucunun son sürümünü kullandığınızdan emin olun.

NOT: Hem CredMgmt hem de VisMgmt kullanıyorsanız Mobile Access'i yalnızca bir kez yüklemeniz gerekir.

– Bu eklentiyi ACS (aynı yerde kurulum) ile aynı sunucuya veya ayrı bir sunucuya (dağıtılmış kurulum) yükleyebilirsiniz.
– Yerel veya uzak bir veritabanı kullanmak için bu eklentiyi yükleyebilirsiniz.

Mobil Erişim arka uç hizmetinin erişilebilirliği

Mobile Access arka uç hizmeti, mobil cihazlar için sürekli olarak ulaşılabilir olmalıdır.

Güvenlik nedeniyle, mobil cihazların bir ACS sunucusuna ağ erişiminin olması olasılığı çok düşüktür. Bu nedenle dağıtılmış kurulum önerilir. Bu, Mobile Access arka uç hizmetini daha yaygın olarak kullanılabilen bir "bulut" sunucusunda çalıştırmanıza imkan tanır.

4.5.1 Kurulum, yapılandırma ve kullanıma genel bakış

Mobile Access için uyum halinde çalışacak birkaç bileşen gereklidir. Genel aşamaları burada listeliyoruz ve ilgili ön koşullar ile prosedürleri bu bölümün sonraki kısımlarında açıklıyoruz:

ACS sunucusunu ayarlama

1. Bir ACS kurulur, lisanslanır ve kalıcı bir kök sertifika ve uyumlu giriş okuyucuları ile çalışır. Operatörler, Mobile Access'i yönetmek için bunun içinde yetkilerle tanımlanmıştır.

Mobil Erişim'i ayarlama

1. Bir sistem yöneticisi, Mobile Access'i kullanan web uygulamalarından birini veya ikisini birden (Credential Management veya Visitor Management) ACS'ye kurar.
2. Sistem yöneticisi Mobile Access arka ucunu kurar.
3. Bir sistem yöneticisi, kurulu olan web uygulamalarında Mobile Access'i etkinleştirir.

Okuyucuları ayarlama

1. Bir sistem yöneticisi, CredMgmt uygulamasında bir teknisyen (Mobile Access okuyucularını yapılandırmak için yetki verilmiş bir kişi) oluşturur.
2. Teknisyen, teknisyen uygulamasını ("Kurulum Erişimi") cihazın olağan ortak uygulama mağazasından mobil cihazına indirir.
3. Bir sistem yöneticisi belirlenen teknisyene bir davetiye gönderir.
4. Teknisyen davetiyeyi teknisyen uygulamasında kabul eder. Bu davetiye, teknisyene giriş okuyucularını Mobile Access için yapılandırmak üzere yetki verir.
5. Teknisyen, teknisyen uygulamasını kullanarak okuyucuları yapılandırır.

Mobil Erişim'i kullanma

1. Mobile Access'i kullanabilecek kimlik bilgileri sahipleri, kimlik bilgileri uygulamasını ("Mobile Access"), cihazın normal ortak uygulama mağazasından mobil cihazlarına indirir.
2. CredMgmt ve/veya VisMgmt operatörleri uygun kimlik bilgisi sahiplerine QR kodu veya e-posta aracılığıyla mobil kimlik bilgileri gönderir.
3. Kimlik bilgisi sahipleri, kimlik bilgisi sahibi ("Mobile Access") uygulamalarında QR kodunu veya e-postayı okutur. Bu, uygulama çalışırken mobil cihazının fiziksel olarak bir kimlik bilgisi işlevi görmesini sağlar.

4.5.2 Mobil Erişim donanım ön koşulları

Mobile Access, BLE modülüne sahip giriş okuyucuları gerektirir. Aşağıdaki Bosch okuyucular uygundur:

ARD-SELECT -BOM, -WOM, -BOKM, -WOKM

- B ve W, rengi, siyah veya beyaz olarak işaret eder
- O, OSDP'yi işaret eder
- K, bir tuş takımı bulunduğunu belirtir
- M, Mobile Access için uygunluğu bildirir:

4.5.3 Mobil Erişim yapılandırma ön koşulları

Uzak veritabanı (uzak veritabanı kullanıyorsanız) için özel kullanıcı

Mobile Access uzak veritabanı sunucusundaki bir veritabanında kullanılacaksa bu uzak sunucuda `MAUser` adında bir yönetici kullanıcıyı hem Windows hem de SQL Server'da oluşturun ve yapılandırın. Aşağıda açıklanan ayar sırasında uzak veritabanı sunucusu seçeneğini seçin ve `MAUser` için tanımladığınız şifreyi girin.

ÖNEMLİ: Bu prosedürü tamamlamadan önce Mobile Access kurulumunu çalıştırmayın.

Prosedür

1. Uzak veritabanı sunucusunda, ACS ile aynı etki alanında yer alan bir etki alanı Windows kullanıcısı oluşturun. Aşağıdaki ayarları kullanın:

– **Kullanıcı adı** (kullanıcı adının kendisi büyük harf duyarlıdır): <ACS-Etki alanı>\`MAUser`
– **Şifre**: Şifreyi tüm bilgisayarlarınız için geçerli olan güvenlik ilkelerine göre ayarlayın. Mobile Access kurulumu için gerekli olduğundan dikkatli şekilde not edin.
– **Kullanıcının bir sonraki oturum açışında şifresini değiştirmesi gerekir**: `NO`
– **Kullanıcı şifresini değiştiremez**: `YES`
– **Şifrenin süresi hiçbir zaman dolmaz**: `YES`
– **Hizmet olarak oturum aç**: `YES`
– **Hesap devre dışı bırakıldı**: `NO`

Ardından uzak SQL Server'da oturum açmak için `MAUser`'ı aşağıdaki gibi ekleyin:

1. SQL Management Studio'yu açın
2. Uzak SQL örneğine bağlanın
3. **Güvenlik** > **Oturum Aç**'a gidin
4. **Sayfa seç** bölmesinde, **Genel**'i seçin.
5. `MAUser` kullanıcısını seçin
6. **Sayfa seç** bölmesinde **Sunucu rolleri**'ni seçin
7. `public` ve `dbcreator` onay kutularını seçin

Yerel veritabanı (yerel bir veritabanı kullanıyorsanız) için özel bir kullanıcı

`MAUser` kullanıcısı, Mobile Access uygulaması adına ACS veritabanına erişir.

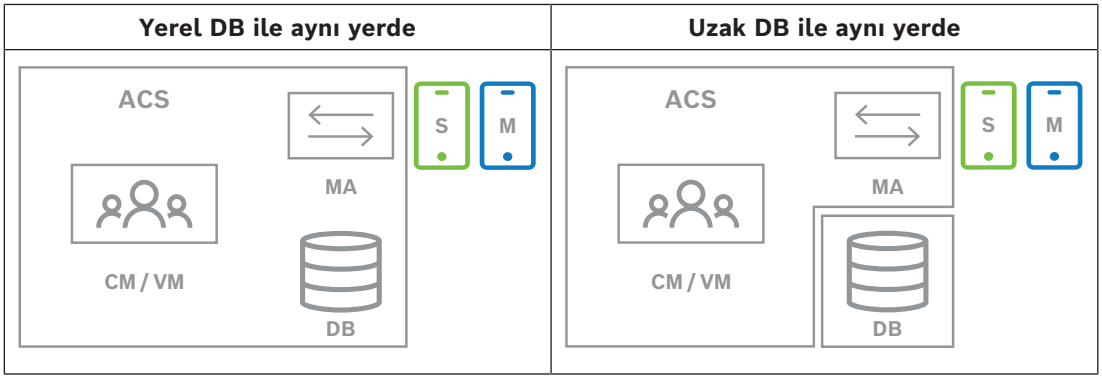
Yerel veritabanı kullanıyorsanız bu kullanıcıyı oluşturmanız gerekmez. Mobile Access kurulum programı ACS sunucusunda otomatik olarak bir `MAUser` Windows kullanıcısı oluşturur.

4.5.4 Aynı yerde kurulum prosedürü

Aynı yerde kurulum, Mobile Access Arka Uç hizmetinin ACS ile aynı sunucuda çalıştığı anlamına gelir.

Dağıtılmış kurulum, Mobile Access Arka Uç hizmetinin farklı bir sunucuda (örneğin, "bulut sunucusu") çalıştığı anlamına gelir.

Dağıtılmış seçeneği için sonraki bölüm olan **Dağıtılmış kurulum prosedürü**'ne bakın.



Tuş	Anlamı
ACS	Birincil giriş kontrol sistemi, AMS veya BIS-ACE
CM/VM	Web uygulaması için arka uç: Credential Management veya Visitor Management
DB	Ana ACS veritabanı
MA	Mobile Access arka ucu
S	Sistem teknisyenlerinin ve yapılandırıcılarının mobil cihazları için "Kurulum Erişimi" teknisyen uygulaması
M	Normal kimlik bilgisi sahiplerinin mobil cihazları için "Mobil Erişim" giriş uygulaması.

Prosedür

1. Aynı zamanda Mobile Access sunucusu olan ve aynı yerde kurulumlar için kullanılan ACS sunucusunda, `BoschMobileAccessBackend.exe`'yi yönetici olarak çalıştırın
– Kurulum programı açılır
2. **Konum** ekranında kurulum türünü seçin: **Aynı yerde**
3. **Bileşenler** ekranında, `Bosch Mobile Access`'in seçili olduğundan emin olun ve **İleri**'ye tıklayın
4. **EULA** ekranında bilgileri dikkatlice okuyun ve Son Kullanıcı Lisans Sözleşmesi'ni (EULA) kabul etmek istiyorsanız **Kabul et**'e tıklayın. Kurulum yalnızca bunu yaptığınızda devam edebilir.
5. **Kurulum dizini** ekranında:
– Kurulum için bir hedef klasöre gidip klasörü seçin veya varsayılanı kabul edin (önerilen)
– Mobil uygulamada ve HTML e-posta şablonlarında görüntülenecek olan şirketinizin adını girin
– **Next**'e (İleri) tıklayın
6. **Sertifika** ekranında
– Mobile Access Arka Ucunun çalıştırılacağı ana bilgisayar adını girin
– İsterseniz veya ağ, ana bilgisayar adı çözümlemesi sağlıyorsa bu ana makinenin IP adresini girin
– **Next**'e (İleri) tıklayın
7. **SQL Server** ekranında veritabanının konumu için iki alternatiften birini seçin. Yapılandırmalar biraz farklıdır. Sonraki adım için bir alternatif seçin:
– 1. ALTERNATİF **Yerel veritabanı** seçeneği:
  – Kurulum programı yerel veritabanını bulur ve önceden seçer.
  – Yönetici kullanıcı için SQL parolası girin (varsayılan `sa`'dır)
  – **Test Bağlantısı**'na tıklayın
  – **Next**'e (İleri) tıklayın

- 2. ALTERNATİF **Uzak veritabanı** seçeneği
  - Ağda bulunan SQL Server'ın adını girin
  - SQL örneğinin adını girin
  - Yönetici kullanıcı için SQL parolası girin (varsayılan `sa`'dır)
  - **Test Bağlantısı**'na tıklayın
  - Kullanıcı adını kontrol edin ve uzak veritabanı kullanımı için oluşturduğunuz Windows ve SQL Administrator kullanıcısının parolasını girin (yukarıdaki ön koşullara bakın)
  - **Next**'e (İleri) tıklayın

8. **Kimlik sunucusu yapılandırma** ekranında
- Varsayılan kimlik sunucusu (önceden seçilen) `44333https://` <NameOfACSserver>`:44333` portuna sahip birincil ACS sunucusudur.
- **Test Bağlantısı**'na tıklayın
- Test başarısız olursa kimlik sunucusunun kullanılabilirliğini yeniden kontrol edin.
- **Next**'e (İleri) tıklayın

9. **Core Components** (Temel Bileşenler) ekranında, **Bosch Mobile Access**'in seçildiğini onaylayın ve **Install** (Yükle) öğesine tıklayın
- Kurulum sihirbazı tamamlanır.

10. **Next**'e (İleri) tıklayın
11. **Temel Bileşenler** ekranında, yüklemenin başarıyla tamamlandığından emin olun ve **Bitir**'e tıklayın.
12. Windows `Services` uygulamasında, `Bosch Mobile Access` hizmetinin çalıştığından emin olun.

4.5.5 Dağıtılmış kurulum prosedürü

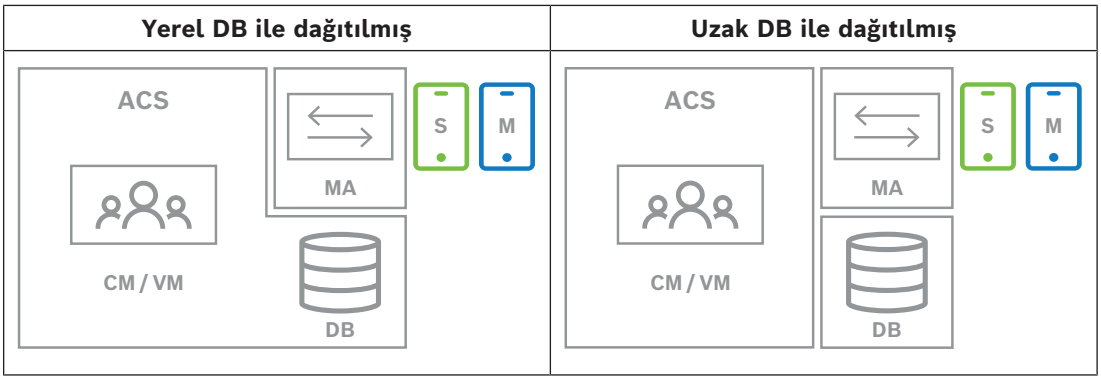
Aynı yerde kurulum, Mobile Access Arka Uç hizmetinin ACS ile aynı sunucuda çalıştığı anlamına gelir.

Dağıtılmış kurulum, Mobile Access Arka Uç hizmetinin farklı bir sunucuda (örneğin, "bulut sunucusu") çalıştığı anlamına gelir.

Aynı yerde seçeneği için, önceki bölüm olan **Aynı yerde kurulum prosedürü**'ne başvurun.

Dağıtılmış bir Mobile Access arka uç sunucusunda, Mobile Access kurulumuna başlamadan önce veya sistemi güncelleme sırasında aşağıdaki ön koşul gereklidir. Bu, ortak konumdaki ortamda gerekli değildir:

- Mobile Access yükleyicisini çalıştırmadan önce dağıtılmış Mobile Access arka uç sunucusunda **ASP.NET Core 8.0 Çalışma Zamanı (v8.0.2) Barındırma Paketi** yükleyin.
- Gerekli Barındırma Paketini indirmek için aşağıdaki bağlantıyı kullanın: https://dotnet.microsoft.com/en-us/download/dotnet/thank-you/runtime-aspnetcore-8.0.2-windows-hosting-bundle-installer.



