Access Management System V5.2

Yapılandırma ve çalıştırma

tr Software manual

İçindekiler

1 Güvenlik

En güncel yazılımı kullanın

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

Aşağıdaki bağlantılar daha fazla bilgi sağlar:

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

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

2 Yardım'ı Kullanma

Bu yardım dosyasının nasıl kullanılacağını öğrenin.

Araç çubuğu düğmeleri

Düğme	İşlev	Açıklama
	Gizle	Yalnızca yardım bölmesini görünür bırakarak gezinti bölmesini (İçindekiler, Dizin ve Arama sekmeleri) gizlemek için bu düğmeye tıklayın.
	Göster	Hide (Gizle) düğmesine tıklandığında, bu düğme Show (Göster) düğmesi ile yer değiştirir. Navigation (Gezinti) bölmesini yeniden açmak için bu düğmeye tıklayın.
	Geri	En son görüntülenen konulara geri dönmek için bu düğmeye tıklayın.
	İleri	Aynı konular arasında yeniden ileriye doğru gitmek için bu düğmeye tıklayın
	Yazdır	Yazdırmak için bu düğmeye tıklayın. “Print the selected topic” (Seçili konuyu yazdır) ve “Print the selected heading and all subtopics” (Seçili başlığı ve tüm alt konuları yazdır) arasında seçim yapın.

Sekmeler

İçindekiler Bu sekme hiyerarşik bir içindekiler tablosu gösterir. Bir kitap simgesine  açmak için tıklayın  ve ardından konuyu görüntülemek için  bir konu simgesine tıklayın.

Dizin Bu sekme terimler dizinini alfabetik sırayla gösterir. Listeden bir konu seçin veya o kelimeyi içeren konuları bulmak için bir kelime yazın.

Arama Herhangi bir metni bulmak için bu sekmeyi kullanın. Alana metni girin ve ardından girilen tüm kelimeleri içeren konuları bulmak için **Konuları Listele** düğmesine tıklayın.

Yardım penceresini yeniden boyutlandırma

İstenilen boyut için pencerenin köşesini veya kenarını sürükleyin.

Bu belgede kullanılan diğer geleneksel yöntemler

– Arayüzde bulunan metinler (etiketler) **kalın** olarak görüntülenir.

Örn. **Araçlar, Dosya, Farklı Kaydet...**

- Tıklama sırası **>** karakteri (büyüktür işareti) kullanılarak sıralanır.
  Örn. **Dosya > Yeni > Klasör**
- Sıralama içindeki kontrol türü değişiklikleri (örn. menü, radyo düğmesi, onay kutusu, sekme) kontrol etiketinden sonra belirtilir.
  Ör. **Extra > Options >** (Daha Fazla > Seçenekler >) menülerine ve **View** (Görüntüle) sekmesine tıklayın
- Tuş kombinasyonları iki şekilde yazılır:
  - Ctrl+Z ilk tuşu basılı tutarken ikinciye de basın anlamına gelir
  - Alt, C ilk tuşa basın ve bırakın, ardından ikinci tuşa basın anlamına gelir
- Simge düğmelerinin işlevleri simgenin kendisinden sonra köşeli parantez içerisine eklenir.
  Ör. [Save] (Kaydet)

3 Bu belge hakkında

Bu, Access Management System'ın ana yazılım kılavuzudur.
Bundan sonra AMS olarak anılacak olan ana iletişim yöneticisi programının kullanımını kapsar.

- AMS'deki bir kartlı geçiş sisteminin yapılandırılması.
- Yapılandırılmış sistemin sistem operatörleri tarafından çalıştırılması.

İlgili belgeler

Aşağıdakiler ayrıca belgelenmiştir:

- AMS ve yardımcı programlarının kurulması.
- AMS - Map View'ın (AMS - Harita Görünümü) çalışması.

4 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.

5 Sistemi lisanslama

Ön koşullar

– Sistem başarıyla kuruldu.
– AMS sunucu bilgisayarında, tercihen Yönetici olarak oturum açtınız.

Satın alınan lisanslara ilişkin prosedür

Ön gereksinimler: Bu bilgisayarın bilgisayar imzasına göre lisanslar satın aldınız. Talimatlar için satış temsilcinize başvurun.

Lisansı etkinleştirme

Yol

– AMS dialog manager (AMS iletişim yöneticisi) > **Main menu (Ana menü)** > **Configuration (Yapılandırma)** > **Licenses (Lisanslar)**

1. **License Manager**'a (Lisans Yöneticisi) tıklayın,
   License Manager (Lisans Yöneticisi) sihirbazı açılır.
2. Sistem bilgilerinizi bir dosyaya kaydetmek için **Save**'e (Kaydet) tıklayın.
3. **Continue**'ya (Devam) tıklayın.
4. remote.boschsecurity.com adresinde şirket bilgilerinizi kullanarak remote portal'da oturum açın.
5. Lisanslanacak ürünü seçin ve lisans dosyanızı oluşturup karşıdan yüklemek için portaldaki yönergeleri izleyin.
6. **License Manager**'a (Lisans Yöneticisi) geri dönün.
7. **Continue**'ya (Devam) tıklayın.
8. Karşıdan yüklediğiniz lisans dosyasını bulmak için **Import**'a (İçe aktar) tıklayın ve dosyayı sisteminize ekleyin.
9. **Finish**'e (Bitir) tıklayın.

Uyarı!
İşlem sırasında herhangi bir hata mesajı ile karşılaşırsanız Bosch destek ile iletişime geçin.

Uyarı!
Donanım ve yazılım değişikliklerinin etkileri
Sunucunuzun donanımında yapılan değişiklikler, lisansınızı geçeriz kılarak yazılımın çalışmasının durmasına neden olabilir. Sunucuda değişiklik yapmadan önce lütfen teknik destek ekibine danışın.

Demo Modu Prosedürü

Demo Modu sınırlı bir süre için tüm sistem özelliklerini lisanslar. Gösterim Modunu yalnızca özellikleri satın almadan önce denemek için üretim dışı ortamlarda kullanın.

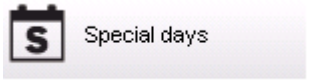
1. Kartlı Geçiş Yöneticisi'nde oturum açın
2. **Configuration** (Yapılandırma) > **Licenses** (Lisanslar) bölümüne gidin.
3. **Activate Demo Mode** (Demo Modunu Etkinleştir) düğmesine tıklayın
4. Özelliklerin **Licenses** (Lisanslar) iletişim penceresinde gösterildiğinden emin olun.

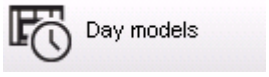
Demo modu için 5 saat boyunca etkindir. Sona erme zamanının **Licenses** (Lisanslar) iletişim kutusunun üst kısmının yanında ve çoğu iletişim penceresinin başlık çubuğunda yer aldığını unutmayın.

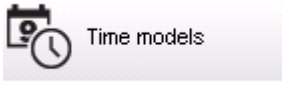
6 Takvimi yapılandırma

Kartlı geçiş etkinliklerinin programlanması **zaman modelleri** ile düzenlenir.
Bir **zaman modeli**, her biri bir **gün modeli** ile açıklanan bir veya daha fazla günden oluşan soyut bir sıralamadır.
Zaman modelleri, kartlı geçiş sisteminin temel aldığı **takvime** uygulandıklarında etkinlikleri kontrol eder.
Kartlı geçiş sisteminin takvimi, ana bilgisayarın işletim sisteminin takvimini temel alır, ancak bunu kartlı geçiş sisteminin yöneticisi tarafından serbestçe tanımlanan **özel günlerle** güçlendirir.
Özel günler, takvimde belirli bir tarihe sabitlenebilir veya Paskalya gibi bir kültürel etkinliğe göre tanımlanabilir. Bunlar yinelenebilir olabilir ya da olmayabilir.
Kartlı geçiş sisteminize ilişkin etkili bir takvim yapılandırması aşağıdaki adımlardan oluşur.

1. Bulunduğunuz konum için geçerli takvimin **özel günlerini** tanımlayın.
2. Her gün türünün etkin ve etkin olmayan dönemlerini tanımlayan **gün modellerini** tanımlayın. Örneğin, bir resmi tatilin gün modeli normal iş gününden farklı olacaktır. Vardiyalı çalışma, istediğiniz gün modellerinin türünü ve sayısını da etkileyecektir.
3. Bir veya daha fazla gün modelinden oluşan **zaman modelleri** tanımlayın.
4. Kart sahipleri, yetkiler ve girişlere zaman modelleri atayın.

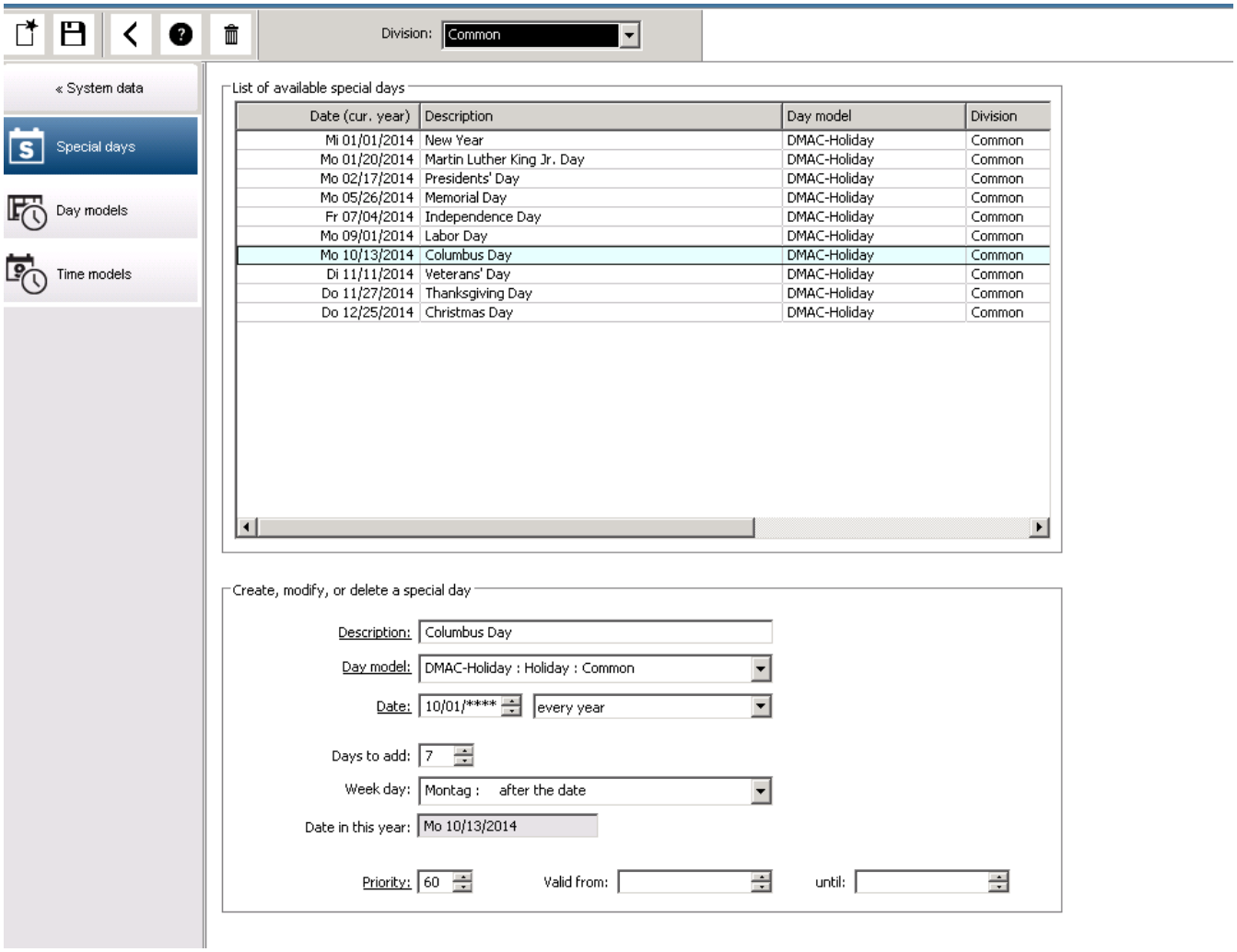






6.1 Özel günleri tanımlama

Bu iletişim kutusu açıldığında, iletişim kutusunun en üstteki liste alanında belirtilen tüm tatilleri içeren bir liste görünür. Gösterilen tüm tatil tarihlerinin yalnızca geçerli yılla ilgili olduğunu lütfen unutmayın. Ancak, takvim girilen verilere uygun olarak yıldan yıla güncellenir.
Listenin altında yeni özel günler oluşturmak ve mevcut özel günleri değiştirmek veya silmek için farklı iletişim kutusu alanları vardır. Yeni bir özel gün eklemek için, bu giriş alanlarının en az üçü veri içermelidir. Öncelikle ilgili alanlara bir **açıklama** ve bir **tarih** girilmelidir. Sonra bu özel günün ait olduğu **sınıf** ilgili seçmeli listeden seçilmelidir.



Tarih birkaç adımda belirtilir. Her şeyden önce, **Tarih** alanına bir başlangıç tarihi girilir. Bu noktada, tarih geçerli yıldaki bir olayı tanımlar. Kullanıcı burada tarih alanının yanındaki seçim listesinde periyodik geri dönüş sıklığını belirtirse dönemsellikle ayarlanan tarihin kısımlar "joker karakterler" (*) ile değiştirilir.

bir kez	__.__.____
yılda bir kez	__.__.****
bir yıllık bir dönemde ayda bir kez	__.**.____
her yıl ayda bir kez	__.**.****
Paskalya'ya bağlı	**.**.****

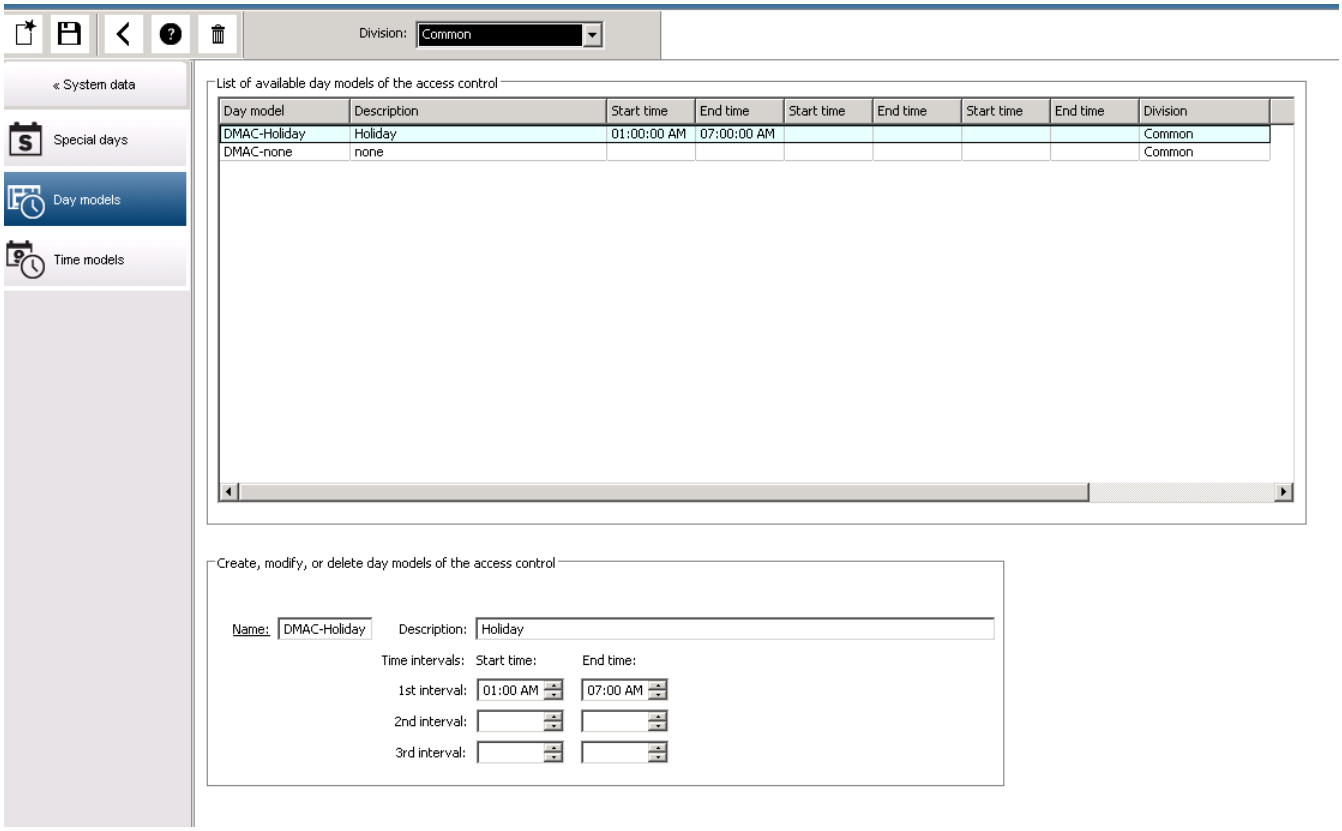
Paskalya'ya bağlı tatiller tarihleriyle değil ancak Paskalya Pazarı'ndaki günlerdeki farkla belirtilir. Geçerli yıldaki Paskalya Pazarı'nın tarihi **Bu yıl içindeki tarih** alanında gösterilir ve bu tarihin değişimi **Eklenecek günler** alanına girilir veya bu alanda seçilir. Maksimum gün sayısı 188'dir, bu nedenle ekleyerek veya çıkararak yılın her gününü tanımlayabilirsiniz.
Diğer veriler, örneğin tatilin **iş günü** isteğe bağlıdır. İş gününün işletim sisteminin (İS) bölgesel ayarlarıyla belirlendiğini lütfen unutmayın. Bu, kaçınılmaz olarak kartlı geçiş sistemi ve işletim sisteminin dillerinin farklı olduğu karışık dil ekranlarına yol açar.
Bir **geçerlilik süresinin** atanması da isteğe bağlıdır. Süre belirtilmediyse varsayılan ayarlar geçerliliği giriş tarihinden itibaren sınırsız hale getirir.

Bir **öncelik** de ayarlanabilir. 1'den 100'e doğru artan öncelik hangi tatilin kullanılması gerektiğini tanımlar. İki tatil aynı güne denk gelirse yüksek öncelikli tatil ilk sıraya gelir. Önceliklerin eşit olması durumunda hangi tatilin kullanılacağı tanımlanmamıştır.
"0" önceliğine sahip tatil devre dışı bırakılır ve kullanılmaz.
Zaman Modelleri iletişim kutusu yalnızca örneğin 0'dan daha yüksek önceliğe sahip etkin tatilleri görüntüler.

Uyarı!
"Ortak" bölümünün zaman modeli yalnızca "Ortak" bölümüne atanan tatilleri kullanabilir.
"A" özel bölümünün zaman modeli yalnızca "A" bölümüne atanan tatilleri kullanabilir.
Tatiller bölümler arasında karıştırılamaz. Örneğin her bölüm yalnızca özel zaman modeline atanan özel tatilleri kullanabilir.

6.2 Gün modellerini tanımlama

Gün modelleri herhangi bir güne ait modeli tanımlar. En fazla üç aralığa sahip olabilir.
İletişim kutusu başlatıldıktan sonra, mevcut tüm gün modelleri görüntülenir.



Model adı, açıklamalar veya aralıkları tanımlamak ya da değiştirmek için bu iletişim kutusunu kullanın.  simgesi yeni bir model başlatır.
Bir aralığın Başlangıç ve Bitiş saatleri saat ve dakika olarak girilir. Böyle bir zamana erişildiğinde aralık sırasıyla etkinleştirilir veya devre dışı bırakılır. Bu saatleri sınırlayıcılar olarak daha net bir şekilde işaretlemek için, liste bölmesi bunları saniyelerle (her zaman 00) görüntüler. Örneğin, bir zaman modelindeki 08:00 ila 15:30 arasındaki bir aralığı kapsayan bir yetki 08:00 ila 15:30 arasında girişe izin verir ancak 15:30:01'deki girişi engeller.

Başlangıç ve bitiş saatleri girildiklerinde mantıksal kontrollere tabidir, örneğin bir başlangıç saati ilgili bitiş saatinden önce olmalıdır.
Bunun sonuçlarından biri hiçbir aralığın gece yarısına uzatılamayacağı, ancak noktada bölünmesi gerektiğidir:

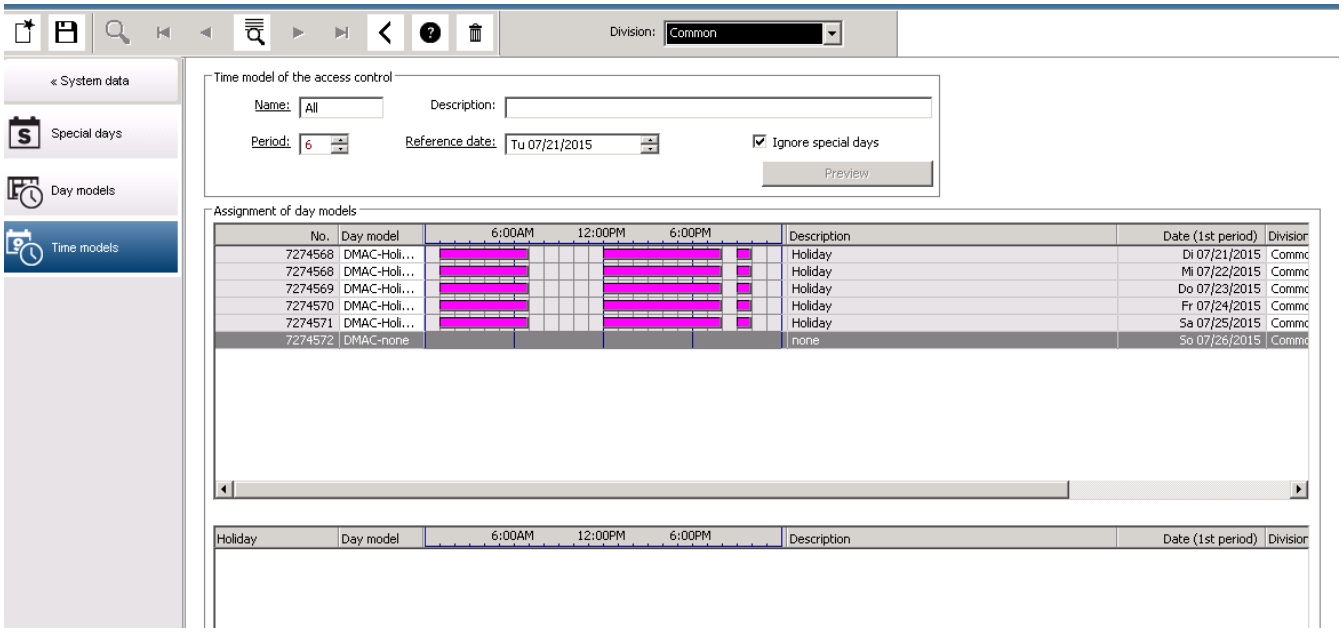
1. Aralık	başlangıç:	...	bitiş:	12:00
Sonraki Aralık	başlangıç:	12:00	bitiş:	...

