Credential 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 Credential Management ve Visitor Management Hakkında

Bundan sonra CredMgmt olarak anılacak Credential Management, Bosch giriş kontrolü sistemi veya ACS ile birlikte çalışan tarayıcı tabanlı bir yazılım aracıdır. Basit ve sezgisel bir kullanıcı arayüzü sayesinde, deneyimsiz operatörlerin bile çalışanların ve harici personelin erişim kimlik bilgilerini yönetmelerini sağlar. Kimlik bilgileri fiziksel kartlar veya mobil kimlik bilgileri olabilir.

Kimlik bilgisi yönetimi

CredMgmt'da ACS operatörleri hem kimlik bilgilerini hem de kimlik bilgilerinin ait olduğu çalışan kayıtlarını yönetebilir.

Varlık	Ekleme	Değiştirme	Sil	Atama/ Atamayı kaldırma
Fiziksel kimlik bilgileri				Evet
Sanal "mobil" kimlik bilgileri (Mobile Access yüklüyse)	Evet		Evet	Evet
Yetkiler				Evet
Kart sahibi kayıtları	Evet	Evet	Evet	

Ziyaretçi yönetimi

VisMgmt'da ACS operatörleri, kimlik bilgilerini, ziyaretçi kayıtlarını ve ziyaret kayıtlarını yönetir.

Varlık	Ekleme	Değiştirme	Sil	Atama/ Atamayı kaldırma
Fiziksel kimlik bilgileri				Evet
Sanal "mobil" kimlik bilgileri (Mobile Access yüklüyse)	Evet			Evet
Ziyaretçi kayıtları	Evet	Evet	Evet	
Ziyaret kayıtları	Evet	Evet	Evet	

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.

3 Yükleme ve kaldırma

3.1 Yazılım ön koşulları

CredMgmt sunucusunu ACS (birincil giriş kontrolü sistemi) ile aynı bilgisayara yükleyin. Aynı yazılım ve donanım gereksinimleri geçerlidir.
Birincil giriş kontrolü sistemi henüz kurulu değilse Credential 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.

CredMgmt ve Mobile Access kurulum programları, ACS'den ayrı olarak kendi yükleme ortamlarına sahiptir. Bosch çevrimiçi ürün kataloglarından indirilebilirler.

Uyarı!
Sabit kök sertifika gerekliliği
Aşağıdaki kurulumlara devam etmeden önce, kendi kurulum kılavuzuna göre ACS kurulumlarının eksiksiz ve lisanslı olduğundan emin olun. Bu, ACS sunucusunun kök sertifikası (kendinden imzalı veya CA tabanlı) ve kararlı uygulanmasıyla ilgili bir nihai karar içerir. Bundan sonra ACS sunucusunun kök sertifikasında yapılacak değişiklikler, giriş kontrolü sisteminin bir parçası olan tüm bilgisayarlarda ve mobil erişim okuyucularında sertifikaların yeniden yapılandırılmasını gerektirir.

Sunucu gereksinimleri
Sunucu, ACS ve CredMgmt uygulamasını çalıştıran bilgisayardır.

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.

İstemci gereksinimleri

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.

3.2 Donanım ön koşulları

Kayıt okuyucuları

CredMgmt, fiziksel kartları kaydetmek için en az bir kayıt okuyucu gerektirir. Kayıt okuyucuları genellikle istemci iş istasyonlarına kurulur. İstemci iş istasyonu, `BoschPeripheralDeviceAddon.exe` adı verilen bir program yoluyla çevre cihazlarıyla iletişim kurar. Bu programın kurulumu aşağıda açıklanmıştır.
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

3.2.1 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.

3.3 Credential Management kurulumu

Giriş

CredMgmt, Bosch giriş kontrolü sistemiyle (ACS) birlikte bir web uygulaması olarak çalışır. Aşağıdaki bölümlerde, bu web uygulamasını yöneten arka uç bileşeninin kurulumu açıklanmaktadır.

– Yerel veya uzak bir veritabanı kullanmak için bu eklentiyi yükleyebilirsiniz.

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.

3.3.1 CredMgmt ön koşulları

Uzak veritabanı (yalnızca uzak veritabanı kullanıyorsanız) için özel kullanıcı

`CMUser` kullanıcısı, CredMgmt uygulaması adına ACS veritabanına erişir.

CredMgmt, uzak bir veritabanı sunucusundaki bir veritabanını kullanacaksa aşağıdaki prosedürü kullanın.

ÖNEMLİ: Bu prosedürü tamamlamadan önce CredMgmt kurulumunu çalıştırmayın.

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>\`CMUser`
– **Şifre**: Şifreyi tüm bilgisayarlarınız için geçerli olan güvenlik ilkelerine göre ayarlayın. CredMgmt 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 `CMUser`'ı aşağıdaki gibi ekleyin:

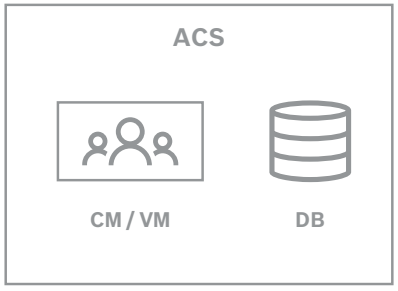
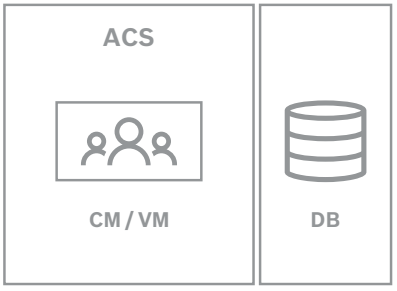
1. SQL Management Studio'yu açın
2. Uzak SQL örneğine bağlanın
3. **Güvenlik** > **Oturum Aç**'a gidin
4. **Sayfa seç** bölmesinde, **Genel**'i seçin.
5. `CMUser` kullanıcısını seçin
6. **Sayfa seç** bölmesinde **Sunucu rolleri**'ni seçin
7. `public` ve `dbcreator` onay kutularını seçin