Tuş	Anlamı
ACS	Birincil giriş kontrol sistemi, AMS veya BIS-ACE
CM/VM	Web uygulaması için arka uç: Credential Management veya Visitor Management
DB	Ana ACS veritabanı
MA	Mobile Access arka ucu
S	Sistem teknisyenlerinin ve yapılandırıcılarının mobil cihazları için "Kurulum Erişimi" teknisyen uygulaması
M	Normal kimlik bilgisi sahiplerinin mobil cihazları için "Mobil Erişim" giriş uygulaması.

Prosedür

Ana Giriş Kontrolü Sistemi'nin en son sürümüne sahip olduğundan emin olun.

1. Mobile Access Arka Uç sunucusunda Yönetici olarak `BoschMobileAccessBackend.exe`'yi çalıştırın
– Kurulum programı açılır
2. **Konum** ekranında kurulum türünü seçin: **Dağıtılmış**
3. **Ana Bilgisayar** ekranında, **Mobile Access Arka Ucu** öğesini seçip **Next** (İleri) öğesine tıklayın
– Not: **ACS** seçeneği, Mobile Access'i ACS sunucusuna yüklediğimiz bu prosedürde daha sonra kullanılacaktır.
4. **Components** (Bileşenler) ekranında, **BoschMobile Access**'in seçildiğini onaylayıp **Next** (İleri) öğesine tıklayın
5. **EULA** ekranında bilgileri dikkatlice okuyun ve Son Kullanıcı Lisans Sözleşmesi'ni (EULA) kabul etmek istiyorsanız **Kabul et**'e tıklayın. Kurulum yalnızca bunu yaptığınızda devam edebilir.
6. **Kurulum dizini** ekranında:
– Kurulum için bir hedef klasöre gidip klasörü seçin veya varsayılanı kabul edin (önerilen)
– Mobil uygulamada ve HTML e-posta şablonlarında görüntülenecek olan şirketinizin adını girin
– **Next**'e (İleri) tıklayın
7. **SQL Server** ekranında veritabanının konumu için iki alternatiften birini seçin. Yapılandırmalar biraz farklıdır. Sonraki adım için bir alternatif seçin:
– 1. ALTERNATİF **Yerel veritabanı** seçeneği:
  – Kurulum programı yerel veritabanını bulur ve önceden seçer.
  – Yönetici kullanıcı için SQL parolası girin (varsayılan `sa`'dır)
  – **Test Bağlantısı**'na tıklayın
  – **Next**'e (İleri) tıklayın
– 2. ALTERNATİF **Uzak veritabanı** seçeneği
  – Ağda bulunan SQL Server'ın adını girin
  – SQL örneğinin adını girin
  – Yönetici kullanıcı için SQL parolası girin (varsayılan `sa`'dır)
  – **Test Bağlantısı**'na tıklayın
  – Kullanıcı adını kontrol edin ve uzak veritabanı kullanımı için oluşturduğunuz Windows ve SQL Administrator kullanıcısının parolasını girin (yukarıdaki ön koşullara bakın)
  – **Next**'e (İleri) tıklayın

Dağıtılmış kurulumun bu noktasında, ACS sunucusunun çalıştığı bilgisayara geçmeniz ve daha sonra yerel bilgisayardaki Mobile Access *arka ucu ile iletişim kurabilmesi için* Mobile Access*'i yapılandırmanız gerekir.*
Burada belirtilen adımları tamamladıktan sonra, kurulum programı, onaylamanız ve devam etmeniz için yerel sunucuya geri döner.

1. ACS sunucu bilgisayarında, `BoschMobileAccessBackend.exe` dosyasını Yönetici olarak çalıştırın.
– Kurulum programı açılır
2. **Konum** ekranında kurulum türünü seçin: **Dağıtılmış**
3. **Ana bilgisayar** ekranında **ACS** 'yi seçin ve **İleri**'ye tıklayın
4. **Yardımcı sihirbaz** ekranındaki açıklayıcı metni okuyun ve **İleri**'ye tıklayın
5. **Sertifika** ekranında
– Mobile Access Arka Ucunun çalıştırılacağı ana bilgisayar adını girin
– İsterseniz veya ağ, ana bilgisayar adı çözümlemesi sağlıyorsa bu ana makinenin IP adresini girin
– **Next**'e (İleri) tıklayın
6. **Kimlik sunucusu yapılandırma** ekranında
– Varsayılan kimlik sunucusu (önceden seçilen) `44333https://` <NameOfACSserver>`:44333` portuna sahip birincil ACS sunucusudur.
– **Test Bağlantısı**'na tıklayın
– Test başarısız olursa kimlik sunucusunun kullanılabilirliğini yeniden kontrol edin.
– **Next**'e (İleri) tıklayın
7. **Dosya oluştur** ekranında
Burada, şifre korumalı bir ZIP dosyasında bir yapılandırma dosyası oluştururuz ve bu dosyayı Mobile Access arka ucu tarafından kullanılabilir hale getiririz.
– **Kullanıcı şifresi**: ZIP dosyası için bir şifre girin
– **Yapılandırma dosyası**: ZIP dosyasının içine yerleştirileceği bir klasöre girin veya gidin. Bu klasöre, Mobile Access Arka ucunun çalıştığı bilgisayarın erişebilmesi gerektiğine dikkat edin. Erişemiyorsa ZIP dosyasını bu bilgisayara başka yollarla aktarmanız gerekir.
– **Yapılandırma dosyası oluştur**'a tıklayın
– **Next**'e (İleri) tıklayın
8. **Makineyi değiştir** ekranında
ACS sunucusundaki kurulum adımları artık tamamlanmıştır.
– Prosedürü sonlandırmak için **Onayla**'ya tıklayın

Dağıtılmış kurulumun bu noktasında, Mobile Access *arka uç bilgisayarındaki kurulum programına dönersiniz.*

1. Bosch Mobile Access sunucu bilgisayarında `BoschMobileAccessBackend.exe` kurulum programına dönün.
2. **Makineyi değiştir** sayfasında
– **ACS makinesinde gerekli adımları zaten tamamladım** olarak etiketlenmiş onay kutusunu seçin.
– **Next**'e (İleri) tıklayın
3. **Dosya yükle** ekranında
– **Yapılandırma dosyasını yükle:** ACS sunucusunda oluşturduğunuz yapılandırma dosyasını seçin
– **Şifre doğrulama:** ACS sunucusundaki ZIP dosyası için ayarladığınız şifreyi girin

– Doğru şifreyi girdikten sonra, yapılandırma dosyasını okumak için **İleri**'ye tıklayabilirsiniz.

4. **Core Components** (Temel Bileşenler) ekranında, **Bosch Mobile Access**'in seçildiğini onaylayın ve **Install** (Yükle) öğesine tıklayın

– Kurulum sihirbazı tamamlanır.

5. **Next**'e (İleri) tıklayın
6. **Temel Bileşenler** ekranında, yüklemenin başarıyla tamamlandığından emin olun ve **Bitir**'e tıklayın.
7. Windows `Services` uygulamasında, `Bosch Mobile Access` hizmetinin çalıştığından emin olun.

4.6 Mobil Erişim uygulamalarını yükleme

Giriş

Bosch, Mobile Access için aşağıdaki uygulamaları sağlar

– Bosch Mobile Access: Sanal bilgileri depolamak ve bunları Mobile Access için yapılandırılan okuyuculara Bluetooth aracılığıyla aktarmak için kullanılan bir kart sahibi uygulaması. Böyle bir okuyucu uygulamanın depolanmış kimlik bilgilerinden birinin geçerli olup olmadığına bağlı olarak giriş izni verir veya reddeder.
– Bosch Setup Access: Okuyucuları Bluetooth aracılığıyla taramak ve yapılandırmak için kullanılan bir teknisyen uygulaması.

Visitor Management ve Credential Management'ın yetkili operatörleri hem kart sahibi hem de teknisyen uygulamaları için sanal kimlik bilgileri gönderebilir.

Kart sahibi olan uygulama çalıştığı ve mobil cihazda etkin olduğu sürece, bu kartı fiziksel bir kartmış gibi kullanabilirsiniz. Uygulamadan komut vermeye veya ekranın kilidini açmaya gerek yoktur.

Uyarı!
ÖNEMLİ: Kart sahibi ve teknisyen uygulamalarını eş zamanlı olarak çalıştırmayın
Kart sahibi uygulaması kullanılırken teknisyen uygulamasını kimsenin kullanmadığından ve bunun tersinin geçerli olmadığından emin olun.

Prosedür

Bosch Mobile Access uygulamaları, Google ve Apple uygulama mağazalarından indirilebilir ve normal şekilde yüklenebilir. Uygulama mağazalarındaki adları şunlardır:

– Bosch Mobile Access
– Bosch Setup Access

4.7 Çevre donanımları

Bu bilgiler yazıldığı sırada aşağıdaki çevresel USB cihazları VisMgmt ve CredMgmt ile kullanılmak üzere test edilip onaylanmıştır. Uyumlu cihazların sürekli olarak güncelleştirilen listesi için ana giriş kontrolü sisteminin veri sayfasına başvurun.

Kart kayıt okuyucusu	LECTUS enroll ARD-EDMCV002-USB, HID OMNIKEY 5427 CK
Kimlik belgeleri için tarayıcı	ARH Combo, ARH Osmond

İmza tarayıcısı	signotec LITE, signotec Omega

Bu cihazları, istemci bilgisayarlarınıza bağlamak için üreticinin talimatlarını izleyin.

Kayıt okuyucuları

Aşağıdaki kayıt okuyucuları ve kart biçimleri desteklenir.

	MIFARE DESFire EV1 Bosch Kodu	MIFARE DESFire EV1 CSN	MIFARE Classic CSN	HID Prox 26 bit	iCLASS 26 bit	iCLASS 35 bit	iCLASS 37 bit	iCLASS 48 bit	EM 26 bit
LECTUS enroll ARD-EDMCV002-USB	X								
OMNIKEY 5427 CK		X	X	X	X	X	X	X	X

4.7.1 İstemci bilgisayarıyla çevre donanımlarını kaydetme.

VisMgmt istemci bilgisayarıyla çevre donanımı kaydetmek için istemcide Bosch Çevresel Cihaz kurulum programını (`BoschPeripheralDeviceAddon.exe`) çalıştırın. Talimatlar için bkz. *Çevresel Cihazlar eklentisini kurma, sayfa 13*.

Bkz.

– *Çevresel Cihazlar eklentisini kurma, sayfa 13*

4.8 Mobil Erişim yüklemelerini onarma

Giriş

İkili dosyaları güncellemek veya Mobile Access sertifikasını yeniden oluşturmak için mevcut bir kurulum sonrasında geçerli veya yeni bir Mobile Access sürümünün yükleyicisini çalıştırabilirsiniz:

Prosedür

1. Mobile Access arka uç sunucusunda Yönetici olarak `BoschMobileAccessBackend.exe` dosyasının yeni sürümünü çalıştırın.

– Aynı yerde kurulumlar için Mobile Access arka uç sunucusunun ACS sunucusu ile aynı olduğunu unutmayın.

2. Kurulum sihirbazını izleyerek orijinal yüklemeyle aynı ayarları yapın.

– Sertifikayı yeniden oluşturmak için, **Sertifikalar** ekranında **Sertifikayı yeniden oluştur** radyo düğmesini seçin.

3. Kurulum programı tamamlandıktan sonra sunucuyu yeniden başlatın.
4. Mobile Access (CredMgmt veya VisMgmt ya da ikisi) kullanan her web uygulamasında yeni bir oturum başlatın.

– Web uygulaması yeni ikili dosyalar kullanır.

– **Sertifikayı yeniden oluştur**'u seçtiyseniz Mobile Access kullanıcılarına ve teknisyenlerine gönderdiğiniz tüm diğer davetiyelerde yeni Mobile Access sertifikası temel alınır.

4.9 Yazılımı kaldırma

Yazılımı sunucudan veya istemciden kaldırmak için:

1. Windows yönetici haklarına sahip olarak Windows programı **Program ekle veya kaldır**'ı başlatın.
2. Programı (sunucu veya istemci) seçin ve **Kaldır**'a tıklayın.
3. (Ziyaretçi yönetimi için ve yalnızca sunucuda) Programın yanı sıra ziyaretçi yönetimi veritabanını da kaldırmak isteyip istemediğinizi seçin.

– **Not**: Veritabanı, program kullanımdayken kayıtlı olan tüm ziyaretlerin kayıtlarını içerir. Veritabanını arşivlemek veya başka bir kuruluma aktarmak isteyebilirsiniz.

4. Günlük dosyalarını kaldırmak isteyip istemediğinizi seçin.
5. Her zamanki şekilde kaldırma işlemini tamamlayın.
6. (Önerilen) Windows kayıt defterinin tam olarak değiştirilmesini sağlamak için bilgisayarı yeniden başlatın.

Not: Mobile Access arka ucu kaldırıldıktan sonra, aşağıdaki yapılandırma izleri istenirse manuel olarak kaldırılmalıdır:

– **MAUser** - Bu kullanıcı kaldırıldıktan sonra kalır. Yönetici bunu manuel olarak kaldırmalıdır.
– **Sertifikalar** - Mobile Access kurulumu nedeniyle yüklenen tüm sertifikaları manuel olarak kaldırmak için *Bilgisayar sertifikalarını yönetin* seçeneğini kullanın.
– **Mobil erişim için kimlik sunucusu yapılandırması** - *appsettings.Extension.MobileAccessBackend* dosyası, arka uç kaldırıldıktan sonra kalır. Manuel olarak silin.

5 Yapılandırma

5.1 ACS'de Ziyaretçi Yönetimi kullanıcıları oluşturma

Giriş

Her Yönetici, Resepsiyonist veya Ziyaret Edilen Kişi VisMgmt kullanıcısı, ACS'de, yani ana giriş kontrol sisteminde ayrı bir operatör tanımı olan bir karta sahip olmalıdır.

Bu Operatör tanımları **Kullanıcı profilleri** biçiminde özel VisMgmt yetkilerini içerir. **Kullanıcı profilleriyle** ilgili ayrıntılı bilgi ve yönergeler için ACS'nizin çevrimiçi yardımına bakın.

– Ziyaretçi yönetiminde çalışan her kart sahibi için ayrı bir operatör tanımlamanız gerekir. Aynı operatöre birden fazla kart sahibi atayamazsınız.