Gece yarısı (00:00) istisnasıyla tek bir gün modelinin aralık sınırlayıcıları arasında çakışmalara izin verilmez. Bunun, aynı saatli bir aralığın sonu ve sonraki aralığın başı için girmeyi engellediğini unutmayın.
İstisna: Bununla birlikte 24 saatlik bir aralık ikisi de 00:00'a ayarlanan başlangıç ve bitiş saatlerine sahiptir.

Uyarı!
İpucu: Aralıkları Zaman modelleri iletişim kutusunda görüntüleyerek kontrol edebilirsiniz. Öncelikle bu aralıkları içeren bir gün modeli oluşturun (Sistem verileri > Takvim > Gün modelleri). Ardından bu gün modelini aynı bir günlük süreye sahip boş bir zaman modeline atayın (Sistem verileri > Takvim > Zaman modelleri). Ardından aralıklar çubuk grafikte gösterilir.
Değişiklikleri kaydetmeden Zaman modelleri iletişim kutusundan çıkın.

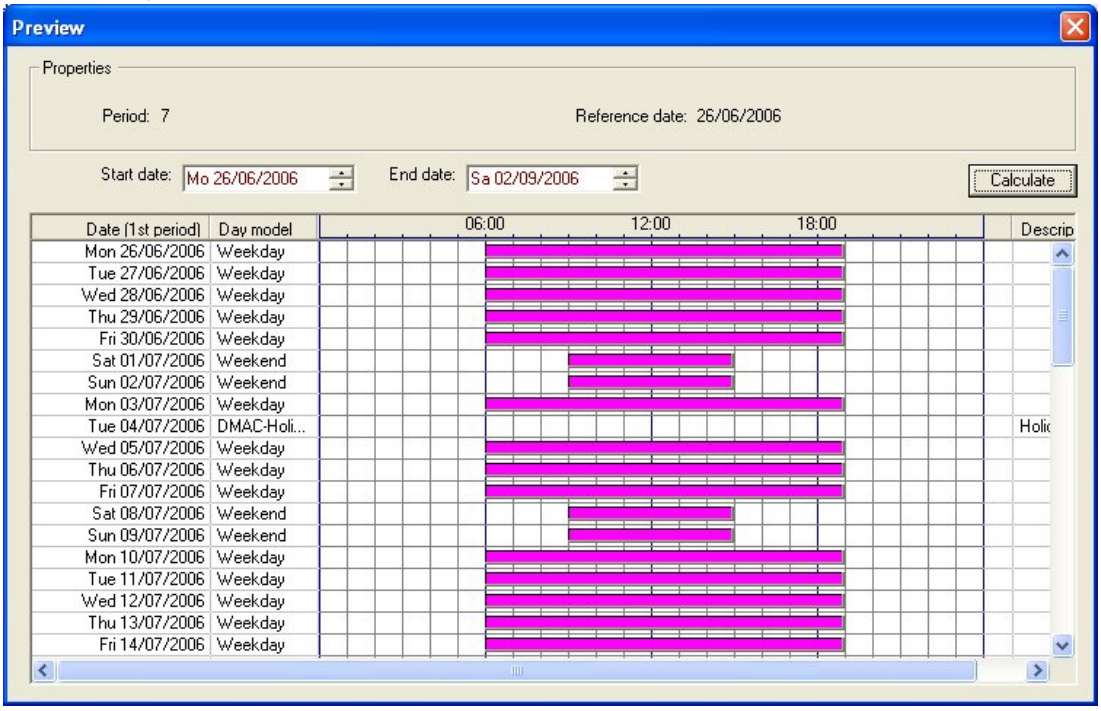
Bir gün modeli yalnızca özel bir güne atanmadıysa ve bir zaman modelinde kullanılmıyorsa silinebilir.

6.3 Zaman modellerini tanımlama

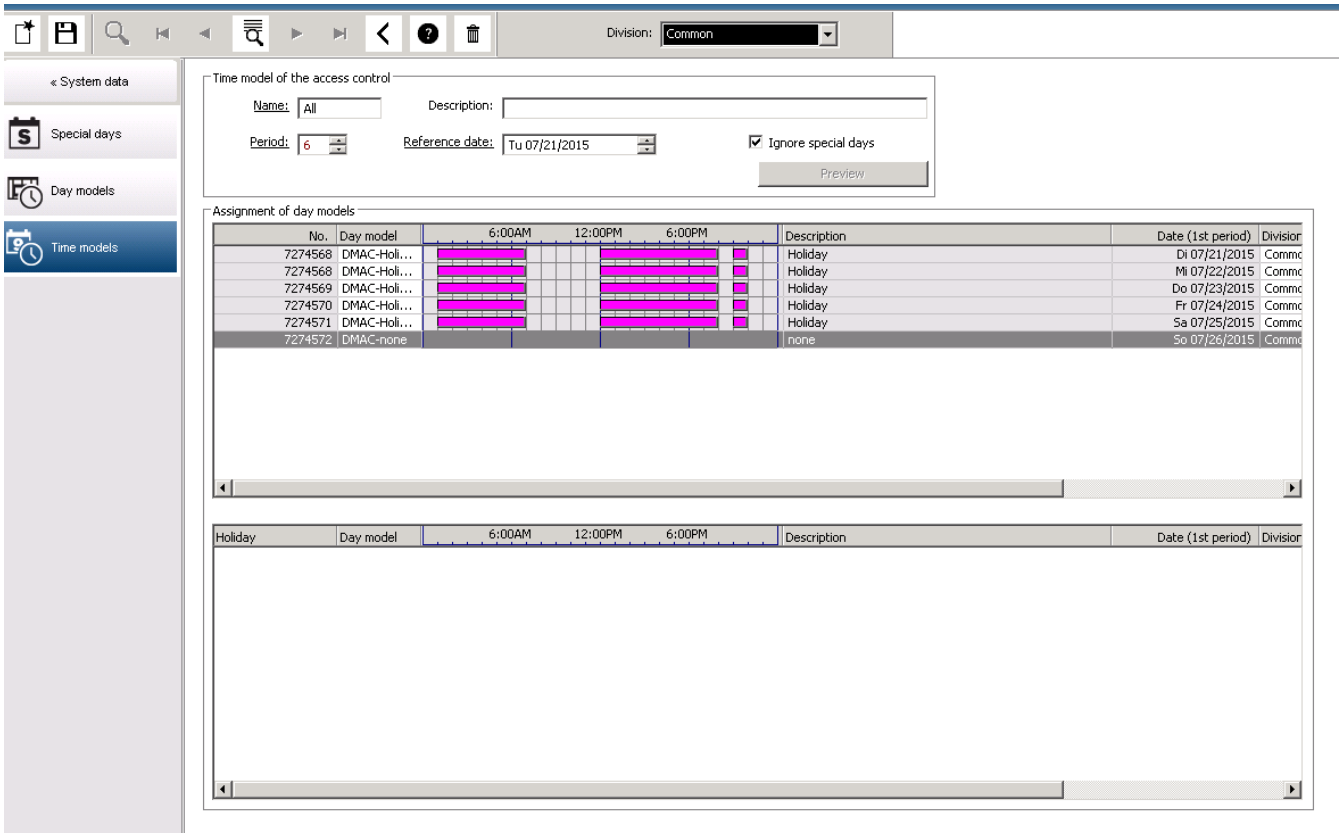


Mevcut zaman modelleri arama listesinden seçilebilir ve ayrıntıları iletişim kutusu alanlarında görüntülenir. Her türlü işleme yeni zaman modelleri oluşturmak için prosedüre uygun olarak gerçekleştirilir.
Maske boşsa zaman modelleri en baştan oluşturulur. Bunu yapmak için, bir **ad** ve **dönemdeki** gün sayısını girerek bir başlangıç veya **referans tarihi** girmeniz gerekir. Bu veriler onaylandığında (**Enter**), bunun altındaki **Gün modellerinin atanması** iletişim kutusunda bir

liste görünür. Bu listedeki satır sayısı yukarıda ayarlanan gün sayısına denk gelir ve sütunlar seçilen başlangıç tarihinden başlayarak zaten bir ilerleyen numara ve dönemin tarihlerini içerir.
Yalnızca **"Ad"** sütunundaki girişler bu listede kullanıcı tarafından değiştirilebilir veya eklenebilir; daha önce bahsedildiği gibi **“No.”** ve **“Tarih”** sütunlarındaki girişler iletişim kutusunun başlığındaki açıklamalardan ortaya çıkar; **"Açıklama"** sütunu, sistem tarafından bir gün modeli seçimiyle ve bu iletişim kutusunda yapılan açıklamalarla doldurulur.
Gün modeli sütununun ilgili satırına çift tıklandığında, bir seçim listesi alanı etkinleştirilir. Bu listeden mevcut gün modellerinden biri seçilebilir. Bu şekilde, belirli bir gün modeli dönemin her gününe atanabilir. Kullanıcı başka bir satıra geçtiğinde, seçilen gün modeline ait mevcut bir açıklama sistem tarafından **Açıklama** sütununda gösterilir.
İlgili gün modelleriyle önceden tanımlanan **tatiller** gezinme ve kontrol amacıyla alt liste alanında gösterilir. Seçilen veya yeni oluşturulan zaman modelinde, gün modellerinin belirli tatillere atanması değiştirilebilir. Ancak, bu değişiklikler yalnızca bu özel zaman modeli için geçerli olacaktır; tüm mevcut ve gelecekteki modellere uygulanacak genel değişiklikler yalnızca Tatiller iletişim kutusunda yapılabilir. Bu ayarlara uygun olarak, iş günlerine tatiller dikkate alınarak atanan gün modelleri verilebilir.
Ardından bu ayarlara uygun biçimde iş günleri özel günler dikkate alınarak atanan gün modelleriyle karşılaştırılır. Gün modellerinin doğru şekilde kullanılıp atandığından hızlıca emin olmak için (özellikle tatillerde) bu iletişim kutusu belirli dönemlere ilişkin gün tahsisini gösteren bir **ön izleme** içerir.
Son olarak, **Ön İzleme** düğmesine tıklanarak ayrı bir iletişim kutusu açılır ve tatiller dahil en fazla 90 günlük bir süre belirtilebilir. **Calculate** (Hesapla) düğmesine tıklandığında, rapor oluşturulur ve aşağıda gösterildiği gibi görüntülenir; bu işlem aralığın uzunluğuna bağlı olarak birkaç saniye sürebilir.



Varsayılan ayarda özel günler tanımlarına göre zaman modellerine uygulanır. Ancak özel günlerde olağanüstü bir husus bulunamazsa bu **Özel günleri yok say** seçeneğinin seçilmesine neden olabilir. Aynı anda iki alt listedeki girişler silinir, böylece kullanıcı özel günlerin ve gün sınıflarının bu modelde hiçbir kullanım alanı bulamadığını derhal öğrenir.


Division:
Common
« System data
Special days
Day models
Time models
Time model of the access control
Name:
All
Description:
Period:
6
Reference date:
Tu 07/21/2015
Ignore special days
Preview
Assignment of day models
No.
Day model
6:00AM
12:00PM
6:00PM
Description
Date (1st period)
7274568 DMAC-Holi... Holiday Di 07/21/2015
7274568 DMAC-Holi... Holiday Mi 07/22/2015
7274569 DMAC-Holi... Holiday Do 07/23/2015
7274570 DMAC-Holi... Holiday Fr 07/24/2015
7274571 DMAC-Holi... Holiday Sa 07/25/2015
7274572 DMAC-none none So 07/26/2015
Holiday
Day model
6:00AM
12:00PM
6:00PM
Description
Date (1st period)

7 Bölümleri Yapılandırma

Giriş

Sistem isteğe bağlı olarak, **Divisions** (Bölümler) adı verilen herhangi bir sayıdaki bağımsız taraf tarafından paylaşılan bir tesis için müşterek kartlı geçiş imkânı sağlayacak şekilde lisanslanır.

Sistem operatörlerine atanmış bir veya daha fazla bölüm bulunabilir. Böylece operatörler yalnızca ilgili bölümlere ilişkin kişiler, cihazlar ve girişleri görür.

Divisions (Bölümler) özelliğinin lisanslanmadığı durumlarda, sistem tarafından yönetilen tüm nesneler **Common** (Ortak) olarak adlandırılan tek bir bölüme aittir.

Ön koşullar

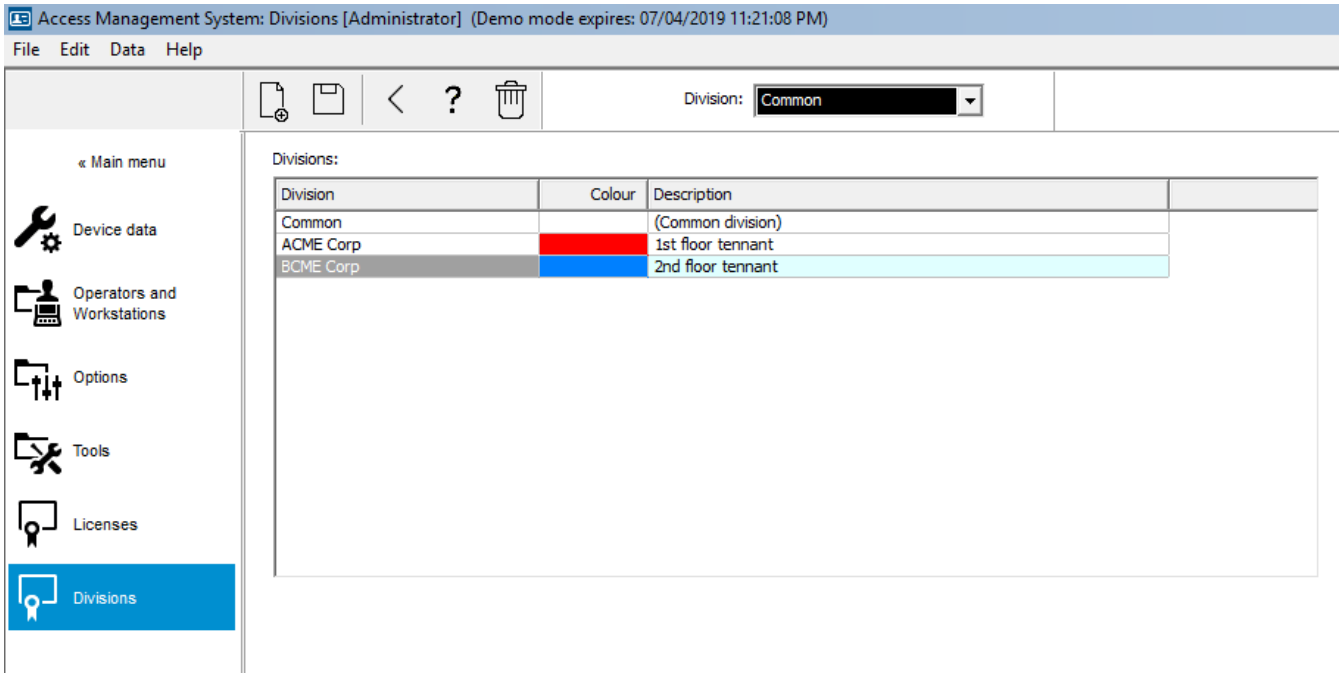
– Divisions (Bölümler) kurulumunuz için lisanslanmış olmalıdır.

İletişim yolu

– Main menu (Ana menü) > **Configuration** (Yapılandırma) > **Divisions** (Bölümler)

Prosedür

1. Araç çubuğundaki simgesine tıklayın.
   – Varsayılan bir ada sahip yeni bir bölüm oluşturulur.
2. Varsayılan adın üzerine yazın ve (isteğe bağlı) diğer operatörlerin yararlanmaları için bir açıklama girin.
3. Kullanıcı arayüzündeki bölüm varlıklarını birbirlerinden ayırt etmenize yardımcı olacak bir renk atamak için **Color** (Renk) sütununun içine tıklayın.
4. Kaydetmek için simgesine tıklayın



7.1 Bölümleri cihazlara atama

Cihaz düzenleyicideki cihazlara bölüm atama

İletişim yolu

Main menu (Ana menü) > **Configuration** (Yapılandırma) > **Device data** (Cihaz verileri)

Ön koşullar

– Divisions (Bölümler) lisanslanmış ve çalışır durumda olmalıdır
– En az bir bölüm oluşturulmuş olmalıdır.

Prosedür

1. Cihaz ağacında atanacak cihazı seçin.
   – Cihaz düzenleyici, ana iletişim bölmesinde görünür.
2. Division (Bölüm) listesinden cihazın yeni bölümünü seçin.
   – Liste kutusunda yeni bölüm gösterilir.
3. Kaydetmek için  (Kaydet) simgesine tıklayın

Uyarı!
Bir girişe ait tüm bileşenlerin bir bölüme ait olması gerekir
Sistem tüm bileşenleri aynı bölüme ait olana kadar bir girişi kaydetmenize izin vermez.

7.2 Bölümleri operatörlere atama

User rights (Kullanıcı hakları) iletişim kutusunda operatörlere bölüm atama

İletişim yolu

Main menu (Ana menü) **Configuration** (Yapılandırma) > **Operators and workstations (Operatörler ve iş istasyonları) > User rights** (Kullanıcı hakları)

Ön koşullar

– Divisions (Bölümler) lisanslanmış ve çalışır durumda olmalıdır
– En az bir bölüm oluşturulmuş olmalıdır.
– Sistemde en az bir operatör oluşturulmuş olmalıdır

Prosedür

1. **User hakları** (Kullanıcı hakları) iletişim kutusunda, atanacak operatörün personel kaydını seçin.
2. **Divisions** (Bölümler) sekmesinde, bölümleri **Available divisions** (Mevcut bölümler) listesinden bu operatörün **Assigned divisions** (Atanan bölümler) listesine taşımak için ok tuşlarını kullanın.
3. Kaydetmek için  (Kaydet) simgesine tıklayın

8 IP adreslerini yapılandırma

Ağdaki yerel giriş kontrol cihazlarının kartlı geçiş sistemine katılmaları için tutarlı bir IP adresi düzeni gereklidir. **AccessIPConfig** aracı, kontrol cihazlarını ağda bulur ve bunların adresleri ile diğer ağ seçeneklerini merkezi olarak yönetmek için uygun bir arayüz sunar.

Ön gereksinimler

– Yerel giriş kontrol cihazları açık ve ağa bağlı olmalıdır.
– Kontrol cihazlarının IP adresleri ve gerekiyorsa şifreleri için bir düzeniniz olmalıdır.

İletişim yolu

Main menu (Ana menü) > **Configuration** (Yapılandırma) > **Tools** (Araçlar)

Prosedür

1. Yukarıdaki iletişim yolunu izleyin ve **Configuration AMC and fingerprint devices 'a (Yapılandırma AMC ve parmak izi cihazları) tıklayınAccessIPConfig** aracı açılır.
2. **Scan AMCs**'e (AMC'leri tara) tıklayın
   Ağda bulunan yerel giriş kontrol cihazlarının her biri aşağıdaki parametrelerle birlikte gösterilir:
   – **MAC address** (MAC adresi): Kontrol cihazının donanım adresi. Bunun, tesadüfen yalnızca MAC olarak adlandırılan Ana Giriş Kontrol Cihazı'nın adresi **olmadığını** unutmayın.
   – **Stored IP address** (Saklanan IP adresi):
   – **Port number** (Port numarası): Varsayılan `10001`'dir
   – **DHCP**: Değer, sadece kontrol cihazı DHCP'den bir IP adresi alacak şekilde yapılandırılmışsa **Yes**'tir (Evet).
   – **Current IP addresss** (Geçerli IP adresi)
   – **Serial number** (Seri numarası)
   – Ağ yapılandırma ekibi tarafından eklenen notlar
3. Açılır penceredeki parametrelerini değiştirmek için listedeki bir AMC'ye çift tıklayın.
   Alternatif olarak, istediğiniz AMC'nin satırını seçin ve **Set IP...**'ye (IP Ayarla...) tıklayın.
   Cihaz için yapılandırılmışsa şifre girmek gerekebileceğini unutmayın.
   Değiştirilen parametreler, siz açılır pencerede OK'e (Tamam) tıklar tıklamaz saklanır.
4. Kontrol cihazlarının IP parametrelerini yapılandırmayı tamamladığınızda, aracı kapatmak için **File** (Dosya) > **Exit**'e (Çıkış) tıklayın.
   Ana uygulamaya geri dönersiniz.

Daha ayrıntılı bilgi için, kendi yardım dosyasını görüntülemek üzere **AccessIPConfig** aracındaki **Help**'e (Yardım) tıklayın.

