Access Management System

tr Kurulum Kılavuzu

İçindekiler

1 Bu belge hakkında

Bu, Access Management System'ın ana kurulum kılavuzudur.

İlgili belgeler

Aşağıdakiler ayrıca belgelenmiştir:

– AMS'nin ve yardımcı programlarının yapılandırması ve çalışması.
– AMS - Map View'ın çalışması.

2 AMS Sistemine genel bakış

Kartlı Geçiş Yönetim Sistemi, tek başına veya Bosch'un amiral gemisi video yönetim sistemi olan BVMS ile uyumlu olarak çalışan güçlü, kusursuz bir kartlı geçiş sistemidir.
Gücü, önde gelen ve kanıtlanmış teknolojileri eşsiz biçimde dengelemesinden kaynaklanır:

- Kullanılabilirlik için tasarlandı: Sürükle ve bırak Harita Görünümü'ne sahip kullanıcı arayüzü ile kullanımı kolay biyometrik kayıt iletişim kutuları.
- Veri güvenliği için tasarlandı: En son standartlar (AB-GDPR 2018), işletim sistemleri, veritabanları ve şifreli sistem arayüzlerini destekler.
- Esneklik için tasarlandı: Orta katman ana giriş kontrol cihazları, ağ arızası durumunda yerel giriş kontrol cihazlarının otomatik olarak yük devri yapmasını ve bütünlenmesini sağlar.
- Gelecek için tasarlandı: Düzenli güncellemeler ve yenilikçi geliştirmelerle dolu gelecek ürünler.
- Ölçeklenebilirlik için tasarlandı: Düşük-yüksek giriş seviyeleri sunar.
- Birlikte çalışabilirlik için tasarlandı: Bosch video yönetimi, olay işleme ve özel iş ortağı çözümlerine yönelik arayüzlere sahip RESTful API'ları.
- Yatırımınızı korumak için tasarlandı: Kurulu kartlı geçiş donanımlarınıza eklemeler yaparken verimliliği de artırmanızı sağlar.

3 Kurulum

Genel prosedür

Sistemin kurulumu iki ayrı yükleyiciden oluşur: Sunucu ve istemci.

Kurulumun genel sırası aşağıdaki gibidir:

1. Sistem gereksinimlerini kontrol etme
2. Yazılımı sunucuya yükleme ve herhangi bir istemci yüklemeden önce doğru kurulumu doğrulama.
3. İstemci makineye HTTPS Sertifikasını yükleme
4. İstemciyi kurma

Bkz.

– *HTTPS Sertifikasını İçe Aktarma, sayfa 9*
– *Sistemin kurulu olup olmadığını kontrol etme, sayfa 12*

3.1 Sistem gereksinimleri

Bir AMS sunucusu için minimum teknik gereksinimler

Sunucu	
Desteklenen işletim sistemleri. Diğer işletim sistemlerine yüklenebilir, ancak bu tamamen garanti dışıdır.	– Windows Server 2016 (64 bit, Standart, Veri Merkezi) – Windows 10, version 1903 (LTSB, LTSC) – **Not:** Bu sistemle sunulan varsayılan veritabanı, gelişmiş hizmetler sunan SQL Server 2017 Express sürümüdür.

Minimum donanım gereksinimleri	– En az 4 fiziksel çekirdekli Intel i5 işlemci
	– 8 GB RAM (32 GB önerilir)
	– 200 GB boş sabit disk alanı (SSD diskler önerilir)
	– Aşağıdakilere sahip grafik adaptörü:
	  – 256 MB RAM
	  – 1280x1024 çözünürlük
	  – En az 32 k renk
	– 1 Gbit/sn. Ethernet kartı
	– Kurulum dosyaları için boş bir USB portu veya ağ paylaşımı

Bir AMS istemcisi için minimum teknik gereksinimler

İstemci	
Desteklenen işletim sistemleri. Diğer işletim sistemlerine yüklenebilir, ancak bu tamamen garanti dışıdır.	– Windows 10, sürüm 1803 (LTSB, LTSC)
Minimum donanım gereksinimleri	– Intel i5 veya üzeri – 8 GB RAM (16 GB önerilir)

İstemci	

	– 20 GB boş sabit sürücü alanı
	– Aşağıdakilere sahip grafik adaptörü:
	  – 256 MB RAM
	  – 1920x1080 çözünürlük
	  – En az 32 k renk
	– DirectX® 11
	– 1 Gbit/sn. Ethernet kartı
	– Kurulum dosyaları için boş bir USB portu veya ağ paylaşımı

Ek bir MAC için minimum teknik gereksinimler

MAC sunucusu	

Minimum donanım gereksinimleri	– Intel i5 veya üzeri
	– 8 GB RAM (16 GB önerilir)
	– 20 GB boş sabit sürücü alanı
	– Aşağıdakilere sahip grafik adaptörü:
	  – 256 MB RAM
	  – 1280x1024 çözünürlük
	  – En az 32 k renk
	– 1 Gbit/sn. Ethernet kartı

3.2 Sunucu kurulumu

Başlamadan önce

1. Sunucu makinede oturum açın
2. Sistemin daha önceden kurulu olup olmadığını kontrol edin (bkz. **Sistemin kurulu olup olmadığını kontrol etme**). Değilse kuruluma devam edin.
3. Kurulum paketini sunucu makinenize kopyalayın.

Sunucu kurulumunu başlatma

1. Yazılım kurulum paketine çift tıklayın.
2. **Server**'a (Sunucu) çift tıklayın.
3. **AMS Server Setup.exe**'ye sağ tıklayın ve bağlam menüsünden **Run as administrator**'ı (Yönetici olarak çalıştır) seçin.

– Kurulum hazırlama sihirbazı açılır. Kurulum hazırlama sihirbazını izleyin.

4. Kurulacak gerekli bileşenleri seçin ve **Next>**'e (İleri) tıklayın.

– Sihirbaz, daha önce kurulu olanlara bağlı olarak, yükleyeceği yazılımların listesini sunar:
– İhtiyaç duymadığınız zorunlu olmayan bileşenler varsa bu noktada bunların seçimlerini kaldırın.