Uyarı!

BT güvenlik ve kullanıcı hesapları

BT güvenliğiyle ilgili en iyi uygulamalara uygun olarak her Resepsiyonist, Ziyaret Edilen Kişi ve Yönetici kullanıcının kendi Windows hesabında çalışmasını öneririz.

Ziyaretçi yönetimi için kullanıcı profilleri oluşturma

1. Ana giriş kontrolü sisteminde yönetici ayrıcalıklarına sahip olarak oturum açın.
2. VisMgmt kullanıcılar için bir veya daha fazla kullanıcı (operatör) profili oluşturun.
   İletişim kutusu yolu:
– **Yapılandırma > Operatörler ve iş istasyonları** > **Kullanıcı profilleri**
– Yapılandırma Tarayıcısı > **Yönetim** > **ACE Kullanıcı profilleri**
3. Bu profillere aşağıdaki kullanıcı haklarından birini atayın.
– Yönetici: `Visitor Management > Administrator`
– Ziyaret edilen kişi: `Visitor Management > Host`
– Danışma görevlisi: `Visitor Management > Receptionist`

Çeşitli VisMgmt rolleri (Yönetici, Resepsiyonist, Ev Sahibi) için ihtiyaç duyduğunuz kullanıcı profillerini oluşturduğunuzda, her profili birden fazla operatöre atayabilirsiniz.

ACS operatörlerine ve kart sahiplerine kullanıcı profilleri atama

İletişim yolu:

– **Configuration** (Yapılandırma) > **Operators and workstations** (Operatörler ve iş istasyonları) > **User rights** (Kullanıcı hakları)
– Yapılandırma Tarayıcısı > **Yönetim** > **Operatörler**

1. Yeni bir operatör türü (ACS'ye bağlı olarak  veya  simgesine tıklayın) ekleyin ve bu türe VisMgmt rollerinden (Yönetici, Ev Sahibi veya Resepsiyonist) biriyle ilgili bir ad verin.
2. **Genel operatör ayarları** sekmesindeki Yetki listesinden `Operator ACE`'yi seçin.
3. **Ace operatörü ayarları** sekmesinde, yukarıda oluşturduğunuz **ACE kullanıcı profilini** atamak için ok düğmelerini kullanın.
   Kart sahibinin ACS'de genel yönetici haklarını zorunlu tuttuğu nadir durumlar haricinde `UP-Administrator` varsayılan profilinin atamasını kaldırın.
4. Hala **ACE operatör ayarları** sekmesindeyken, sistemde VisMgmt rolüne sahip olacak kart sahibini bulmak için **Kişi ata** bölmesini kullanın.
5. Seçilen kart sahibine atamayı tamamlamak için **Kişi ata**'ya tıklayın.

– Ziyaretçi yönetiminde çalışan her kart sahibi için ayrı bir operatör tanımlamanız gerekir. Aynı operatöre birden fazla kart sahibi atayamazsınız.

5.2 ACS'de Ziyaretçi yetkileri ve profilleri oluşturma

Giriş

VisMgmt sisteminin danışma görevlisi veya yöneticisi, her yeni ziyaretçi için bir **Ziyaretçi türü** seçer. Bu ziyaretçi türü, ana giriş kontrolü sistemi nde (ACS) **Ziyaretçi** adında önceden tanımlanmış bir **Kişi türüne** veya ACS'nin yöneticilerinin oluşturduğu bir **Ziyaretçi** alt türüne dayanır.

Bu yöneticiler, ayrıca **Ziyaretçi** kişi türünü ve ACS'nin alt türlerini giriş profillerine yapılandırmalıdır. Giriş profilleri bu kişi türlerinin sitede gerçek kapıları çalıştırmasına izin verir.

5.3 Danışma görevlisi bilgisayarını kurma

Danışma görevlisi bilgisayarı, **Bosch Çevresel Cihazlar** eklentisini çalıştırır. Bu yazılım kart okumak, kimlik belgelerini taramak ve imzaları taramak için çevresel cihazlara fiziksel olarak bağlantı sağlar.

İstemci yazılımını yüklemeden önce tüm gerekli çevresel cihazlarını bağlayın.

Bilgisayarın ve çevresel cihazlarının yetkisiz girişlere karşı düzgün korunduğundan emin olun.

5.4 Ziyaretçiler için hizmet bankosu bilgisayarı kurma

Giriş

Ziyaretçiler, giriş denetimli binanın resepsiyon alanında serbestçe erişilebilen bir bilgisayarda, genellikle ziyaretlerini kaydeder ve kendi profillerini oluşturur. Güvenlik nedenleriyle, bilgisayarın web tarayıcısı hizmet bankosu modunda çalışır. Bu da yalnızca VisMgmt erişimi sunarken birden çok sekmeye, tarayıcı ayarlarına veya bilgisayarın işletim sistemine erişim sunmaz. Tüm desteklenen tarayıcılar, hizmet bankosu modunu sunar ancak bunun tam yapılandırması tarayıcıya bağlıdır.

Hizmet bankosu bilgisayarı, **Bosch Çevresel Cihazlar** eklentisini çalıştırır. Bu da kimlik belgelerinin ve imzaların taranması için çevresel cihazlara fiziksel olarak bağlantı sağlar.

– Hizmet bankosu modu, `https://<My_VisMgmt_server>:5706` şeklindedir

Tarayıcıları hizmet bankosu modu için yapılandırma

Aşağıdaki bağlantılar, VisMgmt tarafından desteklenen tarayıcılar için hizmet bankosu yapılandırmasını açıklar

	Hizmet bankosu ayarlama talimatları
Chrome	https://support.google.com/chrome/a/answer/9273974
Firefox	https://support.mozilla.org/en-US/kb/firefox-enterprise-kiosk-mode
Edge	https://docs.microsoft.com/en-us/deployedge/microsoft-edge-configure-kiosk-mode

Uyarı!

Güvenlik nedenleriyle, şifreleri otomatik olarak kaydetmek için her zaman tarayıcı seçeneğini devre dışı bırakın.

5.5 Yapılandırma görevleri için oturum açma

Yapılandırma ve yönetim görevleri için, yetkisiz girişlerden fiziksel olarak korunan bir bilgisayarı kullanın.

1. Tarayıcınızda, VisMgmt sunucusunun, iki noktadan ve bağlantı noktası numarasından (varsayılan olarak `5706`) sonraki HTTPS adresini girin
   `https://`<My_VisMgmt_server>`:5706/main`
   Oturum açma ekranı görünür
2. Bir VisMgmt **Yönetici** kullanıcısı olarak oturum açın.
3. **Ayarlar** menüsünü açmak için  öğesine tıklayın.

5.6 Yapılandırma için Ayarlar menüsünü kullanma

Ayarlar menüsü, aşağıdaki yapılandırma adımlarını gerçekleştirmenize olanak tanıyan alt bölümler içerir:

Genel ayarlar	– **Saklama süresi (gün)**: Bu ayar, ziyaret kayıtlarının işlenmesini yönetir.
	  – Süre ilk kez sona erdiğinde uygulama, kaydı anonimleştirir.
	  – Süre ikinci kez sona erdiğinde uygulama, kaydı siler.
	  Varsayılan değer `365`şeklindedir.
	  Saklama dönemini tamamen devre dışı bırakmak için 0'a ayarlayın. Bu durumda, ziyaret kayıtları süresiz olarak saklanır.
	– **Belge saklama modu**: Belgelerin, kağıt mı yoksa dijital dosyalar olarak mı saklanmasını istediğinizi seçin.
	– Sitede bir seferde izin verilen **maksimum ziyaretçi sayısı**.
	Varsayılan değer `100` şeklindedir.
	Panodaki ziyaretçi sayaçlarını tamamen devre dışı bırakmak için `0` olarak ayarlayın.
	– **Belge süre sonu dönemi (gün sayısı)**: Gizlilik Sözleşmeleri (NDA) ve Kullanım Şartları gibi karşıya yüklenen belgelerin ne kadar süreyle geçerli kalması gerektiğini girin. Bu süre hem kağıt hem de dijital dosyalar için geçerlidir.
	Bu süre sonunda, belgeler ziyaretçinin profilinde süresi geçmiş olarak işaretlenir (kırmızı noktalı saat simgesi).
	Varsayılan değer: `365`
	– **Belge süre sonu uyarı süresi (gün)**: Süre sonu tarihinden önceki uyarı döneminin uzunluğunu girin.
	Bu uyarı süresi boyunca, belgeler ziyaretçinin profilinde işaretlenir (turuncu nokta bulunan saat simgesi). Uyarı simgesinin sonunda, saat simgesi yeşil bir nokta içerir.
	– **Logo:** İletişim kutularında özelleştirilmiş bir logo mu yoksa varsayılan logonun mu gösterileceğini ve Bosch **supergraphic**'in gösterilip gösterilmeyeceğini düzenleyen onay kutularını seçin veya temizleyin.
	  – Özelleştirilmiş logo dosyalarının kriterleri için bkz. *Şirket logosunu özelleştirme, sayfa 34*
	– İletişim kutusu sayfasını bu ayarlarda görüneceği şekilde göstermek için **Ön izleme**'ye tıklayın. Ön İzleme modunda daha fazla ayrıntı için sonraki bölümü seçin.

	– **Diller**: Kullanıcı arayüzünde hangi dillerin kullanılabilir olduğunu seçin (tercih edilen **tarih** ve **saat** biçimleriyle birlikte). – **Posta sunucusu** Uygulamadan e-postaların gönderilmesini etkinleştirmek için e-posta sunucunuzun IP adresini, bağlantı noktası numarasını ve hesap ayrıntılarını girin. Harici posta sunucusunun ekstra bir SSL/TSL sertifikası gerektirmesi durumunda, bunu mobil erişim arka ucu çalıştıran makineye aktarın. İçe aktarma işleminden sonra `VisitorManagerServer`'ın yeniden başlatılması gerekmektedir. – **E-posta şablonları** Birkaç HTML e-posta şablonu sunulur, bunları genellikle kendi gereksinimlerinize göre özelleştirebilirsiniz. Ayrıntılar için aşağıdaki ayrı **E-posta şablonları** bölümüne bakın. – **Mobile Access** Önce **Mobile Access** onay kutusunu seçerek Mobile Access öğesini etkinleştirin. **Bağlantı**: Mobile Access sunucusunun adresini (kayıt hizmeti adresi) girin. `https://`<MyMobileAccessBackendServer>`:5700` Çoklu etki alanı ortamlarında <MyMobileAccessBackendServer> için bir (FQDN) kullanın. **Not:** Bir FQDN yerine bir IP adresi kullanmak için **Sertifika oluşturma**'nın altında, Mobile Access Arka Ucu için kurulum sihirbazını çalıştırdığınızda, bu IP adresini girmeniz gerekir. **Teknisyen ekleme:** Teknisyenlerden istediğiniz bilgileri seçin, böylece teknisyenler Bosch Setup Access ile mobil erişim okuyucularını yapılandırabilir. Mobile Access Özelliğini hemen kullanmak için web uygulamasından çıkış yapın ve yeniden giriş yapın.

Danışma görevlisi	– Bu ayarlar ekranı, danışma görevlisinin ziyaretçi kaydı iletişim kutularındaki veri alanları için 2 onay kutusu içerir.
	  – Veri alanının tüm kayıt iletişim kutularında **görünür** olup olmayacağını belirlemek için ilk onay kutusunu temizleyin veya seçin.
	  – Veri alanının **zorunlu** olup olmadığını yönetmek için ikinci onay kutusunu (yıldız işaretiyle işaretlenir) temizleyin veya seçin.
	– Veri toplama iletişim kutularındaki varsayılan başlık metinlerini özelleştirin.
	Daha ayrıntılı bilgi için aşağıdaki *Kullanıcı arabirimini özelleştirme, sayfa 34* bölümüne bakın.

	Özel seçenek: Kart olmadan giriş/çıkış seçeneğini etkinleştir

	Ziyaretçilerin yakın refakatçıları varsa veya yalnızca herkese açık alanlara girebiliyorlarsa her ziyaretçiye ayrı kart verilmesine gerek olmayabilir. Böyle durumlar için, ziyaretçilerin kartlar olmadan giriş ve çıkış yapabilme seçeneği bulunur. Güvenlik nedenleriyle bu seçenek varsayılan olarak devre dışıdır. Etkinleştirmek için onay kutusunu seçin: – **Not:** Seçenek etkinleştirilirse hizmet bankosu bilgisayarında kendi kendine kayıt yapan tüm **Ziyaretçiler** otomatik olarak onaylanır ve aynı anda kendi ziyaretleri için giriş yapmış olur. – Bir **Danışma görevlisi** kullanıcısının kartlar olmadan ziyaretçi işlemleri yapma konusunda ayrıntılar için bu belgenin **Çalışma**, *Kart olmadan giriş ve çıkış yapma, sayfa 50* bölümüne bakın.
Ziyaret edilen kişi	**Ziyaret edilen kişi** ve **Ziyaretçi** kullanıcıları ayarları, siz **Danışma görevlisi** ayarlarını düzenleyip kaydedene kadar salt okunurdur. **Danışma görevlisi** ayarlarında görünmez olarak işaretlediğiniz alanlar, **Ziyaret edilen kişi** ve **Ziyaretçi** için otomatik olarak görünmez şeklinde ayarlanır. Bundan sonra yapılandırma prosedürü aynıdır.
Ziyaretçi	

Bkz.
- *Fiziksel kimlik bilgilerini atama, sayfa 47*
- *Kullanıcı arabirimini özelleştirme, sayfa 34*

5.6.1 E-posta şablonları

Birkaç HTML e-posta şablonu sunulur, bunları genellikle kendi şirket gereksinimlerinize göre özelleştirebilirsiniz. Her şablonda Bilgi, Gizli ve test alıcısı için posta adreslerini, anında bir test e-postası gönderebilmek için saklayabilirsiniz. Bir şablonu düzenlemek için indirdiğinizde, bu şablon tarayıcınızın varsayılan indirmeler klasörüne kopyalanır.
- `MobileAccess.html` Akıllı telefon tabanlı kimlik bilgilerini kullanmak için kart sahibine davetiye.
- `SetupAccess.html` Bir teknisyenin Mobile Access için okuyucuları yapılandırmasına yönelik bir davetiye.
- `VisitorInvite.html` Bir kişinin, bir iCalendar dosyasını e-postaya ekleme seçeneğiyle birlikte sitenizi ziyaret etmesine yönelik bir davet.
- `InformHostAboutCheckin.html` Ana bilgisayara ziyaretçinin geldiğini bildirmek için bir e-posta.