Yerel veritabanı (yalnızca yerel bir veritabanı kullanıyorsanız) için özel bir kullanıcı
`CMUser` kullanıcısı, CredMgmt uygulaması adına ACS veritabanına erişir.
CredMgmt kurulum programı ACS sunucusunda otomatik olarak Windows kullanıcısı `CMUser` oluşturduğundan CredMgmt yerel bir veritabanı kullanıyorsa bu kullanıcıyı oluşturmanıza gerek YOKTUR.

ACS'de atanmış bir kullanıcı

1. ACS'de, **sınırsız API kullanımı** özelliğine sahip bir kullanıcı oluşturun.
– AMS'deki iletişim yolu: **Configuration** (Yapılandırma) > **Operators and Workstations** (Operatörler ve İş İstasyonları) > **User rights** (Kullanıcı hakları) sekmesi: **User account** (Kullanıcı hesabı) > **API Access rights control (API Giriş hakları kontrolü).** Listeden `Unlimited access` seçin.
– BIS'de iletişim yolu: **Configuration Browse**r (Yapılandırma Tarayıcısı) > **Administration** (Yönetim) > **Operators** (Operatörler) > Select operator (Operatör seçin) > sekmesi: **ACE API Access rights (ACE API Giriş hakları).** `Unlimited access`'i seçin.
– Daha ayrıntılı talimatlar için ACS operatör kılavuzunda yer alan **Kullanıcı (operatör) profilleri atama** bölümüne bakın.
2. Web uygulamasının kurulum sihirbazı tarafından gerekli olacağı için kullanıcı adını ve şifreyi dikkatlice not alın.

3.3.2 Kurulum prosedürü

Yerel DB ile CredMgmt	Uzak DB ile CredMgmt
	

Prosedür

1. ACS sunucusunda, Yönetici olarak `BoschCredentialManagementServer.exe` çalıştırın.
– Kurulum programı açılır
2. **Core components** (Temel bileşenler) ekranında, `Bosch Credential Management`'ı seçip **Next** (İleri) öğesine tıklayın.
3. Son Kullanıcı Lisans Anlaşmasını (EULA) kabul etmek isterseniz dikkatle okuyun ve **Accept** (Kabul et) düğmesine tıklayın. Kurulum yalnızca bunu yaptığınızda devam edebilir.
4. Kurulum için bir hedef klasöre gidip klasörü seçin veya varsayılanı kabul edin (önerilen), **Next** (İleri) öğesine tıklayın
5. **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

6. **ACS giriş yapılandırması** ekranında:

– ACS sunucusunun ana bilgisayar adını girin.
– Sınırsız API kullanımına sahip bir ACS kullanıcı adını girin (yukarıdaki Ön koşullara bakın).
– Bu ACS kullanıcısı için ACS şifresini girin ve onaylayın.

7. **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, CredMgmt'ın seçildiğini onaylayın ve **Install** (Yükle) düğmesine tıklayın.
10. Kurulum tamamlandığında aşağıdaki URL ile CredMgmt'ı başlatın:

`https://` <ACSsunucusununAdı>`:5806`

3.4 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.

3.4.1 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.

3.4.2 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:

3.4.3 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.

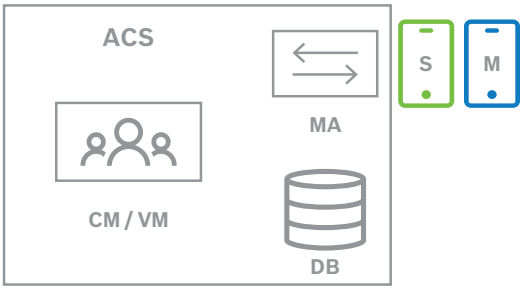
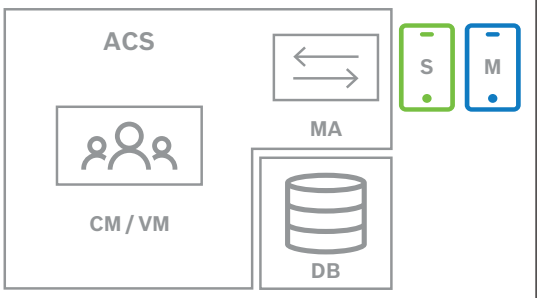
Yerel veritabanı kullanıyorsanız bu kullanıcıyı oluşturmanız gerekmez. Mobile Access kurulum programı ACS sunucusunda otomatik olarak bir `MAUser` Windows kullanıcısı oluşturur.

3.4.4 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.

Yerel DB ile aynı yerde	Uzak DB ile aynı yerde
	

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.