5. **Son Kullanıcı Lisans Sözleşmesi**'ni okuyun ve devam etmek için **Accept**'e (Kabul et) tıklayın. Kabul etmiyorsanız yüklemeyi durdurmak için **Decline**'a (Reddet) tıklayın.
6. SQL Veritabanı Sunucusu yapılandırma verilerini girin.

– SQL Veritabanı Sunucusu yapılandırma verileri:
  – SQL Server: SQL Server örneğinin çalıştırılacağı ana bilgisayarın adı. Yerel makinenin kullanılması önerilir.

- SQL örneği: SQL örneği adı
- AMS veritabanı: Veritabanının adı
- SQL kullanıcı adı: SQL'de oturum açma adı
- SQL şifresi: SQL'de oturum açmak için kullanılan SQL şifresi. **Varsayılan şifre:** `sa_s3k_pw`

7. SQL şifresini girdikten sonra, **Test Server**'a (Sunucuyu Test Et) tıklayın.
– Test başarılı olursa SQL şifresi alanının altında yeşil arka plana sahip bir mesaj görünür.
8. **Next>**'e (İleri) tıklayın.
9. Sunucu için varsayılan kurulum yolu uygunsa **Next>**'e (İleri) tıklayın. Farklı bir kurulum yolunu (yalnızca yerel sürücüler) seçmek isterseniz **Browse**'a (Göz at) tıklayın.
– Dosyalar yalnızca sistem yöneticileri tarafından değiştirilebildiğinden, varsayılan kurulum yolu olan `C:\Program Files` sürücüsü önerilir.
– Farklı bir kurulum yolu seçerseniz yolun kurallara aykırı erişimden yeterince korunduğundan emin olun.
10. Devam etmek için **Next>**'e (İleri) tıklayın.
– Bu sayfada API ana bilgisayarı adı yapılandırılmaktadır.
– Sunucu adı **16** karakterden uzun olmamalıdır. Varsayılan değer (önerilir) kurucunun çalıştığı geçerli bilgisayarın ana bilgisayar adıdır.
11. Kurulum öncesi özetini kontrol edin ve **Install**'a (Kur) tıklayın.
– Kurmayı seçtiğiniz tüm bileşenleri içeren bir özet görüntülenir.
12. Kurulum ilerleme çubuğunu gözleyin.
– Hareketli yeşil çubuk, ilerleme çubuğunun yaklaşık olarak ortasına ulaştığında, tekrar hareket etmeye başlaması birkaç dakika sürer. Lütfen bekleyin.
– Access Engine (ACE) Veritabanı Kurulumu ile ilgili başka bir iletişim kutusu açılır. Bu ayar ACE veritabanını günceller. Veritabanı zaten kuruluysa güncellenir, aksi takdirde yeni bir veritabanı oluşturulur. Bu, birkaç dakika sürebilir. İletişim kutusu kapanana kadar bekleyin.
13. İşlem tamamlandıktan sonra, **Next>**'e (İleri) tıklayın ve kurulum sonrası özetini inceleyin.
– Kurulan tüm bileşenlerin bir özeti görüntülenir.
14. Kurulumu bitirmek için **Finish**'e (Bitir) tıklayın.
– Yeniden başlatma isteğinde bulunan bir iletişim kutusu açılır. Sistemin kurulumunu tamamlamak için bilgisayarı yeniden başlatmanız gerekir.
15. Bilgisayarı yeniden başlatmak için **Yes**'e (Evet) tıklayın.
– Bilgisayar yeniden başlatılır.
16. Sistemin doğru şekilde kurulu olduğundan emin olun (bkz. **Sistemin kurulu olup olmadığını kontrol etme**).
– Kuruluysa sistem uygulamasının ilk kez kurulumu tamamlanmıştır. Masaüstünde sisteme ait bir simge görünür.

İlk kez oturum açma

1. Masaüstünüzdeki, sisteme ait uygulama simgesine çift tıklayın.
2. Varsayılan kullanıcı adını ve şifreyi girin.
   - Varsayılan kullanıcı adı ve şifresi **Administrator** (Yönetici) olarak belirlenir. Şifrenin büyük ve küçük harf duyarlı olduğunu unutmayın (kullanıcı adı değildir).
3. **Log in**'e (Oturum Aç) tıklayın.
   - Şifre değişikliği isteğinde bulunan bir iletişim kutusu görünür.
   - İlk kez oturum açarken açılan iletişim kutusundaki şifreyi değiştirmeniz gerekir.
4. Oturum açmak için **OK**'e (Tamam) tıklayın.

Bkz.
- *Sistemin kurulu olup olmadığını kontrol etme, sayfa 12*
- *Sunucu güncellemesini başlatma, sayfa 17*

3.3 Güvenlik duvarını devre dışı bırakma

Sunucunun başarılı bir şekilde kurulmasından sonra ve istemci iş istasyonlarını kurmadan önce güvenlik duvarını devre dışı bırakın. Bu, istemci iş istasyonlarının ve harici MAC bilgisayarlarının başlangıç yapılandırması sırasında sunucuya kolayca bağlanmasını sağlar.

3.4 İstemci kurulumu

İstemci HTTPS Sertifikası

Sistemin sunucusu, çeşitli API'ları, yani Kartlı Geçiş API'sı, Harita API'sı ve Durum API'sını barındırır. Bu API'lar HTTPS ile iletişim kurar ve güven oluşturmak için kendinden imzalı bir sertifika kullanır. Kendinden imzalı sertifika, sunucu kurucusu tarafından oluşturulur ve sunucu makinesine kurulur.

Harita istemcisi, doğru çalışmak için bu API'ları kullanır ve böylece istemci makinenin API'lara güvenmesini gerektirir. Bunu etkinleştirmek için, sunucudan bir sertifika kopyalanarak istemci makineye manuel olarak aktarılmalıdır (bkz. **HTTPS Sertifikasını İçe Aktarma**).

HTTPS Sertifikasını İçe Aktarma

1. `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System \Certificates\Access Management System Internal CA.cer` dizinine gidin
2. Sertifikayı istemci makineye kopyalayın.
3. İstemci makinede, sertifikaya çift tıklayın.
   – Bir sertifika iletişim kutusu görünür.
4. **Install Certificate**'a (Sertifikayı Yükle) tıklayın.