E-posta şablonlarında kullanmak için yer tutucular

E-posta şablonları metindeki veritabanı alanlarını içermesi için çeşitli metin yer tutucuları sağlar. Bu yer tutucular, kullanılabilecekleri şablonlara göre aşağıdaki tablolarda açıklanmaktadır.

Mobil Erişim

Mobil erişim verildiğinde kart sahibine (Mobile Access uygulaması için) gönderilen e-posta

Yer tutucu	Açıklama
`{{Title}}`	kişinin unvanı (Bay, Bayan, Dr. vb.)
`{{FirstName}}`	kişinin adı

Yer tutucu	Açıklama
{{LastName}}	kişinin soyadı
{{CompanyName}}	kişinin şirketi
{{QrcodeLink}}	Uygulama aracılığıyla kart sahibine mobil erişim sunan bağlantıya karşılık gelen QR kodu
{{InviteLink}}	Uygulama aracılığıyla kart sahibine mobil erişim sunan bağlantı

Kurulum Erişimi

Okuyucuları kurmaları için teknisyenlere mobil erişim verildiğinde Mobile Access teknisyenine gönderilen e-posta (Setup Access uygulaması için).

Yer tutucu	Açıklama
{{Title}}	teknisyenin unvanı (Bay, Bayan, Dr. vb.)
{{FirstName}}	teknisyenin adı
{{LastName}}	teknisyenin soyadı
{{CompanyName}}	teknisyenin şirketi
{{QrcodeLink}}	Okuyucuların Setup Access uygulaması aracılığıyla kurulması için teknisyene mobil erişim sunan bağlantıya karşılık gelen QR kodu
{{InviteLink}}	Okuyucuları Setup Access uygulaması aracılığıyla kurmak için teknisyene mobil erişim sunan bağlantı

Ziyaretçi davetiyesi

Bir ziyaret oluşturulduğunda veya düzenlendiğinde ziyaretçiye gönderilen e-posta.

Yer tutucu	Açıklama
{{VisitorID}}	Ziyaretçinin VisMgmt uygulaması tarafından oluşturulan kimlik kodu
{{Title}}	ziyaretçinin unvanı (Bay, Bayan, Dr. vb.)
{{FirstName}}	ziyaretçinin adı
{{LastName}}	ziyaretçinin soyadı
{{CompanyName}}	ziyaretçinin şirketi
{{HostFirstName}}	ziyaret edilen kişinin adı
{{HostLastName}}	ziyaret edilen kişinin soyadı
{{ExpArrivalDate}}	planlanan ziyaret tarihi

Ziyaretçi Geldi

Danışma görevlisi ziyareti onayladığında ziyaret edilen kişiye gönderilen e-posta

Yer tutucu	Açıklama
{{VisitorID}}	Ziyaretçinin VisMgmt uygulaması tarafından oluşturulan kimlik kodu
{{Title}}	ziyaretçinin unvanı (Bay, Bayan, Dr. vb.)
{{FirstName}}	ziyaretçinin adı
{{LastName}}	ziyaretçinin soyadı
{{CompanyName}}	ziyaretçinin şirketi
{{HostFirstName}}	ziyaret edilen kişinin adı
{{HostLastName}}	ziyaret edilen kişinin soyadı
{{ExpArrivalDate}}	planlanan ziyaret tarihi
{{ArrivalDate}}	gerçek ziyaret tarihi

Ziyaretçi Geçiş Kartı

Yazdırılabilen ve ziyaretçiye verilen belge. Bu, binanın bir haritasını veya kontrol listesini içerebilir.

Yer tutucu	Açıklama
{{VisitorID}}	Ziyaretçinin VisMgmt uygulaması tarafından oluşturulan kimlik kodu
{{Title}}	ziyaretçinin unvanı (Bay, Bayan, Dr. vb.)
{{FirstName}}	ziyaretçinin adı
{{LastName}}	ziyaretçinin soyadı
{{CompanyName}}	ziyaretçinin şirketi
{{HostFirstName}}	ziyaret edilen kişinin adı
{{HostLastName}}	ziyaret edilen kişinin soyadı
{{ExpArrivalDate}}	planlanan ziyaret tarihi
{{ArrivalDate}}	gerçek ziyaret tarihi

5.6.2 Ön izleme modu

Belirli seçenek kümeleri, iletişim kutularını bu seçenekler ayarlandığında göründükleri gibi görebilmenizi sağlayan ön izleme modunu etkinleştiren bir **Ön izleme** düğmesi sağlar.

Ön izleme modunda aşağıdaki koşullar geçerlidir:

– Panonun üst kısmında bir başlık görüntülenir.

– Panoda veya menülerde yapılan değişiklikler **kaydedilmez**.
– Ön izleme modunu kapatmak için başlık içinde **Ön izleme modunu kapat**'a tıklayın.
– Farklı kullanıcı türleri için arayüz görünümüne önizleme yapmak üzere başlık içindeki **Rolü değiştir** listesini kullanın.

5.6.3 Belge şablonları

Çeşitli belge ve e-postalar için şablonlar indirebilir ve bu şablonların özelleştirilmiş sürümlerini **Pano** > **Ayarlar > Genel** iletişim kutusunda yükleyebilirsiniz.

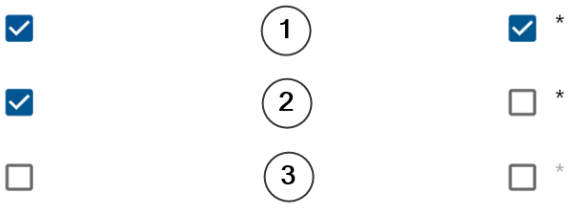
5.7 Kullanıcı arabirimini özelleştirme

Kullanıcı arayüzünü **Kontrol paneli** > **Ayarlar** iletişim kutularında özelleştirin,

5.7.1 Seçenekleri görünür, görünmez ve zorunlu olarak ayarlama

İletişim kutularında hangi veri alanlarının görülebileceğini ve bu verilerin hangisinin zorunlu olacağını seçin.

Örnek:



- (1) görünür ve zorunludur,
- (2) görünür ancak zorunlu değildir
- (3) görünür değildir.

5.7.2 Yerelleştirme için kullanıcı arayüzü metinlerini özelleştirme

Her dil için kullanıcı arayüzünün metinlerini kolayca özelleştirebilirsiniz.

Varsayılan olarak **yerelleştirme metni**, veri toplama iletişim kutularındaki veri alanlarının blokları için standart başlıkları içerir.

Bu başlıkları yerel gereksinimlere göre özelleştirmek için:

1. Listeden bir kullanıcı arayüzü dili seçin.
2. Metin kutusundaki metinlerin üzerine yazın.
   Basit biçimlendirme için HTML etiketleri kullanabilirsiniz; örneğin:
   ```
   <b>this text will appear bold </b>
   <i>italics</i>
   <u>underline</u>
   ```

5.7.3 Hizmet bankosu modunu özelleştirme

Sitenizde bir veya daha fazla çevresel donanım cihazı (örneğin bir belge tarayıcısı) eksikse ilgili kayıt adımlarının onay kutularını temizleyerek ziyaretçinin kendi kendine kayıt işlemini hizmet bankosu modunda özelleştirebilirsiniz.

5.7.4 Şirket logosunu özelleştirme

Şirket logonuz için yüklediğiniz grafik dosyalarının aşağıdaki kriterleri karşılaması gerekir:

Desteklenen biçimler	PNG, JPEG, JPG
Tam genişlik (piksel)	125

Tam yükseklik (piksel)	63
Maks. boyut (MB)	1

5.8 Güvenlik duvarı ayarları

Sunucu ve istemci bilgisayarların güvenlik duvarı yapılandırmasına yardımcı uygulamalar ekleyin:

1. Windows Güvenlik Duvarını Başlat > **Denetim Masası** > **Windows Güvenlik Duvarı** yolundan başlatın
2. **Gelişmiş ayarları** seçin
3. **Gelen Kuralları** seçin
4. **Eylemler** bölmesinde **Yeni Kural...**'ı seçin
5. **Kural Türü** iletişim kutusunda **Bağlantı Noktası**'nı seçin ve **İleri**'ye tıklayın
6. Sonraki sayfada **TCP ve belirli yerel bağlantı noktaları**'nı seçin
7. Aşağıdaki bağlantı noktaları üzerinden iletişime izin ver:

– Sunucu bilgisayarda veya bilgisayarlarda

<sunucu adı>:44333 - AMS kimlik sunucusu tarafından kullanılıyor **(*)**

<sunucu adı>:5706 (VisMgmt sunucusu tarafından kullanılıyor)

<sunucu adı>:5806 (CredMgmt sunucusu tarafından kullanılıyor)

<sunucu adı>:5701 - Mobile Access arka uç sunucusu tarafından kullanılır

– İstemci bilgisayarlarda

localhost:5707 - Bosch Çevresel Cihaz eklentisi tarafından kullanılır

(*) AMS ve BIS kimlik sunucularını ilgili kurulum kılavuzlarında açıklandığı gibi kullanırız.

Sistem içinde port kullanımı

Giden Sunucu	Port Çıkış	Gelen Sunucu	Port Giriş	Protokol	Yorumlar
VisMgmt veya CredMgmt	*	Mobile Access arka ucu	5701	HTTPS	Mobil kimlik bilgileri oluşturmak ve/veya silmek için web uygulamasından gelen komutlar
İnternetteki mobil cihazlar	*	Mobile Access arka ucu	5701	HTTPS	Mobil cihazlar internet aracılığıyla mobil kimlik bilgileri alır
Mobile Access Arka Ucu	*	Google Firebase (İnternet)	*	HTTPS	Mobil cihazlar anında ileti bildirimleri alır, lütfen güvenlik duvarları ayarlarıyla ilgili Google Firebase belgelerine başvurun https://firebase.google.com/docs/cloud-messaging/concept-options
VisMgmt kullanıcısının istemci bilgisayarı	*	VisMgmt arka uç	5706	HTTPS	VisMgmt istemci bilgisayarından VisMgmt arka ucuna gelen komutlar

Giden Sunucu	Port Çıkış	Gelen Sunucu	Port Giriş	Protokol	Yorumlar
CredMgmt kullanıcısının istemci bilgisayarı	*	CredMgmt arka ucu	5806	HTTPS	CredMgmt istemci bilgisayarından CredMgmt arka ucuna gelen komutlar
Yönetici bilgisayarı	*	Mobile Access arka ucu	3389	Uzak Masaüstü (RDP)	Güvenlik nedeniyle, yöneticilerin Mobile Access arka uç bilgisayarına erişmesine yalnızca geçici olarak izin vermeniz gerekir.

Uyarı!
Mobil Erişim'in ve ACS'nin, ne gelen ne de giden olmak üzere doğrudan bağlantısı olmadığını unutmayın.

5.8.1 Güvenlik duvarı özel durumları olarak programlar ve hizmetler

Güvenlik duvarını, program ve hizmetleri özel durum olarak ekleyerek de yapılandırabilirsiniz.

1. Windows Güvenlik Duvarı kullanıcı arabirimini başlatın, **Başlat > Ayarlar > Denetim Masası > Windows Güvenlik Duvarı**'nı seçin.
2. **Güvenlik Duvarı aracılığıyla bir uygulamaya veya özelliğe izin ver** sekmesini seçin.
3. **Başka bir uygulamaya izin ver**'i seçin (gri değilse **Ayarları değiştir**'i seçerek düğmeyi etkinleştirin).
4. Aşağıdaki programları ekleyebilirsiniz:

Programlar

Varsayılan yükleme yolu: `C:\Program Files (x86)\Bosch Sicherheitssysteme\`

Program	Dosya Konumu
acsp.exe	[Yükleme yolu]\AccessEngine**AC**\BIN
ACTA-3.exe	[Yükleme yolu]\AccessEngine**AC**\BIN
BioVerify.exe	[Yükleme yolu]\AccessEngine**AC**\BIN
BioIdentify.exe	[Yükleme yolu]\AccessEngine**AC**\BIN
Bosch.Ace.CredentialManagement.exe	[Yükleme yolu]\Bosch Credential Management
Bosch.Access.MobileAccessBackend.exe	[Yükleme Yolu]\Bosch Mobile Access
Bosch.Ace.VisitorManagement.exe	[Yükleme yolu]\Bosch Visitor Management
CalTa-3.exe	[Yükleme yolu]\AccessEngine**AC**\BIN
CDTA-1.exe	[Yükleme yolu]\AccessEngine**AC**\BIN
EMDP.exe	[Yükleme yolu]\AccessEngine**AC**\BIN
KCKemas.exe	[Yükleme yolu]\AccessEngine**AC**\BIN

Program	Dosya Konumu
KCS.exe	[Yükleme yolu]\AccessEngine**AC**\BIN
Loggifier-2.exe	[Yükleme yolu]\AccessEngine**AC**\BIN
PictureServer.exe	[Yükleme yolu]\AccessEngine**AC**\BIN
ReplServer.exe	[Yükleme yolu]\AccessEngine**AC**\BIN
reps.exe	[Yükleme yolu]\AccessEngine**AC**\BIN
TAccExc.exe	[Yükleme yolu]\AccessEngine**AC**\BIN
EMAILSP.exe	[Yükleme yolu]\AccessEngine**AC**\BIN
master-3.exe	[Yükleme yolu]\AccessEngine**AC**\BIN
querySrv-2.exe	[Yükleme yolu]\AccessEngine**AC**\BIN
webSrv-1.exe	[Yükleme yolu]\AccessEngine**AC**\BIN
LicenseGateway.exe	[Yükleme yolu]\AccessEngine**AC**\BIN
DMS.exe	[Yükleme yolu]\AccessEngine**MAC**\BIN
lac.exe	[Yükleme yolu]\AccessEngine**MAC**\BIN

Hizmetler

Varsayılan yükleme yolu: `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System`

Servis	Dosya Konumu
Bosch.States.Api	[Yükleme yolu]\States API
Bosch.Map.Api	[Yükleme yolu]\Map API
Bosch.MapView.Api	[Yükleme yolu]\Map View API
Bosch.Events.Api	[Yükleme yolu]\Events API
Bosch.Alarms.Api	[Yükleme yolu]\Alarms API
Bosch.Ace.IdentityServer	[Yükleme yolu]\Identity Server
Bosch.Ace.Api	[Yükleme yolu] \Access API
Bosch.DialogManager.Api	[Yükleme yolu]\Dialog Manager API
Bosch.Intrusion.Api	[Yükleme yolu]\Intrusion API
Bosch Ace Visitor Management	[VM yükleme yolu]\
Bosch Ace Visitor Management İstemcisi	[VM istemcisi yükleme yolu]\
Bosch.OSS-SO	[Yükleme yolu]\OSS-SO
Bosch.OSS-SO.Configurator	[Yükleme yolu]\OSS-SO.Configurator
Bosch.Access.ProductApi.Api	[Yükleme yolu]\ProductApi
Bosch.MUM	[MUM-install-path]\