3.4.5 Dağıtılmış kurulum prosedürü

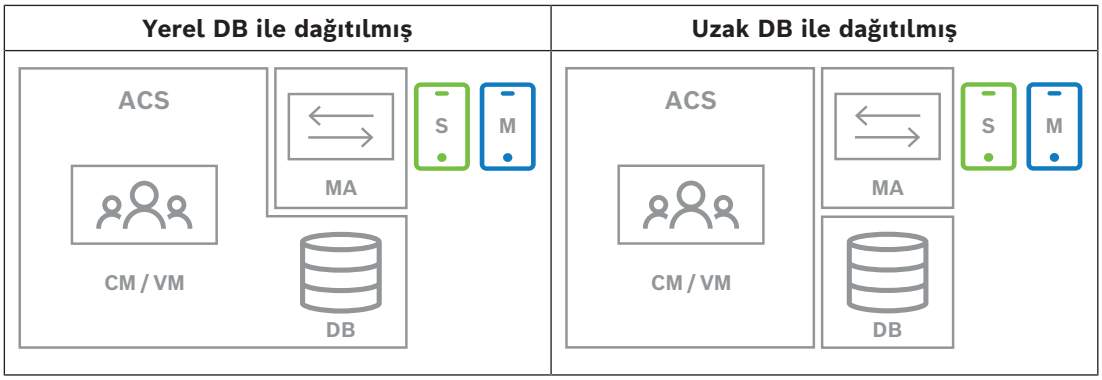
Aynı yerde kurulum, Mobile Access Arka Uç hizmetinin ACS ile aynı sunucuda çalıştığı anlamına gelir.

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.

3.5 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	/	/	/	/

3.5.1 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.

3.5.2 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.

3.5.3 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

3.6 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.

3.7 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.

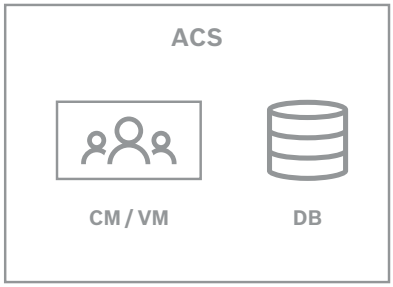
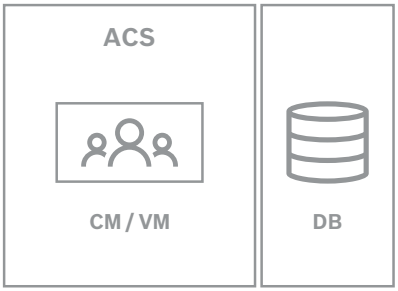
Not: Mobile Access arka ucu kaldırıldıktan sonra, aşağıdaki yapılandırma izleri istenirse manuel olarak kaldırılmalıdır:

– **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.

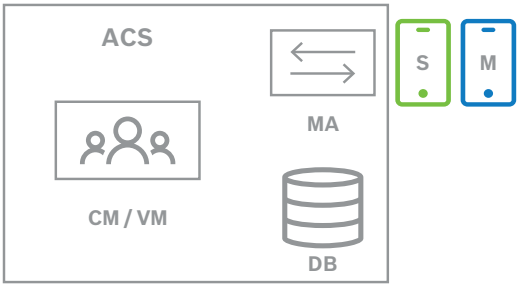
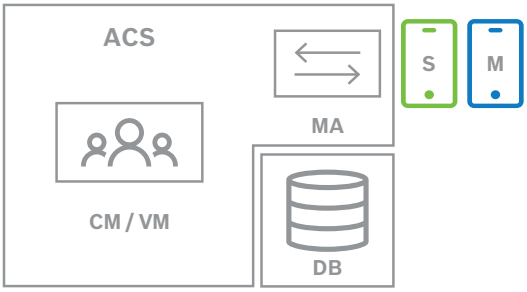
4 Credential Management'a genel bakış

Aşağıda, Mobile Access ile veya olmadan Credential Management kurulumlarının olası topolojileri gösterilmektedir. Her kapalı kutu, ayrı bir bilgisayarı temsil eder.

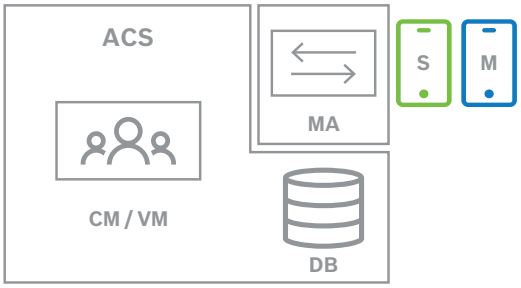
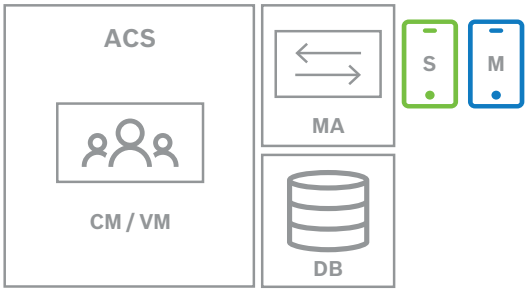
Tuş	Anlamı
ACS	Birincil giriş kontrol sistemi, AMS veya BIS-ACE
CM/VM	Web uygulaması için arka uç: Credential Management veya Visitor Management
DB	Ana ACS veritabanı
MA	Mobile Access arka ucu
S	Sistem teknisyenlerinin ve yapılandırıcılarının mobil cihazları için "Kurulum Erişimi" teknisyen uygulaması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

Credential Management, yerel DB	Credential Management, uzak DB
	

Tablo 4.1: Credential Management topolojileri

Mobile Access, ortak konum, yerel DB	Mobile Access, ortak konum, uzak DB
	

Tablo 4.2: Mobile Access ortak konum topolojileri

Mobile Access, dağıtılmış, yerel DB	Mobile Access, dağıtılmış, uzak DB
	

Tablo 4.3: Mobile Access dağıtılmış topolojileri

İlgili yazılımın uyumlu sürümleri

Aşağıdaki tabloda, sistemin bu sürümüyle uyumlu olan yardımcı yazılım araçlarının sürümleri listelenmiştir.