– Sertifika İçe Aktarma Sihirbazı açılır.

5. **Local Machine**'i (Yerel Makine) (önerilir) seçin ve **Next>**'e (İleri) tıklayın.
6. Sertifika için bir yer belirtmek üzere (önerilir) **Place all certificates in the following store**'u (Tüm sertifikaları aşağıdaki depoya yerleştir) seçin.
7. **Browse**'a (Göz At) tıklayın.

– Sertifika deposunu seçmek için bir iletişim kutusu açılır.

8. `Trusted Root Certification Authorities`'i (Güvenilir Kök Sertifika Yetkilileri) seçin ve **OK**'e (önerilir) tıklayın.

– Sertifika deposunu seçmek için kullanılan iletişim kutusu kapanır.

9. Sertifika İçe Aktarma Sihirbazı'nda **Next>**'e (İleri) tıklayın.
10. Sertifikayı içe aktarmak için **Finish**'e (Bitir) tıklayın.
    – Sertifika içe aktarma işlemi tamamlanmıştır.

Uyarı!
HTTPS sertifikası yüklü değilse uygulama başlatılamaz.

Sunucu kurulumu sırasında otomatik olarak yapıldığından, sertifikayı sunucu makineye aktarmanız gerekmediğini unutmayın. Bu, yalnızca istemci iş istasyonları için geçerlidir.

BVMS ile Kartlı Geçiş API'sı entegrasyonu
AMS Kartlı Geçiş API'sını BVMS (Bosch Video Management System) -sürüm 9.1 veya üzeri- ile entegre etmek için, son bölümde açıklanan sertifikayı BVMS makinesine aktarın (bkz. **HTTPS Sertifikasını İçe Aktarma**).

Desteklenen işletim sistemi
İstemci için desteklenen işletim sistemi **Windows 10, sürüm 1803 (LTSB, LTSC)**'dir.

Uyarı!
İstemcinin bu kapsamın dışında kurulması, uyumluluk sorunlarına neden olabilir.

İstemci kurulumunu başlatma

1. Yazılım kurulum paketine çift tıklayın.
2. **Client**'a (İstemci) çift tıklayın.
3. **AMS Client Setup.exe**'ye çift tıklayın.
   – Kurulum hazırlama sihirbazı açılır. Kurulum hazırlama sihirbazını izleyin.
4. Yüklemek istediğiniz bileşenleri seçin ve **Next>**'e (İleri) tıklayın.

– Zaten kullanılabilenlere bağlı olarak sihirbaz aşağıdaki ön koşul niteliğindeki zorunlu yazılımları işaretler:
  – Microsoft Visual C++ 2010 Redistributable
  – Microsoft Visual C++ 2015 Redistributable
  – Microsoft Visual C++ 2017 Redistributable
  – .NET 4.8
– İsteğe bağlı bileşenler:
  – İstemci
  – Harita Görünümü
– Her isteğe bağlı bileşen için kurmayı veya atlamayı tercih edebilirsiniz.

5. **Son Kullanıcı Lisans Sözleşmesi**'ni okuyun ve devam etmek için **Accept**'e (Kabul et) tıklayın. Kabul etmiyorsanız **Decline**'a (Reddet) tıklayarak geri dönün ve işlemi iptal edin.
6. İstemci iş istasyonuna ilişkin varsayılan yükleme yolu uygunsa **Next>**'e (İleri) tıklayın. Farklı bir kurulum yolunu (yalnızca yerel sürücüler) seçmek isterseniz **Browse**'a (Göz at) tıklayın.
7. Sunucu adresini girin. Adres biçimi: Hostname:4999/tcp

– Varsayılan olarak, kurulum sihirbazı sistem istemcisini yerel `C:/Program Files` sürücüsüne (önerilir) kurar.
– Yerel `C:/Program Files` sürücüsü altına kurulan dosyalar sadece yönetici haklarına sahip kullanıcılar tarafından değiştirilebilir. Bu, yönetici hakları olmayan kullanıcıların sistemle ilgili dosyaları değiştirememesini sağlayarak güvenlik sunar.
– Farklı bir kurulum yolu seçmek isterseniz sunulan avantajlar kaybolur.

8. Harita Görünümü uygulamasıyla ilgili varsayılan yükleme yolu uygunsa **Next>**'e (İleri) tıklayın.
9. Farklı bir kurulum yolunu (yalnızca yerel sürücüler) seçmek isterseniz **Browse**'a (Göz at) tıklayın.
10. Keşif adresini girin.

– Varsayılan olarak, kurulum sihirbazı Harita Görünümü uygulamasını yerel `C:/Program Files` sürücüne (önerilir) kurar.
– Harita Görünümü uygulaması, sistemin uç noktalarını keşfetmek için keşif adresine bağlanır. Bu adres, keşif uç noktasının barındırıldığı sunucu adı ile port numarasını içeren bir URL'dir.
11. Kurulum öncesi özetini kontrol edin ve **Install**'a (Kur) tıklayın.
– Kurmayı seçtiğiniz tüm bileşenleri içeren bir özet görüntülenir.
12. Kurulum ilerleme çubuğunu gözleyin.
– İşlem tamamlanana kadar bekleyin.
13. İşlem tamamlandıktan sonra, **Next>**'e (İleri) tıklayın ve kurulum sonrası özetini inceleyin.
– Kurulan tüm bileşenlerin bir özeti görüntülenir.
14. Kurulumu bitirmek için **Finish**'e (Bitir) tıklayın.
15. Bilgisayarınızı yeniden başlatın (önerilir).
16. Sistemin kurulu olup olmadığını kontrol edin (bkz. **Sistemin kurulu olup olmadığını kontrol etme**).
– Kuruluysa istemcinin kurulumu ve Harita Görünümü (isteğe bağlı) tamamlanmıştır. Her iki istemci uygulaması simgesi de masaüstünde görünür. Varsayılan kullanıcı adı ve şifresi **Administrator** (Yönetici) olarak belirlenir. Şifrenin büyük ve küçük harf duyarlı olduğunu unutmayın (kullanıcı adı değildir).