9 Cihaz Düzenleyici'yi kullanma

Giriş

Cihaz Düzenleyici giriş ve cihaz eklemek, silmek veya değiştirmek için kullanılan bir araçtır. Cihaz Düzenleyici, aşağıdaki düzenlenebilir hiyerarşilere ait görünümler sunar:

- **Device configuration** (Cihaz yapılandırması): Kartlı geçiş sistemindeki elektronik cihazlar.
- **Workstations** (İş İstasyonları): Kartlı geçiş sistemindeki iş birliği yapan bilgisayarlar.
- **Areas** (Alanlar): Kartlı geçiş sisteminin bölündüğü fiziksel alanlar.

Ön koşullar

Sistemin doğru şekilde kurulması, lisanslanması ve ağda yer alması gerekir.

İletişim yolu

- **Main menu** (Ana menü) >**Configuration** (Yapılandırma) > **Device data** (Cihaz verileri)

Cihaz Düzenleyici araç çubuğunu kullanma

Cihaz Düzenleyici araç çubuğu düğmeleri, örneğin **Devices** (Cihazlar), **Workstations** (İş İstasyonları) veya **Areas** (Alanlar) olmak üzere hangi görünümün etkin olduğundan bağımsız olarak aşağıdaki işlevleri sunar.

Düğme	Kısayol	Açıklama
	Ctrl + N	Seçilen düğümün altında yeni bir öğe oluşturur. Alternatif olarak, bağlam menüsünü çağırmak için düğüme sağ tıklayın.
	Del	Seçilen öğeyi ve altındaki tüm öğeleri siler.
	Ctrl-Page up	Ağaçtaki ilk öğe
	Ctrl -	Önceki öğe
	Ctrl +	Sonraki öğe
	Ctrl-Page down	Ağaçtaki son öğe
	Ctrl-A	Ağacı genişletir ve daraltır.
	Ctrl-K	Verileri veritabanından yeniden yükleyerek yeniler. **Kaydedilmeyen tüm değişiklikler iptal edilir.**
	Ctrl-S	Geçerli yapılandırmayı kaydeder
	Ctrl-F	Bir arama penceresi açar
		**Device configuration** (Cihaz yapılandırması) ağacını açın

		**Workstations** (İş İstasyonları) ağacını açın
		**Areas** (Alanlar) ağacını açın

Tüm Cihaz Düzenleyici görünümlerinde, ağacın kökünden başlayın ve araç çubuğu düğmeleri, menü veya her öğenin bağlam menüsünü kullanarak öğeleri ekleyin (çağırmak için sağ tıklayın). Bir cihaza alt öğeler eklemek için önce alt öğelerin altında görünmesi gereken ana cihazı seçin.

AMC cihazlarını kopyalayıp yapıştırma

AMC cihazlarını ağacın bir bölümünden diğerine kopyalamak için:

1. AMC cihazına sağ tıklayın ve bağlam menüsünden **Copy**'yi (Kopyala) seçin.
2. Ağaçta başka bir yerde bulunan uygun bir ana cihaza sağ tıklayın ve bağlam menüsünden **Paste**'i (Yapıştır) seçin.
   - Cihaz, alt cihazları ve ayarları ile birlikte yeni konuma kopyalanır.
   - **IP address** (IP adresi) ve **Name** (Ad) gibi benzersiz olması gereken cihaz parametreleri **kopyalanmaz**.
3. Zorunlu olan cihaz parametreleri için benzersiz değerler girin. Bunu yapana kadar cihaz ağacını kaydedemezsiniz.

Çalışmanızı kaydetme

Ağaca öğe eklemeyi ve değiştirmeyi bitirdiğinizde, yapılandırmayı kaydetmek için **Save**'e  (Kaydet) tıklayın.

Cihaz Düzenleyici'yi kapatmak için **File** (Dosya) > **Exit**'e (Çıkış) tıklayın.

9.1 Yapılandırma modları ve geçersiz kılma işlemleri

Yapılandırma modu, cihaz düzenleyicisindeki kartlı geçiş kontrol cihazlarının varsayılan durumudur. Yapılandırma modunda, AMS'nin veya BIS ACE'nin yetkili bir kullanıcısı cihaz düzenleyicisinde cihazlarda değişiklik yapabilir ve ACS, değişiklikleri derhal alt cihazlara yayar.

Bir operatör, komutları doğrudan cihaz düzenleyicisinin dışından kartlı geçiş cihazlarına göndererek yapılandırma modunu **geçersiz kılabilir**. Bu, örneğin bir operatörün gelen mesajları ve alarmları ele alması sırasında yaygın görülür. Operatör **Restore configuration** (Yapılandırmayı geri yükle) komutunu gönderene kadar cihaz Çalışma modu**'nda kalır**.

Bir yapılandırma kullanıcısı çalışma modundayken cihaz düzenleyicisinde bir cihaz seçerse cihazın ana özellik sayfasında şu bildirim görüntülenir:

Bu cihaz yapılandırma modunda değil.

Bunlar yapılandırma değişikliklerini yapıp kaydedebilir, ancak değişiklikler arabelleğe alınabilir ve alarm işlem modu sonlanana kadar ve yapılandırma modu geri yüklenene kadar geçerlilik kazanmaz.

10 Kartlı geçiş alanlarını yapılandırma

Alanlara Giriş

Güvenli tesisler Alanlara ayrılabilir. Alanlar herhangi bir boyutta olabilir: Bir veya birkaç bina, tek katlar veya tek odalar.

Alanların bazı kullanım alanları şunlardır:

- Tek kişilerin güvenli tesislerde bulunması.
- Tahliye veya başka bir acil durumda belirli bir alandaki kişi sayısının tahmin edilmesi.
- Bir alandaki kişi veya araç sayısının sınırlandırılması:
  Önceden tanımlanan sayı sınırına ulaşıldığında, kişiler veya araçlar alandan ayrılana kadar başka girişler reddedilebilir.
- Giriş sırası kontrolü ve anti-passback uygulama

Sistem iki tip giriş kontrollü alan arasında ayrım yapar

- Kişilere ait alanlar
- Araçlara ait alanlar (otoparklar)

Her alanın daha küçük boyutlu bir kontrol için alt alanları olabilir. Kişilere ait alanlar 3 seviyeye kadar iç içe geçebilir, otopark alanları ise sadece 2 seviyeye kadar iç içe geçebilir, yani 1 ile 24 arasında toplam park yeri ve park alanlarına sahip olabilir.

Tüm kurulumlarda bulunan varsayılan alana **Outside** (Dışarı) adı verilir. Kişi ve otoparklar olmak üzere iki türün de kullanıcı tanımlı alanları için üst öğe görevi yapar.

Bir alan en az bir girişi bulunmadığı sürece kullanılamaz.

Cihaz Düzenleyici **DevEdit** herhangi bir girişe bir konum alanı ve hedef alan atamak için kullanılabilir. Birisi bir kartı bir girişe ait bir okuyucuda taratırsa kişinin yeni konumu söz konusu girişin hedef alanı haline gelir.

Uyarı!

Giriş sırası kontrolü ve anti-passback için alanların girişlerinde hem giriş hem çıkış okuyucularının bulunması gerekir.

Yanlışlıkla veya kasıtlı olarak başkasını "takip etmesini" önlemek için turnike tipi girişler kesinlikle önerilir.

Alan oluşturma prosedürü

Ön gereksinimler

Bir sistem operatörü olarak sistem yöneticinizden alan oluşturmak üzere yetki istemeniz gerekir.

İletişim yolu (AMS)

1. AMS iletişim yöneticisinde **Main menu** (Ana menü) > **Configuration** (Yapılandırma) > **Device data**'yı (Cihaz verileri) seçin
2. Areas'a  (Alanlar) tıklayın
3. **Outside** (Dışarı) düğümünü veya alt öğelerinden birini seçin ve araç çubuğundaki  simgesine tıklayın. Alternatif olarak, bağlam menüsü aracılığıyla bir alan eklemek için **Outside**'a (Dışarı) sağ tıklayın.
   Başlangıçta oluşturulan tüm alanlara benzersiz bir **Area** (Alan) adı ve sayısal bir ek verilir.

4. Açılır pencerede kişiler için **Area** (Alan) veya araçlar için **Parking lot** (Otopark) olmak üzere türünü seçin.
   Yalnızca **Outside**'ın (Dışarı) her iki tipte de alt öğesi olabileceğini unutmayın. Bu alt öğelerin herhangi bir alt alanı her zaman üst öğenin türünü devralır.
   – Kişilere ait **Areas** (Alanlar) üç seviyeye kadar iç içe geçebilir. Her alan veya alt alan için maksimum nüfusu tanımlayabilirsiniz.
   – **Parking lots** (Otoparklar) en az bir **park bölgesinden** oluşan sanal varlıklardır. Park yerinin popülasyonunun sistem tarafından kısıtlanması gerekmiyorsa, 0 rakamı görüntülenir. Aksi takdirde, bölge başına maksimum park alanı sayısı 9999 olur ve otopark ana bölmesi, bölgelerindeki tüm boşlukların toplam sayısını görüntüler.

Alanları düzenleme prosedürü

1. Seçmek için hiyerarşideki bir alana tıklayın.
2. İletişim kutusunun ana bölmesinde yer alan aşağıdaki özniteliklerin bir veya daha fazlasının üzerine yazın.

Name (Ad)	Üzerine yazabileceğiniz varsayılan ad.
Açıklama	Alanın serbest metinli açıklaması.
Maximum number of persons / cars (Maksimum kişi / araba sayısı)	Sınır yoksa varsayılan değer 0'dır (sıfır). Aksi takdirde, maksimum popülasyon için bir tam sayı girin.

Notlar:

– Bir alan, hiyerarşinin farklı bir dalına sürüklenip bırakılarak taşınamaz. Gerekirse alanı silin ve başka bir dalda yeniden oluşturun.

Alanları silme prosedürü.

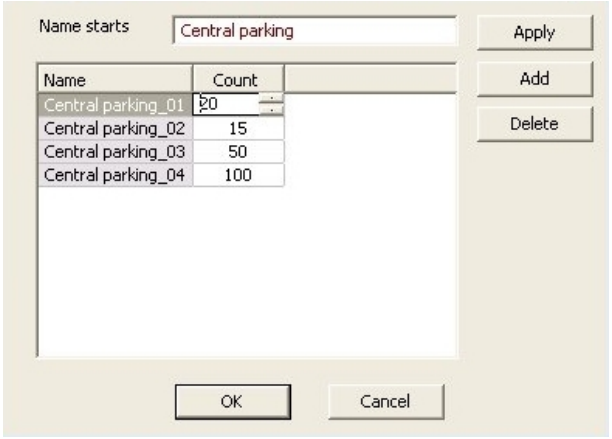
1. Seçmek için hiyerarşideki bir alana tıklayın.
2. **Delete**'e  tıklayın veya bağlam menüsü aracılığıyla silmek için sağ tıklayın.

Not: Bir alan, tüm alt öğeleri silinene kadar silinemez.

10.1 Araçlara ait alanları yapılandırma

Araçlar için alan (otopark, park bölgesi) oluşturma

Bir **Parking lot** (Otopark) alan tipi seçerseniz bir açılır pencere görünür.



1. Tüm park alt alanları veya **park bölgeleri** için bir devre adı oluşturmak üzere **Name starts with** (Şununla başlayan ad) alanına bir ad girin.
   Add (Ekle) düğmesi kullanılarak 24 adede kadar **park bölgesi** oluşturulabilir ve her bölge, devre adının yanı sıra 2 basamaklı bir eke sahip olur.
2. Sistem bu alanların popülasyonunu sınırlayacaksa park alanlarının sayısını **Count** (Sayı) sütununa girin. Popülasyon sınırı gerekli değilse 0 değerini girin.

Not: Tüm otoparkın maksimum popülasyonu bu sayıların toplamıdır. Sadece park bölgeleri park yerleri içerebilir; **otopark** en az bir **park bölgesinden** oluşan sanal bir varlıktır. Bölge başına maksimum park yeri sayısı 9999'dur.

Otoparklar için girişler oluşturma

Normal alanlarda olduğu gibi, otoparklar için de bir giriş gereklidir. Uygun kapı modeli **Parking lot 05c**'dir (Otopark 05c).

Bir otoparkın popülasyonunun izlenmesi için, aynı AMC'de biri giriş, diğeri çıkış için olmak üzere bu kapı modeline sahip 2 giriş gereklidir.

Ön koşul

Yukarıda açıklandığı gibi en az bir park alanına sahip bir otopark oluşturun.

İletişim yolu

Main menu (Ana menü) > **Configuration** (Yapılandırma) > **Device data** (Cihaz verileri)

LACs/Entrances/Devices'a (LAC'ler/Girişler/Cihazlar)  tıklayın

Prosedür

1. Cihaz hiyerarşisinde bir AMC oluşturun veya bağımlı girişleri olmayan bir AMC seçin.
2. AMC'ye sağ tıklayın ve **New entrance**'ı (Yeni giriş) seçin.
3. **New entrance** (Yeni giriş) açılır penceresinde **Parking lot 05c** (Otopark 05c) ve otopark girişine takılı tipte bir gelen okuyucusu ekleyin.
4. Açılır pencereyi kapatmak için **OK**'e (Tamam) tıklayın.
5. Cihaz hiyerarşisinden bu yeni oluşturulmuş girişi seçin.
   – Sistemin okuyucuyu otomatik olarak bir Giriş okuyucu olarak belirlediğini unutmayın.
6. Ana düzenleme bölmesinde, **Parking lot 05c** sekmesinde **Destination** (Hedef) açılır menüsünden daha önce oluşturduğunuz otoparkı seçin.
7. AMC'ye tekrar sağ tıklayın ve yukarıdaki gibi başka bir **Parking lot 05c** (Otopark 05c) tipi giriş oluşturun.
   – Bu kez yalnızca bir giden okuyucusu seçebileceğinizi unutmayın.
   – Açılır pencereyi kapatmak için **OK**'e (Tamam) tıklayın.
8. Cihaz hiyerarşisinden bu yeni oluşturulmuş ikinci girişi seçin.
   – Sistemin ikinci okuyucuyu otomatik olarak bir Çıkış okuyucusu şeklinde atadığını unutmayın.

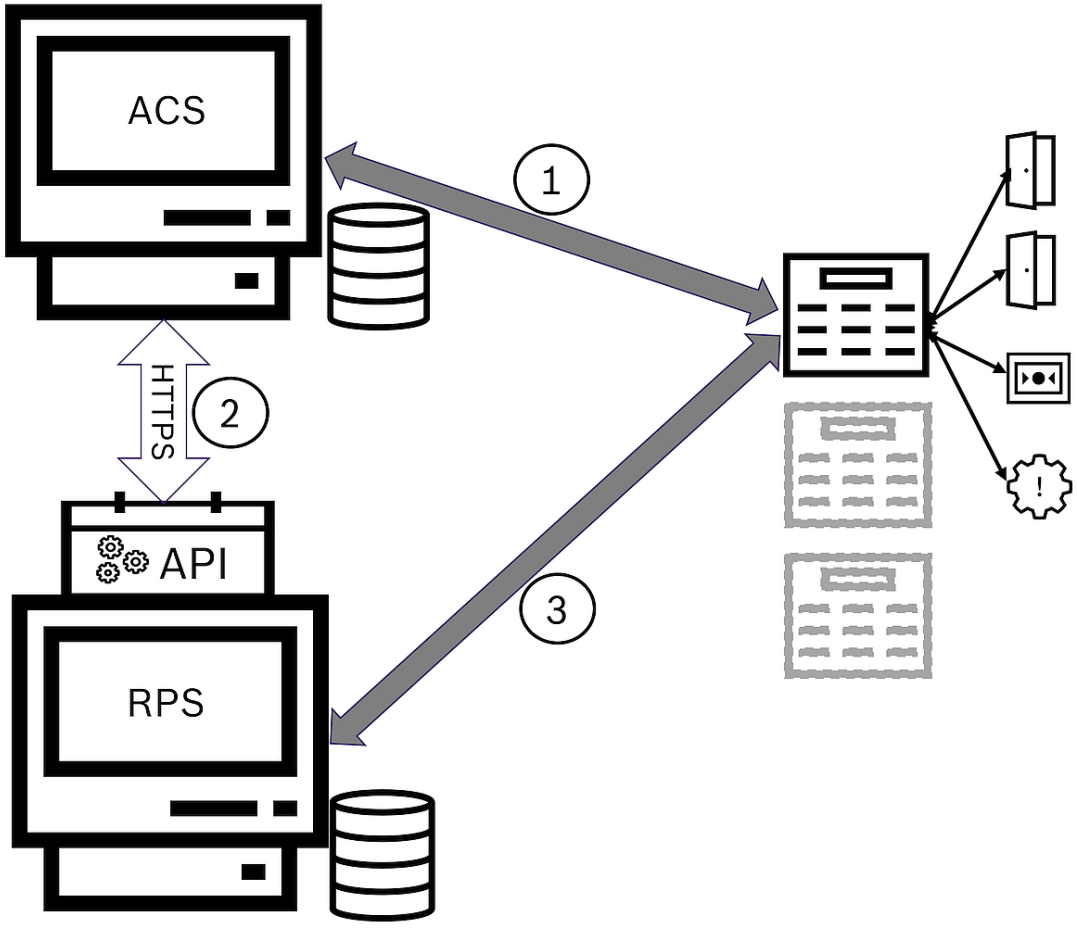
11 Hırsız alarmı alanlarını ve panellerini yapılandırma

Giriş

Kartlı geçiş sistemi Bosch hırsız alarmı panellerinin yönetimini ve çalışmasına dahildir. Desteklediği modellerin ayrıntıları için kartlı geçiş sisteminin veri sayfasına başvurun. Kartlı geçiş sistemi, hırsız alarm paneli **kullanıcılarının**yönetimine belirli bir değer katar. Bu kullanıcılar, genel kartlı geçiş sisteminin kart sahiplerinin bir alt kümesidir. Kartlı geçiş sistemi yöneticileri, bu kart sahiplerine ACE İletişim Kutusu Yöneticisi aracılığıyla hırsız alarm panellerini çalıştırmak için özel yetkiler sağlar.

Hırsız alarm panelleri, daha önce olduğu gibi kendi Uzaktan Programlama Yazılımı (RPS) aracılığıyla yapılandırılır ve güncellenir. ACE verileri sürekli olarak RPS'den okur ve içindeki panelleri görüntüler.

ACE, yetki profillerini oluşturmak ve atamak ve RPS'deki panel kullanıcılarını yönetmek için iletişim kutuları içerir.



Şekil 11.1: Basitleştirilmiş ACS-Hırsız Alarm sistemi topolojisi

ACS	The main Access Control System (Ana Kartlı Geçiş Sistemi): AMS veya BIS-ACE
API	Uygulama Programlama Arayüzü
RPS	Remote Programming System (Uzak programlama sistemi): Hırsız alarm panellerini kontrol eden uygulama

1	ACS to panel (ACS'den panele): Panel komutları. Panel to ACS (Panelden ACS'ye): hırsız alarmı noktalarından olaylar.
2	ACS to RPS (ACS'den RPS'ye): Kart sahibi verileri
3	RPS to Panel (RPS'den panele): Yapılandırma ayarları

Ön koşullar

- Desteklenen Bosch hırsızlık panellerinin RPS'si ACE sunucusunun kendisine **değil**, ACE sunucusuna ağ bağlantısı bulunan ayrı bir bilgisayara kurulur. Kurulum talimatları için RPS kurulum kılavuzuna başvurun.
- RPS, ACE kartlı geçiş sistemine ait olan hırsız alarm panelleriyle yapılandırılmıştır. Talimatlar için RPS kullanım kılavuzuna veya çevrimiçi yardıma başvurun.
- Panellerdeki saatler, otomatik eşitlemeyi etkinleştirmek için ACE sunucusundaki saatin 100 günü içindedir.
- Mod 2 iletişim kuralı tüm katılımcı panellerde ayarlanır.
- Aşağıdaki standart kart tanımlarından birine sahip kartlar:
  - HID 37 BIT-> 32767 veya daha düşük bir tesis/saha kodu olan hırsız alarmı 37 BIT.
  - HID 26 BIT- > Hırsız alarmı 26 BIT
  - EM 26 BIT-> Hırsız alarmı 26 BIT

Genel bilgiler

Yapılandırma işlemi, bu bölümün sonraki kısımlarında açıklanan aşağıdaki aşamalardan oluşur:

1. Hırsız alarmı RPS API'yi RPS bilgisayarına yükleme
2. Kartlı geçiş sistemini hırsız alarm panellerine bağlama.
   - RPS API'ye yönelik bağlantıyı tanımlama.
   - Panel bağlantılarını yapılandırma.
3. Bağlı panellerin hangi işlevlerinin kullanılabileceğini belirleyen panel yetki profilleri oluşturma.
4. Panel yetki profillerini kart sahiplerine atama.
   - Bu kart sahipleri böylece hırsız alarm panellerinin operatörü haline gelir.

11.1 Hırsız alarmı RPS API'yi RPS bilgisayarına yükleme

Hırsız alarmı RPS API, AMS ile kendi bilgisayarlarındaki RPS uygulamaları arasındaki iletişim kanalıdır. Önce API'yi RPS bilgisayarına yüklemeniz, ardından kurulumun AMS bilgisayarında oluşturduğu sertifikaları yüklemeniz gerekir.

Prosedür

1. RPS API kurulum dosyasını kendi belgelerine göre çalıştırın.

- Kurulum dosyası ve belgeleri AMS kurulum ortamında bulunur:
  `AddOns\Intrusion-RPS-API\Bosch_RPS_API_Setup_v*.exe`
  `AddOns\Intrusion-RPS-API\RPS-API_Application_note_v*.pdf`
- Kurulum programı 2 sertifika üretir ve bunları RPS bilgisayarına kaydeder:
  `%AppData%\Roaming\Bosch_RPS_API\BoschRpsAPI.cer`
  `%AppData%\Roaming\Bosch_RPS_API\BoschRpsAPI.pfx` (bir şifre belirlemenizi gerektirir)

2. Sertifika dosyalarını AMS bilgisayara kopyalayın.
3. Sertifikaları, AMS bilgisayarında **Store location**'a (Depolama konumu) yükleyin: `Local Machine`, **Certificate store** (Sertifika deposu): `Trusted Root Certification Authority`.