Bileşen	Sürüm	Location (Konum)
Access Management System (AMS)	5.5 (Mobile Access uzantısı içerir)	Mağaza/Ürün Kataloğunu İndirin
Visitor Management (VisMgmt)	5.5 (Mobile Access uzantısı içerir)	Mağaza/Ürün Kataloğunu İndirin

Uyarı!

Bölümler

Credential Management, Visitor Management ve Mobile Access, birden fazla bağımsız kiracının giriş kontrolünün yönetildiği (ACS) Bosch giriş kontrolü sistemlerinin "Bölümler" özelliğini desteklemez.

5 Yapılandırma

5.1 ACS'de Credential Management kullanıcıları oluşturma

ACS'de (ACE veya AMS), her Credential Management kullanıcısı ayrı bir Operatör tanımına sahip bir kart sahibi olmalıdır.

Bu Operatör tanımları **Kullanıcı profilleri** biçiminde özel CredMgmt yetkilerini içerir. CredMgmt'da çalışan her kart sahibi için ayrı bir operatör tanımlamanız gerekir. Aynı operatöre birden fazla kart sahibi atayamazsınız.
Kullanıcı profilleriyle ilgili ayrıntılı bilgi ve yönergeler için ACS'nizin çevrimiçi yardımına bakın.
Credential Management kullanıcılarının AMS'de oluşturulmaları gerekir:

İletişim yolu
Configuration (Yapılandırma) > **Operators and workstations** (Operatörler ve iş istasyonları) > **User profiles** (Kullanıcı profilleri)

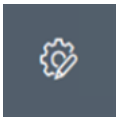
Prosedür

1. Yeni profil oluşturmak için  simgesine tıklayın
2. **Profile Name** (Profil Adı) alanına bir profil adı girin (zorunlu)
3. **Description** (Açıklama) alanına bir profil açıklaması girin (isteğe bağlıdır ancak önerilir)
4. Yaptığınız değişiklikleri kaydetmek için  simgesine veya **Apply**'a (Uygula) tıklayın
5. Profil türüne göre işlevi seçin:
   - Liste bölmesinde, profile erişebilecek işlevleri (ilk sütun) ve bu işlev (**Execute** (Yürüt), **Change** (Değiştir), **Add** (Ekle), **Delete** (Sil)) içindeki yetenekleri seçin. Ayarlarını `Yes` (Evet) olarak ayarlamak için bunlara çift tıklayın.
   - Aynı şekilde erişilebilir olmayan tüm işlevlerin `No` (Hayır) olarak ayarlandığından emin olun.
6. Yaptığınız değişiklikleri kaydetmek için  simgesine veya **Apply**'a (Uygula) tıklayın

Credential Management için kullanıcı rolleri hakkında daha fazla bilgi için *Kullanıcı rollerine genel bakış* bölümüne başvurun.

5.2 Yapılandırma görevleri için oturum açma

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

1. Tarayıcınızda, CredMgmt sunucusunun, iki noktadan ve bağlantı noktası numarasından (varsayılan olarak `5806`) sonraki HTTPS adresini girin
   `https://`<My_CredMgmt_server>`:5806`
   Oturum açma ekranı görünür
2. Bir CredMgmt **Yönetici** kullanıcısı olarak oturum açın.
3. **Ayarlar** menüsünü açmak için  öğesine tıklayın.

5.3 Yapılandırma için Ayarlar menüsünü kullanma

Genel	– **Saklama süresi (gün)**: Bu ayar, kişi 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, kayıtlar süresiz olarak saklanır. – **Logo**: İletişim kutularının özelleştirilmiş bir logo mu yoksa varsayılan logo mu görüntülediğini yöneten onay kutusunu işaretlemek veya işareti kaldırmak için. – Özelleştirilmiş logo dosyalarının kriterleri için bkz. *Şirket logosunu özelleştirme, sayfa 28* – **Süpergrafik:** İletişim kutularının Bosch üst öğesini görüntüleyip görüntülemeyeceklerini yöneten onay kutusunu işaretlemek veya işareti kaldırmak için. – **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.

5.3.1 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.
Bunları **Ayarlar** menüsünden indirdikten sonra şablonlar, tarayıcınızın varsayılan indirilenler klasöründe saklanır.

- `MobileAccess.html` Akıllı telefon tabanlı kimlik bilgilerini kullanmak için kart sahibine davetiye.
- `SetupAccess.html` Bir teknisyenin Mobile Access için okuyucuları yapılandırmasına yönelik bir davetiye.

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
`{{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

5.3.2 Belge şablonları

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

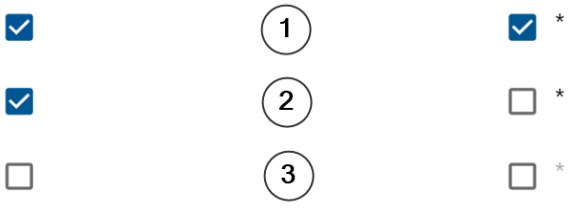
5.4 Kullanıcı arabirimini özelleştirme

Kullanıcı arayüzünü Dashboard (Pano) > **Settings** (Ayarlar) iletişim kutularında özelleştirin.

5.4.1 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.