5.8.2 Mobile Access API

Mobile Access 5.2 ve sonrası, Credential Management 5.2 ve sonrası ile Visitor Management 5.2 ve sonrası sürümlerinden başlayarak Mobile Access Arka Uç API'si bir ön kanal parçasına ve bir arka kanal parçasına bölünmüştür. Ön kanalın cep telefonlarıyla iletişim kurması ve arka kanalın da Credential Management ve/veya Visitor Management ile iletişim kurması beklenir.
Bu, BT güvenliğini güçlendirmek için güvenlik duvarı kuralları ve güzergahların ağ trafiğini düzenlemesini sağlar. API'nin bölünmesi iki ayrı port numarasıyla birlikte gelir. Diğer bir ifadeyle, cep telefonlarının port numarası 5700 iken Credential Management ve Visitor Management adres port numarası 5701'dir.
Hem Credential Management hem de Visitor Management, sırasıyla ön kanal URL'si ve arka kanal URL'si için iki ayrı ayara sahiptir. Kullanıcı arayüzü, onlara "Yönetim hizmeti adresi" (arka kanal) ve "Kayıt hizmeti adresi" (ön kanal) adını verir.
"Yönetim hizmeti adresi" (arka kanal) için varsayılan port 5701'tir. Müşteriye özel bir güvenlik duvarı kuralında, port yalnızca, çoğu durumda AMS sunucusu olan Credential Management ve/veya Visitor Management arka ucu çalışan makineyle iletişim kurmak üzere yapılandırıldı.
"Kayıt hizmeti adresi" (ön kanal) için varsayılan port 5700'dür. Müşteriye özel bir güvenlik duvarı kuralında bu porta Mobile Access mobil uygulamaları üzerinden ulaşılacak şekilde yapılandırılmalıdır. Birçok senaryoda, bu uç noktaya dışarıdan erişilebilir. Ancak bu, büyük oranda müşteri senaryosuna bağlıdır.
Müşteri, AMS'nin daha önceki bir sürümünden en son sürümüne güncelliyorsa Credential Management ve Visitor Management ayarlarının yapılması gerekir. Bu ayara, Visitor Management ve Credential Management ayarlar sayfasında Yönetici rolüyle erişilebilir.
Arka kanal, herkese açık internetten veya herhangi bir yetkisiz ağdan ulaşılamaz olacak şekilde güvence altına alınmalıdır.

5.9 BT güvenliği

Bir kuruluşun giriş kontrolü sisteminin güvenliği, kuruluşun altyapısının önemli bir bölümüdür. Bosch, kurulum ülkesi için belirlenmiş olan BT güvenlik kurallarına kesin bir şekilde yetki verir.
Giriş kontrolü sistemini kullanan kuruluş, en azından aşağıdakiler konusunda sorumluluğa sahiptir:

5.9.1 Donanım sorumlulukları

- RJ45 bağlantıları gibi ağ bileşenlerine yetkisiz olarak fiziksel erişimin engellenmesi.
  - Saldırganların, sinsi saldırıları gerçekleştirmek için fiziksel erişime ihtiyacı vardır.
- AMC2 kontrol cihazı donanımına yetkisiz olarak fiziksel erişimin engellenmesi.
- Giriş kontrolü için adanmış bir ağ kullanımı.
  - Saldırganlar aynı ağ içindeki diğer cihazlardan erişim kazanabilirler.
- Bosch koduyla **DESFire** ve biyometriyle çok faktörlü kimlik doğrulama gibi güvenli kimlik bilgilerinin kullanımı.
- **Kurulum Erişimi**uygulaması aracılığıyla, BLE (Bluetooth Low Energy) modüllerine sahip mobil erişim okuyucularına ilişkin istem kaydı. Kayıtsız, gücü açık okuyucular üçüncü taraflarca ele geçirilmeleri bakımından savunmasızdır. Böyle bir ele geçirme ile ilgili sorunu gidermek üzere fabrika varsayılanlarına sıfırlama hakkındaki talimatlar için okuyucunun kurulum kılavuzuna bakın.
- Giriş kontrolü sistemi için bir yük devri mekanizması ve bir yedek güç kaynağı sağlama.
- Eksik veya yanlış girilmiş olan kimlik bilgilerinin izlenmesi ve devre dışı bırakılması.

- Artık kullanımda olmayan donanımın doğru şekilde devre dışı bırakılması, özel olarak fabrika varsayılan ayarlarına sıfırlama ve kişisel verileri ve güvenlik bilgilerini silme.

5.9.2 Yazılım sorumlulukları

- Giriş kontrolü ağının güvenlik duvarının uygun bakımı, güncellenmesi ve çalışması.
- Kart okuyucuları veya AMC2 kontrol cihazları gibi donanım bileşenlerinin ne zaman çevrimdışı olduğunu gösteren alarmların izlenmesi.
  - Bu alarmlar, donanım bileşenlerini değiştirme girişimini gösteriyor olabilir.
- Kontrol cihazları, okuyucular ve elektrik dolapları gibi giriş kontrolü donanımındaki elektrik temaslarıyla tetiklenen dış müdahale algılama alarmlarını izleme.
- Adanmış ağ içindeki UDP yayınlarının sınırlandırılması.
- Giriş kontrolü yazılımına güncelleştirmeler, özellikle güvenlik güncelleştirmeleri ve düzeltme ekleri.
- Donanım belleniminin güncelleştirmeleri, özellikle güvenlik güncelleştirmelerini ve düzeltme ekleri.
  - Yeni teslim edilen donanımın bile bir bellenim güncelleştirmesi gerektirebileceğine dikkat edin. Talimatlar için donanım kılavuzuna bakın.
  - Bosch, güncel olmayan bellenimle işleme konulmuş ürünlerin neden olduğu zararlardan kaynaklanan bir yükümlülüğün olmadığını varsayar.
- OSDPv2 güvenli kanal iletişimi kullanımı.
- Güçlü şifre tümceciklerinin kullanımı.
- Yalnızca yasal amaçlarına yönelik olarak ihtiyaç duydukları kaynaklara erişmelerini sağlamak için *En az ayrıcalık ilkesinin* uygulanması.
- Operatörler için Kullanıcı profillerinin doğru bir şekilde atanması ve yapılandırılması, normal operatörlerin iki kişi ilkesi olmadan yüksek güvenlik yetkileri atamasını önlemek için gereklidir.

5.9.3 Mobil kimlik bilgilerinin güvenliğini ele alma

- Yapılandırılmamış Mobil Erişim okuyucularını korumasız olarak bırakmayın.
  - Bir saldırgan, okuyucuyu farklı bir ACS için ele geçirebilir. Bunun için maliyetli bir fabrika sıfırlaması gerekir.
- Mobil kimlik bilgilerini taşıyan bir mobil cihaz kaybolursa veya çalınırsa cihazı kayıp kart olarak kabul edin: Tüm mobil kimlik bilgilerini mümkün olduğunca çabuk engelleyin veya silin.
- Bosch, yüksek güvenlikli ortamlarda iki faktörlü kimlik doğrulamayı önerir. Bunun kimlik bilgisi olarak kullanılabilmesi amacıyla kimlik bilgisi sahibinin mobil cihazın kilidini açması gerekir.
- Telefon bir yedekten geri yüklendiğinde mobil kimlik bilgileri geri yüklenmez. Mobil kimlik bilgileri sahibi yeni bir mobil cihaz alırsa tüm geçerli davetiyeleri yeniden göndermeniz gerekir.
- Bir saldırgan, mobil erişim okuyucularıyla iletişimi engellemek için bir iletişim karıştırıcısı kullanabilir. Alanlara erişimleri çok önemli olan çalışanlar fiziksel kimlik bilgilerini yedek olarak taşımalıdır.
  - Mobile Access'in yedeği olarak, yalnızca güvenli bir kodlamaya (Bosch kodu gibi) sahip fiziksel kartları kullanın.
- Mobile Access sunucusunu yetkisiz fiziksel erişime karşı koruyun. Bosch, örneğin BitLocker disk şifrelemesi gibi ek önlemler önerir.
- Mobile Access sunucusunu Hizmet Reddi (DoS) saldırılarına karşı koruyun. Hız sınırlayıcı gibi korumalar sağlayan güvenli bir ağ ortamının parçası olmalıdır.

- Teknisyen davetiyesi QR kodlarını Yönetici kimlik bilgileri olarak kabul edin. Etkin teknisyen kimlik bilgileri bulunan çalıntı bir teknisyen telefonu, bir saldırganın Mobil Erişim okuyucularını kötü amaçla yeniden yapılandırmasını sağlayabilir.
  - Okuyucu kurulumu için teknisyenlere derhal davetiye gönderin ve kurulum tamamlanır tamamlanmaz bu kimlik bilgilerini sildiklerinden emin olun.
  - E-postayla gönderilen davetiyeler yerine "Ekrandaki QR kodlarını tara" işlevini kullanın. İstenen teknisyenin kimlik bilgisini hemen yüklediği emin olun.

5.10 Sistemi yedekleme

VisMgmt, ana giriş kontrolü sistemi için yardımcı bir web uygulamasıdır. Sistem veritabanlarının yedeklenmesiyle ilgili ana giriş kontrolü sistemi belgelerine başvurun.

6 Çalışma

6.1 Kullanıcı rollerine genel bakış

Kullanıcı türü	Kullanım örnekleri
Danışma görevlisi	Yeni ziyaretleri ve ziyaretçileri kaydetme Ziyaretleri onaylama ve reddetme Ziyaretçileri kara listeye alma Ziyaretçi kartlarını atama ve atamayı kaldırma İlişkili belgeleri yönetme Binadaki ziyaretçi sayısını izleme
Ziyaretçi	Kendi kendine kayıt ve ön kayıt Ziyaretçi profili oluşturma ve sürdürme Belgeleri imzalama
Ziyaret edilen kişi	Ziyaretlerin ve ziyaretçilerin programlarını ve listelerini yönetme Ziyaretlerin ön kaydını yapma
Yönetici	Genel ayarlar yapma Aracın davranışını ve kullanıcı arayüzünü özelleştirme Ayrıca: Tüm Resepsiyonist kullanım senaryoları

6.2 Panoyu kullanma

Pano, tüm diğer iletişim kutularına yol gösteren merkezi bir iletişim kutusu olan ana ekrandır.

Genel bakış ve hızlı filtreler
Panonun en üstü, o gün yapılan ziyaretlerin hızlı bir özetini içerir. Bu, kullanıcının binadaki ziyaretçi sayısını kolayca izlemesini sağlar.

Bugün beklenen ziyaretçiler: _%	**Binaya giren ziyaretçiler: _%**	**Bugün çıkış yapacak ziyaretçiler**	**Çıkış zamanı geçen ziyaretçiler**
`<current count> / <total capacity>`	`<current count> / <total capacity>`	`<current count>`	`<current count>`

Ziyaret tablosunu başlığın anlamı doğrultusunda filtre uygulamak için başlıklardan herhangi birine tıklayın. Örneğin, yalnızca bir kartın atandığı ziyaretçilere bakmak için **Giriş yapan ziyaretçiler**'e tıklayın.
`<total capacity>` değeri, sistem yöneticisi tarafından yapılan yapılandırma ayarıdır. Bkz. *Yapılandırma için Ayarlar menüsünü kullanma, sayfa 29*.

6.2.1 Kişi sayfasına genel bakış

Panoda, belirli bir kişinin adına tıklayın. Kişisel verilerin olduğu bir iletişim kutusu açılır. Veriler açılır. Bu kişi sayfasına genel bakış alanında, dört kişisel veri alanı bölümü vardır:
- Kimlik görüntüsü
- Kimlik belgesi
- Genel bilgiler
- Belgeler

6.2.2 Ziyaretler tablosu

Tablodaki her satır, ziyaret için bir randevuyu temsil eder.

- Sütun başlığına tıklayarak tabloyu herhangi bir sütundan sıralayabilirsiniz.
- Klavyeyi ve fareyi kullanarak tek seferde tek tek ziyaretleri ya da birden fazla ziyaret seçebilirsiniz:
  - Tek tek satırların birden fazla seçimi için CTRL tuşuna basarken tıklayın.
  - Seçimden kaldırmak için zaten seçili bir satırı Shift tuşuna basarken tıklayın.
  - Bitişik çizgilerin birden fazla seçimi için Shift tuşuna basarken tıklayın
- Tabloya yeni ziyaretler ekleyebilirsiniz
- İşlem düğmelerine tıklayarak ziyaret ve ziyaretçi ayrıntılarını işleyebilirsiniz
  - Ziyareti onayla
  - Ziyareti reddet
  - Ziyaretçiye kartlar ata
  - Ziyaret ve ziyaretçi ayrıntılarını düzenle
- Tüm verileri bir .CSV veya .XLSX dosyasına aktarabilirsiniz. Yalnızca bazı belirli veriler isteniyorsa filtre işlevini kullanın. İstenen verileri seçerek dışa aktarmak mümkün değildir. Yalnızca filtrelenmiş geçerli hatlar .CSV veya .XLSX dosyasına dışa aktarılabilir.

Yatay araç çubuğu aşağıdaki işlevlere sahiptir:

Etiket	İşlev
1 N **giriş**	Ziyaretlerin toplam sayısı N (her ziyaret, tablodaki bir satırdır).
2 **Arama**	Tablodaki ziyaretler arasından rastgele metin arayın
3	Tabloya en son eklenen ziyaretleri göster.
4	Filtre kriterlerini seçmek için bir iletişim kutusu açın
5	Tabloyu varsayılan görünümüne sıfırlayın ve tüm filtreleri geri döndürün.
6 **Kart atamasını kaldır**	Bağlı bir kayıt okuyucusu kullanarak atanan kartların atamasını kaldırma iletişim kutusunu açın.
7	Tabloda yeni bir ziyaret girişi oluşturmak için bir iletişim kutusu açın

Etiket	İşlev
...	Filtre uygulanmış ziyaretlerin yanı sıra belgeleri çeşitli dosya biçimlerine; örneğin `CSV` ve `.XLSX`, dışa aktarmak için menünün üç nokta simgesine tıklayın. Veri güvenliği nedenleriyle yalnızca istemciniz güvenli bir sertifikalı HTTPS bağlantısında çalışıyorsa dışa aktarabilirsiniz.