İstemciyi başlatmadan önce

İstemcide oturum açmadan önce, sunucuda istemci iş istasyonunu yapılandırmanız gerekir. Aşağıdaki prosedürü izleyin:
1. İstemciyi sunucu makinesinde başlatın.
2. **Configuration>Device Data**'ya (Yapılandırma>Device Data) tıklayın.
– Yeni bir iletişim kutusu açılır.
3. Üst araç çubuğunda **Workstations** (İş İstasyonları) simgesini seçin.
4. Üst araç çubuğunda **New** (Yeni) simgesini seçin.
5. Workstation (İş İstasyonu) sekmesinde boş alanları doldurun.
– Alanlar:
  – Name (Ad): İstemci iş istasyonunun ana bilgisayar adını girin (zorunlu)
  – Description (Açıklama): Bir açıklama girin (isteğe bağlı)
  – Login via reader (Okuyucu ile oturum aç): Okuyucu aracılığıyla oturum açın (isteğe bağlı)
  – Automatic Logout after (Şu Süreden Sonra Oturumu Otomatik Olarak Kapat): X saniye (isteğe bağlı). Uygulamanın belirli bir süre sonra otomatik olarak oturumu kapatmasını istiyorsanız otomatik oturum kapatma özelliğini ayarlayın.
– Altı çizili alanların zorunlu olduğunu unutmayın.
6. Değişiklikleri kaydetmek için üstteki araç çubuğunda **Save**'e (Kaydet) tıklayın.
– Artık istemci iş istasyonundan başarıyla oturum açabilirsiniz.

İlk kez oturum açma
1. Masaüstünüzdeki, sistem uygulama simgesine çift tıklayın.
2. Varsayılan kullanıcı adını ve şifreyi girin.
  – İki istemci uygulaması için de varsayılan kullanıcı adı ve şifre **Administrator**'dır. Şifrenin büyük ve küçük harf duyarlı olduğunu unutmayın (kullanıcı adı değildir).
3. **Log on**'a (Oturum Aç) tıklayın.
  – Şifre değişikliği isteğinde bulunan bir iletişim kutusu görünür.

– İlk kez oturum açarken şifreyi değiştirmeniz gerekir.

4. Sonraki iletişim kutusunda yeni bir şifre girmek için **OK**'e (Tamam) tıklayın.
5. Yeni şifrenizi girin ve **Change**'e (Değiştir) tıklayın. Şifre değişikliğini iptal etmek için **Cancel**'a (İptal) tıklayın.
   – Şifre değişikliğini onaylayan bir iletişim kutusu görünür.
6. Oturum açmak için **OK**'e (Tamam) tıklayın.

Uyarı!
Hem sunucu hem de istemci aynı sürümde kurulu olmalıdır. Sunucuya farklı bir istemci sürümü ile erişmeyi denemeyin.

Bkz.

– *Sistemin kurulu olup olmadığını kontrol etme, sayfa 12*
– *HTTPS Sertifikasını İçe Aktarma, sayfa 9*

3.5 Sistemin kurulu olup olmadığını kontrol etme

Sistemin kurulu olup olmadığını kontrol etme
Sistem şu durumlarda kuruludur:
– Sistemin simgeleri masaüstünde görünüyorsa.
– Windows Hizmetleri uygulamasında şu hizmetler varsa: (**Başlat** > **Arama** > `service.msc`): DMS, MAC Erişimi PI'sı, Kimlik hizmeti, MAP API'sı, Durum API'sı.
– Sistem şu varsayılan yükleme yolundaysa: `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\`

3.6 Özel sertifikaları kullanma

AMS API'ları, kurulum sırasında otomatik olarak oluşturulan kendinden imzalı sertifikaları kullanmak yerine farklı sertifikalar kullanacak şekilde yapılandırılabilir.
Bu, bir kuruluş kendi Sertifika Yetkilisine (CA) sahip bir genel anahtar altyapısına (PKI) sahip olduğunda kullanışlıdır.

3.6.1 Ön koşullar

– Güvenilir bir kök sertifika dosyasına sahip olma.
– Sertifikanın genel ve özel bölümleri AMS sunucu dizini olan C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Certificates dizininde yer almalıdır.

Sertifikanın genel ve özel kısımlarına ilişkin örnekler:
– `Access Management System Test CA.cer` (genel kısım)
– `CustomRootTestCA.pfx` (özel kısım)

3.6.2 Özel sertifikaları kullanma

PowerShell oturumu açma
`C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System \Certificates` dizininde AMS sunucusunda bir PowerShell oturumu açın

Yüklenen sertifikaları kaldırma

1. AMS kurulumu sırasında yüklenen sertifikaları kaldırın.
2. Açılan PowerShell oturumunda "`RemoveAceApiCertificates.ps1`" kodunu yürütün.

API Sertifikası oluşturma komut dosyasını düzenleme

1. "`CreateAceApiCertificatesFromOwnRoot.ps1`" PowerShell dosyasını bir metin editöründe açın ve şu dosyaların adlarını dosya adlarınızla değiştirin:

– `CustomRootTestCA.pfx`

2. `Access Management System Test CA.cer`

– Dosya adlarının komut dosyasında yalnızca bir kez görüneceğini unutmayın.

3. Değişiklikleri kaydedin.

API Sertifikası oluşturma komut dosyasını çalıştırma

1. 1. adımda açtığınız PowerShell oturumunda "`CreateAceApiCertificatesFromOwnRoot.ps1`" kodunu yürütün.
2. Özel sertifikanın şifresini girin.

– Aşağıdaki Alt API Sertifikaları oluşturulmuş ve yüklenmiştir:
  – Kartlı Geçiş Yönetim Sistemi Kartlı Geçiş API'sı
  – Kartlı Geçiş Yönetim Sistemi Kimlik Sunucusu
  – Kartlı Geçiş Yönetim Sistemi Harita API'sı
  – Kartlı Geçiş Yönetim Sistemi Durum API'sı
– Kök sertifika yüklenir.