11.2 Kartlı geçiş sistemini hırsız alarm panellerine bağlama

Giriş

Bu bölümde, hırsız alarm panellerinin nasıl görüntüleneceği ve kontrol için ACE client aracılığıyla nasıl kullanıma hazır hale getirileceği açıklanmaktadır. Kartlı geçiş sistemi, API aracılığıyla kendi ağındaki RPS'ye bağlanır. API aracılığıyla mevcut uyumlu hırsız alarm panellerinin güncel bir dahili listesini tutar.

AMS'yi hırsız alarm panellerine bağlamak için iki adım gereklidir:

– 1. Adım: RPS API bağlantısını tanımlama
– 2. Adım: Panel bağlantılarını yapılandırma

İletişim yolu

– Ana menü > **Configuration** (Yapılandırma) > **Panels** (Paneller) ve alt iletişim kutuları

11.2.1 1. Adım: RPS API bağlantısını tanımlama

1. adım, kartlı geçiş sistemine RPS bilgisayarının adresi ve yönetici oturum açma bilgilerini sağlamaktır.

İletişim yolu

Ana menü > **Configuration** (Yapılandırma) > **Panels (Paneller) > RPS API configuration** (RPS API'sı yapılandırması)

Prosedür

1. Aşağıdaki bilgileri girin:

Bilgiler	Açıklama
Host name / IP address (Ana bilgisayar adı/IP adresi)	RPS'nin çalıştığı bilgisayarın HTTPS adresi ve RPS'nin iletişim kurduğu port numarası. `localhost`'un kullanılmasına izin verilmez. Varsayılan port numarası `9000`'dür.
Kullanıcı adı	API için bir RPS yönetici kullanıcısının kullanıcı adı.
Şifre	RPS yönetici kullanıcısının şifresi.

2. RPS'nin çalıştığından ve kullanıcı adı ile şifrenin geçerli olduğundan emin olmak için **Test the connection** (Bağlantıyı test et) düğmesine tıklayın.
3. Değişiklikleri kaydetmek için  (Kaydet) simgesine tıklayın.

11.2.2 2. Adım: Panel bağlantılarını yapılandırma

2. adım, kartlı geçiş sisteminin ağda yer alan bağımsız paneller üzerindeki kontrolünün miktarını yapılandırmaktır.

İletişim yolu

Ana menü > **Configuration** (Yapılandırma) > **Panels (Paneller) > Panel administration** (Panel yönetimi)

İletişim kutusu, RPS API'sının ACE'ye sağladığı uyumlu hırsız alarm panellerinin listesini bulundurur.

Liste arka planda düzenli olarak güncellenir. İletişim kutusunu açtıktan sonra, anında manuel olarak güncelleştirmeye zorlamak için zaman zaman simgesine tıklayın.
Liste, aşağıdaki bölümde açıklanan kontroller hariç salt okunurdur.

Prosedür

1. Listeden bir panel seçin.
2. Kartlı geçiş sisteminin seçilen hırsız alarmı panelinde neler yapabileceğini tanımlamak için aşağıdaki kontrolleri kullanın.

User administration (Kullanıcı yönetimi) liste sütunu	Bu satırdaki hırsız alarm paneli kullanıcılarının panelin kendinde **değil** kartlı geçiş sisteminde tutulmasını sağlamak için onay kutusunu seçin. **ÖNEMLİ**: Bu ayar RPS'de yerel olarak oluşturulan tüm panel kullanıcılarının üzerine yazılmasına neden olur.
Map View liste sütunu	Bu paneli ACE client aracılığıyla Komuta ve Kontrol için kullanılabilir hale getirmek için bu onay kutusunu seçin.
Verilere erişim sütunundaki Settings (Ayarlar) (cog) simgesi.	**Map View** (Harita Görünümü) sütunundaki onay kutusunu seçtiyseniz, aşağıdakileri girmek için simgeye tıklayın: – IP adresi – port numarası (varsayılan 7700) – bağımsız panel için şifre. Şifre RPS'de ayarlanır.
Düğme: **Delete selected panel** (Seçilen paneli sil)	RPS'de bir panel silinmişse listede **Removed** (Kaldırıldı) durumuyla görünür. Paneli seçin ve veritabanından tamamen silmek için bu düğmeye tıklayın.

11.3 Panellerin yetki profillerini oluşturma

Giriş

Bu bölümde panel yetki profillerinin nasıl oluşturulacağı açıklanmaktadır.
Panel yetki profili, özel bir hırsız alarm paneli kümesini çalıştırmak için kullanılan özel bir yetki kümesidir. Bir ACE yöneticisi çeşitli kart sahibi gruplarının farklı sorumlulukları için birden fazla panel yetki profili oluşturabilir.

İletişim yolu

– Ana menü > **System data** (Sistem verileri) > **Authorization profiles for intrusion panels** (Hırsız alarm panellerinin yetki profilleri)

Prosedür

1. Yeni profil oluşturmak için simgesine tıklayın
2. (Zorunlu) Profil için bir ad girin
3. (İsteğe Bağlı) Panel için serbest metinli bir açıklama girin
4. Ağda bulunan panelleri içeren bir açılır listeden bir veya daha fazla panel eklemek için **Assigned panels** (Atanan paneller) listesinin altındaki **Add...**'e (Ekle) tıklayın.
   Tersi durumda, bir veya daha fazla panel seçin ve bunları listeden kaldırmak için **Remove**'a (Kaldır) tıklayın.
5. Seçmek için **Assigned panels** (Atanan paneller) listesindeki bir panele tıklayın.
   – **Authorizations** (Yetkiler) bölmesinde seçilen panele ait tüm hırsız alarmı alanlarını içeren bir liste görünür.

6. **Authorizations** (Yetkiler) listesindeki **Authority level** (Yetki seviyesi) sütununda, panelin bu profile eklenecek her hırsız alarmı alanı için bir yetki seviyesi seçin.
   – Yetki seviyeleri RPS'de tanımlanır ve saklanır. Ayrıca yine burada özelleştirilebilir. Bir profile atamadan önce yetki seviyesinin RPS'deki tanımını bildiğinizden emin olun.
   – Varsayılan olarak **L1**; **L2**, **L3** vb. ile birlikte giderek sınırlandırılan en yüksek yetki seviyesidir.
   – Bir hücreyi boş bırakırsanız bu profilin alıcısının seçilen panelin seçilen hırsız alarmı alanı üzerinde **hiçbir** yetkisi olmaz.
7. Bu profile eklenecek tüm panellerin tüm hırsız alarmı alanları için bu işlemi tekrarlayın.
8. (İsteğe Bağlı) Yetkileri belirli sürelere göre kısıtlamak için **User group** (Kullanıcı grubu) listesinden bir panel kullanıcı grubu seçin.
   – Kullanıcı grupları RPS'de tanımlanır ve saklanır. Ayrıca yine burada özelleştirilebilir. Kullanıcı grubunu bir profile atamadan önce, RPS'deki kullanıcı grubunun tanımını bildiğinizden emin olun.
9. Değişiklikleri kaydetmek için  (Kaydet) simgesine tıklayın.

11.4 Panel yetki profillerini kart sahiplerine atama

Giriş

Bu bölümde farklı kart sahibi tiplerine veya gruplarına farklı panel yetki profillerinin nasıl atanacağı açıklanmaktadır.

Ön koşul

Kartlı geçiş sisteminde bir veya daha fazla panel yetki profili tanımladınız.

İletişim yolu

Main menu (Ana menü) > **Persons** (Kişiler) > **Cards** (Kartlar)

Prosedür

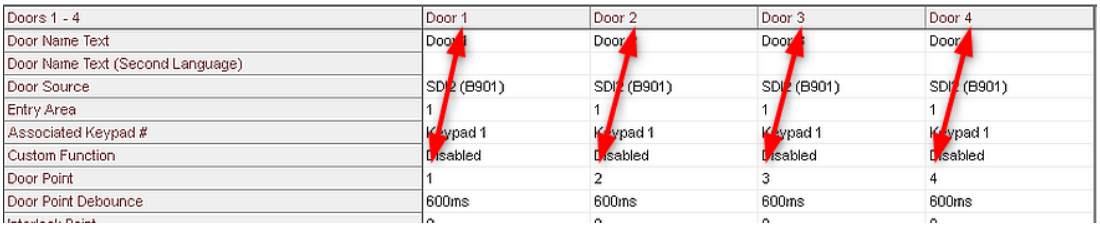
1. Her zamanki gibi, istediğiniz kart sahibini veritabanından bulun ve seçin.
2. **Intrusion** (Hırsız alarmı) sekmesine tıklayın.
3. **Intrusion** (Hırsız alarmı) sekmesinden **Panel user** (Panel kullanıcısı) onay kutusunu seçin.
4. (Zorunlu) **Passcode** (Parola) alanına, bu kart sahibinin hırsız alarm panellerini çalıştırabileceği bir parola yazın.
   – Gerekirse kullanılmamış, yeni bir parola oluşturmak için bu düğmeyi kullanın.
5. **ID card** (Kimlik kartı) listesinde, bu kart sahibine atanan kartlı geçiş kimlik bilgilerinden birini seçin.
6. (İsteğe Bağlı) **Number of remote** (Kumanda sayısı) alanına, hırsız alarm panelleri için kart sahibinin uzaktan kumanda cihazında yazılı olan sayıyı girin.
7. **Language** (Dil) listesinde, kart sahibinin okuma paneli iletişim kutularını okumayı tercih ettiği dili seçin.
8. Kart sahibi, hırsız alarm panelleri için Bosch akıllı telefon uygulamasını kullanacaksa **Remote access** (Uzaktan erişim) onay kutusunu seçin.
9. **Authorization profile** (Yetki profili) listesinden kart sahibi için uygun bir panel yetki profili seçin.
10. Değişiklikleri kaydetmek için  (Kaydet) simgesine tıklayın.
    – Bu panel yetki profili tüm panelleri ve yetkileri ile birlikte kart sahibine atanır. Böylece kart sahibi hırsız alarm panelleri için operatör haline gelir.

Veritabanındaki kart sahiplerini bulmak için bu iletişim kutusundaki veri alanlarını düğmesiyle de kullanabilirsiniz.

11.5 Kapıları, hırsız alarmı panellerindeki B901 modüller aracılığıyla kontrol etme.

AMS 4.0.1 ve sonraki sürümlerde, B901 Kartlı Geçiş Arayüz Modülleri AMS Map View aracılığıyla kontrol edilebilir.
B901, sistem yöneticisinin Bosch hırsız alarmı panellerine bağlandığı basit bir kapı denetleyicisidir. İlgili hırsız alarmı panelini AMS'ye önceki bölümlerde açıklandığı gibi bağlayın.
B901'i Cihaz Düzenleyici'de yapılandırmayın.
B901, kapıları kilitleyebilir veya kilidini açabilir, güvenli hale veya güvenli olmayan hale getirebilir ve kapatıp açabilir, ancak kartlı geçiş sistemine sınırlı durum bilgisi sağlar. Örneğin, bir kapının kilidinin açılması yerine fiziksel olarak açılıp açılmadığını bildirmez.
Diğer tüm izinsiz giriş cihazları gibi, AMS Map View'den B901'e komut göndermek üzere ilgili panel için Map View'ı AMS iletişim kutusunda etkinleştirmelisiniz:
Main menu (Ana menü) > **Configuration (Yapılandırma)** > **Panels (Paneller) > Panel administration (Panel yönetimi)**

Map View Kart geçirme ekranı ve B901 kapıları
AMS Map View'da **Kart geçirme akranı** uygulaması için doğru bilgileri sağlamak amacıyla B901 kapılarının kimlik bilgileri kapı noktalarının kimlik bilgileriyle eşleşmelidir. Yani 1 numaralı Kapı 1 numaralı Kapı Noktası'na, 2 numaralı Kapı 2 numaralı Kapı Noktasına atanmalıdır.



B901 kapı kontrol cihazına bu atamaları, hırsız alarm panellerini ve kontrol cihazlarını yapılandıran RPS aracında yapın.

12 Operatörleri ve iş istasyonlarını yapılandırma

Kartlı geçiş yönetim haklarına giriş

Kartlı geçiş sisteminin yönetim hakları, hangi sistem iletişim kutularının açılabileceğini ve buralarda hangi işlevlerinin gerçekleştirilebileceğini belirler.

Haklar hem operatörlere hem de iş istasyonlarına atanabilir.

Bir iş istasyonunun hakları, operatörünün haklarını geçici olarak kısıtlayabilir, çünkü güvenlik açısından kritik işlemler yalnızca özellikle güvenli olan iş istasyonlarından gerçekleştirilmelidir.

Haklar, **Profiles** (Profiller) adı verilen paketlerdeki operatörlere ve iş istasyonlarına atanır.

Her profil, belirli bir operatör veya iş istasyonu tipinin görevlerine göre uyarlanır.

Her operatör veya iş istasyonu birden fazla yetki profiline sahip olabilir.

Genel prosedür ve iletişim yolları

1. Cihaz Düzenleyicisi'nde iş istasyonlarını oluşturun:
   Configuration (Yapılandırma) > **Device data** (Cihaz verileri) > **Workstations** (İş istasyonları) 
2. Şu iletişim kutusunda iş istasyonu profilleri oluşturun:
   Operators and workstations (Operatörler ve iş istasyonları) > **Workstation profiles** (İş istasyonu profilleri).
3. Şu iletişim kutusunda iş istasyonlarına profil atayın:
   Operators and workstations (Operatörler ve iş istasyonları) > **Workstation rights** (İş istasyonu hakları)
4. Şu iletişim kutusunda operatör profilleri oluşturun:
   Operators and workstations (Operatörler ve iş istasyonları) > **User profiles** (Kullanıcı profilleri) iletişim kutusu.
5. Şu iletişim kutusunda operatörlere profil atayın:
   Operators and workstations (Operatörler ve iş istasyonları) > **User rights** (Kullanıcı hakları) iletişim kutusu

12.1 İş istasyonlarını oluşturma

İş istasyonları, operatörlerin kartlı geçiş sistemini çalıştırdığı bilgisayarlardır.

Öncelikle bir iş istasyonu "oluşturulmalıdır", yani bilgisayar kartlı geçiş sistemi içinde kayıtlı olmalıdır.

İletişim yolu

Configuration (Yapılandırma) > **Device data** (Cihaz verileri) > **Workstations** (İş istasyonları)

Prosedür

1. **DMS**'ye sağ tıklayın ve bağlam menüsünden **New object**'i (Yeni nesne) seçin veya araç çubuğundan ✚ simgesine tıklayın.
2. Parametrelerin değerlerini girin:
   - İş istasyona ait **Name**'in (Ad) bilgisayar adıyla tam olarak uyuşması gerekir
   - **Description** (Açıklama) isteğe bağlıdır. Örneğin, iş istasyonunun işlevini ve konumunu tanımlamak için kullanılabilir

- **Login via reader** (Okuyucu ile oturum aç) Operatörlerin bu iş istasyonunda, bu iş istasyonuna bağlı bir kayıt okuyucusuna kart göstererek oturum açmaları gerekmedikçe bu onay kutusunu işaretlemeden bırakın. Ayrıntılar için bölümüne bakın.
- **Automatic logout after inactive time (Hareketsiz kalma süresinden sonra oturumu otomatik olarak kapat):** Kayıt okuyucu aracılığıyla açılmış oturumun otomatik olarak sonlandırılacağı saniye cinsinden süre. Sınırsız süre için `0` olarak bırakın.

12.2 İş istasyonu profilleri oluşturma

İş istasyonu profillerine giriş

Fiziksel konumuna bağlı olarak, bir kartlı geçiş iş istasyonu, kullanımı ile ilgili olarak dikkatlice yapılandırılmalıdır, örneğin:

- Hangi operatörler kullanabilir?
- Kullanmak için hangi kimlik bilgileri gereklidir?
- İş istasyonundan hangi kartlı geçiş görevleri gerçekleştirilebilir?

Bir iş istasyonu profili, aşağıdakileri tanımlayan bir hak koleksiyonudur:

- İletişim kutusu yöneticisinin menüleri ve bir iş istasyonunda kullanılabilecek iletişim kutuları
- Bir operatörün bu iş istasyonunda oturum açmak için hangi kullanıcı profillerine sahip olması gerekir?

Uyarı!

İş istasyonu profilleri kullanıcı profillerini geçersiz kılar

Bir operatör, yalnızca oturum açtığı bilgisayarın iş istasyonu profilinde de bulunan kullanıcı profili haklarını kullanabilir. İş istasyonu ve operatör profilleri ortak haklara sahip değilse kullanıcı iş istasyonundaki hiçbir hakka sahip değildir.

İletişim yolu

Configuration (Yapılandırma) > **Operators and workstations** (Operatörler ve iş istasyonları) > **Workstation profiles** (İş istasyonu profilleri)

İş istasyonu profili oluşturma

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

Sistem işlevleri için yürütme hakları atama

1. **Functions** (İşlevler) listesinde, bu iş istasyonuna erişilebilecek işlevleri seçin ve **Execute** (Yürüt) sütununun değerini `Yes` (Evet) olarak ayarlamak için bunlara çift tıklayın.
   - Aynı şekilde erişilebilir olmayan tüm işlevlerin `No` (Hayır) olarak ayarlandığından emin olun.
2. Yaptığınız değişiklikleri kaydetmek için  simgesine veya **Apply**'a (Uygula) tıklayın

Kullanıcı profillerini İş istasyonu profillerine atama

User Profile (Kullanıcı Profili) bölmesinde.
Assigned Profiles (Atanan Profiller) listesi bu iş istasyonu profiliyle bir iş istasyonunda oturum açma yetkisi olan tüm kullanıcı profillerini içerir.
Available Profiles (Mevcut Profiller) alanı tüm diğer profilleri içerir. Bunlar henüz bu iş istasyonu profiliyle bir iş istasyonunda oturum açma yetkisine sahip değildir.

1. Seçilen profilleri bir listeden diğerine aktarmak için listeler arasındaki ok düğmelerine tıklayın.
2. Yaptığınız değişiklikleri kaydetmek için simgesine veya **Apply**'a (Uygula) tıklayın

Uyarı!
Kullanıcının varsayılan yönetici profilleri (**UP-Administrator**) ve iş istasyonu (**WP-Administrator**) değiştirilemez veya silinemez.
WP-Administrator profili iş istasyonuna geri alınamaz bir şekilde bağlıdır. Bu, sunucu iş istasyonunda oturum açabilecek en az bir kullanıcı olmasını garanti eder.

12.3 İş istasyonu profillerini atama

İş İstasyonu profillerinin İş İstasyonlarına atanmasını yönetmek için bu iletişim kutusunu kullanın. Her iş istasyonunda en az bir iş istasyonu profili olmalıdır. Birden çok profil varsa bu profillerdeki tüm haklar aynı anda uygulanır.

İletişim yolu
Configuration (Yapılandırma) > **Operators and workstations** (Operatörler ve iş istasyonları) > **Workstation rights** (İş istasyonu hakları)

Prosedür
Assigned Profiles (Atanan Profiller) listesi, zaten bu iş istasyonuna ait olan tüm iş istasyonu profillerini içerir.
Available Profiles (Mevcut Profiller) listesi, bu iş istasyonuna henüz atanmamış tüm iş istasyonu profillerini içerir.

1. İş istasyonları listesinde, yapılandırmak istediğiniz iş istasyonunu seçin
2. Seçilen profilleri birinden diğerine aktarmak için **Assigned** (Atanan) ve **Available** (Mevcut) listeleri arasındaki ok düğmelerine tıklayın.
3. Yaptığınız değişiklikleri kaydetmek için simgesine veya **Apply**'a (Uygula) tıklayın

Uyarı!
Kullanıcının varsayılan yönetici profilleri (**UP-Administrator**) ve iş istasyonu (**WP-Administrator**) değiştirilemez veya silinemez.
WP-Administrator profili iş istasyonuna geri alınamaz bir şekilde bağlıdır. Bu, sunucu iş istasyonunda oturum açabilecek en az bir kullanıcı olmasını garanti eder.

12.4 Kullanıcı (operatör) profilleri oluşturma

Kullanıcı profillerine giriş
Not: Kullanıcı terimi Kullanıcı hakları bağlamında **Operatör** ile eş anlamlıdır.
Bir kullanıcı profili, aşağıdakileri tanımlayan bir hak koleksiyonudur:

– İletişim kutusu yöneticisinin menüleri ve operatörün görebileceği iletişim kutuları.
– Operatörün bu iletişim kutularındaki yetenekleri, temel olarak bu iletişim kutularının öğelerini yürütme, değiştirme ekleme ve silme haklarıdır.

Kullanıcı profilleri, kişinin deneyimi, güvenlik izinleri ve sorumluluklarına bağlı olarak dikkatli bir şekilde yapılandırılmalıdır:

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

Uyarı!
Profilin yeteneklerini ve sınırlamalarını net ve doğru bir şekilde tanımlayan profil adları seçin.

Sistem işlevleri için düzenleme ve yürütme hakları ekleme

1. 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.
2. Yaptığınız değişiklikleri kaydetmek için  simgesine veya **Apply**'a (Uygula) tıklayın

12.5 Kullanıcı (operatör) profillerini atama

Not: Kullanıcı terimi Kullanıcı hakları bağlamında **Operatör** ile eş anlamlıdır.

Ön gereksinimler

– Bu kullanıcı profilini alacak operatör, kartlı geçiş sisteminde bir **Person** (Kişi) olarak tanımlanmıştır.
– Kartlı geçiş sisteminde uygun bir kullanıcı profili tanımlanmıştır.
   – Kısıtlanmamış kullanıcı profili olan **UP-Administrator**'ı atamanın her zaman mümkün olduğunu, ancak bu uygulamanın güvenlik nedeniyle kaldırıldığını unutmayın.