6.2.3 Tablo sütunları ve eylemleri

Sütunlar

Sütun	Değer	Açıklama
Durum	 Beklenen ziyaret  Onaylanan ziyaret  Reddedilen ziyaret  Atanan kart  Kartın süresi doldu  Biten ziyaret (Ziyaretçinin kartları alındı ve ziyaretçi tesisten ayrıldı)	Ziyaretin durumunu yansıtan bir simge
Name (Ad)	Köprü olarak ziyaretçi adı	Ziyaretçinin ayrıntılarını ve geçerli ziyaretlerini görüntülemek için köprüye tıklayın.
Beklenen varış	Tarih ve saat	Ziyaretçinin beklenen varış tarihi ve saati
Beklenen ayrılış	Tarih ve saat	Ziyaretçinin beklenen ayrılma tarihi ve saati
Giriş yapıldı	Tarih ve saat	Ziyaretçinin ilk kartının atamasının tarih ve saati.
Çıkış yapıldı	Tarih ve saat	Ziyaretçinin son kart atamasını kaldırma işleminin tarih ve saati.

Sütun	Değer	Açıklama
Kart numaraları	Sayısal	Bu ziyaretçiye atanan kartların sayısı.
İşlemler	Simgeler	Aşağıdaki ayrı tabloyu göster

İşlemler

Simge	İşlev
	Ziyareti **onaylayın**. NOT: Kara listede ziyaretçilere bir kart atanamaz. Önce ziyaretçiyi kara listeden kaldırın veya geçici olarak hariç tutun. Bkz. *Kara listeye ekleme, bu listeden kaldırma ve muaf tutma, sayfa 51*
	Ziyareti **reddedin**. Bu düğme, ziyaretçi giriş yaptıktan sonra, yani zaten bir kartı varsa, devre dışı bırakılır.
	Ziyaretçiye bir veya daha fazla kart **atama**
	Ziyaret olayını ve/veya ziyaretçi kimlik bilgilerini **düzenleme**

6.3 Danışma görevlisi

6.3.1 Danışma görevlisi rolünde oturum açma

1. Tarayıcınızda, oturum açma ekranı için `https://`<My_VisMgmt_server>`:5706/main/` bağlantısını açın.
2. Rolünüz için gerekli haklara sahip bir hesabın kullanıcı adını girin.
   Hesabınız yoksa sistem yöneticinize başvurun.
3. Şifreyi girin.
4. **Oturum aç** düğmesine tıklayın.

6.3.2 Ziyaretleri arama ve filtreleme

VisMgmt panosunda, ziyaretler tablosunun üzerindeki araç çubuğunda.

Ara

Adları ve ziyaret edilen kişileri aramak için arama kutusuna alfa sayısal metin girin ve Geri tuşuna basın.

Filtreleme

- Geçerli saate en yakın ziyaretleri görmek için **En son** düğmesine tıklayın
- Ziyaret durumu, giriş ve çıkış tarihleri ve kart numaralarından karmaşık filtre oluşturmak için **Filtrele**'ye tıklayın.
  - Açılır iletişim kutusuna istenen filtre kriterlerini girin
  - **Uygula**'ya tıklayın
    Sistem, ziyaretler tablosunu yalnızca filtre ölçütüne uyan randevulara karşı azaltır.
- Tüm filtre ölçütlerini silmek için **Sıfırla**'ya tıklayın.

6.3.3 Ziyaretleri kaydetme

Giriş

Bir danışma görevlisi, ziyaretleri kaydetmek için iki temel senaryoya sahiptir:

- **A:** Ziyaretçi, kendi ziyaretçi kimliğini oluşturmak ve belgeleri karşıya yüklemek için ziyaretçi hizmet bankosunu kullandığında, danışma görevlisinin yalnızca eksik olan gerekli bilgileri ve imzaları tamamlaması ve ziyaretçiye bir kart ataması gerekir.
- **B:** Ziyaretçi, ziyaretçi hizmet bankosunu geçerek doğrudan resepsiyona yaklaştığında danışma görevlisi, ziyaretçi formunu baştan sona doldurur: gerekli bilgileri toplar, gerekli bilgiler için imzaları toplama ve ziyaretçiye kart atama.

A senaryosu, **B** senaryosunun bir alt kümesidir, yani eksiksiz senaryo **B** burada açıklanır. Bir ziyaretçi tarafından hizmet bankosu kullanımı, kendi bölümünde açıklanmaktadır. Bkz. *Hizmet bankosu moduna giriş, sayfa 54*.

Prosedür

VisMgmt panosunda, ziyaretler tablosunun üzerindeki araç çubuğunda.

1. Ziyaretler tablosuna ziyaret randevusu eklemek için  öğesine tıklayın.
2. **Kişisel Veriler** iletişim kutusunda, ziyaretçilerin ihtiyaç duyduğu verileri girin. Zorunlu alanlar yıldız işaretiyle (*) işaretlenmiştir.
   Danışma görevlisinin iş istasyonunda varsa, bir belge tarayıcısı aracılığıyla verileri manuel olarak ancak daha hızlı ve doğru şekilde girebilirsiniz. Desteklenen çevresel cihazlarla ilgili ayrıntılar için bkz. *Çevre donanımları, sayfa 24*.
   - **Genel bilgiler**
     - Önceki ziyarette oluşturulan bir ziyaretçi profilinin tamamını bulun ve yükleyin.
       Profilleri bulmak için **Soyadı*** alanında bulunan  (ara) simgesine tıklayın. Ziyaretçi profili oluşturulduğunda, ileride ziyaret amacıyla kayıt işlemini hızlandırmak için ziyaretçinin dikkatlice kaydetmesi gereken benzersiz bir alfa sayısal kod alır.
     - Aksi takdirde, verileri elle girin.
   - **Kimlik fotoğrafları**
     - Dosya sisteminden bir fotoğrafı **karşıya yükleyin**.
     - Bağlı bir web kamerasından ziyaretçinin fotoğrafını **çekin**.
   - **Kimlik belgeleri**
     - Belge tarayıcısı (varsa) verilerini okumak ve iletişim kutusundaki ilgili veri alanlarını otomatik olarak doldurmak için **Belge tara**'ya tıklayın.
     - Aksi takdirde, sisteminizde bir belge tarayıcısı yoksa, metni elle girin.
   - **Yasal belgeler**
     - Ziyaretçinin hizmet bankosunda elektronik olarak imzaladığı belgeleri yükleyin.
     - Sisteminizde ziyaretçi hizmet bankosu yoksa dosya sisteminde depolanan gerekli PDF belgelerini (ziyaretçinin imzasıyla birlikte) yazdırın ve dosyalayın.
3. **Ziyaretler** iletişim kutusuna ilerlemek için **İleri**'ye tıklayın.
4. **Ziyaretler** iletişim kutusunda, **Geçerli ziyaret** bölmesinde, sitenizin gerektirdiği verileri girin. Zorunlu alanlar yıldız işaretiyle (*) işaretlenmiştir.
   - **Ziyaretçi türü** seçin.
     Bu, **Ziyaretçi** (varsayılan) veya ana giriş kontrolü sisteminde bir **Kişi türü** olarak tanımlanan **Ziyaretçi** özelleştirilmiş bir alt sınıfıdır.
   - **Ziyaret edilen kişi** altında ziyaret edilen çalışanın adını seçin.
     - Ana giriş kontrolü sisteminin yalnızca kart sahiplerini seçmeyi unutmayın.
     - İpucu, tanımaya yardımcı olması için kişinin e-posta adresini görüntüler.

– Ziyaretçiye tesis içinde eşlik edilmesi gerekiyorsa lütfen **Eskort** altında eşlik edecek çalışan adını seçin.
  – Ana giriş kontrolü sisteminin yalnızca kart sahiplerini seçmeyi unutmayın.
  – İpucu, tanımaya yardımcı olması için kişinin e-posta adresini görüntüler.
– Ziyaretçinin kapıdan geçmesi için ek süre gerekiyorsa **Uzatılmış kapı açılma süresi** onay kutusunu seçin

5. **Kaydet**'e tıklayın.
   Tüm zorunlu alanlar tamamlanana kadar verileri kaydedemeyeceksiniz.

Bkz.
– *Çevre donanımları, sayfa 24*

6.3.4 Ziyaretleri onaylama ve reddetme

Arka plan: Fiziksel kartları onaylama
Bir ziyaretçiye kart atamadan önce bir ziyareti onaylamanız gerekir.

Arka plan: Mobil kimlik bilgilerini onaylama
Fiziksel kart atamaya benzer şekilde ziyaret tarihinde mobil bir kimlik bilgisi oluşturabilir ve paylaşabilirsiniz.
– **Not:** Mobil kimlik bilgisi siz ziyareti onaylayana kadar çalışmaz.
Alternatif olarak, mobil kimlik bilgisini oluşturup önceden paylaşabilirsiniz. Ziyaretçi danışmaya ulaştığında, kimlik bilgisini son olarak etkinleştirmek için ziyareti aşağıda açıklandığı gibi onaylayın.
– **Not:** Mobil kimlik bilgisi siz ziyareti onaylayana kadar çalışmaz.
– Ziyaret için tahmini ayrılış süresini ayarladıysanız bu süre geçerli olur.
– Tahmini ayrılış süresini ayarlamadıysanız varsayılan değer olan saat sayısı (8) geçerli olacaktır. Yöneticiler bu varsayılan ayarı **Ayarlar** menüsünde değiştirebilir.

Onaylama ve reddetme prosedürleri
Ziyareti onaylamak veya reddetmek için iki yer vardır:
– panodaki ziyaret tablosunda
– ziyaret düzenleyicide

Panodaki ziyaret tablosunda:

– **Onayla**: Ziyaretler tablosunda, tablodan bir satır seçin ve  öğesine tıklayın. Onay açıldıktan sonra simge, ziyaretin onaylanıp onaylanmadığını göstermek için simge griye döner.

– **Reddet**: Ziyaretler tablosunda, tablodan bir satır seçin ve  öğesine tıklayın. Onay açıldıktan sonra, ziyaretin hala onaylanması gerektiğini göstermek için **Onayla** simgesi maviye geri döner.

Ziyaret düzenleyicide:

1. Panoda, ziyaretler tablosunda tablodan bir satır seçin ve ziyareti düzenlemek için  öğesine tıklayın.
2. **Kişisel Veriler** iletişim kutusunda **İleri**'ye tıklayın.
3. **Ziyaretler** iletişim kutusunda **Onayla** veya **Reddet** düğmesine tıklayın.
4. Açılır penceredeki eyleminizi onaylayın.

6.3.5 Fiziksel kimlik bilgilerini atama

Giriş

Tesiste izin verdiğiniz her ziyaretçiye bir ziyaretçi kartı atayın. Gerekirse tek bir ziyaretçiye birden fazla kart atayabilirsiniz.

– Bir ziyaretin **giriş** zamanı ilk kartın atama zamanı olur.
– Bir ziyaretin **çıkış** zamanı, ziyaretçinin hala ziyaretçiye atanmış olan son kartın kaldırma zamanı olacaktır.

Danışma görevlisinin bilgisayarına bir kayıt kartı okuyucusu bağlıysa danışma görevlisi, panoya kartları kolayca atayıp atamasını kaldırabilir.

Yine de böyle bir okuyucu yoksa, ziyaret düzenleyicisi kart numaraları atamanın bir yolunu sağlar.

Uyarı!

Kara listeye alınan kişiler kart alamaz

Kara listede bulunan ziyaretçilere kart atama olanağı yoktur. Bir kart atamaya çalışmadan önce, ziyaretçiyi kara listeye kaldırın veya ziyaretçi için geçici bir muafiyet oluşturun.

Panodan kart atama (kayıt okuyucusu gerektirir)

1. Kayıt okuyucuya sunmak için hazır bir fiziksel ziyaretçi kartı bulundurun.
2. Ziyaretler tablosunda, ziyareti onaylayın. Bkz. *Ziyaretleri onaylama ve reddetme, sayfa 46*
3. Ziyaret satırını seçin ve  öğesine tıklayın.
4. Kayıt okuyucunun kullanılması için açılır penceredeki yönergeleri izleyin.

Panodan kart atamasını kaldırma (kayıt okuyucusu gerektirir)

1. Kart sahibinin fiziksel kartını alın ve kayıt okuyucusuna sunmak için hazır bulundurun.
2. Araç çubuğunda **Kart atamasını kaldır**'a tıklayın. 
3. Kayıt okuyucunun kullanılması için açılır penceredeki yönergeleri izleyin.

Ziyaret düzenleyicide kart atama

1. Panoda, ziyaretler tablosunda tablodan bir satır seçin ve o ziyareti düzenlemek için  öğesine tıklayın.
2. **Kişisel veriler** iletişim kutusunda **İleri**'ye tıklayın.

3. **Ziyaretler** iletişim kutusunda, ziyaret henüz onaylanmadıysa **Onayla**'ya tıklayın.
4. Bağlı bir kayıt okuyucusu varsa **Kartı oku**'ya tıklayın ve kayıt okuyucunun kullanımı için açılan penceredeki talimatları izleyin.

– Aksi takdirde hâlâ mevcut olan ziyaretçi kartlarının listesini görüntülemek için **Serbest kartları göster**'e tıklayın.
Alternatif olarak, yazılı sayılarla sıralanmamış fiziksel kartlarınız varsa herhangi bir kart seçip **Arama** aracını kullanarak listede hızlıca numarasını bulabilirsiniz.

– O kartı geçerli ziyaretçiye atamak için bir kart numarasının yanındaki  düğmesine tıklayın.
– Gerekirse daha fazla kart atamak için son adımları tekrarlayın.

5. Kart atamalarıyla geçerli ziyareti kaydetmek için **Kaydet**'e tıklayın.

Ziyaret düzenleyicide kart atamasını kaldırma

1. Panoda, ziyaretler tablosunda tablodan bir satır seçin ve o ziyareti düzenlemek için  öğesine tıklayın.
2. **Kişisel veriler** iletişim kutusunda **İleri**'ye tıklayın.
3. **Ziyaretler** iletişim kutusunda, Ziyaretçi kartları bölmesinde, atamasını kaldırmak istediğiniz kartın yanındaki  öğesine tıklayın ve açılır penceredeki eyleminizi onaylayın.
Atamasını kaldırmak istediğiniz tüm kartları kaldırdığınızda bu adımı tekrarlayın.
4. Kart atamalarıyla geçerli ziyareti kaydetmek için **Kaydet**'e tıklayın.
5. Ziyaretçiye atanan son kartı kaldırdığınızda sistem, bu tarihi ve saati ziyaretçinin çıkış zamanı olarak kaydeder.