Geçerli Kullanıcı ve Yerel Bilgisayar için Windows Sertifikaları bölümünde sertifikaların yüklendiğinden emin olun.

Sertifika şu durumlarda yüklenmiştir:

– Kök sertifika `Current User Personal Certificates, Trusted Root Certificates` (Geçerli Kişisel Kullanıcı Sertifikaları, Güvenilir Kök Sertifikalar) ve `Local Computer Trusted Root Certificates`'ın (Yerel Bilgisayar Güvenilir Kök Sertifikaları) altında yüklüyse
– API Sertifikaları `Local Computer Personal Certificates`'ın (Yerel Bilgisayar Kişisel Sertifikaları) altında yüklüyse

Her API için Parmak izi uygulaması ayarlarını güncelleme

Her API için, parmak izi güncellenmelidir.

Kartlı Geçiş API'sı	1. `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Access API` dizinini açın 2. `appsettings.json` dosyası, "`Thumbprint`" satırındaki değerleri değiştirin: 3. **Certificates Local Computer > Personal > Certificates > Friendly Name (Sertifikalar Yerel Bilgisayar > Kişisel > Sertifikalar > Kolay Ad):** `Access Management System Access API`'yı (Kartlı Geçiş Yönetim Sistemi Kartlı Geçiş API'sı) açın 4. "`Access Management System Access API`" **> Details**'i (Kartlı Geçiş Yönetim Sistemi Kartlı Geçiş API'sı > Ayrıntılar) seçip yüklü sertifikayı açın

	5. Listede "Thumbprint"'e (Parmak İzi) kadar aşağı inin 6. Thumbprint.'i (Parmak İzi) seçin. 7. Görüntülenen Parmak izini (ör. "da") kopyalayın. 8. Parmak izini boşluk bırakmadan C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Access API dizinindeki appsettings.json dosyasına yapıştırın – (ör. "Thumbprint": "53d3588285bd570c9799e883b27ef1b139ba28da")

Harita API'sı	1. C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Map API dizinini açın 2. appsettings.json dosyası, "Thumbprint" satırındaki değerleri değiştirin: 3. **Certificates Local Computer > Personal > Certificates > Friendly Name (Sertifikalar Yerel Bilgisayar > Kişisel > Sertifikalar > Kolay Ad):** Access Management System Map API'yı (Kartlı Geçiş Yönetim Sistemi Kartlı Geçiş API'sı) açın 4. "Access Management System Map API" **> Details**'i (Kartlı Geçiş Yönetim Sistemi Kartlı Geçiş API'sı > Ayrıntılar) seçip yüklü sertifikayı açın 5. Listede "Thumbprint"'e (Parmak İzi) kadar aşağı inin. 6. Thumbprint'i (Parmak İzi) seçin. 7. Görüntülenen Parmak izini (ör. "e8") kopyalayın. 8. Parmak izini boşluk bırakmadan C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Map API dizinindeki appsettings.json dosyasına yapıştırın – (ör. "Thumbprint": "3cef0c43be36ee01d8a6ea2f59f170cde96168e8")

Durum API'sı	1. C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\States API dizinini açın 2. appsettings.json dosyası, Thumbprint" satırındaki değerleri değiştirin: 3. **Certificates Local Computer > Personal > Certificates > Friendly Name:** Access Management System States API'yı (Sertifikalar Yerel Bilgisayar > Kişisel > Sertifikalar > Kolay Ad: Kartlı Geçiş Yönetim Sistemi Kartlı Geçiş API'sı) açın 4. "Access Management System States API" **> Details**'i (Kartlı Geçiş Yönetim Sistemi Kartlı Geçiş API'sı > Ayrıntılar) seçip yüklü sertifikayı açın 5. Listede "Thumbprint".'e (Parmak İzi) kadar aşağı inin 6. Thumbprint.'i (Parmak İzi) seçin. 7. Görüntülenen Parmak izini (ör. "e2") kopyalayın.

	8. Parmak izini boşluk bırakmadan `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\States API` dizinindeki `appsettings.json` dosyasına yapıştırın – (ör. "Parmak izi": "37c0bb09d4cab985b620da1c667597ef43b5f8e2"

Kimlik Sunucusu:	1. `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Identity Server` dizinini açın 2. `appsettings.json` dosyası, `"Thumbprint"` satırındaki değerleri değiştirin: 3. **Certificates Local Computer > Personal > Certificates > Friendly Name:** `Access Management System Identity Server`'ı (Sertifikalar Yerel Bilgisayar > Kişisel > Sertifikalar > Kolay Ad: Kartlı Geçiş Yönetim Sistemi Kimlik Sunucusu) açın 4. `"Access Management Identity Server"` **> Details**'i (Kartlı Geçiş Yönetim Sistemi Kimlik Sunucusu > Ayrıntılar) seçip yüklü sertifikayı açın 5. Listede `"Thumbprint"`.'e (Parmak İzi) kadar aşağı inin 6. `Thumbprint`.'i (Parmak İzi) seçin. 7. Görüntülenen Parmak izini kopyalayın. 8. Parmak izini boşluk bırakmadan `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Identity Server` dizinindeki `appsettings.json` dosyasına yapıştırın 9. Diğer API'ların Parmak izlerini de bu dosyadaki ilgili Parmak izi giriş alanlarına yapıştırın. – Örnek: – `"Name": "AccessApi" için "Thumbprint": "53d3588285bd570c9799e883b27ef1b139ba28da"` – `"Name": "MapApi" için "Thumbprint": "3cef0c43be36ee01d8a6ea2f59f170cde96168e8"` – `"Name": "StatesApi" için "Thumbprint": "37c0bb09d4cab985b620da1c667597ef43b5f8e2"`

Hizmetleri Durdurma ve Başlatma

1. Windows hizmetlerini açın.
2. Aşağıdaki hizmetlere sağ tıklayın ve bunların her birinden sonra yer alan "Durdur"u seçin:

– Kartlı Geçiş Yönetim Sistemi Kartlı Geçiş API'sı
– Kartlı Geçiş Yönetim Sistemi Kimlik Sunucusu
– Kartlı Geçiş Yönetim Sistemi Harita API'sı
– Kartlı Geçiş Yönetim Sistemi Durum API'sı

– Dört hizmetin tamamı durduktan sonra, aynı hizmetlere yeniden sağ tıklayın ve her birinden sonra yer alan **Başlat**'ı seçin.