İletişim yolu

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

Prosedür

1. İstediğiniz kullanıcının personel kaydını iletişim kutusuna yükleyin.
2. Gerekirse **Valid from** (Geçerlilik başlangıcı) ve **Valid until** (Geçerlilik bitişi) alanlarına tarihleri girerek kullanıcı profilinin geçerliliğini sınırlayın.

Kullanıcı profillerini operatörlere atama
User Profiles (Kullanıcı Profilleri) bölmesinde:
Assigned Profiles (Atanan Profiller) listesi, bu kullanıcıya atanan tüm kullanıcı profillerini içerir.
Available Profiles (Mevcut Profiller) alanı, atama için kullanılabilen tüm profilleri içerir.

1. Seçilen profilleri bir listeden diğerine aktarmak için listeler arasındaki ok düğmelerine tıklayın.
2. Bu operatöre **Administered globally** (Genel olarak yönetilir) niteliğinin etkin olduğu personel kayıtları için okuma+yazma erişimi vermek için **Global administrator** (Genel yönetici) onay kutusunu seçin. Bu gibi personel kayıtlarına varsayılan operatör erişimi salt okunurdur.
3. Yaptığınız değişiklikleri kaydetmek için  simgesine tıklayın.

Operatörlere API kullanım hakları atama
Yapılandırılmış ve lisanslanmışsa harici program kodu, bir Uygulama Programlama Arayüzü veya API aracılığıyla kartlı geçiş sisteminin özelliklerini çağırabilir. Harici program sistem içinde bir proxy operatörü aracılığıyla hareket eder. **API usage** (API kullanımı) açılır listesi, harici kod tarafından bir proxy operatörü olarak kullanılırsa mevcut operatörün yeteneklerini kontrol eder.
Configuration (Yapılandırma) > **Operators and workstations** (Operatörler ve iş istasyonları) > **User rights** (Kullanıcı hakları)
– **API usage** (API kullanımı) listesinden bir ayar seçin.
Seçenekler şunlardır:

No access (Giriş yok)	Operatör, API tarafından sistem işlevlerini gerçekleştirmek için kullanılamaz.
Read only (Salt okunur)	Operatör, API tarafından sistem verilerini okumak için kullanılabilir ancak eklemek, değiştirmek veya silmek için kullanılamaz.
Unlimited (Sınırsız)	Operatör, API tarafından sistem verilerini okumak, eklemek, değiştirmek ve silmek için kullanılabilir.

– Yaptığınız değişiklikleri kaydetmek için  simgesine tıklayın

12.6 Operatörler için şifre belirleme

Birisi ve diğerleri için güvenli şifreler belirleme.

Giriş
Sistem için en az bir operatör gereklidir. Yeni bir kurulumdaki varsayılan operatörün kullanıcı adı **Administrator**, şifresi ise yine **Administrator**'dır. Sistemin yapılandırılmasındaki ilk adım her zaman bu kimlik bilgileriyle oturum açmak ve **Administrator** (Yönetici) şifresini kuruluşunuzun şifre politikalarına uygun olarak değiştirmektir.
Bundan sonra, hem ayrıcalıklı hem de ayrıcalıklı olmayan başka operatörler ekleyebilirsiniz.

Bir kişinin kendi şifresini değiştirmesine ilişkin prosedür.
Ön koşullar
İletişim kutusu yöneticisine giriş yaptınız.

Prosedür

1. İletişim yöneticisinde, şu menüyü seçin: **File** (Dosya) > **Change password** (Şifreyi değiştir)
2. Açılan pencerede, mevcut şifreyi, yeni şifreyi ve onaylamak için yeni şifreyi tekrar girin.
3. **Change**'e (Değiştir) tıklayın.

Bu prosedürün Yönetici şifresini değiştirmenin tek yolu olduğunu unutmayın.
Bir kurulumdan sonra ilk kez oturum açıldığında sistem, Yönetici parolasını değiştirmenizi ister.

Diğer operatörlerin şifrelerini değiştirmeye ilişkin prosedür.

Ön koşullar

Diğer kullanıcıların şifrelerini değiştirmek için, iletişim kutusu yöneticisinde Yönetici ayrıcalıklarına sahip bir hesap kullanarak oturum açmış olmanız gerekir.

Prosedür

1. İletişim kutusu yöneticisinin ana menüsünde, **Configuration** (Yapılandırma) > **Operators and Workstations** (Operatörler ve İş İstasyonları) > **User rights** (Kullanıcı hakları) bölümüne gidin.
2. Ana iletişim kutusu bölmesinde, şifresini değiştirmek istediğiniz operatörü yüklemek için araç çubuğunu kullanın.
3. **Change password...**'e (Şifreyi değiştir) tıklayın
4. Açılır pencerede, yeni şifreyi ve onaylamak için bir kez daha yeni şifreyi girin.
5. Açılır pencerede, yeni şifrenin geçerlilik süresini **Unlimited** veya birkaç gün olarak girin.
   – Üretim ortamları için, derhal bir geçerlilik süresi belirlemeniz önerilir.
6. Açılır pencereyi kapatmak için **OK**'e (Tamam) tıklayın.

Kullanıcı kaydını saklamak için ana iletişim penceresinde  simgesine tıklayın.

Change password... (Şifreyi değiştir...) düğmesinin altındaki **Valid from** (Geçerlilik başlangıcı) ve **Valid until** (Geçerlilik bitişi) tarih seçicilerinin şifrenin değil bu iletişim kutusundaki kullanıcı haklarının geçerliliğiyle ilgili olduğunu unutmayın.

Daha fazla bilgi

Şifreleri her zaman kuruluşunuzun şifre politikasına göre ayarlayın. Böyle bir politika oluşturmayla ilgili rehberlik için, örneğin, Microsoft tarafından aşağıdaki konumda sağlanan kılavuza başvurabilirsiniz.
https://www.microsoft.com/en-us/research/publication/password-guidance/

13 Kartları yapılandırma

13.1 Kart Tanımı

Kartlı geçiş sisteminiz tarafından kullanılacak kart tanımlarını etkinleştirmek, devre dışı bırakmak, değiştirmek veya eklemek için bu iletişim kutusunu kullanın.

İletişim yolu

– AMS ana menüsü > **Configuration** (Yapılandırma) > **Options** (Seçenekler) > **Card definition** (Kart tanımı)

Sistem, bir dizi önceden tanımlanmış kart tipiyle birlikte sunulur. Önceden tanımlanmış kart tipleri **Available card types** (Kullanılabilir kart tipleri) tablosunda arka planı gri olarak görüntülenir ve değiştirilemez. Yalnızca **Active Card types** (Aktif Kart tipleri) ve **Available card types** (Mevcut kart tipleri) arasında taşınabilirler.

13.1.1 Oluşturma ve Değiştirme

Yeni bir liste girişi oluşturmak için sağ taraftaki liste kutusunun üzerindeki ✚ (yeşil +) düğmesine tıklayın. Önceden tanımlanmış kart tiplerinin aksine yeni oluşturulan tiplere ait veriler serbestçe düzenlenebilir. Düzenlemek için **Name** (Ad), **Description** (Açıklama) ve **Number of Bits** (Bit Sayısı) alanlarına çift tıklayın.

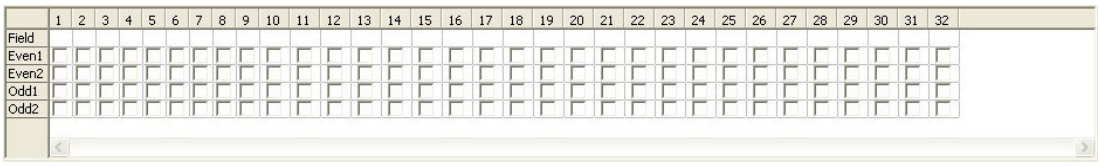
Ad maksimum 80, açıklama ise 255 karakterden oluşabilir. Bit sayısı 64 ile sınırlıdır (daha yüksek bir sayı girilirse metin alanı giriş odağını kaybeder kaybetmez bu değer en fazla izin verilen değere sıfırlanır).

Uyarı!
Bit uzunlukları Wiegand tanımlarını birbirlerinden ayırt etmek için kullanılır. Bu nedenle her yeni tanım, mevcut bir tanım tarafından kullanılmamış benzersiz bir bit uzunluğuna sahip olmalıdır.

- Bir veri bitini değiştirmek için ilgili alana çift tıklayın. Silmek için ise önce veri bitini seçin, ardından ✕ (kırmızı x) düğmesine tıklayın.

Uyarı!
Yalnızca kullanıcı tarafından oluşturulan kart tipleri değiştirilebilir veya silinebilir.

Tek bir kart tipi seçildiğinde (sol veya sağ taraftaki listelerde), iletişim kutusunun alt bölümünde bu tipin kodlaması görüntülenir. Ekranda, veri bitleri 5 satır ve tanımda bulunan bit sayısıyla aynı sayıda sütun olarak gösterilir.



Field (Alan) satırının her sütununa kodun söz konusu parçasının nasıl yorumlanması gerektiğini belirleyen bir etiket eklenebilir. Mevcut etiketler şunlardır:

F	Tesis: Tesis ilişkisi için kod bölümünü işaretler	
C	Kod no: Tek kart numarasını içeren kod parçası	
E1	Çift 1: Birinci Çift Eşlik Maskesini dengeleme biti	Bu değerlerin açıklanması ilgili satırın onay kutusunu etkinleştirir.
E2	Çift 2: İkinci Çift Eşlik Maskesini dengeleme biti	
O1	Tek 1: Birinci Tek Parite Maskesini dengeleme biti	
O2	Tek 2: İkinci Tek Parite Maskesini dengeleme biti	
1	Kodda bulunan bit değerlerini düzeltme	
0		

E1, E2, O1 ve O2 etiketleri bulunduğunda, söz konusu satırda onay kutusunu seçmeniz yeterlidir. **Field** (Alan) satırındaki kutu otomatik olarak uygun şekilde işaretlenir.
Açıklama:
Bir kart gösterildiğinde bir okuyucu tarafından gönderilen sinyal bir dizi sıfır ve birden oluşur. Her kart tipi için bu sinyalin uzunluğunu (yani bit sayısı) tam olarak tanımlanır. Sinyal, kod verileri olarak kaydedilen gerçek kullanıcı verilerine ek olarak a) sinyal, kart sinyali olarak tanımlamak ve b) iletimi doğrulamak için de kontrol verileri içerir.
Genel olarak, sabit sıfırlar ve birler sinyal türünü belirlemek için faydalıdır.
Sinyalin seçilen bitler üzerinden sağlama toplamı olarak bir sıfır (Çift Eşlik) veya bir (Tek Eşlik) olarak göstermesi gereken eşlik bitleri doğru iletimi doğrulamak için kullanılır. Kontrol cihazları, Çift Eşlikler için bir veya iki sağlama toplamı, Tek Eşlikler için ise bir veya iki sağlama toplamı hesaplayacak şekilde yapılandırılabilir.
Bu bitler, liste kontrolünde sağlama toplamına eklenmesi gereken eşlik sağlama toplamları (Çift 1, Çift 2, Tek 1 ve Tek 2) için ilgili satırlarda işaretlenebilir. Kullanılan her sağlama toplamı için en üstteki satırda (Alan), eşlik türüne göre sağlama toplamını dengelemek için bir bit tanımlanmıştır. Eşlik seçeneği kullanılmazsa ilgili satır boş kalır.

13.1.2 Kart tanımlarını etkinleştirme/devre dışı bırakma

En fazla 8 kart tanımı eş zamanlı olarak etkin olabilir. Etkinleştirilecek tanımlar sol taraftaki **Active Card Types** (Etkin Kart Tipleri) listesine taşınmalıdır. Bu, sağ taraftaki bir veya daha fazla tanım seçilerek (çoklu seçim yapılabilir) ve sol ok (**<**) düğmesine tıklanarak yapılır. Aynı anda dörtten fazla tanım taşınamaz. Dört tanım yerleştirildikten sonra, her türlü fazlalık taşıma işleminden çıkarılır. **Etkin Kart Tiplerine** daha fazla tanım eklemek için (**>**) düğmesini kullanmak yoluyla devre dışı bırakarak bunların birini veya daha fazlasını seçip (çoklu seçim yapılabilir) sağ tarafa taşıyarak silmek gerekli olabilir.

Uyarı!
L-Bus veya BG900 protokollerine sahip okuyucular kullanmak için **Serial Reader** (Seri Okuyucu) kart türünü etkinleştirin. Bu, **Dialog Bosch** manuel giriş iletişim kutusunu kartlı geçiş sisteminin iletişim kutusu yöneticisi tarafından kullanılabilir hale getirir.

13.1.3 İletişim kutusu yöneticisinde kart verileri oluşturma

Manuel veri girişi

Wiegand ve Bosch kartlar için farklı giriş yöntemleri kullanılır.
Tüm Wiegand tanımları (HID 26, HID 35, HID 37 ve 32 Bit CSN) için **Dialog (Wiegand)** iletişim kutusu, **Customer code** (Müşteri kodu) ve **Card no.** (Kart no.) girmenizi sağlar.
Seri okuyucular için **Dialog (Bosch)** iletişim kutusu **Version** (Sürüm) ve **Country code** (Ülke kodu) için ek alanlar içerir.

Kayıt okuyucusu ile veri girişi

Her iş istasyonu, manuel veri girişine ek olarak kart verilerini toplamak için bir iletişim kutusu okuyucusu ile donatılabilir. Aşağıdaki iletişim kutusundaki listeden bir okuyucu kullanın:

– AMS ana menüsü > **Configuration** (Yapılandırma) > **Options** (Seçenekler) > **Card reader** (Kart okuyucusu)

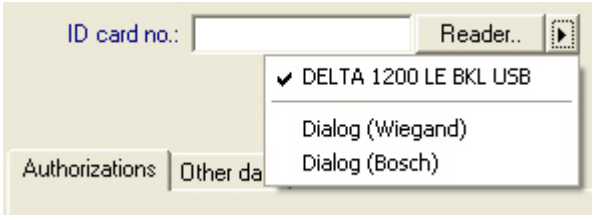
Seçilen okuyucu Wiegand kartları için bir giriş okuyucuysa tüm etkin Wiegand kart tipleri okuyucuyla birlikte listelenir.

– AMS ana menüsü > **Personnel data** (Personel verileri) > **Cards** (Kartlar) > Okuyucu düğmesi > ▶ (sağ ok)

Kart kodlamasının doğru kaydedilmesini sağlamak için bu kart tiplerinden biri seçilmelidir. Yani okuyucu kendisi doğrudan seçilemez ancak Wiegand tanımı seçimi aracılığıyla yalnızca dolaylı olarak seçilebilir.
Gerekli kart tipi açılır listede görünmezse kart tanımı iletişim kutusunda etkinleştirmeniz gerekir.

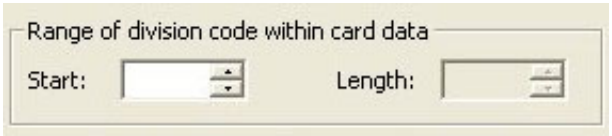
– AMS ana menüsü > **Configuration** (Yapılandırma) > **Options** (Seçenekler) > **Card definition** (Kart tanımı)

HITAG, LEGIC ve MIFARE kayıt okuyucuları listeden doğrudan seçilebilir.



Divisions (Bölümler) için kart tanımı (birden fazla taraf özelliği)

Kartlı geçiş sistemine sahip tesislerde birden fazla tarafı (yani "Bölümleri") yönetmek için Bölümler özelliğini lisansladıysanız kart üzerinde operatörün çeşitli bölümlerin kartlarını birbirinden ayırmasına imkan tanıyan bir kod alanı yapılandırılabilir. İsteğe bağlı alanları (yalnızca Divisions (Bölümler) özelliğinin lisanslandığı durumlarda seçilebilir) kullanarak kartların üzerindeki **başlangıç** bitinin konumunu ve Bölüm kodlarının **uzunluğunu** tanımlayın.



13.2 Kart kodlarını yapılandırma

Kartlı geçiş kartlarının kodlanması, tüm kart verilerinin benzersiz olmasını sağlar.

İletişim yolu
Main Menu (Ana Menü) > **Configuration** (Yapılandırma) > **Options** (Seçenekler) > **Card coding configuration** (Kart kodlama yapılandırması)
İletişim kutusuna sayı girme
İletişim kutusuna sayı girme
Daha fazla kolaylık için sayıları ondalık veya onaltılık biçimlerde girebilirsiniz. Kart üreticisinin belirttiği biçime göre **Hexadecimal** (On altılık) veya **Decimal** (Ondalık) radyo düğmesini seçin.
Ana iletişim kutusu bölmesi, aşağıda daha ayrıntılı olarak açıklanan iki gruba ayrılmıştır:
- **Card default code data** (Kart varsayılan kod verileri)
- **Check membership only values** (Yalnızca üyelik değerlerini kontrol et)

Kart varsayılan kod verileri
Kart sisteme kaydedildiğinde kart numarasına atanan **Version** (Sürüm), **Country code** (Ülke kodu) ve **Facility code** (Tesis kodu) değerlerini tanımlamak için bu metin giriş alanlarını kullanın. Alanlar yazılabilir değilse etkin kart tanımlarından hiçbiriyle ilgili değildir. Bosch kodu için tüm alanlar yazılabilir niteliktedir.
Kart bir operatör iş istasyonunda manuel olarak kayıtlıysa her kart için özelleştirilebilecek varsayılan değerleri gösteren bir iletişim kutusu görüntülenir.

Kod verilerini girme:
Veriler üretici tarafından ondalık değerler halinde sunuluyorsa Ondalık radyo düğmesini seçin ve belirtilen değerleri girin, örneğin:
Version (Sürüm): `2`
Country code (Ülke kodu): `99`
Facility code (Tesis kodu): `56720`
Verileri saklamak için **Apply**'a (Uygula) tıklayın.

Varsayılan kod verilerinin girilmesiyle ilgili notlar:
Varsayılan veriler, işletim sisteminin kayıt defterinde saklanır ve her kimlik kartı numarası kodlama zamanında eklenir. Kayıt gerekirse başında sıfırlarla birlikte **8 basamaklı on altılık** bir değer alır.
Kod numaraları tamamen aktarılırsa sistem onluktan on altılığa dönüşebilir, baştaki sıfırlarla birlikte 8 basamağa sahip olabilir ve ilgili sistem parametresini kaydedebilir.
- Örnek:
  - Input: 56720
  - Dönüştürme: DD90
  - Şu şekilde kaydedilir: 0000DD90

Kod sayıları ayrıca (bölünmüş biçim) aktarılırsa sadece **ondalık** form kullanılır. Aşağıdaki şekilde oluşturulmuş 10 basamaklı bir ondalık sayıya dönüştürülürler:

- Version (Sürüm): 2 basamak
- Country code (Ülke kodu): 2 basamak
- Facility code (Tesis kodu): 6 basamak
- 10 basamağın herhangi biri hala boşsa başa sıfır eklenerek tamamlanır.
  - Örnek: 0299056720

Bu 10 basamaklı ondalık değer dönüştürülür ve 8 basamaklı on altılık bir değer olarak saklanır.

- Örnek:
  - ondalık: 0299056720
  - on altılık: 11D33E50

Uyarı!
Sistem, bölünmüş kod numaraları durumunda, geçersiz ülke kodlarının (on altılık 63 veya ondalık 99'un üzerinde) ve geçersiz tesis kodlarının (on altılık F423F veya ondalık 999.999'un üzerinde) girişini önlemek için on altılık değerleri doğrular.

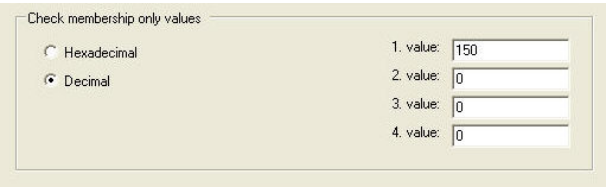
Uyarı!
Kart yakalama, bağlı bir iletişim kutusu okuyucusu aracılığıyla gerçekleşirse varsayılan değerler otomatik olarak atanır. Varsayılanları bir okuyucudan yakalarken geçersiz kılmak mümkün değildir.
Bunu yapmak için yakalama türü **Dialog** (İletişim Kutusu) olarak değiştirilmelidir

Kart numarasının manuel olarak girişi ondalık biçimdedir.
Verileri kaydederken, 10 basamaklı bir ondalık değer (baştaki sıfırlarla) oluşturulur ve ardından bu 8 basamaklı on altılık bir değere dönüştürülür. Bu değer artık kartın 16 basamaklı kod numarası olarak varsayılan kod verisiyle birlikte saklanır.

- Örnek:
  - Kart numarasının girilmesi: 415
  - 10 basamaklı: 0000000415
  - On altılığa dönüştürüldü: 0000019F
  - Varsayılan Kod verileriyle (yukarıya bakın) birleştirilir ve kimlik kartı kod numarası olarak kaydedilir: 11D33E500000019F

Yalnızca Üyelik değerlerini kontrol etme
Sadece üyeliği kontrol etmek, bir kişinin kimliğini değil, yalnızca bir şirketin veya kuruluşun üyeliği için kimlik bilgilerinin kontrol edildiğini gösterir. Bu nedenle yüksek güvenlik alanlarına erişim sağlayan okuyucular için **Membership check only**'yi (Yalnızca üyeliği kontrol et) kullanmayın.

En fazla dört şirket veya müşteri kodu girmek için bu seçenek grubunu kullanın. Veriler, ondalık veya on altılık olarak girilebilir, ancak işletim sisteminin kayıt defterinde ondalık değerler olarak depolanır.