Ziyaretler tablosunda, bu ziyaret kaydının durumu  olur

Bkz.

– *Yapılandırma için Ayarlar menüsünü kullanma, sayfa 29*
– *Ziyaretleri kaydetme, sayfa 45*
– *Ziyaretleri onaylama ve reddetme, sayfa 46*

6.3.6 Mobil kimlik bilgilerini atama

Ön koşullar

– Mobile Access sisteminize yüklenip yapılandırılmıştır.
  – Talimatlar için, bu belgenin kurulum bölümündeki ilgili kısma bakın.
– Alıcı kişi Mobile Access uygulamasını yüklemiştir ve akıllı cihazında çalışıyordur.
  – Talimatlar için, bu belgenin kurulum bölümündeki ilgili kısma bakın.

Prosedür

Doğrudan pano simgesinden ya da kişi sayfasına genel bakıştan mobil kimlik bilgileri atamak mümkündür.

Pano alanında:

1. Mobil kimlik bilgilerini alacak kişiye ait satırı seçin

2. Seçili satırda  simgesine tıklayın

Kişi sayfasına genel bakıştan:

1. **Pano**'da kişinin adını seçin ve kişi sayfasına genel bakış açılır.
2. **Credential** (Kimlik bilgileri) > **Add mobile access** (Mobil erişim ekle) sekmelerini seçin.

Aşağıdaki talimatlara uyun:

1. Seçenekler için büyük simgelerden birini seçin:

– **QR kodu**
veya
– **Davetiye e-postası**

2. **QR kodu seçeneğini** seçerseniz:

– Sistem bir QR kodu görüntüler
– Kişi, kendi taşınabilir cihazındaki Mobile Access uygulaması ile QR kodunu tarar
– Kimlik bilgisinin işe yaraması için ziyareti **onaylamanız** gerekir.
Talimatlar için şu bölüme bakın: *Ziyaretleri onaylama ve reddetme, sayfa 46*
– Uygulama çalıştığı sürece mobil cihaz bir fiziksel giriş kartı gibi çalışır

3. **Davetiye e-postası** seçeneğini seçerseniz:

– Varsayılan olarak, program seçilen kişi için tanımlanan e-posta adresini seçer. Gerekirse alternatif bir e-posta adresi girin
– Sistem seçilen adrese bir e-posta gönderir
– Kişi, e-postayı Mobile Access uygulamasının çalıştığı mobil cihazında alır
– Kişi e-postadaki bağlantıyı açar
– Kimlik bilgisinin işe yaraması için ziyareti **onaylamanız** gerekir.
Talimatlar için şu bölüme bakın: *Ziyaretleri onaylama ve reddetme, sayfa 46*
– Uygulama çalıştığı sürece mobil cihaz bir fiziksel giriş kartı gibi çalışır

Düzenleme iletişim kutularındaki prosedür

1. Mobil kimlik bilgilerini alacak kişiye ait satırı seçin
2. Seçili satırda  simgesine tıklayın

– Düzenleme iletişim kutusu açılır

3. VisMgmt'de, **İleri**'ye tıklayarak **Ziyaret ayrıntıları** ekranına geçin
4. **Add** (Ekle) düğmesine tıklayın**Mobile Access**
5. Seçenekler için büyük simgelerden birini seçin:

– **QR kodu**
veya
– **Davetiye e-postası**

6. **QR kodu seçeneğini** seçerseniz:

– Sistem bir QR kodu görüntüler
– Kişi, kendi taşınabilir cihazındaki Mobile Access uygulaması ile QR kodunu tarar
– Kimlik bilgisinin işe yaraması için ziyareti **onaylamanız** gerekir.
Talimatlar için şu bölüme bakın: *Ziyaretleri onaylama ve reddetme, sayfa 46*
– Uygulama çalıştığı sürece mobil cihaz bir fiziksel giriş kartı gibi çalışır

7. **Davetiye e-postası** seçeneğini seçerseniz:

– Varsayılan olarak, program seçilen kişi için tanımlanan e-posta adresini seçer. Gerekirse alternatif bir e-posta adresi girin
– Sistem seçilen adrese bir e-posta gönderir
– Kişi, e-postayı Mobile Access uygulamasının çalıştığı mobil cihazında alır

– Kişi e-postadaki bağlantıyı açar
– Kimlik bilgisinin işe yaraması için ziyareti **onaylamanız** gerekir.
  Talimatlar için şu bölüme bakın: *Ziyaretleri onaylama ve reddetme, sayfa 46*
– Uygulama çalıştığı sürece mobil cihaz bir fiziksel giriş kartı gibi çalışır

Bkz.
– *Mobil Erişimi Yükleme, sayfa 17*
– *Mobil Erişim uygulamalarını yükleme, sayfa 16*

6.3.7 Kimlik bilgilerin atamasını kaldırma

Panodan kart atamasını kaldırma (kayıt okuyucusu gerektirir)

1. Kart sahibinin fiziksel kartını alın ve kayıt okuyucusuna sunmak için hazır bulundurun.
2. Araç çubuğunda **Kart atamasını kaldır**'a tıklayın. 
3. Kayıt okuyucunun kullanılması için açılır penceredeki yönergeleri izleyin.

Kimlik bilgileri düzenleyicisinde bir kartın atamasını kaldırma

1. Panoda, ana tablodan bir satır seçin ve kart sahibini düzenlemek için  simgesine tıklayın.
2. Düzenleme iletişim kutusundaki **Çalışan kartları** sütununda, atamasını kaldırmak istediğiniz kartın yanındaki  simgesine tıklayın ve açılır pencerede eyleminizi onaylayın.
   Bu adımı, atamasını kaldırmak istediğiniz tüm kartları kaldırana kadar tekrarlayın.
3. Kart atamalarıyla geçerli ziyareti kaydetmek için **Kaydet**'e tıklayın.

6.3.8 Kart olmadan giriş ve çıkış yapma

Giriş

Ziyaretçilerin yakın refakatçıları varsa veya yalnızca herkese açık alanlara girebiliyorlarsa her ziyaretçiye ayrı kart verilmesine gerek olmayabilir. Böyle durumlar için, ziyaretçilerin kartlar olmadan giriş ve çıkış yapabilme seçeneği bulunur. Güvenlik nedenleriyle bu seçenek varsayılan olarak devre dışıdır.

Ön koşul.

Sistem yöneticiniz **Ayarlar** > **Danışma görevlisi > Ziyaretler** iletişim kutusunda **Kartsız giriş ve çıkış yapma** özel seçeneğini etkinleştirmiş olmalıdır. Talimatlar için *Yapılandırma için Ayarlar menüsünü kullanma, sayfa 29* yapılandırma bölümüne bakın.

İşlem

Seçenek etkinleştirildiğinde aşağıdaki durum gerçekleşir:
– Hizmet bankosu bilgisayarında kendi kendine kayıt yapan tüm ziyaretçiler aynı anda otomatik olarak ziyareti onaylar ve giriş yapar.
– Sistem, giriş tarihini ve saatini kayıt zamanına göre ayarlar.

– **Kartsız giriş/çıkış yapma** düğmesi, aynı ziyaret için ziyaret düzenleyicide ve panoda görünür.

Prosedür: Kart olmadan bir ziyaretçinin girişini yapma
Ziyaretçi hizmet bankosunda kendi kaydını yapamazsa ancak kartsız giriş yapması gerekiyorsa:
1. *Ziyaretleri kaydetme, sayfa 45* bölümünde açıklandığı gibi ziyareti manuel olarak kaydedin
2. Ziyaretler tablosundaki panoda, tablodaki ziyaretçinin adına veya o ziyareti düzenlemek için  öğesine tıklayın.
3. **Kişisel veriler** iletişim kutusunda **İleri**'ye tıklayın.
4. **Ziyaretler** iletişim kutusunda, **Ziyaretçi kartları** bölmesinde, **Kart olmadan giriş yap** öğesine tıklayın.

Prosedür: Kart olmadan bir ziyaretçinin çıkışını yapma
Kartsız bir ziyaretçi tesisten ayrılırsa:
1. Ziyaretler tablosundaki panoda, tablodaki ziyaretçinin adına veya o ziyareti düzenlemek için  öğesine tıklayın.
2. **Kişisel veriler** iletişim kutusunda **İleri**'ye tıklayın.
3. **Ziyaretler** iletişim kutusunda, **Ziyaretçi kartları** bölmesinde, **Kart olmadan çıkış yap** öğesine tıklayın.

Bkz.
– *Ziyaretleri kaydetme, sayfa 45*

6.3.9 Kara listeye ekleme, bu listeden kaldırma ve muaf tutma

Tesise girişine izin verilmeyen ziyaretçiler kara listeye eklenebilir. Ziyaretçi kara listeye dahil olduğu sürece o kişiye kart atayamazsınız. Bir kart atamak için ziyaretçinizi istediğiniz zaman kara listeden çıkarabilirsiniz veya geçici bir istisna verebilirsiniz.

Kara Listeye Alma
1. Panoda, ziyaretler tablosunda tablodan bir satır seçin ve ziyareti düzenlemek için  öğesine tıklayın.
2. **Kişisel Veriler** iletişim kutusunda **Kara Liste**'ye tıklayın.
3. Açılır pencerede, bu kişiyi gerçekten kara listeye almak istediğinizi onaylayın.
4. Sonraki açılır pencerede kara liste için bir neden girin ve onaylayın.

– **Kara Listede Eklendi** başlığı, ziyaret düzenleyicisinde, 

, görünür
– Başlık altında iki düğme görünür: bir, kara listeden ziyaretçiyi kaldırmak ve biri de geçici istisna vermek içindir.
– Ziyaretler tablosunda kara listeye eklenen her ziyaretçinin adı bir uyarı üçgeni ile görüntülenir. Örneğin: 

Kaldırma ve muaf tutma

1. Panoda, ziyaretler tablosunda, ziyaretçinin kara listeye eklenmiş olarak işaretlendiği tablodan bir satır seçin ve ziyareti düzenlemek için  öğesine tıklayın.
2. **Kişisel Veriler** iletişim kutusunda aşağıdakilerden birine tıklayın:

– Ziyaretçiyi kara listeden kalıcı olarak kaldırmak için **kaldır** seçeneğini kullanın.
– Ziyaretçiyi kara listede tutmak ancak yalnızca bu ziyaret için bir kart atamaya izin vermek için **muaf tutun**.

3. Açılır penceredeki eyleminizi onaylayın.

6.3.10 Ziyaretçi profillerini sürdürme

Sistem, ziyaretçilerin kendileri ya da danışma görevlileri veya yöneticiler silene kadar ziyaretçi profillerini saklar.
Sistem ayarlarında bir saklama süresi tanımlandıktan sonra (varsayılan değer 12 aydır), sistem ziyaret kayıtlarını siler.
Ziyaretçi veya danışma görevlisi yeni bir ziyaretçi profili oluşturduğunda profil, benzersiz bir alfa sayısal kod alır. Ziyaretçiler, ziyaretçi hizmet bankosunda bu kodla oturum açmalarını sağlar ve bu nedenle kendi profillerini korumak için erişim elde edebilirler.

Uyarı!
Ziyaretçi kimliklerini koru
Kişisel verilere erişim sağladığı için, ziyaretçi kimliklerini yetkisiz erişimlere karşı dikkatlice koruyun.

6.3.11 Ziyaret kayıtlarını görüntüleme

1. Panoda, ziyaretler tablosunda tablodan bir satır seçin ve o ziyareti düzenlemek için  öğesine tıklayın.
2. **Kişisel Veriler** iletişim kutusunda **İleri**'ye tıklayın
3. **Geçerli ziyaret** iletişim kutusunda **Tüm ziyaretleri göster**'e tıklayın
   Geçerli ziyaret iletişim kutusu önceki ziyaretlerin listesini gösterir.

6.4 Ziyaret edilen kişi

Ziyaret edilen kişi, ziyaretleri alan çalışanlardır. Kendi randevularını kaydedebilirler ve ziyaretçiler ve ziyaretlerinin kayıt ayrıntıları için sisteme atabilirler: geçmiş, bugünkü ve gelecekteki.

6.4.1 Ziyaret edilen kişi rolünde oturum açma

1. Tarayıcınızda, oturum açma ekranı için `https://<My_VisMgmt_server>:5706/main/` bağlantısını açın.
2. Rolünüz için gerekli haklara sahip bir hesabın kullanıcı adını girin.
   Hesabınız yoksa sistem yöneticinize başvurun.
3. Şifreyi girin.

4. **Oturum aç** düğmesine tıklayın.

6.4.2 Arama ve filtreleme

Ziyaret edilen kişi panosu için araç çubuğu aşağıdaki işlevleri içerir:

Etiket	İşlev
1 N **giriş**	Ziyaretlerin toplam sayısı N (her ziyaret, tablodaki bir satırdır).
2 **Arama**	Tablodaki ziyaretler arasından rastgele metin arayın
3	Tabloya en son eklenen ziyaretleri göster.
4	Filtre kriterlerini seçmek için bir iletişim kutusu açın
5	Tabloyu varsayılan görünümüne sıfırlayın ve tüm filtreleri geri döndürün.
6	Tabloda yeni bir ziyaret girişi oluşturmak için bir iletişim kutusu açın

Ara

Adları ve ziyaret edilen kişileri aramak için arama kutusuna alfa sayısal metin girin ve Geri tuşuna basın.

Filtreleme

- Geçerli saate en yakın ziyaretleri görmek için **En son** düğmesine tıklayın
- Ziyaret durumu, giriş ve çıkış tarihleri ve kart numaralarından karmaşık filtre oluşturmak için **Filtrele**'ye tıklayın.
  - Açılır iletişim kutusuna istenen filtre kriterlerini girin
  - **Uygula**'ya tıklayın
    Sistem, ziyaretler tablosunu yalnızca filtre ölçütüne uyan randevulara karşı azaltır.
- Tüm filtre ölçütlerini silmek için **Sıfırla**'ya tıklayın.

6.4.3 Ziyaretleri kaydetme

İlk kez gelen ziyaretçinin ziyaret randevusu kaydetmek için:
VisMgmt panosunda, ziyaretler tablosunun üzerindeki araç çubuğunda.

1. Ziyaretler tablosuna satır eklemek için  öğesine tıklayın

2. **Kişisel Veriler** iletişim kutusundaki **Genel bilgiler** bölümünde, tesisinizin ziyaretçilerden ihtiyaç duyduğu kişisel verileri girin.
3. **Ziyaret ayrıntıları** bölümünde, genellikle beklenen varış ve ayrılış süreleri ile birlikte ziyaret nedeni gibi gerekli ayrıntıları girin.
4. Ziyaret randevusunu kaydetmek için **Kaydet**'e tıklayın.
   Ziyaretler tablosunda bir satır olarak panoda ziyaret görünür.