İstemci makineye Kök Sertifikayı yükleme

1. Kök sertifikanız olan "`Access Management System Test CA.cer`" dosyasını kopyalayıp "Harita Görünümü" ve "AMS"nin (İletişim Kutusu Yöneticisi) kurulu olduğu istemci makinesine yapıştırmak için Windows dosya yöneticisini kullanın.
   Örneğin, İndirilenler klasörüne yapıştırın.
2. Kök Sertifikayı yükleyin:

– Dosya Yöneticisi'nde, **sertifika dosyasına** sağ tıklayın ve **Install Certificate (Sertifika Yükle) > Current User (Geçerli Kullanıcı) > Next'i (İleri)** seçtikten sonra **"Place all certificates in the following store" (Tüm sertifikaları aşağıdaki depoya yerleştir) > Browse'u (Göz At) >** ve **"Trusted Root Certification Authorities" (Güvenilir Kök Sertifika Yetkilileri) > Next (İleri) > Finish (Bitir) > OK'i (Tamam)** seçin

İstemci makinede API sertifikalarını test edin.

API Sertifikaları, Harita Görünümü ve AMS (İletişim Kutusu Yöneticisi) uygulamasının kurulu olduğu istemci makinede test edilmelidir.

İstemci makinede, Google Chrome tarayıcısını başlatın.

– Kimlik Sunucusunu test etmek için şu adrese girin: `https://[ServerHostname]:44333/.well-known/openid-configuration`
  – Kilit simgesi> Doğrula "Sertifika (Geçerli)" web sitesi bilgilerine sağ tıklayın ve "Gönderen" bölümünde doğru sertifikanın kullanılmakta olduğundan emin olun.
– Kartlı Geçiş API'sını test etmek için şu adresi girin: `https://[ServerHostname]:44347/swagger`
  – Kilit simgesi> Doğrula "Sertifika (Geçerli)" web sitesi bilgilerine sağ tıklayın ve "Gönderen" bölümünde doğru sertifikanın kullanılmakta olduğundan emin olun.
– Durum API'sını test etmek için şu adresi girin: `https://[ServerHostname]:62901/swagger`
  – Kilit simgesi> Doğrula "Sertifika (Geçerli)" web sitesi bilgilerine sağ tıklayın ve "Gönderen" bölümünde doğru sertifikanın kullanılmakta olduğundan emin olun.
– Harita API'sını test etmek için şu adresi girin: `https://[ServerHostname]:61801/odata/$metadata`
  – Kilit simgesi> Doğrula "Sertifika (Geçerli)" web sitesi bilgilerine sağ tıklayın ve "Gönderen" bölümünde doğru sertifikanın kullanılmakta olduğundan emin olun.

Sertifikayı AMS'de kullanın.

İstemci Makinede Harita Görünümü uygulamasını başlatın ve oturum açın.

3.7 Sorun giderme

Kurulum yapılamazsa ilerleme çubuğu kırmızıya döner. Ek hata metni görüntülenebilir.
Hangi bileşenin hata verdiğini gösteren özet sayfasına geçmek için **Next>**'e (İleri) tıklayın.

3.8 Sistemi güncelleme

Başlamadan önce

1. Sunucu makinede oturum açın
2. Sistemin önceki sürümünün kurulu olduğundan emin olun (bkz. **Sistemin kurulu olduğundan emin olma**).
3. Yeni kurulum paketini sunucu makinenize kopyalayın.

Uyarı!
Hem sunucu hem de istemci aynı sürümde kurulu olmalıdır. Sunucuya farklı bir istemci sürümü ile erişmeyi denemeyin.

Sunucu güncellemesini başlatma

1. Yazılım kurulum paketinin yeni sürümüne çift tıklayın.
2. Arayüz dilini seçin.
3. **Server**'a (Sunucu) çift tıklayın.
4. **AMS Server Setup.exe**'ye sağ tıklayın ve bağlam menüsünden **Run as administrator**'ı (Yönetici olarak çalıştır) seçin.

– Kurulum hazırlama sihirbazı açılır.
– Güncellemek istediğiniz bileşenleri seçin ve **Next>**'e (İleri) tıklayın.
– Kullanılabilenlere bağlı olarak, sihirbaz varsayılan olarak güncellenebilen bileşenleri işaretler.
– Bileşenleri güncellemeyi veya güncellemeyi atlamayı tercih edebilirsiniz.
– Güncellenemeyen bileşenler varsayılan olarak **Skip** (Atla) olarak işaretlenir.

5. **Son Kullanıcı Lisans Sözleşmesi**'ni okuyun ve devam etmek için **Accept**'e (Kabul et) tıklayın. Kabul etmiyorsanız **Decline**'a (Reddet) tıklayarak geri dönün ve işlemi iptal edin.
6. SQL Veritabanı Sunucusu yapılandırma verilerini girin.

– SQL Veritabanı Sunucusu yapılandırma verileri:
  – SQL Server: SQL Server örneğinin çalıştığı ana bilgisayar adı, yani yerel makine (önerilir)
  – SQL örneği: SQL örneği adı
  – AMS veritabanı: Veritabanının adı
  – SQL kullanıcı adı: SQL'de oturum açma adı
  – SQL şifresi: SQL'de oturum açmak için kullanılan SQL şifresi. Standart şifre: `sa_s3k_pw`

7. SQL şifresini girdikten sonra, **Test Server**'a (Sunucuyu Test Et) tıklayın.

– Test başarılı olursa SQL şifresi alanının altında yeşil arka plana sahip bir mesaj görünür.
– Veritabanı zaten varsa bir geçiş işlemi denenir.

8. **Next>**'e (İleri) tıklayın.