5.4.2 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>
   ```

5.4.3 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

5.5 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
CredMgmt kullanıcısının istemci bilgisayarı	*	CredMgmt arka ucu	5806	HTTPS	CredMgmt istemci bilgisayarından CredMgmt arka ucuna gelen komutlar

Giden Sunucu	Port Çıkış	Gelen Sunucu	Port Giriş	Protokol	Yorumlar
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.

5.5.1 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
KCS.exe	[Yükleme yolu]\AccessEngine**AC**\BIN
Loggifier-2.exe	[Yükleme yolu]\AccessEngine**AC**\BIN
PictureServer.exe	[Yükleme yolu]\AccessEngine**AC**\BIN

Program	Dosya Konumu
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]\

5.5.2 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.

5.6 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:

5.6.1 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.

5.6.2 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.

5.6.3 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.

5.7 Bosch'ta veri gizliliği ve koruması

Giriş

Tüm iş süreçlerinde ve yürürlükteki yasal gerekliliklerle uyumlu olarak, gizliliğin korunmasını, kişisel verilerin korunmasını ve iş bilgilerinin güvende kalmasını sağlarız. Teknik ve organizasyonel olarak ve özellikle yetkisiz erişim ve kayıplara karşı koruma konusunda, en son teknolojinin durumunu yansıtan ve ilgili riskleri dikkate alan uygun bir standart uygularız. Bosch ürünleri ve yeni iş modelleri geliştirirken veri koruma ve bilgi güvenliğini yöneten yasal gereksinimlerin erken bir aşamada dikkate alınmasını sağlarız.

Uyumluluk kuruluşuna ve yasal bölüme ek olarak, verilerin nasıl doğru şekilde ele alındığıyla ilgili sorularınız için birincil iletişim noktası veri koruma görevlisidir.

Mobile Access uygulaması ve Mobile Access arka uç sisteminde kişilerle ilgili verilerin işlenmesi

- Kişisel veri kategorileri
  - Mobil Access uygulamaları, kişiye ilişkin veriler içerir. Bunlar, okuyucularda erişim elde etmek için kullanılan kart numarası bilgileridir. Gerçek kişilere ait asıl verilere erişim yalnızca AMS, ACE veya Visitor Management programlarının ek kullanımıyla mümkündür.
  - **Ayarlar** menüsündeki Yükleyici kayıt prosedürünün kişisel verileri saklamasına gerek yoktur. Bununla birlikte, e-posta adresleri gibi bazı kullanıcı bilgileri isteğe bağlı olarak saklanabilir.
  - Mobile Access uygulamasının arka uç sunucusu, kimlik bilgileri yönetimi için kişiyle ilgili verileri depolar.
- Veri transferi
  - Okuyuculara erişimi kontrol etmek için kimlik bilgileri arka uç sistemi, Mobile Access uygulaması ve Visitor Management sistemi arasında aktarılır.
- Verilerin günlüğe kaydı
  - Mobile Access uygulaması teknik günlükler tutar. Bu günlükler mobil cihazda yerel olarak depolanır ve gerekirse teknik destek gibi üçüncü taraflara da gönderilebilir.
  - Arka uç sunucusu da teknik günlükler tutar. Veriler, sunucu sisteminde yerel olarak depolanır.
  - Varsayılan olarak, arka uç sunucusu günlük dosyalarını otomatik olarak silmez. Bununla birlikte, otomatik silme, kalan depolama kapasitesine veya bir zaman takvimine bağlı olarak yapılandırılabilir.

Ürünü veri koruma dostu hale getirmek için ne yaptık?

Bosch giriş kontrolü sistemleri, kişilerin erişim haklarını yönetir. Bu kişileri korumak için Bosch, GDPR gereksinimlerini doğrudan ürün geliştirmeye entegre etmek için "tasarıma dayalı gizlilik" yaklaşımını izler.

- Son teknoloji şifreleme kullanılır.
- Kimlik bilgilerine takma ad verilir.
- Uygulamanın kullanıcısının, QR Kodu veya posta yoluyla sanal kimlik bilgileri almak için kişisel bilgiler girmesine gerek yoktur.

- Kimlik bilgilerinin silinmesi, Mobile Access uygulamalarından, birincil giriş kontrol sistemlerinden ve Visitor ve Credential Management gibi yardımcı uygulamalardan mümkündür.
- Kimlik bilgileri, ana giriş kontrol sistemlerinin operatörleri ve yardımcı uygulamaları tarafından her zaman engellenebilir.
- Telemetri verileri yapıları gereği anonimdir.
- Günlük dosyaları, kullanıcının aktif izni ve onayı olmadan, teknik destek gibi diğer taraflara mobil cihazlardan aktarılmaz.
- Günlük dosyalarının programlanmış otomatik silinmesi, birincil giriş kontrol sisteminde yapılandırılabilir.
- Bosch, App Store'da veya uygulamada kayıt işlemi gerektirmez. App Store hiçbir kişisel veriyi Bosch'a iletmez.
- Uygulamanın çalışması için Bluetooth gereklidir, ancak kullanıcının Bluetooth'u manuel olarak etkinleştirmesini ister ve gerektirir.

Diğer sorular

Veri gizliliğiyle ilgili daha fazla bilgi için Mobile Access uygulamasındaki veri gizlilik bildirimine bakın veya Bosch proje ekibinizle iletişime geçin.