6.4.4 Ziyaret randevularını kopyalama

Aynı ziyaretçiyle başka bir randevu planlamak için

1. VisMgmt panosunda, ziyaretler tablosunda aynı ziyaretçiye sahip mevcut bir randevuyu bulun.
2. Satırın sonundaki küçük  simgesine tıklayın.
3. **Kişisel Veriler** iletişim kutusundaki **Ziyaret ayrıntıları** bölümünde, genellikle beklenen varış ve ayrılış zamanları ile birlikte ziyaret nedeni gibi gerekli ayrıntıları girin.
4. Ziyaret randevusunu kaydetmek için **Kaydet**'e tıklayın.
   Ziyaretler tablosunda bir satır olarak panoda ziyaret görünür.

6.5 Ziyaretçi

Ziyaretçiler, kendi ziyaretçi profillerini oluşturmak için sistemi tesisteki hizmet bankosu modunda kullanabilirler ve ziyaretçi kartlarını toplamaya geçmeden önce gerekli belgeleri imzalayabilirler.

6.5.1 Hizmet bankosu moduna giriş

Ziyaretçiler, giriş denetimli binanın resepsiyon alanında serbestçe erişilebilen bir bilgisayarda, genellikle ziyaretlerini kaydeder ve kendi profillerini oluşturur. Güvenlik nedenleriyle, bilgisayarın web tarayıcısı hizmet bankosu modunda çalışır. Bu da yalnızca VisMgmt erişimi sunarken birden çok sekmeye, tarayıcı ayarlarına veya bilgisayarın işletim sistemine erişim sunmaz. Tüm desteklenen tarayıcılar, hizmet bankosu modunu sunar ancak bunun tam yapılandırması tarayıcıya bağlıdır.

Hizmet bankosu bilgisayarı, **Bosch Çevresel Cihazlar** eklentisini çalıştırır. Bu da kimlik belgelerinin ve imzaların taranması için çevresel cihazlara fiziksel olarak bağlantı sağlar.

– Hizmet bankosu modu, `https://`<My_VisMgmt_server>`:5706` şeklindedir
– Bunun aksine; Yönetici, Danışma Görevlisi veya Ziyaret Edilen Kişi olarak oturum açma URL'si `https://`<My_VisMgmt_server>`:5706/main/` şeklindedir

6.5.2 Ziyaretçi profili oluşturma: Kendi kendine giriş

İlk kez gelen ziyaretçiler

Kesin prosedürün; hizmet bankosu bilgisayarında bulunan belge ve imza tarayıcıları ve fotoğraf kameraları gibi çevresel cihazlara bağlı olduğunu unutmayın.

1. Hizmet bankosu bilgisayarındaki karşılama ekranında **Ziyaretçi kimliği olmadan devam et**'e tıklayın.
2. Sonraki ekranda **Kendi kendine giriş**'e tıklayın.
3. Sonraki ekranda **Belgeyi tara**'yı seçin.
4. Ekrandaki yönergeleri izleyerek aşağıdaki gibi tesise özel gereksinimleri izleyin:

– kimlik belgeleri tarama,

– gerekli diğer yasal belgeleri imzalama,
– fotoğraf çekme.
5. Sistem, toplanan bilgileri sizin düzeltip tamamlamanız için görüntüler.
6. Sistem, özel giriş yetkilerinin gerekli olup olmadığını sorar ve gerekirse bunu danışma masasına iletir.
7. Giriş işleminin sonunda, ekran benzersiz bir ziyaretçi kimliği görüntüler.
Ziyaretçi kartınızı almak için bu kimliği, resepsiyon masasına götürün.

Uyarı!
Benzersiz ziyaretçi kimliğiniz
Ziyaretçi kimliğinizi dikkatlice not alın ve yetkisiz kullanıma karşı koruyun. Ziyaretçi profilinize giriş sağlar. Hizmet bankosu bilgisayarında oturum açmak için bu uygulamayı kullanabilir ve bir sonraki giriş işlemini hızlandırabilirsiniz.

Tekrar gelen ziyaretçiler
1. Benzersiz ziyaretçi kimliğinizle hizmet bankosunda oturum açın.
2. Sistem, gerekirse, toplanan bilgileri sizin düzeltip tamamlamanız için görüntüler.
3. Ziyaretçi kartınızı almak için resepsiyon masasına gidin.

6.6 Mobil erişim okuyucularının teknisyenlerini yetkilendirme

Giriş
Mobil erişim okuyucularının teknisyenleri BLE aracılığıyla okuyucuları taramak ve yapılandırmak için Bosch Setup Access'i kullanır.
Credential Management ve **Visitor Management**'ın yetkili operatörleri teknisyeni yetkilendirmek için teknisyen uygulamasına sanal kimlik bilgileri gönderir. Bu bölümde bu prosedür açıklanmaktadır.

Ön koşullar
– Mobile Access sisteminize yüklenip yapılandırılmıştır.
  – Talimatlar için, bu belgenin kurulum bölümündeki ilgili kısma bakın.
– Yetkiyi alan teknisyenin Bosch Setup Access uygulamasını yüklediğinden ve cihazında çalıştırdığından emin olun.
  – Talimatlar için, bu belgenin kurulum bölümündeki ilgili kısma bakın.

Prosedür

1. Ana menüden, **Teknisyen ekleme** iletişim kutusunu açmak için  simgesine tıklayın.
2. Listeye bir teknisyen eklemek için **Ekle**'ye veya mevcut bir teknisyeni silmek için  simgesine tıklayın
– **Teknisyen ekle** açılır penceresi görünür.
3. **Teknisyen ekle** açılır penceresinde, aşağıdakiler gibi gerekli ayrıntıları girin:
– Kişisel adlar, şirket adı, e-posta adresi, telefon numarası
– Not: Seçilen bir teknisyenin ayrıntılarını ileriki bir tarihte değiştirmek için  simgesine tıklayabilirsiniz.
4. **Next**'e (İleri) tıklayın

5. Seçenekler için büyük simgelerden birini seçin:
– **QR kodu**
veya
– **Davetiye e-postası**
6. **QR kodu seçeneğini** seçerseniz:
– Sistem bir QR kodu görüntüler
– Kişi, kendi taşınabilir cihazındaki Mobile Access uygulaması ile QR kodunu tarar
– Böylece teknisyenin kayıt işlemi tamamlanır
– Uygulama çalıştığı sürece mobil cihazın mobil giriş okuyucularını taramasını ve BLE ile yapılandırmasını sağlar
7. **Davetiye e-postası** seçeneğini seçerseniz:
– Varsayılan olarak, program seçilen kişi için tanımlanan e-posta adresini seçer. Gerekirse alternatif bir e-posta adresi girin
– Sistem seçilen adrese bir e-posta gönderir
– Kişi, e-postayı Bosch Setup Access'in çalıştığı mobil cihazında alır
– Kişi e-postadaki bağlantıyı açar
– Böylece teknisyenin kayıt işlemi tamamlanır
– Uygulama çalıştığı sürece mobil cihazın mobil giriş okuyucularını taramasını ve BLE ile yapılandırmasını sağlar

Davetiyeleri yeniden gönderme

1. Teknisyen ekleme iletişim kutusunda istediğiniz teknisyeni seçin.
2. Yetkiyi seçilen teknisyene QR koduyla veya e-postayla yeniden göndermek için aynı satırdaki  simgesine tıklayın.
NOT: Yalnızca teknisyen henüz etkinleştirmediyse yetkiyi yeniden gönderebilirsiniz.

6.6.1 Mobil Erişim okuyucularını sıfırlama

Yeniden yapılandırmasını etkinleştirmek için giriş okuyucularının fabrika varsayılanlarına sıfırlanması gerekebilir.
Örneğin, bir teknisyenin daha önce farklı bir site için yapılandırılmış mobil erişim okuyucularını yeniden yapılandırması gerekiyorsa bu okuyucular için sıfırlama işlemi gerekir.
Okuyucunun DIP anahtarlarını kullanarak nasıl sıfırlanacağı hakkında açıklama için LECTUS select okuyucu kılavuzuna bakın.

6.7 Mobil cihazlarda Mobil Erişim uygulamalarını kullanma

NOT: Bosch Mobile Access uygulamalarının kullanımı, ayrı **Hızlı Kullanıcı Kılavuzlarında** ilgili kullanıcılar için ayrıntılı olarak açıklanmaktadır. Bu belgeler Bosch çevrimiçi ürün kataloğundan alınabilir.

Giriş

Bosch, Mobile Access için aşağıdaki uygulamaları sağlar
– Bosch Mobile Access: Sanal bilgileri depolamak ve bunları Mobile Access için yapılandırılan okuyuculara Bluetooth aracılığıyla aktarmak için kullanılan bir kart sahibi uygulaması. Böyle bir okuyucu uygulamanın depolanmış kimlik bilgilerinden birinin geçerli olup olmadığına bağlı olarak giriş izni verir veya reddeder.
– Bosch Setup Access: Okuyucuları Bluetooth aracılığıyla taramak ve yapılandırmak için kullanılan bir teknisyen uygulaması.

Visitor Management ve Credential Management'ın yetkili operatörleri hem kart sahibi hem de teknisyen uygulamaları için sanal kimlik bilgileri gönderebilir.

Uyarı!
ÖNEMLİ: Kart sahibi ve teknisyen uygulamalarını eş zamanlı olarak çalıştırmayın
Kart sahibi uygulaması kullanılırken teknisyen uygulamasını kimsenin kullanmadığından ve bunun tersinin geçerli olmadığından emin olun.

6.7.1 Kurulum Erişimi uygulamasında RSSI eşiklerini ayarlama

Giriş

RSSI eşiği ve BLE aralığı Bosch Mobile Access bağlamında kabaca eş değer kavramlar olarak kabul edilebilir.

Mobile erişim cihazları yakındaki okuyuculara BLE sinyalleri iletir. Okuyucu yapılandırmasının önemli bir bölümü, her okuyucu için bir RSSI eşiği ayarlanmasıdır. Bu eşik, okuyucunun (R) girme isteği olarak kabul edeceği, dBm cinsinden ölçülen minimum BLE sinyal gücüne sahiptir. Okuyucu daha zayıf olan tüm BLE sinyallerini yok sayar.

RSSI değerleri, iletim cihazının türü, pil düzeyi ve yakındaki duvarların malzemesi ve kalınlığı da dahil olmak üzere birçok etkene göre büyük ölçüde farklılık gösterebilir. RSSI değeri ile verici ile alıcı arasındaki mesafe arasında doğrusal bir ilişki yoktur.

Bu nedenle, Setup Access uygulaması, okuyucunun RSSI'sını mobil cihazın geçerli konumundan ölçmesine yönelik bir araç sağlar. Aşağıdaki prosedürde bu aracın nasıl kullanılacağı açıklanmaktadır.

BLE aralığı için uygun bir eşik değeri bulduğunuzda, bu değeri okuyucu yapılandırmasında saklamak için Setup Access uygulamasını kullanın.

Prosedür

Aşağıdaki seçeneklerden birini (A veya B) kullanarak **BLE** aralığını yapılandırın:

A: Okuyucunun gösterdiği RSSI değerlerini kullanma

1. Mobil kimlik bilgisi kullanıcısının olmasını beklediğiniz noktada okuyucunun önünde durun.
2. **Geçerli aralığı kontrol et ve kullan**'a dokunun

– Bir açılır mesaj görünür. **Tamam**'a dokunun

3. Bir RSSI değeri görünür.

– Önerilen: Bu adımı aynı konumdan birkaç kez yineleyerek algılanan sinyal gücündeki sapma derecesine ilişkin bir fikir edinin.

4. Uygun bir eşik değeri bulduğunuzda **Kaydet**'e dokunun.

B: RSSI eşiğini manuel olarak ayarlama

1. RSSI eşiğine bir değer girin.
   Aşağıdaki tipik eşikler tablosuna bakın
2. **Kaydet**'e dokunun

Tipik eşik değerleri (yalnızca yaklaşık):

Mobil cihazdan okuyucuya kadar olan tahmini mesafe	**Önerilen RSSI eşiği**
Yakın (5 cm-10 cm)	-30 ... -40 dBm
Orta (0,5 m-2 m)	-50 ... -60 dBm
Uzak (>2m)	-70 ... -90 dBm

Uyarı!
RSSI değerleri, iletim cihazının türü, pil düzeyi ve yakındaki duvarların malzemesi ve kalınlığı da dahil olmak üzere birçok etkene göre büyük ölçüde farklılık gösterebilir.

Sözlük

ACS

örneğin, AMS (Access Management System) veya ACE (BIS Access Engine) gibi Bosch kartlı geçiş sistemine ait genel bir terim.

BLE

Bluetooth Low Energy, Bluetooth'a benzer bir iletişim aralığı sağlayan ancak daha düşük enerji tüketimine sahip bir kablosuz ağ teknolojisidir.

FQDN

Tam nitelikli etki alanı adı, Etki Alanı Ad Sistemi (DNS) hiyerarşisindeki mutlak konumunu ifade eden bir ağ etki alanı adıdır.

hizmet bankosu modu

Genellikle yalnızca tek bir web uygulamasına erişime izin veren ve tarayıcı ayarlarına, birden çok sekmeye ya da bilgisayarın işletim sistemine erişimine izin vermeyen son derece kısıtlı tarayıcı kullanımı modu.

Mobil Erişim

kişinin akıllı telefonu gibi mobil bir cihazda depolanan sanal kimlik bilgilerini kullanan kişilerin giriş kontrolüdür.

OSDP

Açık Denetimli Cihaz Protokolü, Güvenlik Endüstrisi Birliği (SIA) tarafından 2011'da tanıtılan bir giriş kontrol iletişim standardıdır. Şifreleme, biyometri, kullanım kolaylığı ve birlikte çalışabilirlik alanlarındaki eski protokollere göre avantajlar sunar.

RSSI

Alınan Sinyal Gücü Göstergesi (RSSI), dBm cinsinden ölçülen bir alıcı cihaz tarafından algılanan sinyal gücüne sahiptir. Mobil cihazlarda tipik olarak RSSI, bir sinyal gücü çubuk grafiğiyle gösterilir.

ziyaret edilen kişi

ziyaretçi yönetimi bağlamında, ziyaret edilen kişi, ziyaretçinin kendisi için geldiği kişidir.

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Hollanda
www.boschsecurity.com

Daha iyi bir yaşama yönelik bina çözümleri

202405132131