– Sonraki iletişim kutusunda sistemin sunucusunun saklanacağı kurulum yolu gösterilir.
– Varsayılan olarak, kurulum sihirbazı sistemin sunucusunu yerel `C:\Program Files` sürücüsüne (önerilir) kurar.
– Yerel `C:\Program Files` sürücüsü altına kurulan dosyalar sadece yönetici haklarına sahip kullanıcılar tarafından değiştirilebilir. Bu, yönetici hakları olmayan kullanıcıların sistemle ilgili dosyaları değiştirememesini sağlayarak güvenlik sunar.

9. Devam etmek için **Next>**'e (İleri) tıklayın.
10. Kurulum öncesi özetini kontrol edin ve **Install**'a (Kur) tıklayın.

– Güncellemeyi seçtiğiniz tüm bileşenleri içeren bir özet görüntülenir.

11. Kurulum ilerleme çubuğunu gözleyin.

– Hareketli yeşil çubuk, ilerleme çubuğunun yaklaşık olarak ortasına ulaştığında, tekrar hareket etmeye başlaması birkaç dakika sürer. Lütfen bekleyin.
– Access Engine (ACE) Veritabanı Kurulumu ile ilgili başka bir iletişim kutusu açılır. Bu ayar ACE veritabanını günceller. Veritabanı zaten kuruluysa güncellenir, aksi takdirde yeni bir veritabanı oluşturulur. Bu, birkaç dakika sürebilir. İletişim kutusu kapanana kadar bekleyin.

12. İşlem tamamlandıktan sonra, **Next>**'e (İleri) tıklayın ve güncelleme sonrası özetini inceleyin.

– Güncellenen tüm bileşenlerin bir özeti görüntülenir.

13. Sistemin güncellenen sürümünün kurulumunu bitirmek için **Finish**'e (Bitir) tıklayın.
14. Bilgisayarı yeniden başlatın (önerilir).

– Bilgisayar yeniden başlatılır.

15. Sistemin kurulu olup olmadığını kontrol edin (bkz. **Sistemin kurulu olup olmadığını kontrol etme**).

– Kuruluysa sistem uygulamasının güncellenen sürümünün yüklenmesi tamamlanmıştır.
– Varsayılan kullanıcı adı ve şifresi **Administrator** (Yönetici) olarak belirlenir. Şifrenin büyük ve küçük harf duyarlı olduğunu unutmayın (kullanıcı adı değildir).

İstemci güncellemesini başlatma

1. Yazılım kurulum paketinin yeni sürümüne çift tıklayın.
2. Arayüz dilini seçin.
3. **Client**'a (İstemci) çift tıklayın.
4. **AMS Client Setup.exe**'ye sağ tıklayın ve bağlam menüsünden **Yönetici olarak çalıştır**'ı seçin.

– Kurulum hazırlama sihirbazı açılır.
– Güncellemek istediğiniz bileşenleri seçin ve **Next>**'e (İleri) tıklayın.
– Kullanılabilenlere bağlı olarak, sihirbaz varsayılan olarak güncellenebilen bileşenleri işaretler.
– Bileşenleri güncellemeyi veya güncellemeyi atlamayı tercih edebilirsiniz:
– Güncellenemeyen bileşenler varsayılan olarak **Skip** (Atla) olarak işaretlenir.

5. **Son Kullanıcı Lisans Sözleşmesi**'ni okuyun ve devam etmek için **Accept**'e (Kabul et) tıklayın. Kabul etmiyorsanız **Decline**'a (Reddet) tıklayarak geri dönün ve işlemi iptal edin.

– Sonraki iletişim kutusunda sistemin istemcisinin saklanacağı kurulum yolu gösterilir.
– Varsayılan olarak, kurulum sihirbazı sistemin istemcisini yerel `C:\Program Files` sürücüsüne (önerilir) kurar.
– Yerel `C:\Program Files` sürücüsü altına kurulan dosyalar sadece yönetici haklarına sahip kullanıcılar tarafından değiştirilebilir. Bu, yönetici hakları olmayan kullanıcıların sistemle ilgili dosyaları değiştirememesini sağlayarak güvenlik sunar.

6. Sunucu adresini girin. Adres biçimi: Hostname:4999/tcp
7. Devam etmek için **Next>**'e (İleri) tıklayın.

– Sonraki iletişim kutusu, sistemin Harita Görünümü uygulamasının saklanacağı kurulum yolunu gösterir.
– Varsayılan olarak, kurulum sihirbazı sistemin Harita Görünümü uygulamasını yerel `C:\Program Files` sürücüne (önerilir) kurar.

8. Keşif adresini girin.

– Harita Görünümü uygulaması, sistemin uç noktalarını keşfetmek için keşif adresine bağlanır. Bu adres, keşif uç noktasının barındırıldığı sunucu adı ile port numarasını içeren bir URL'dir.

9. Kurulum öncesi özetini kontrol edin ve **Install**'a (Kur) tıklayın.
– Güncellemeyi seçtiğiniz tüm bileşenleri içeren bir özet görüntülenir.
10. Kurulum ilerleme çubuğunu gözleyin.
– İşlem tamamlanana kadar bekleyin.
11. İşlem tamamlandıktan sonra, **Next>**'e (İleri) tıklayın ve güncelleme sonrası özetini inceleyin.
– Güncellenen tüm bileşenlerin bir özeti görüntülenir.
12. Sistemin güncellenen sürümünün kurulumunu bitirmek için **Finish**'e (Bitir) tıklayın.
13. Bilgisayarı yeniden başlatın (önerilir).
– Bilgisayar yeniden başlatılır.
14. Sistemin kurulu olup olmadığını kontrol edin (bkz. **Sistemin kurulu olup olmadığını kontrol etme**).
– Kuruluysa sistem uygulamasının güncellenen sürümünün yüklenmesi tamamlanmıştır.
– Varsayılan kullanıcı adı ve şifresi **Administrator** (Yönetici) olarak belirlenir. Şifrenin büyük ve küçük harf duyarlı olduğunu unutmayın (kullanıcı adı değildir).