5.8 Yüksek güvenlik yetkileri

5.8.1 İki kişi ilkesi

AMS 5.5 ve üzeri sürümlerinden itibaren, İki kişi ilkesini etkinleştirmek mümkündür. Bu işlevin temel amacı, bir onaylayan ekleyerek yetki atarken güvenliği zorlamaktır. Credential Management'da operatör, belirli bir kişi için bir veya daha fazla yetki atayabilir. Derhal bir kişiye atanan tipik bir yetki atamasının aksine, İki kişi ilkesi etkinleştirildiğinde yetkiler, yetki talebini onaylamaya veya reddetmeye hakkı olan farklı bir operatöre bir talep olarak gönderilir. Bu, hassas alanlardaki yetkileri korumak için kullanılabileceğinden yanlış atamaları önler; örneğin, bir çalışana sadece iki operatör (talep eden ve onaylayan) onay verdiğinde yetki verilebilir.

5.8.2 Yüksek güvenlik yetkilerini yapılandırma

İki kişi ilkesini etkinleştirmek için aşağıdaki gereklilikler zorunludur:

- AMS'nin en son sürümüne güncellenmiş olması.
- AMS yöneticisi olmak.

İki kişi ilkesiyle erişim yetkileri oluşturma

Ana giriş kontrolü sisteminde:

İletişim yolu

AMS Main menu (AMS Ana menüsü) > **System data** (Sistem verileri) > **Authorizations** (Yetkiler)

1. Araç çubuğundaki **New**'a (Yeni)  tıklayarak giriş alanlarını temizleyin.
   Alternatif olarak, mevcut olana göre yeni bir yetki oluşturmak için **Copy**'ye (Kopyala)  tıklayın.
2. Yetki için benzersiz bir ad girin
3. (İsteğe bağlı) Bir açıklama girin
4. (İsteğe bağlı) Bu yetkiyi düzenlemek için bir zaman modeli seçin
5. (İsteğe bağlı) Listeden bir **Inactivity limit** (Hareketsizlik sınırı) seçin.

6. (Zorunlu) En az bir **Entrance** (Giriş) atayın.
7. **Approval required** (Onay gerekli) onay kutusunu seçin (bu seçenek İki Kişi İlkesini etkinleştirir).
8. Yetkiyi kaydetmek için Save'e (Kaydet)  tıklayın

Uyarı!
Güvenlik tavsiyesi
Bu özellik sadece Credential Management için geçerlidir. AMS'de, iletişim kutularının erişilemez olması için yöneticilerin, operatörler için Kullanıcı profillerini uygun şekilde atamaları ve yapılandırmaları gerekir. Bu, normal operatörlerin iki kişi ilkesi olmadan yüksek güvenlik yetkileri atamasını önler.

Daha fazla bilgi için *Access Management System Yapılandırma ve Çalıştırma* Yazılım kılavuzunun en son sürümüne başvurun.

6 Çalışma

6.1 Kullanıcı rollerine genel bakış

Credential Management kullanıcılarının özellikleri, ACS'deki Kullanıcı Profilleri tarafından belirlenir:

Kullanıcı türü	Kullanım örnekleri
Yönetici	Genel ayarlar yapma Aracın davranışını ve kullanıcı arayüzünü özelleştirme ve Tüm Operatör kullanım senaryoları
Operatör	Fiziksel erişim kartlarının atanması ve atamalarının kaldırılması ve mobil erişim için sanal kimlik bilgileri
İki kişi ilkesi: Talep eden	Yüksek güvenlik yetkileri talep eder
İki kişi ilkesi: Onaylayan	Yüksek güvenlik yetkilerini onaylar veya reddeder Normal yetkileri kaldırma

Bkz.

– *ACS'de Credential Management kullanıcıları oluşturma, sayfa 25*

6.2 Panoyu kullanma

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

Personel tablosunun genel kullanımı

Tablodaki her satır bir kişiyi temsil eder. Bunlar, tesislere erişim için kimlik bilgileri gerektiren dahili veya harici personel üyeleridir.

– Klavyeyi ve fareyi kullanarak tek seferde tek tek kişileri ya da birden fazla kişi 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 kişiler ekleyebilirsiniz
– İşlem düğmelerine tıklayarak kimlik bilgileri atayabilir ve atamalarını kaldırabilirsiniz
  – Fiziksel bir kimlik bilgisi atama
  – Sanal kimlik bilgisi atama (mobil erişim için)
  – Kişinin ayrıntılarını düzenleme
– 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.

Panonun işlevleri

Etiket	İşlev
(1) N **giriş**	Toplam N kişi sayısı (her kişi tabloda bir satırdır).
(2) **Arama**	Tablodaki kişiler arasından rastgele metin arayın
(3) 	Listede yer alan tüm öğeleri seçin
(4)  **Delete** (Sil)	Seçili öğeleri siler
(5)  **Latest** (Son)	Tabloya en son eklenen kişileri gösterir.
(6)  **Reset** (Sıfırla)	Tabloyu varsayılan görünümüne sıfırlayın ve tüm filtreleri geri döndürün.
(7)  **Deassign card** (Kart atamasını kaldır)	Bağlı bir kayıt okuyucusu kullanarak atanan kartların atamasını kaldırma iletişim kutusunu açın.
(8) **. . .**	Kişilerin 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.
(9) 	Yeni bir kişi oluşturmak için bir iletişim kutusu açın

Panonun sütunları

Sütun	Açıklama
Name (Ad)	Kişinin ayrıntılarını görüntülemek için köprüye tıklayın.
E-posta	
Department (Departman)	

Sütun	Açıklama
Position (Konum)	
Company (Şirket)	
Kart numaraları	Bu kişiye atanan kartların sayısı.
İşlemler	Aşağıdaki ayrı tabloyu göster

Pano tablosundaki personel kayıtları üzerinde gerçekleştirilecek eylemler