Cihaz Düzenleyici, DevEdit'de okuyucuyu seçin ve **Membership check** (Üyelik kontrolü) okuyucu parametresini etkinleştirin.
Sadece kart verilerindeki şirket veya müşteri kodları saklanan değerlere göre okunur ve doğrulanır.

Uyarı!
Membership check (Üyelik kontrolü) sadece sistemde önceden tanımlanmış kart tanımlarıyla (gri arka planlı) çalışır, özelleştirilmiş tanımlarla çalışmaz.

14 Kontrol cihazlarını yapılandırma

Giriş

Kartlı geçiş sistemindeki kontrol cihazları, girişlerdeki (okuyucular ve kapılar) çevre donanımlarına komutlar gönderen ve ardından okuyuculardan ve kapılardan aldıkları istekleri yeniden merkezi karar verme yazılımına ileten sanal ve fiziksel cihazlardır.

Kontrol cihazları merkezi yazılımın cihaz ve kart sahibi bilgilerinin bazılarını depolar ve bu şekilde yapılandırıldılarsa geçici olarak merkezi yazılımdan ayrıldıklarında bile kartlı geçiş kararları oluşturabilirler.

Karar verme yazılımı Veri Yönetim Sistemi'dir.

Kontrol cihazları iki çeşittir:

– MAC'ler olarak bilinen ana giriş kontrol cihazı ve bunun yedek karşılığı olan RMAC.
– LAC'ler veya AMC'ler olarak bilinen yerel giriş kontrol cihazları.

Kontrol cihazları, cihaz düzenleyici DevEdit'te yapılandırılır

Cihaz düzenleyiciye iletişim yolu

Main menu (Ana menü) > **Configuration** (Yapılandırma) > **Device data** (Cihaz verileri) > **Device tree** (Cihaz ağacı) 

Cihaz düzenleyici, DevEdit'i kullanma

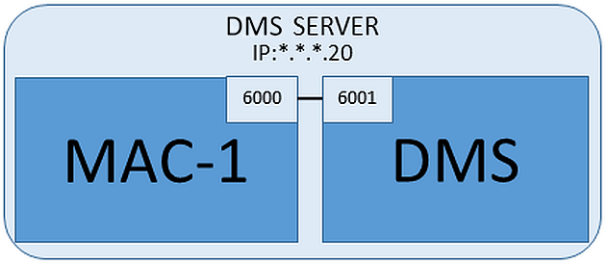
DevEdit'in temel kullanımı aşağıdaki bağlantıda yer alan **Cihaz düzenleyiciyi kullanma** bölümünde açıklanmıştır.

Bkz.

– *Cihaz Düzenleyici'yi kullanma, sayfa 22*

14.1 MAC'leri ve RMAC'leri Yapılandırma

14.1.1 DMS sunucusundaki bir MAC'i yapılandırma



En düşük sistem yapılandırması için bir adet MAC gereklidir. Bu durumda MAC, DMS sunucusunda bulunabilir.

Prosedür

DMS sunucusunda Cihaz Düzenleyici'yi açın ve **Cihaz düzenleyiciyi kullanma** bölümünde açıklandığı gibi cihaz ağacında bir MAC oluşturun.

Cihaz Düzenleyici'de MAC'i seçin. **MAC** sekmesinde, aşağıdaki parametre değerlerini girin:

Parametre	Açıklama
Name (Ad)	Cihaz ağacında görünecek isim, örneğin MAC-1.
Açıklama	Sistem operatörlerinin yararı için isteğe bağlı açıklama

Parametre	Açıklama
With RMAC (RMAC ile) (onay kutusu)	**<Boş bırakın>**
RMAC Port (RMAC Portu)	**<Boş bırakın>**
Active (Etkin) (onay kutusu)	Bu MAC ve DMS arasındaki geçici zaman senkronizasyonunu geçici olarak askıya almak için bu onay kutusunu **temizleyin**. Bu, tüm MAC'lerin aynı anda yeniden başlatılmasını önlemek için büyük sistemlerdeki DMS güncellemelerinden sonra avantajlıdır.
Load devices (Cihazları yükle) (onay kutusu)	Bu MAC ve kendi alt cihazları arasındaki gerçek zamanlı senkronizasyonu geçici olarak askıya almak için bu onay kutusunu **temizleyin**. Bu, cihaz düzenleyicide bir MAC açmak için gereken süreyi kısaltır.
IP address (IP adresi)	`Localhost 127.0.0.1`
Time zone (Saat dilimi)	**ÖNEMLİ:** MAC ve tüm alt AMC'lerin saat dilimi.
Division (Bölüm)	(Varsa) MAC'ın ait olduğu Bölüm.

Bu yerel MAC yedek yük devretme MAC'ine sahip olmadığından bunun için MACInstaller aracını çalıştırmak gerekli değildir. **MAC** sekmesindeki iki RMAC parametresini boş bırakmanız yeterlidir.

14.1.2 MAC sunucu bilgisayarlarını MAC'leri ve RMAC'leri çalıştırmak için hazırlama

Bu bölümde bilgisayarların MAC sunucuları olacak şekilde nasıl hazırlanacağı anlatılmaktadır.

Varsayılan olarak bir kartlı geçiş sistemindeki ilk MAC aynı bilgisayarda bunun Veri Yönetimi Sunucusu (DMS) olarak çalışır. Bununla birlikte, daha fazla esneklik için MAC'in, DMS bilgisayarı bozulursa kartlı geçiş görevlerini üstlenebilen ayrı bir bilgisayarda çalıştırılması önerilir.

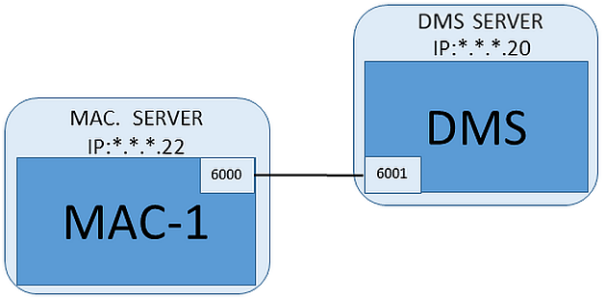
MAC'ler veya RMAC'lerin bulunduğu ayrı bilgisayarlar, bir MAC veya bir RMAC barındırıp barındırmadıklarından bağımsız olarak MAC sunucuları olarak bilinir.

Yük devri özelliği sağlamak için, MAC'ler ve RMAC'ler ayrı MAC sunucularında **çalıştırılmalıdır**.

Tüm katılan MAC sunucularında aşağıdaki koşulların yerine getirildiğinden emin olun:

1. Tüm MAC sunucularının işletim sistemleri şu anda Microsoft tarafından desteklenmelidir ve son güncelleştirmelerin yüklenmiş olması gerekir.
2. Tüm sunuculardaki Yönetici kullanıcı aynı şifreye sahiptir
3. Yönetici olarak oturum açmışsınızdır (MSTC kullanıyorsanız sadece /Yönetici /Konsol oturumlarını kullanın)
4. IP V6'yı devre dışı bırakın. Her sunucunun IP V4 adresini dikkatlice not edin.
5. Tüm katılan bilgisayarlarda .NET 3.5'i etkinleştirin.
   Not: Windows 10 ve Windows Server işletim sistemlerinde özellik olarak etkinleştirilmiştir.
6. Bilgisayarı yeniden başlatın.

14.1.3 Bir MAC'i kendi MAC sunucusunda yapılandırma



– MAC sunucu bilgisayarı bölümünde açıklandığı gibi hazırlanmıştır.

1. DMS sunucu bilgisayarında, Cihaz Düzenleyicisi'nde,
   – MAC'e sağ tıklayın ve **Disable all LACs**'i (Tüm LAC'leri devre dışı bırak) seçin.
   – Bu MAC için **Activate** (Etkinleştir) ve **Load devices** (Cihazları yükle) onay kutularını temizleyerek MAC'i devre dışı bırakın.
2. MAC sunucusu bilgisayarında, `services.msc` Windows programını kullanarak
   – **AUTO_MAC2** MAC hizmetini durdurun
   – Bu MAC hizmetinin **Startup type**'ını (Başlatma tipi) **Manual** (Manuel) olarak ayarlayın.
3. `MACInstaller.exe`'yi başlatın
   – AMS için bu, `\AddOns\MultiMAC\MACInstaller` AMS kurulum ortamında bulunur (aşağıdaki MACInstaller aracını kullanma bölümüne bakın).
4. Aşağıdaki parametreler için değerleri girerek aracın ekranlarında gezinin.

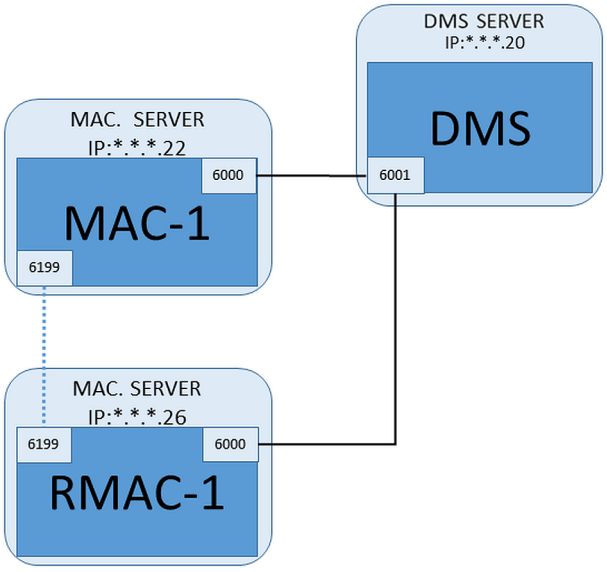
Ekran No.	Parametre	Açıklama
3	**Destination Folder** (Hedef Klasör)	MAC'in yükleneceği yerel dizin. Mümkün olan her yerde varsayılanı alın.
4	**Server** (Sunucu)	DMS'in çalıştığı sunucunun adı veya IP adresi.
4	**Port (Port to DMS)** (Port (DMS Port))	MAC'ten iletişim almak için kullanılacak DMS sunucusundaki port**.** DMS'teki ilk MAC için 6001 kullanın ve sonraki her bir MAC için 1 artırın.
4	**Number (MAC System Number)** (Numara (MAC Sistem Numarası))	Bu ve tüm MAC'ler için 1 olarak ayarlayın (RMAC'lerin tersine)**.**
4	**Twin (Name or IP address of partner MAC)** (İkiz (Ortak MAC'in adı veya IP adresi))	Bu MAC hiçbir RMAC'e sahip olmadığı sürece bu alanı boş bırakın.

5. DMS sunucusunda, Cihaz Düzenleyici'deki MAC'i seçin.
6. **MAC** sekmesinde, aşağıdaki parametrelerin değerlerini girin:

Parametre	Açıklama
Name (Ad)	Cihaz ağacında görünecek isim, örneğin MAC-1.
Açıklama	Sistem operatörlerinin yararı için isteğe bağlı açıklama
With RMAC (RMAC ile) (onay kutusu)	**<Boş bırakın>**
RMAC Port (RMAC Portu)	**<Boş bırakın>**
Active (Etkin) (onay kutusu)	Şimdi bu onay kutusunu seçin
Load devices (Cihazları yükle) (onay kutusu)	Şimdi bu onay kutusunu seçin
IP address (IP adresi)	MAC sunucu bilgisayarının IP adresi.
Time zone (Saat dilimi)	**ÖNEMLİ:** MAC ve tüm alt AMC'lerin saat dilimi.
Division (Bölüm)	(Varsa) MAC'ın ait olduğu **Bölüm**.

14.1.4 MAC'lere RMAC ekleme

Uyarı!
Sıradan MAC'lar yüklenip doğru şekilde çalışana kadar RMAC'leri sıradan MAC'lere eklemeyin.
Aksi takdirde veri çoğaltma işlemi engellenebilir veya zarar görebilir.



– Bu RMAC'e ait MAC, önceki bölümlerde açıklandığı gibi kuruldu ve düzgün şekilde çalışıyor.
– RMAC'e ait MAC sunucu bilgisayarı bölümünde açıklandığı gibi hazırlanmıştır

MAC'ler yük devri özelliği ve böylece daha esnek kartlı geçiş olanağı sağlamak için yedek MAC'lerle (RMAC'ler) ikiz olarak kullanılabilir. Bu durumda, kartlı geçiş verileri ikisi arasında otomatik olarak çoğaltılır. Çiftlerden biri hata verirse diğeri altındaki yerel giriş kontrol cihazlarının kontrolünü alır.

DMS sunucusunda, Configuration (Yapılandırma) tarayıcısında

1. Cihaz Düzenleyici'de, RMAC'nin ekleneceği MAC'i seçin.
2. **MAC** sekmesinde, aşağıdaki parametrelerin değerlerini değiştirin:

Parametre	Açıklama
With RMAC (RMAC ile) (onay kutusu)	Yedek yük devri bağlantı sunucusunda ilgili RMAC'i yükleyene kadar bu onay kutusunu **temizleyin**
Active (Etkin) (onay kutusu)	Bu MAC ve DMS arasındaki geçici zaman senkronizasyonunu geçici olarak askıya almak için bu onay kutusunu **temizleyin**. Bu, tüm MAC'lerin aynı anda yeniden başlatılmasını önlemek için büyük sistemlerdeki DMS güncellemelerinden sonra avantajlıdır.
Load devices (Cihazları yükle) (onay kutusu)	Bu MAC ve kendi alt cihazları arasındaki gerçek zamanlı senkronizasyonu geçici olarak askıya almak için bu onay kutusunu **temizleyin**. Bu, cihaz düzenleyicide bir MAC açmak için gereken süreyi kısaltır.

3. **Apply** (Uygula) düğmesine tıklayın
4. Cihaz Düzenleyici'yi şu anda ona geri dönecekmişiz gibi açık tutun.

RMAC için MAC sunucusunda

RMAC'i yapılandırmak için aşağıdaki işlemleri yapın:

– Kendi ayrı ve hazırlanmış MAC sunucu bilgisayarında, MACInstaller aracını çalıştırın (bkz. MACInstaller aracını kullanma) ve aşağıdaki parametreleri ayarlayın:
  – **Server** (Sunucu): DMS sunucu bilgisayarının adı veya IP adresi
  – **Port**: `6001` (MAC için olanla aynı)
  – **Number** (Numara): `2` (tüm RMAC'lerin Numarası 2'dir)
  – **Twin** (İkiz): İkiz MAC'nin çalıştığı bilgisayarın IP adresi.

DMS sunucusunda Cihaz düzenleyici'ye geri dönün

1. **ÖNEMLİ:** Hem MAC hem de RMAC'in ilgili bilgisayarlarında çalışır durumda ve birbirlerini görüyor olduğundan emin olun.
2. **MAC** sekmesinde, parametreleri aşağıdaki gibi değiştirin:

Parametre	Açıklama
With RMAC (RMAC ile) (onay kutusu)	**Seçili** **MAC** sekmesinin yanında **RMAC** etiketli yeni bir sekme görünür.
RMAC Port (RMAC Portu)	`6199` (statik varsayılan) Tüm MAC'ler ve RMAC'ler, ortaklarının çalışıp çalışmadığını kontrol etmek için bu portu kullanır**.**
Active (Etkin) (onay kutusu)	**Seçili** Bu, bu MAC ve alt cihazları arasında senkronizasyon sağlar.
Load devices (Cihazları yükle) (onay kutusu)	**Seçili** Bu, cihaz düzenleyicide bir MAC açmak için gereken süreyi kısaltır.

3. **RMAC** sekmesinde, aşağıdaki parametrelerin değerlerini girin:

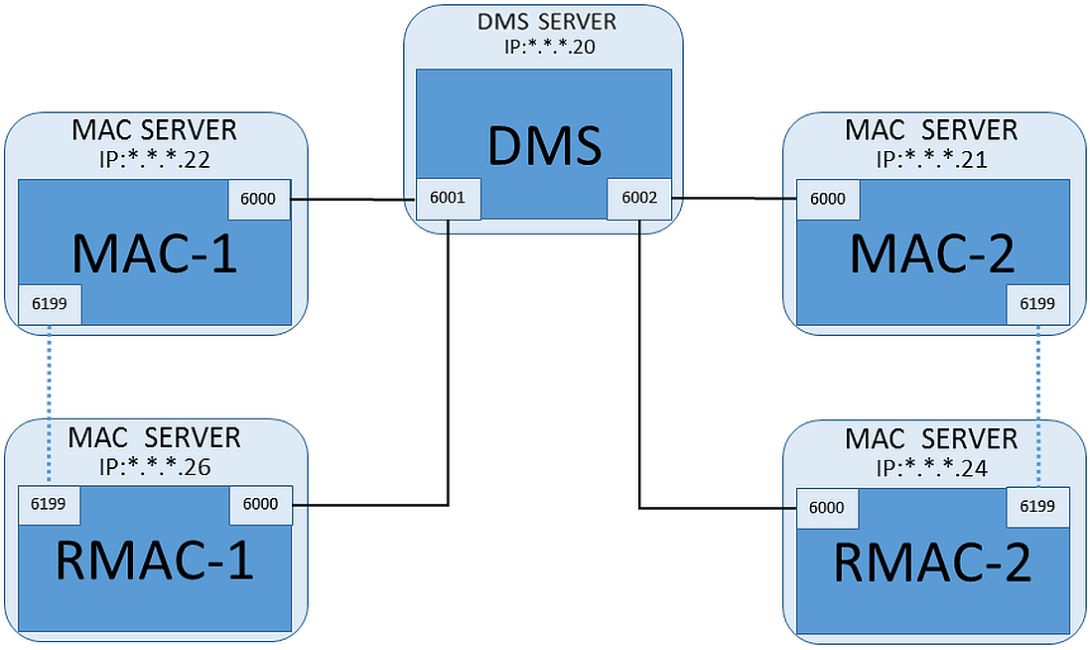
Parametre	Açıklama
Name (Ad)	Cihaz ağacında görünecek ad. Örneğin, ilgili MAC'in adı MAC-01 ise bu RMAC, RMAC-01 olarak adlandırılabilir.
Açıklama	Kartlı geçiş operatörleri için isteğe bağlı belgeler.
IP address (IP adresi)	RMAC'in IP adresi.
MAC Port (MAC Portu)	`6199` (statik varsayılan) Tüm MAC'ler ve RMAC'ler, ortaklarının çalışır ve erişilebilir durumda olduklarından emin olmak için bu portu kullanır**.**

Bkz.

– *MAC kurucu aracını kullanma, sayfa 51*

14.1.5 Daha fazla MAC/RMAC çifti ekleme

Kontrol edilecek girişlerin sayısına ve gereken hata payı derecesine bağlı olarak, sistem yapılandırmasına çok sayıda MAC/RMAC çifti eklenebilir. Sürümünüzün desteklediği tam sayı için, lütfen ilgili veri sayfasına bakın.



Her ek MAC/RMAC çifti için...

1. MAC ve RMAC için ayrı bilgisayarları bölümünde açıklandığı gibi hazırlayın
2. MAC'i bölümünde açıklandığı gibi ayarlayın
3. Bu MAC için RMAC'i bölümünde açıklandığı gibi ayarlayın

Her MAC/RMAC çiftinin DMS sunucusunda ayrı bir porta iletim yaptığını unutmayın. Bu nedenle, `MACInstaller.exe`'de **Port (Port to DMS)** (Port (DMS Portu)) parametresi için aşağıdakileri kullanın:

– İlk MAC/RMAC çiftindeki bilgisayarlar için `6001`
– İkinci MAC/RMAC çiftindeki bilgisayarlar için `6002`

– vb.

Cihaz Düzenleyici'de `6199` portu her zaman **MAC Port** (MAC Portu) ve **RMAC Port** (RMAC Portu) parametreleri için kullanılabilir. Bu port numarası, her MAC/RMAC çifti içinde "el sıkışma" için ayrılmıştır, böylece her biri ortağının erişilebilir olup olmadığını bilir.

Uyarı!
MAC'leri sistem yükseltmelerinden sonra yeniden etkinleştirme
Bir sistem yükseltmesinden sonra, MAC'ler ve AMC'leri varsayılan olarak devre dışı bırakılır. Cihaz düzenleyici'deki ilgili onay kutularını seçerek bunları yapılandırma tarayıcısında yeniden etkinleştirmeyi unutmayın.

14.1.6 MAC kurucu aracını kullanma

`MACInstaller.exe` MAC'ler ile RMAC'leri kendi bilgisayarlarına (MAC sunucuları) yüklemek için kullanılan standart araçtır. Bir MAC veya RMAC için parametre değerlerini toplar ve Windows Kayıt Defteri'nde gerekli değişiklikleri yapar.

Uyarı!
Araç Windows Kayıt Defteri'nde değişiklik yaptığından, yeniden yapılandırmadan önce çalışan her türlü MAC işleminin durdurulması gerekir.

MACInstaller aracı, kurulum ortamında aşağıdaki yolda bulunabilir:

– `\AddOns\MultiMAC\MACInstaller.exe`

Bir dizi ekran aracılığıyla, aşağıdaki parametreler için değerleri toplar.

Ekran No.	Parametre	Açıklama
3	**Destination Folder** (Hedef Klasör)	MAC'in yükleneceği yerel dizin.
4	**Server** (Sunucu)	DMS'in çalıştığı sunucunun adı veya IP adresi.
4	**Port (Port to DMS)** (Port (DMS Port))	MAC ve DMS arasında iletişim için kullanılacak DMS sunucusundaki port numarası. **Ayrıntılar için aşağıya bakın.**
4	**Number (MAC System Number)** (Numara (MAC Sistem Numarası))	Tüm orijinal MAC'ler için 1 olarak ayarlayın. Tüm yedek yük devri MAC'leri (RMAC'ler) için 2 olarak ayarlayın.
4	**Twin (Name or IP address of partner MAC)** (İkiz (Ortak MAC'in adı veya IP adresi))	Bu MAC sunucusu için yedek yük devri ortağının çalışacağı bilgisayarın IP adresi. Yoksa bu alanı boş bırakın.