Bkz.
– *Sistemin kurulu olup olmadığını kontrol etme, sayfa 12*

3.9 Kaldırma

Sistemin yazılımını tamamen kaldırmak için, aşağıdaki adımları izleyin:

Sunucuyu kaldırma

1. Windows **Başlangıç** düğmesine tıklayın.
2. **Denetim Masası**'nı arayın ve açmak için çift tıklayın.
3. Şu yolu izleyin: **Programlar** > **Programlar ve Özellikler** > **Program kaldır**
– Kurulu programların listesi açılır.
4. **Kartlı Geçiş Yönetim Sistemi** - **Sunucu'ya sağ tıklayın** ve bağlam menüsünden **Kaldır**'ı seçin.
– Sistemin kaldırma sihirbazı açılır.
5. Kaldırmak istediğiniz bileşenleri seçin ve **Next>**'e (İleri) tıklayın. İşlemi iptal etmek için **Cancel**'a (İptal) tıklayın.
– Bileşenleri kaldırmayı veya atlamayı seçebilirsiniz. Çoğu bileşen zorunludur ve atlanamaz.
6. Kaldırmak istediğiniz bileşenleri seçin ve **Next>**'e (İleri) tıklayın. **SQL şifresini** girdikten sonra, **Test Server**'a (Sunucuyu Test Et) tıklayın.
– SQL Veritabanı Sunucusu yapılandırma verileri:
  – SQL Server: SQL Server'ın çalıştığı ana bilgisayar adı, yani yerel makine
  – SQL örneği: SQL örneği adı.
  – AMS veritabanı: Oluşturduğunuz veritabanının adı.
  – SQL kullanıcı adı: Oluşturduğunuz SQL oturum açma adı.
  – SQL şifresi: SQL oturumu açma işlemi için oluşturduğunuz SQL şifresi.
7. **Next>**'e (İleri) tıklayın.
8. Kaldırma ilerleme çubuğunu izleyin.
9. İşlem tamamlandıktan sonra, **Next>**'e (İleri) tıklayın ve kaldırma sonrası özetini inceleyin.
– Kaldırılan veya atlanan tüm bileşenleri içeren bir özet görüntülenir.
10. Sunucu kaldırma işlemini bitirmek için **Finish**'e (Bitir) tıklayın.
– Kaldırma sihirbazı kapanır.
– Sistem, kurulu programlar listesinden kaybolur.

– Sistemin simgesi masaüstünden kaybolur.

İstemciyi kaldırma

1. Windows **Başlangıç** düğmesine tıklayın.
2. **Denetim Masası**'nı arayın ve açmak için çift tıklayın.
3. Şu yolu izleyin: **Programlar** > **Programlar ve Özellikler** > **Program kaldır**

– Kurulu programların listesi açılır.

4. **Kartlı Geçiş Yönetim Sistemi** - **İstemci'ye sağ tıklayın** ve bağlam menüsünden **Kaldır**'ı seçin.

– Sistemin kaldırma sihirbazı açılır.

5. Kaldırmak istediğiniz bileşenleri seçin ve **Next>**'e (İleri) tıklayın. İşlemi iptal etmek için **Cancel**'a (İptal) tıklayın.

– Bileşenleri kaldırmayı veya atlamayı seçebilirsiniz. Çoğu bileşen zorunludur ve atlanamaz.

6. Kaldırma ilerleme çubuğunu izleyin.
7. İşlem tamamlandıktan sonra, **Next>**'e (İleri) tıklayın ve kaldırma sonrası özetini inceleyin.

– Kaldırılan veya atlanan tüm bileşenleri içeren bir özet görüntülenir.

8. İstemci kaldırma işlemini bitirmek için **Finish**'e (Bitir) tıklayın.

– Kurulum sihirbazı kapanır.
– Sistem, programlar listesinden kaybolur.
– Sistemin simgesi masaüstünden kaybolur.

Kaldırma işlemini tamamlamak için, yerel `C:` sürücünüzde `Program Files (x86)`'a gidin ve `Bosch Sicherheitssysteme` klasörünü silin.

4 Teknik veriler

Sunucu	
Desteklenen işletim sistemleri. Diğer işletim sistemlerine yüklenebilir, ancak bu tamamen garanti dışıdır.	– Windows Server 2016 (64 bit, Standart, Veri Merkezi) – Windows 10, version 1903 (LTSB, LTSC) – **Not:** Bu sistemle sunulan varsayılan veritabanı, gelişmiş hizmetler sunan SQL Server 2017 Express sürümüdür.

Minimum donanım gereksinimleri	– En az 4 fiziksel çekirdekli Intel i5 işlemci
	– 8 GB RAM (32 GB önerilir)
	– 200 GB boş sabit disk alanı (SSD diskler önerilir)
	– Aşağıdakilere sahip grafik adaptörü:
	  – 256 MB RAM
	  – 1280x1024 çözünürlük
	  – En az 32 k renk
	– 1 Gbit/sn. Ethernet kartı
	– Kurulum dosyaları için boş bir USB portu veya ağ paylaşımı

İstemci	
Desteklenen işletim sistemleri. Diğer işletim sistemlerine yüklenebilir, ancak bu tamamen garanti dışıdır.	– Windows 10, sürüm 1803 (LTSB, LTSC)

Minimum donanım gereksinimleri	– Intel i5 veya üzeri
	– 8 GB RAM (16 GB önerilir)
	– 20 GB boş sabit sürücü alanı
	– Aşağıdakilere sahip grafik adaptörü:
	  – 256 MB RAM
	  – 1920x1080 çözünürlük
	  – En az 32 k renk
	– DirectX® 11
	– 1 Gbit/sn. Ethernet kartı
	– Kurulum dosyaları için boş bir USB portu veya ağ paylaşımı

MAC sunucusu	

Minimum donanım gereksinimleri	– Intel i5 veya üzeri
	– 8 GB RAM (16 GB önerilir)
	– 20 GB boş sabit sürücü alanı
	– Aşağıdakilere sahip grafik adaptörü:
	  – 256 MB RAM
	  – 1280x1024 çözünürlük
	  – En az 32 k renk
	– 1 Gbit/sn. Ethernet kartı

Uyarı!
Hem sunucu hem de istemci aynı sürümde kurulu olmalıdır. Sunucuya farklı bir istemci sürümü ile erişmeyi denemeyin.

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