Simge	İşlemler
	Kişiye bir veya daha fazla fiziksel kart **atama**
	Mobil erişim için kişiye sanal kimlik bilgisi **atama**
	Kişinin ayrıntılarını **düzenleme**. Değişiklikler ACS'ye yayılır. ACS'de yapılan değişiklikler CredMgmt uygulamasına yayılır.

6.2.1 Kişi sayfasına genel bakış

Belirli bir kişinin adına tıkladıktan sonra, kişisel verilerin olduğu bir iletişim kutusu açılır. Bu iletişim kutusunda, kişinin ana bilgileri görüntülenebilir ve düzenlenebilir ancak temel kişisel bilgiler iletişim kutusunun sol tarafında kalıcı olarak görüntülenir.
Mevcutsa, kara liste girişleri hakkındaki bilgiler, bu temel kişisel bilgi sütununun alt kısmında görüntülenir.
İpucu: **Title** (Başlık) alanı, açılır listede bulunan seçenekler dışında serbest metine de olanak tanır.
Aynı iletişim kutusunda, **Details, Credentials, Authorizations** (Ayrıntılar, Kimlik Bilgileri, Yetkiler) şeklinde kendi görünümüne sahip üç sekme bulunur.
Credential Management'da bu kişi engellenmişse **Blacklisted** (Kara Listede) kelimesiyle turuncu bir uyarı görüntülenir. Ayrıca kara listeye kimlerin atanmış olduğunu ve nedenini görüntüler.
Bir yönetici ve hakları olan bir operatör, kişiyi engellemek için **Blacklist (Kara Liste) düğmesini kullanabilir.**

– Bir uyarı penceresi açılır
1. **Yes** (Evet) öğesine tıklayın
2. **Reason** (Neden) sihirbazında, nedeni yazın > **Save > Ok** (Kaydet > Tamam) öğelerine tıklayın

Kara listedeki bir kişi, atanan yetkilerine sahip olmaya devam eder. Ancak bu kişi bir girişi/kapıyı açamaz.
Kişiyi kara listeden kaldırmak için **X Remove from blacklist** (X Kara listeden kaldır) düğmesine tıklayın.

Hakları doğru şekilde yapılandırın. Kullanıcı haklarıyla ilgili daha fazla bilgi için *Access Management System Yapılandırma ve Çalıştırma Yazılım kılavuzuna* başvurun.

Details (Ayrıntılar)
Bu sekmede, sürekli olarak görünür olması gerekmeyen kişisel verileri girebilirsiniz.
PIN
Bu **Details** (Ayrıntılar) sekmesinde, bir kart sahibi için PIN'leri (doğrulama PIN'i)[1] görüntülemek ve değiştirmek mümkündür. PIN'i değiştirken bir sona erme tarihi belirlenebilir.
Not: PIN değişirse veya bu ayar değişirse onay için PIN'in yeniden yazılması gerekir.
Seçilen kişinin kimlik bilgileri için bir veya daha fazla **PIN** kilidi varsa temel kişisel bilgiler sütununun alt kısmında bir uyarı görüntülenir. Operatör bu uyarıya tıkladığında **Credentials** (Kimlik Bilgileri) sekmesi seçilir ve operatör, **PIN** kilidi hakkında daha fazla bilgi görebilir.
Bir sekmede doğrulama hatası varsa hata çözülünceye kadar başka bir sayfa seçilemez.
[1]Credential Management yalnızca standart PIN'i destekler. Tanımlama PIN'leri VE ayrı IDS PIN'leri/kurma PIN'leri desteklenmez.
PIN kodları ile ilgili daha fazla bilgi için *Access Management System Yapılandırma ve Çalıştırma Yazılım kılavuzuna* başvurun.

Kimlik Bilgileri
Bu sekmede, **Read card** (Kart oku) düğmesine tıklayarak fiziksel bir kart atamak veya **Add mobile access** (Mobil erişim ekle) düğmesine tıklayarak mobil kimlik bilgileri atamak mümkündür. Daha fazla bilgi için *Mobil kimlik bilgileri atama* ve *Fiziksel kimlik bilgileri atama* bölümlerine bakın.
Not: Telefon simgesinde turuncu bir nokta görünürse bu, kimlik bilgilerinin zaten cep telefonunda olduğu anlamına gelir ancak mobil erişim onayı gereklidir. Ancak bu onaydan sonra nokta yeşile döner.

Yetkiler
Bu sekmede, atanmış tüm yetkileri görüntülemek ve yetkileri değiştirmek mümkündür. Daha fazla bilgi için *Kişisel bilgiler sayfasından yetkiler atama* bölümüne bakın.
Herhangi bir sekme iletişim kutusunda, **Save & Close** (Kaydet ve Kapat) düğmesi sizi **Dashboard** (Pano) iletişim kutusuna yönlendirir.

6.3 Yetkiler atama

Kişisel bilgiler sayfasından yetkiler atama
– Pano iletişim kutusunda kişilerin listesi görüntülenir.
1. Kişinin adına tıklayın.

– Kişi bilgileri iletişim kutusu açılır.
1. İletişim kutusunun sağ üst köşesinde **Authorizations** (Yetkiler) sekmesine tıklayın.
2. Yeni bir yetki atamak için **Modify authorizations** (Yetkileri değiştir) seçeneğine tıklayın.

Tüm yetkiler listesinin yer aldığı bir sihirbaz görüntülenir. Bu yetkilerin hepsi, Access Management System'de önceden yapılandırılmıştır. Bu adımdan itibaren, hangi yetkilerin atanacağını seçin.

1.  > **Confirm** (Onayla) > **Save** (Kaydet) seçeneklerine tıklayın.

Not: İki kişi ilkesi işlevi etkinleştirildiğinde, yüksek güvenlik yetkileri  ile görüntülenir.

Pano iletişim kutusu açılır. Normal bir yetki atanmışsa kişinin adına tekrar tıklayarak ve **Authorizations** (Yetkiler) sekmesini kontrol ederek yetkinin gerçekten atanmış olup olmadığını kontrol etmek mümkündür.