Parametre: Port (Port to DMS) (Port (Port-DMS))

Port numaraları aşağıdaki numaralandırma düzenine sahiptir:

– Yalnızca bir DMS sunucusunun bulunduğu hiyerarşik olmayan bir sistemde, her MAC ve ilgili RMAC'i genellikle 6000 olmak üzere aynı port numarasından iletim yapar. DMS, bir seferde her MAC/RMAC çiftinden yalnızca biriyle iletişim kurabilir.

– DMS, 6001 portundaki ilk MAC veya MAC/RMAC çiftinden, 6002 portundaki ikinci MAC veya MAC/RMAC çiftinden sinyal alır ve bu şekilde devam eder.

Parametre: Number (MAC System Number) (Numara (MAC Sistem Numarası))
Bu parametrenin amacı orijinal MAC'leri RMAC'lerden ayırmaktır:
– Tüm orijinal MAC'lerin numarası 1'dir.
– Tüm yedek yük devri MAC'lerinin (RMAC'ler) numarası 2'dir.

Parametre: Configure Only (Yalnızca Yapılandır) (radyo düğmesi)
Var olan bir MAC yapılandırmasını ana DMS sunucusunda değiştirmek, özellikle de yeni kurulmuş bir RMAC'i farklı bir bilgisayarla ilgili olarak bilgilendirmek için bu seçeneği seçin.
Bu durumda, **Twin** (İkiz) parametresine IP adresini veya RMAC'in ana bilgisayar adını girin.

Parameter: Update Software (Yazılımı Güncelle) (radyo düğmesi)
Bir RMAC yüklemek veya yapılandırmasını değiştirmek için ana DMS sunucusundan başka bir bilgisayarda bu seçeneği seçin.
Bu durumda, **Twin** (İkiz) parametresine IP adresini veya RMAC'in ikiz MAC'inin ana bilgisayar adını girin.

14.2 LAC'leri Yapılandırma

AMC yerel giriş kontrol cihazı oluşturma
Access Modular Controller'lar (AMC'ler), cihaz düzenleyicideki Ana Giriş Kontrol Cihazları'ndan (MAC'ler) alt seviyededir.
AMC oluşturmak için:
1. Cihaz Düzenleyici'de bir MAC'e sağ tıklayın ve bağlam menüsünden **New Object**'i (Yeni Nesne) seçin
   veya
2. ✚ düğmesine tıklayın.
3. Görünen iletişim kutusundan aşağıdaki AMC türlerinden birini seçin:

AMC 4W (varsayılan)	En fazla dört okuyucuya bağlanmak için dört Wiegand okuyucu arayüzü ile
AMC 4R4	En fazla sekiz okuyucuyu bağlamak için dört RS485 okuyucu arayüzü ile

Sonuç: DevEdit hiyerarşisinde seçilen türün yeni bir AMC girişi oluşturulur

AMC2 4W	Dört Wiegand okuyucuya sahip **A**ccess **M**odular **C**ontroller.	En fazla dört Wiegand okuyucu, en fazla dört girişi bağlayacak şekilde yapılandırılabilir. Kontrol cihazı sekiz giriş ve sekiz çıkış sinyalini destekler. Gerekirse genişletme kartları 48 adede kadar ek giriş ve çıkış sinyali sağlayabilir.
AMC2 4R4	Dört RS485 okuyucu arayüzüne sahip **A**ccess **M**odular **C**ontroller	En fazla sekiz RS485 okuyucu en fazla sekiz girişe bağlanacak şekilde yapılandırılabilir.

		Kontrol cihazı sekiz giriş ve sekiz çıkış sinyalini destekler. Gerekirse genişletme kartları 48 adede kadar ek giriş ve çıkış sinyali sağlayabilir.
AMC2 8I-8O-EXT	Sekiz giriş ve çıkış sinyaline sahip AMC için genişletme kartı	Ek sinyalleri kullanılabilir hale getirin. Bir AMC'ye en fazla üç genişletme kartı bağlanabilir
AMC2 16I-16O-EXT	On altı giriş ve çıkış sinyaline sahip AMC için genişletme kartı	
AMC2 8I-8O-4W	Sekiz giriş ve çıkış sinyaline sahip Wiegand AMC için genişletme kartı	

Kontrol cihazlarını etkinleştirme/devre dışı bırakma

Yeni bir kontrol cihazı ilk kez oluşturulduğunda şu seçili olan seçeneği (onay kutusu) içerir: **Communication to host enabled** (Ana bilgisayarla iletişim etkin).

Bu, MAC ve kontrol cihazları arasındaki ağ bağlantısını açar, böylece değiştirilen veya genişletilen her türlü yapılandırma verisi otomatik olarak kontrol cihazlarına yayılır.

Ağ bant genişliğini kaydetmek için bu seçeneği devre dışı bırakın ve böylece birden çok kontrol cihazı ile bunların bağımlı cihazlarını (girişler, kapılar, okuyucular, genişletme kartları) oluştururken performansı artırın. Böylece cihaz düzenleyicide cihazlar grileştirilmiş simgelerle işaretlenir.

ÖNEMLİ: Cihazların yapılandırması tamamlandığında, bu seçeneği yeniden etkinleştirdiğinizden emin olun. Bu, kontrol cihazlarını diğer seviyelerde yapılan her türlü yapılandırma değişikliğiyle sürekli güncel tutar.

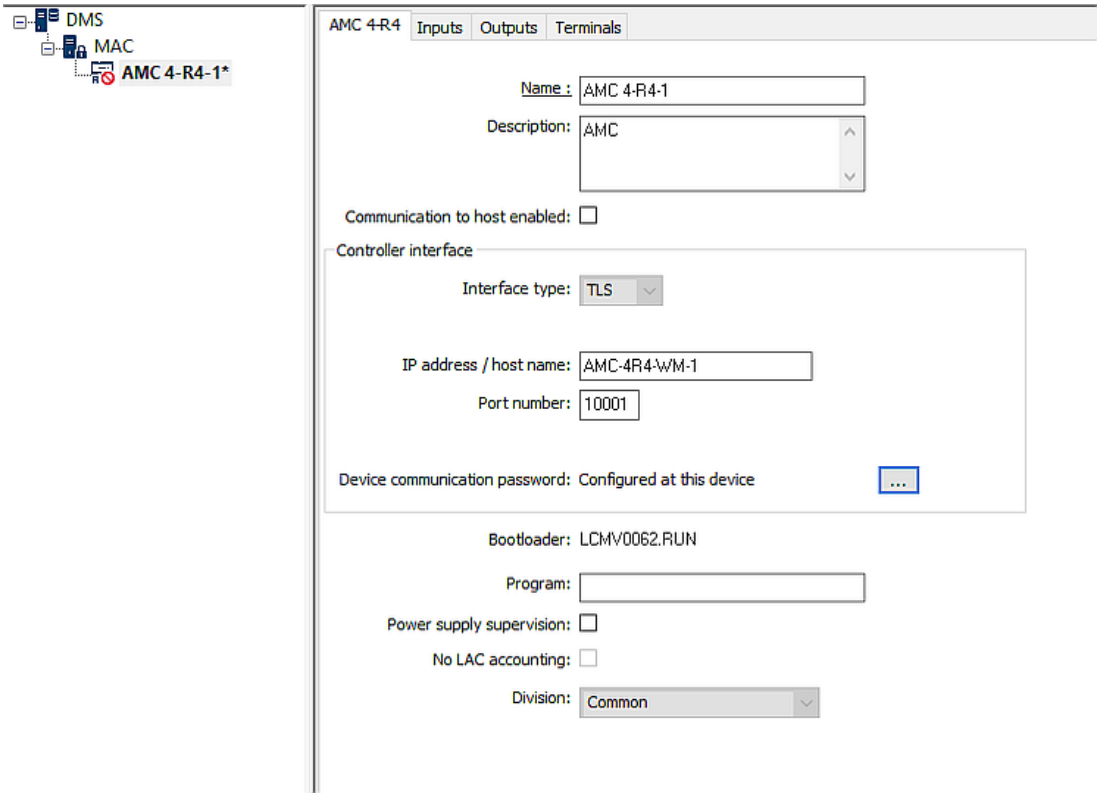
Kontrol cihazı tiplerini bir kurulumda birlikte kullanma

Kartlı geçiş sistemleri normalde sadece bir tip kontrol cihazı ve okuyucuyla donatılmıştır. Yazılım yükseltmeleri ve büyüyen kurulumlar, mevcut donanım bileşenlerini yenileriyle güçlendirmeyi gerekli kılabilir. RS485 çeşitlerini (AMC 4R4) Wiegand çeşitleriyle (AMC 4W) birleştiren yapılandırmalar bile, aşağıdaki uyarılar dikkate alındığı sürece gerçekleştirilebilir:

- RS485 okuyucular, kod numarasını okunmuş olarak içeren bir "telgraf" iletir.
- Wiegand okuyucular, kod numarasını doğru şekilde korumak için verilerini kimlik kartı tanımının yardımıyla çözülmesi gerekecek şekilde iletir.
- Karışık kontrol cihazı çalışması, yalnızca iki kod numarası da aynı şekilde oluşturulmuşsa işe yarar.

14.2.1 AMC parametreleri ve ayarları

AMC'nin Genel Parametreleri



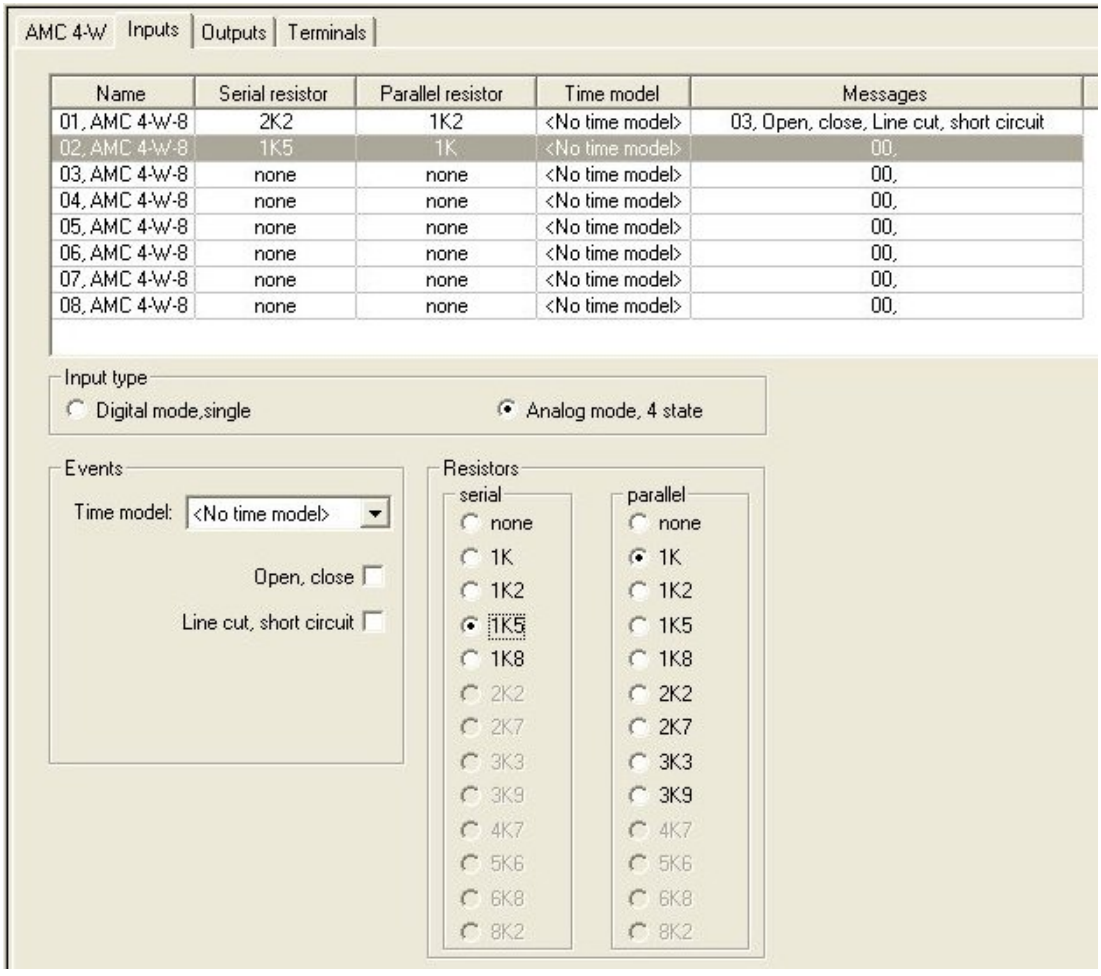
AMC parametrelerini yapılandırma

Parametre	Olası değerler	Açıklama
Controller name (Kontrol cihazı adı)	Sınırlandırılmış alfa sayısal: 1-16 basamak	Kimlik oluşturma (varsayılan) benzersiz adlar sağlar, ancak kullanıcılar bunların üzerine yazabilir. Bir adın üzerine yazarsanız kimliklerin benzersiz olduğundan emin olmanız gerekir.
Controller description (Kontrol cihazı açıklaması)	alfa sayısal: 0 - 255 basamak	Serbest metin.
Communication to host enabled (Ana bilgisayar iletişimi etkin)	0 = devre dışı (onay kutusu temizlenmiştir) 1 = etkin (onay kutusu işaretlidir)	Varsayılan = etkin Cihaz ağacındaki kontrol cihazlarında bulunan simgeler ana bilgisayar bağlantısının durumunu gösterir (etkin/devre dışı). Onay kutusu temizlendiğinde, AMS çevrimdışı olur ve bu, yeniden yapılandırma ve test için yararlıdır. Kartlı geçiş sistemi yeni bir sürüme güncellendiğinde, tüm kontrol cihazlarının onay kutularını otomatik olarak temizlenir.

		AMC'lerin onay kutularını test etmek için güncellenen yazılımda tek tek seçip temizleyin.
		DTLS'nin "yukarıdan aşağıya" uygulanması sırasında AMC'de bir DCP (cihaz iletişim şifresi) ayarlamak için Cihaz Düzenleyicisi'ni kullanırken onay kutusunu seçin. Bu, DCP'yi aşağıya doğru AMC'lere yaymak için 15 dakikalık bir zaman aralığı açar. Temizleyin ve zaman aralığını yeniden başlatmak için onay kutusunu seçin.
Kontrol Cihazı Arayüzü		
Interface Type (Arayüz Tipi)	UDP TLS	Bağlantının ağ aracılığıyla olduğu ve AMC'de DCP'nin (cihaz iletişim şifresi) henüz ayarlı olmadığı durumlarda UDP (= kullanıcı veri birimi protokolü). TLS (= aktarım katmanı güvenliği): AMC için bir DCP (cihaz iletişim şifresi) ayarladığınızda, MAC ile iletişim artırılmış güvenliğe sahip DTLS aracılığıyla gerçekleştirilir. Hem UDP hem de TLS için AMC'deki DIP anahtarı 1 ve 5'in AÇIK olarak ayarlanmış olduğundan emin olun.
IP Address/ Hostname (IP Adresi/ Ana Bilgisayar Adı)	AMC'nin ağ adı veya IP adresi	Bu metin alanı yalnızca port tipi olarak **UDP** seçildiyse ayarlanabilir. IP adresleri DHCP tarafından tahsis edilirse, IP adresi değişmiş olsa bile bir yeniden başlatmanın ardından AMC'nin yerleştirilebilmesi için AMC'nin ağ adı girilmelidir. DHCP bulunmayan ağlarda IP adresini girin.
Port numarası	sayısal: 10001 (varsayılan)	Bu, MAC mesajlarını alacak olan AMC portudur.
Diğer Parametreler		
Program	Alfa sayısal	AMC'ye yüklenecek programın dosya adı. Mevcut programlar MAC'in BIN dizininde bulunur ve bir listeden seçilebilir. Kolaylık için protokol ve açıklama da gösterilmektedir.

		Bu parametre, hangi okuyucuların bağlı olduğuna bağlı olarak programlar otomatik şekilde yüklendikçe otomatik olarak ayarlanır ve bir okuyucu/program uyumsuzluğu durumunda parametre geçersiz kılınır.
Power supply supervision (Güç kaynağı denetimi)	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	Besleme gerilimini denetleme. Güç kaynağı düşerse bir bilgilendirme mesajı oluşturulur. Denetim işlevi, bir UPS (kesintisiz güç kaynağı) ön koşulu olduğunu varsayar, böylece bir mesaj oluşturulabilir. 0 = denetim yok 1 = denetim etkin
No LAC accounting (LAC hesaplaması yok)	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	Sadece üst MAC'in giriş ve çıkış yapan birimlerin hesabını tuttuğu otoparklara erişim sağlamak üzere birlikte çalışan AMC cihazları için bu onay kutusunu işaretleyin. Bu seçenek seçildiyse ve AMC çevrimdışıysa AMC'nin tüm popülasyon sayısına erişimi olmadığından aşırı kalabalık alanlara erişimi engelleyemeyeceğini **unutmayın**.
Division (Bölüm)	Varsayılan değer "Common" (Ortak)	Yalnızca **Divisions** (Bölümler) özelliği lisanslandığında geçerlidir.

AMC girişlerini yapılandırma



Bu iletişim kutusu dört bölüme ayrılmıştır:
- Girişlerin ada göre listesi
- Giriş tipleri
- Girişler tarafından bildirilecek olaylar
- Analog modla kullanılan direnç tipleri

Giriş parametreleri

AMC girişlerinin parametreleri aşağıdaki tabloda açıklanmıştır:

Sütun adı	Açıklama
Name (Ad)	Girişin numaralandırılması (01'den 08'e kadar) ve ilgili AMC veya AMC-EXT'nin adı.
Serial resistor (Seri direnç)	Seri direnç için ayarlanmış direnç değerinin görüntülenmesi. "yok" veya "---" = dijital mod
Parallel resistor (Paralel direnç)	Paralel direnç için ayarlanmış direnç değerinin görüntülenmesi. "yok" veya "---" = dijital mod

Time model (Zaman modeli)	Seçilen zaman modelinin adı
Messages (Mesajlar)	Oluşturulacak mesajların girinti numarası ve ataması 00 = mesaj yok 01 = olaylar **Open** (Açık) ise **close** (kapat) etkinleştirilmiştir 02 = olaylar **Line cut** (Hat kesildi) ise **short circuit** (kısa devre) etkinleştirilmiştir 03 = iki etkinlik seçeneği de etkinleştirilmişse
Assigned (Atandı)	Giriş Modeli 15 kullanıldığında, DIP'nin sinyal adı görüntülenir.

Aynı anda birden çok giriş seçmek için tıklarken Ctrl ve Shift tuşlarını kullanın.
Değiştirdiğiniz her türlü değer seçilen tüm girişlere uygulanır.

Olaylar ve Zaman modelleri
Çalışma moduna bağlı olarak, şu kapı durumları algılanır ve bildirilir: **Open** (Açık), C**losed** (Kapalı), **Line cut** (Hat kesildi) ve **Short circuit** (Kısa devre).
AMC'nin bu durumları sistem geneline olaylar olarak iletmesini sağlamak için ilgili onay kutularını seçin.
Olayların iletimini model tarafından tanımlanan zamanla sınırlamak için aynı adın açılır listesinden bir **Time model** (Zaman modeli) seçin. Örneğin, **Open** (Açık) olay yalnızca normal iş saatleri dışında önemli olabilir.

Giriş türü
Dirençler **Digital mode**'da (Dijital mod) veya **Analog mode**'da (Analog mod) (4 durum) çalıştırılabilir.
Varsayılan **Digital mode**'dur (Dijital mod): Yalnızca **open** (açık) ve **close** (kapalı) kapı durumları algılanır.
Ayrıca Analog modda kablo durumları **Line cut** (Hat kesildi) ve **Short** circuit **(Kısa devre)** algılanır.

Kapı açık	seri (R_S) ve paralel (R_P) direnç değerlerinin toplamı: $R_S + R_P$
Kapı kapalı	seri direnç değerlerine eşittir: R_S
Devre kesildi	seri (R_S) ve paralel (R_P) direnç değerlerinin sonsuza yaklaşan değerleri.
Kısa Devre	seri (R_S) ve paralel (R_P) direnç değerlerinin toplamı sıfıra eşittir.

Dirençler
Dirençler varsayılan **Digital mode**'da (Dijital mod) "yok" veya "---" olarak ayarlanmıştır.
Analog mode'da (Analog mod) seri ve paralel dirençlerin değerleri, ilgili radyo düğmeleri seçilerek ayarlanabilir.
yok, 1K, 1K2, 1K5, 1K8, 2K2, 2K7, 3K3, 3K9, 4K7, 5K6, 6K8, 8K2 (100 ohm'da)
Seçilen direnç değerine bağlı olarak, ilgili direnç için yalnızca kısıtlı aralıklar kullanılabilir.
Aşağıdaki tablolar, soldaki sütunlarda seçilen değerleri, sağ sütunlarda ise diğer dirençlerin kullanılabilir aralıklarını gösterir.