İki kişi ilkesiyle bir yetki atanmışsa o zaman çıktı farklı olur. Başka bir ifadeyle, yetki kaydedildikten hemen sonra değil, talep edildiğinde aktif hale gelir. **Authorizations** (Yetkiler) ve **Actions** (Eylemler) sütunlarında, kimin yetki talep ettiği görülebilir. **Authorizations** (Yetkiler) sekmesinde , İki kişi ilkesine sahip yetkiler onaylanmış veya reddedilmiş olarak görünür. Fareyle yetki adının üzerine gelindiğinde, yetkiyi kimin hangi tarihte ve saatte talep ettiğini görmek mümkündür. Bir ipucu görüntülenir.

Yetki türüne ve kullanıcı rolü ile kullanıcı haklarına bağlı olarak, görüntülenen **Actions** (Eylemler) düğmeleri aşağıdakiler olabilir:

Request (Talep Et)
Retract (Geri çek): Henüz onaylanmamış olan kendi yetki atama talebinizi iptal eder.
Approve (Onayla): Başka bir operatör tarafından yetki atama talebini onaylar.
Deny (Reddet): Başka bir operatör tarafından yapılan yetki atama talebini reddeder.
Remove (Kaldır): Atanan yetkiyi kaldırır. Bu, normal ve yüksek güvenlikli yetkiler için geçerlidir.

Not: Yalnızca eylem düğmesine tıklandığında hiçbir eylem geçerli olmaz. Her zaman **Save** (Kaydet) öğesine tıklayın.
Daha fazla bilgi için *Kullanıcı rollerine genel bakış* bölümüne bakın.

AMS'de, **User profiles** (Kullanıcı profilleri), iki kişi ilkesine uygun olarak mevcut haklarla doğru bir şekilde yapılandırılmalıdır:
– Yönetici
– Operatör
– İki kişi ilkesi: Talep eden
– İki kişi ilkesi: Onaylayan

Kullanıcı profillerinin nasıl yapılandırılacağı hakkında daha fazla bilgi için *Access Management System Yapılandırma ve Çalıştırma* Yazılım kılavuzunun son sürümüne başvurun.

Bekleyen Yetki talepleri
Onaylayan veya talep eden haklarına sahip bir Operatör ve bir Yönetici, menüde **Yetki Taleplerini** görüntüleyebilir. Bu iletişim kutusunda, her bir kişinin adına gitme gereği olmadan, tek bir görünümde tüm **Bekleyen Yetki Talepleri** görülebilir.
Onaylayan yetkisi olan bir Operatör, bu iletişim kutusu aracılığıyla yetkileri onaylayabilir ve Yönetici yetkileri geri çekebilir. Talep eden yetkisi olan bir Operatör bekleyen yetkileri yalnızca görüntüleyebilir. Onaylayan ve talep eden hakları olmayan bir Operatör bu iletişim kutusunu görüntüleyemez.
Not: Yalnızca eylem düğmesine tıklandığında hiçbir eylem geçerli olmaz. Eylem düğmesine tıkladıktan sonra düğme gri olur; ardından **Save** (Kaydet) öğesine tıklayın.

6.4 Fiziksel kimlik bilgilerini atama

Ön koşullar

Yeni bir kart, kart yazıcısı ve kayıt okuyucu kullanarak yeni personele yeni kimlik bilgileri atamanız önemle tavsiye edilir.

Kart atama (bir kayıt okuyucu gerektirir)

Prosedür

Doğrudan pano simgesinden ya da kişi sayfasına genel bakıştan bir kart atamak mümkündür.

Pano alanında:

1. Kayıt okuyucuya sunmak için hazır bir fiziksel giriş kartı bulundurun.
2. Kişi satırını seçin ve  öğesine tıklayın.
3. Kayıt okuyucunun kullanılması için açılır penceredeki yönergeleri izleyin.

Kişi sayfasına genel bakıştan:

1. **Pano**'da kişinin adını seçin ve kişi sayfasına genel bakış açılır.
2. **Credential** (Kimlik bilgisi) sekmesini > **Read card** (Kart oku) öğesini seçin.

Kimlik bilgileri düzenleyicide kart atama (kayıt okuyucusu gerektirir)

1. Panodaki kişiler tablosunda, bir kişi seçin ve o kişinin kimlik bilgilerini düzenlemek için  öğesine tıklayın.
2. **Read card** (Kart oku) öğesine tıklayın ve kayıt okuyucusunun kullanımı için açılır penceredeki talimatları izleyin.

– Gerekirse daha fazla kart atamak için son adımları tekrarlayın.

3. Kart atamalarıyla geçerli kişiyi kaydetmek için **Save** (Kaydet) öğesine tıklayın.

6.5 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
– 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
– 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
– 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
– Uygulama çalıştığı sürece mobil cihaz bir fiziksel giriş kartı gibi çalışır

Bkz.

– *Mobil Erişimi Yükleme, sayfa 12*

– *Mobil Erişim uygulamalarını yükleme, sayfa 21*

6.6 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.

6.7 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.

6.7.1 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.

6.8 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.

6.8.1 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.

GDPR

Genel Veri Koruma Düzenlemesi (GDPR), Avrupa Birliği (AB) tarafından yapılmış ve 2018'de yürürlüğe giren bir gizlilik ve güvenlik yasasıdır. AB'deki kişilerle ilgili verileri toplayan her yerdeki kuruluşlara yükümlülükler yükler.

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.

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

Daha iyi bir yaşama yönelik bina çözümleri

202405132129