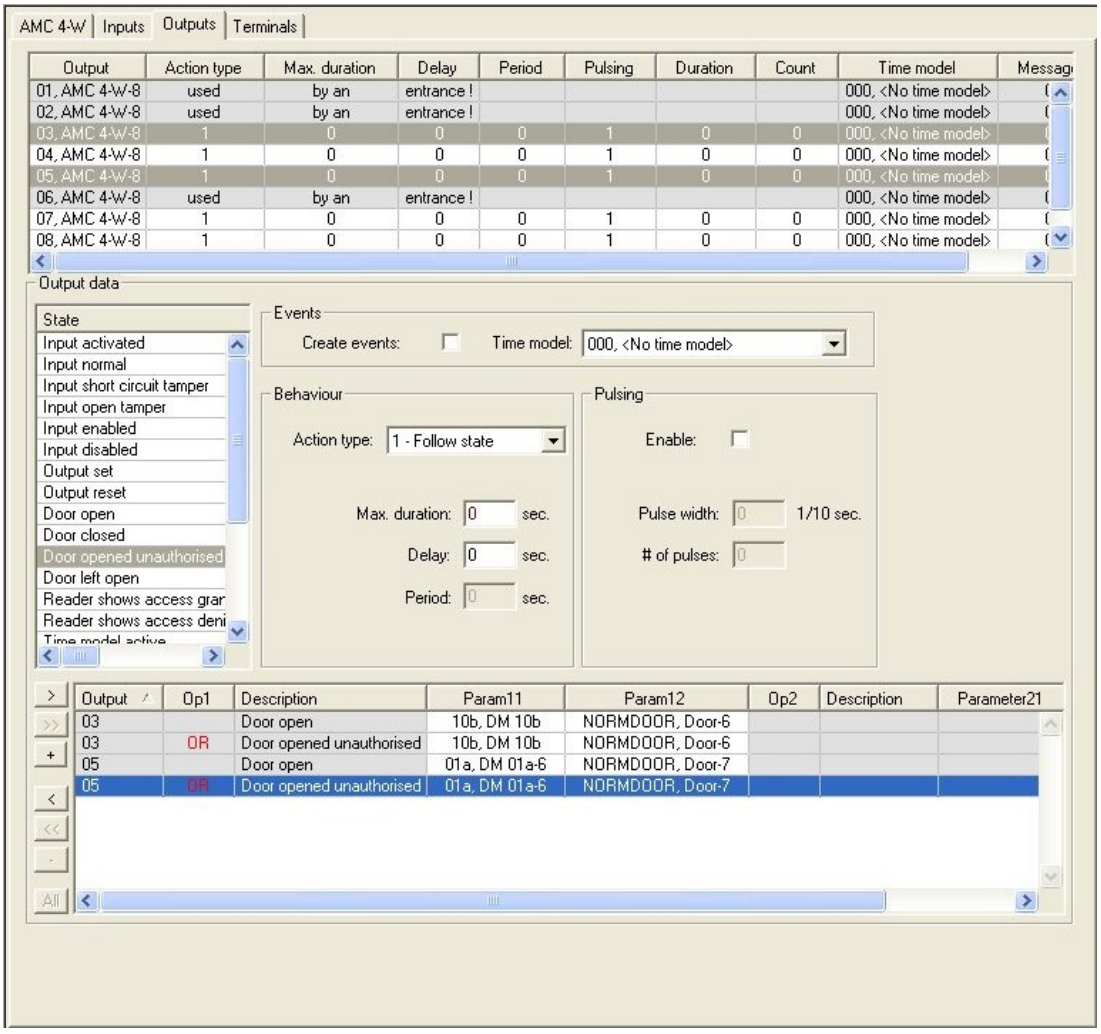
Seri	**Aralık**		**Paralel**	**Aralık**
"yok" veya "---"	1K-8K2		"yok" veya "---"	1K-8K2

1K	1K-2K2		1K	1K-1K8
1K2	1K-2K7		1K2	1K-2K7
1K5	1K-3K9		1K5	1K-3K3
1K8	1K-6K8		1K8	1K-3K9
2K2	1K2-8K2		2K2	1K-4K7
2K7	1K2-8K2		2K7	1K2-5K6
3K3	1K5-8K2		3K3	1K5-6K8
3K9	1K8-8K2		3K9	1K5-8K2
4K7	2K2-8K2		4K7	1K8-8K2
5K6	2K7-8K2		5K6	1K8-8K2
6K8	3K3-8K2		6K8	1K8-8K2
8K2	3K9-8K2		8K2	2K2-8K2

AMC Çıkışlarını Yapılandırma - Genel Bakış

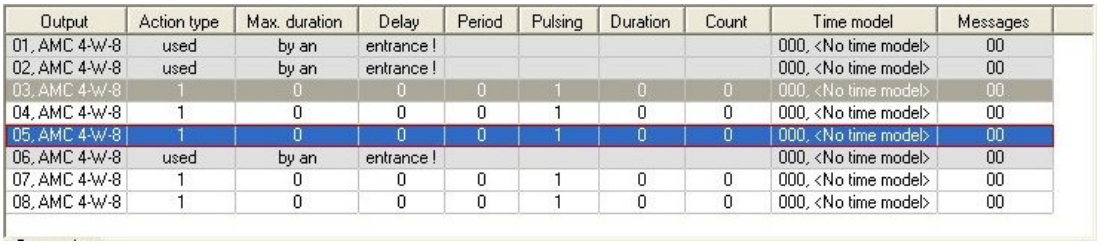
Bu iletişim sayfası, bir AMC veya AMC-EXT'deki her çıkışın yapılandırılmasını sağlar ve üç ana alan içerir:

– Her çıkış için ayarlanan parametreye genel bakışı içeren liste kutusu
– Listede seçilen çıkışlara yönelik yapılandırma seçenekleri
– Çıkışların etkinleştirilmesine yönelik koşulların tanımı



Tablodaki AMC çıkışlarını seçme

Çıkış kontaklarını yapılandırmak için önce üst tablodaki ilgili satırı seçin. Gerekiyorsa birden fazla satırı seçmek için Ctrl ve Shift tuşlarını kullanın. Pencerenin alt kısmında yapılan değişiklikler yalnızca seçtiğiniz çıkışları etkiler.



Çıkışları daha önce bir kapı modeli aracılığıyla veya başka bir yerden atanan çizgiler, "**used by an entrance!**" (bir giriş tarafından kullanılıyor!) bilgisiyle birlikte açık gri renkte gösterilir. Bu tür çıkışlar daha fazla yapılandırılamaz.

Sizin seçtiğiniz satırlar koyu gri renktedir.

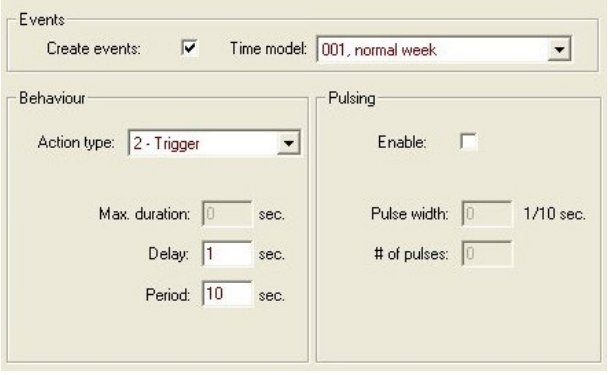
AMC çıkışlarının parametreleri

Sütun adı	Açıklama
Output (Çıkış)	ilgili AMC veya AMC-EXT'deki çıkışların geçerli numaralandırması AMC ve AMC_IO08 ile 01-08 AMC_IO16 ile 01-16

Action type (İşlem tipi)	seçilen işlem tipinin gösterimi 1 = Takip durumu 2 = Tetikleyici 3 = Dönüşümlü
Max. duration (Maks. süre)	saniye cinsinden sinyal uzunluğu [1 - 9999; 0 = her zaman, karşıt mesaj görünmezse] - sadece işlem tipi "1" ile
Delay (Gecikme)	sinyal verilene kadar saniye cinsinden gecikme [0 - 9999] - sadece işlem tipi "1" ve "2" ile
Period (Süre)	saniye cinsinden sinyalin verildiği süre - sadece işlem tipi "2" ile
Pulsing (Darbe Gönderme)	darbenin etkinleştirilmesi - aksi takdirde sinyal sürekli verilir
Duration (Süre)	darbe uzunluğu
Count (Sayı)	saniyedeki darbe sayısı
Time model (Zaman modeli)	seçilen zaman modelinin adı
Messages (Mesajlar)	mesaj etkinliğinin işaretlenmesi 00 = mesaj yok 03 = olaylar bildirildi
Assigned (Atandı)	Giriş Modeli 15 kullanıldığında, DOP'nin sinyal adı görüntülenir.

Çıkışlar: Olaylar, Eylem, Darbe Gönderme

Yukarıdaki listedeki tüm girişler, **Events** (Olaylar), **Action** (Eylem) ve **Pulsing** (Darbe Gönderme) iletişim kutularındaki onay kutuları ve giriş alanları kullanılarak oluşturulur. Bir liste girişi seçmek, bu alanlardaki ilgili ayarları gösterir. Bu, seçilen tüm çıkışlara yönelik parametrelerin eşit olması koşuluyla çok sayıda liste girişi için de geçerlidir. Listeden seçilen tüm girişler için parametre ayarlarındaki değişiklikler benimsenir.



Etkin çıkış için bir mesaj gönderilmesi gerekiyorsa **Create events** (Olay oluştur) onay kutusunu seçin. Bu mesajlar sadece özel dönemlerde, örneğin geceleri veya hafta sonları gönderilecekse uygun bir **zaman modeli** atayın.

Tek işlem türleri için aşağıdaki parametreler ayarlanabilir:

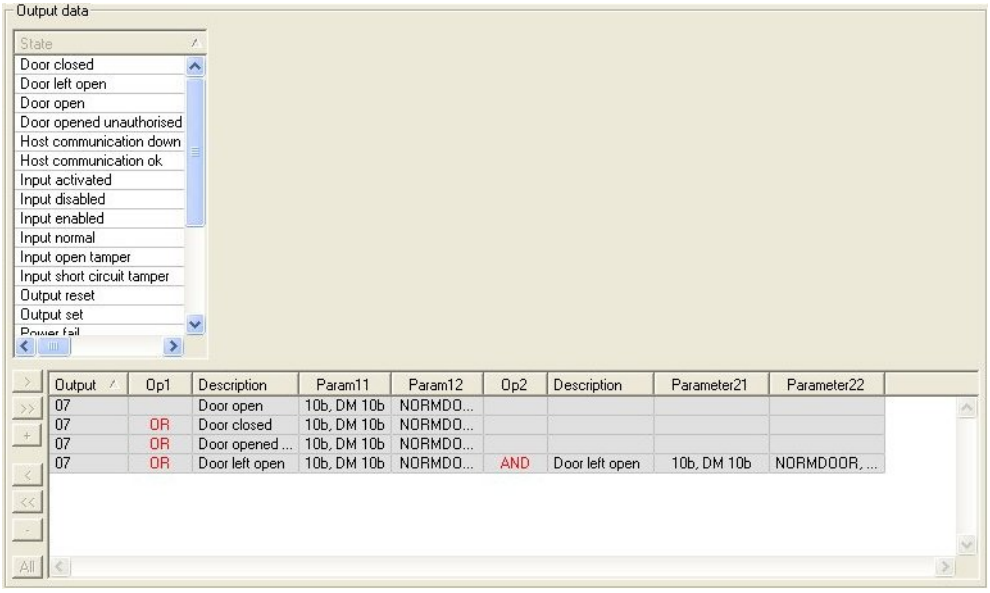
Action type (İşlem tipi)	**Max. duration** (Maks. süre)	**Delay** (Gecikme)	**Period** (Süre)	**Pulsing/ Enable** (Darbe Gönderme/ Etkinleştirme)	**Pulse width** (Darbe genişliği)	**Number of pulses** (Darbe sayısı)
Takip durumu	0 = her zaman 1 - 9999	0 - 9999	hayır	evet	1 - 9999	Yok
Tetikleyici	hayır	0 - 9999	0 - 9999 darbe gönderme etkin **değilse**	evet süreyi devre dışı bırakır	1 - 9999	1 - 9999
Dönüşümlü	hayır	hayır	hayır	evet	1 - 9999	hayır

AMC çıkış verileri

Outputs (Çıkışlar) iletişim kutusunun alt kısmı şunları içerir:

– Seçilen çıkışlar için kullanılabilen **durumları** içeren bir liste kutusu.

– Çıkışları ve bu çıkışları tetiklemek için yapılandırılmış durumları içeren bir tablo.



Çıkışları belirli durumlar tarafından tetiklenecek şekilde yapılandırma

Yukarıda seçtiğiniz çıktıları, tek durumlar veya mantıksal durum birleşimleri tarafından tetiklenecek şekilde yapılandırabilirsiniz.

– Üst liste kutusundan bir veya daha fazla çıkış seçin.

– **State** (Durum) listesinden bir durum seçin.

– Bu durumu iletebilecek seçili duruma sahip birden fazla cihaz veya kurulum varsa » düğmesi › düğmesinin yanında etkinleştirilir.
Seçilen her çıkış için › simgesine tıklayarak (veya duruma çift tıklayarak), ilk cihaz (örneğin AMC, ilk giriş) ve kurulum (örneğin ilk sinyal, ilk kapı) ile durumdan oluşan bir giriş oluşturun.

Exit	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2

» simgesine tıklandığında, seçilen durum listeye aktarılır ve her kurulu cihaz (örneğin, tüm AMC girişleri) için mantıksal VEYA operatörü ile birlikte oluşturulur.

Exit	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 02, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 03, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 04, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 05, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 06, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 07, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 08, AMC 4-W-2

– Bir VEYA kısayolu üzerinden birkaç durum atanabilir.

Exit	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
04	OR	Input normal	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Door open	06a, Timemgm	<< !!! >>

VE bulunan kısayollar da mümkündür:

– Rastgele bir sütundan seçilerek başka bir koşulun eklendiği durum zaten atanmış olmalıdır.
– Ardından başka bir durum seçilir ve · simgesine tıklanarak işaretli duruma bağlanır.

Exit	Operand1	Description	Param11	Param12	Operand2	Description	Parameter21	Parameter22
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2				
04	OR	Input normal	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2				
04	OR	Door open	06a, Timemgm	<< !!! >>	AND	Door opened unauthorised	06a, Timemgm	<< !!! >>

Uyarı!
Her çıkışa en çok 128 VEYA koşulu atanabilir.
Her koşulun içinde **bir** VE koşulu olabilir.

Bir durum bir cihaz veya kurulum için atandıktan sonra, bu diğer tüm mevcut cihazlar ve kurulumlar için de atanabilir.

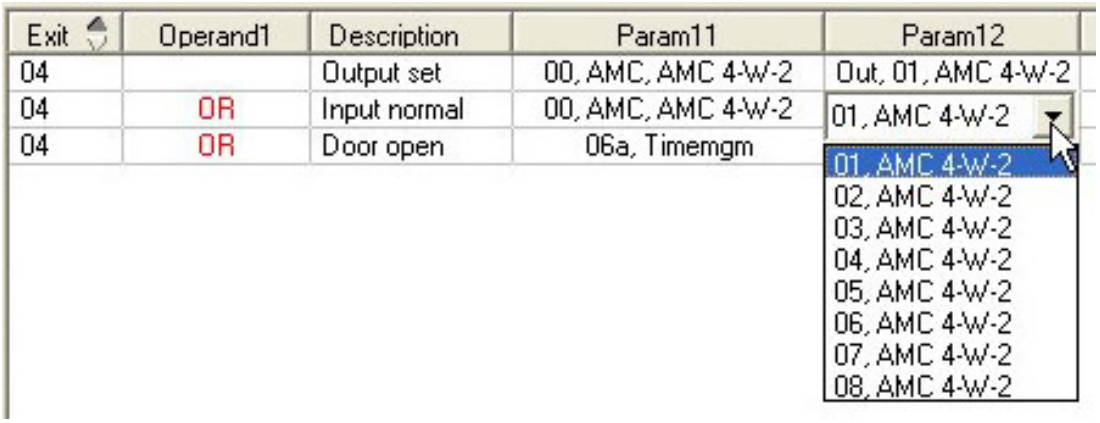
– Rastgele bir sütunda atanan girişi seçin.
– Bu durum, tüm mevcut cihazlar ve kurulumlar için All simgesine tıklanarak oluşturulur.

Çıkışların parametrelerini değiştirme
Listedeki satırları değiştirebilirsiniz
Atanan durumun eşleşebileceği bazı cihazlar veya kurulumlarda, bu tipteki ilk cihazlar ve kurulumlar her zaman ayarlanır.
Param11 ve **Param21** (AND kısayollarıyla) sütunlarında cihazlar (örneğin, AMC, giriş) görüntülenir. **Param12** ve **Param22** sütunları ise özel kurulumları (örneğin, giriş sinyali, kapı, okuyucu) içerir.

Birkaç cihaz (örneğin G/Ç kartları) veya kurulum (örneğin, ek sinyaller, okuyucular) mevcutsa fare işaretçisi bu sütunu gösterirken değişir.

Exit	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
04	OR	Input normal	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Door open	06a, Timemgm	<< !!! >>

Sütun girişine çift tıklandığında, bir düğme parametre için geçerli girişlerden oluşan bir açılır listeyi açar.



Param11 ve **Param21** sütunlarındaki girişler değiştirildiğinde, **Param12** ve **Param22** sütunlarındaki girişler güncellenir:

Exit	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
04	OR	Door open	06a, Timemgm	<< !!! >>
04	OR	Input normal	01, AMC_IO, AMC_IO16_002_1	In, 01, AMC_IO16_002_1

Uyarı!
Bu sadece **Param11**, **Param12**, **Param21** ve **Param22** sütunları için mümkündür.
Başka seçenek yoksa (örneğin, yalnızca bir giriş yapılandırıldığından), fare işaretçisi değişmez ve tüm alanlar gri renktedir. Bu girişe çift tıklanmışsa bu bir silme komutu olarak yorumlanır ve silme işlemini doğrulamak için mesaj kutusu görüntülenir.

Çıkışları tetikleyen durumları silme

Seçilen atamalar '**<**' simgesine tıklanarak (veya liste girişine çift tıklanarak) kaldırılabilir. Bir mesaj kutusu silme için onay ister.

Birkaç durum bir çıkışla ilişkilendirilmişse bunların hepsi aşağıdaki gibi birlikte silinebilir:

- İlk liste girişini (**Op1** sütununda girişi olmayan) seçin ve ardından '**<<**' düğmesine tıklayın.
- Alternatif olarak, ilk girişe çift tıklayın.
  - Bir açılır pencere görünür. Silme işlemini onaylayın veya durdurun.
  - Silme işlemini onaylarsanız ikinci bir açılır pencere ilişkili tüm girişleri (**Yes** (Evet) yanıtı) ya da yalnızca seçilen girişi (**No** (Hayır) yanıtı) silmek isteyip istemediğinizi sorar.

İlk durumu **Op2** sütunundaki bir VE operatörü ile niteleyen ek durumları silmek için, satırda herhangi bir yere ve ardından "eksi" düğmesine tıklayın. Bu düğme yalnızca bu satırda uygun bir VE durumu varsa etkindir.

Durum açıklaması

Aşağıdaki tabloda tüm seçilebilir durumlar, bunların tip numarası ve açıklamasına genel bir bakış sunulmaktadır.

State (Durum) liste alanı bu parametreleri de içerir; listede sağa doğru gidilerek gösterilir.

Durum	Tip	Açıklama
Giriş etkin	1	Yerel giriş
Giriş normal	2	Yerel giriş
Giriş kısa devre dış müdahalesi	3	Dirençli yerel giriş yapılandırıldı
Giriş açık dış müdahalesi	4	Dirençli yerel giriş yapılandırıldı
Giriş devre dışı	5	Yerel giriş zaman modeliyle devre dışı bırakıldı
Giriş etkin	6	Yerel giriş zaman modeliyle etkinleştirildi
Çıkış ayarlandı	7	Yerel çıkış, geçerli çıkış değil
Çıkış sıfırlandı	8	Yerel giriş, geçerli giriş değil
Kapı açık	9	Girişin GID'si, kapı numarası
Kapı kapalı	10	Girişin GID'si, kapı numarası
Kapı yetkisiz olarak açıldı	11	Girişin GID'si, kapı numarası, "Açık kapı"yı değiştirir (9)
Kapı açık bırakıldı	12	Girişin GID'si, kapı numarası
Okuyucu giriş izni verildiğini gösteriyor	13	Okuyucu adresi
Okuyucu girişin reddedildiğini gösteriyor	14	Okuyucu adresi
Zaman modeli etkin	15	Yapılandırılan zaman modeli
Dış müdahale okuyucu	16	Okuyucu adresi
Dış Müdahale AMC'si	17	---
Dış müdahale G/Ç kartı	18	---
Güç arızası	19	yalnızca pille çalışan AMC için
Güç iyi	20	yalnızca pille çalışan AMC için
Ana bilgisayar iletişimi tamam	21	---
Ana bilgisayar iletişimi kesildi	22	---
Okuyucudan mesaj	23	Okuyucu adresi
LAC'den mesaj	24	Board number (Kart numarası)
Kart kontrolü	25	Okuyucu adresi, kart kontrol işlevi.

Çıkışları yapılandırma

Kapı modelleri ya da tek atama ile birlikte sinyal atamanın yanı sıra henüz tahsis edilmeyen çıkışlar için koşullar tanımlanabilir. Bu koşullar oluşursa ayarlı parametreye karşılık gelen çıkış etkinleştirilir.

Neyin çıkış üzerinden değişeceğine karar vermeniz gerekir. Belirli bir kapı modeli, kapıları ve okuyucuları ile ilişkilendirilebilen sinyallerin aksine, bu durumda bir AMC'ye bağlı tüm cihazların ve kurulumların sinyalleri uygulanabilir.

Örneğin, optik, akustik bir sinyal veya harici bir cihaza gönderilen bir mesaj **Input short circuit tamper** (Giriş kısa devre müdahalesi) ve **Door opened unauthorized** (Kapı yetkisiz açıldı) sinyalleri tarafından tetiklenirse bu dikkate alınacak giriş veya girişler ilgili hedef çıkışa atanır.

Her durumda yalnızca bir kontağın seçildiği örnek:

Exit	Operand1	Description	Param11	Param12
04		Input short cir...	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Door opened ...	06a, Timemgm	<< !!! >>

Tüm kontakları içeren örnek:

Exit	Operand1	Description	Param11	Param12
04		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 02, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 04, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 07, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 08, AMC 4-W-2
04	OR	Door opened unauthorised	06a, Timemgm	---
04	OR	Door opened unauthorised	03a, Entrance B:B	REVDOOR, Revolving Door

Seçilen kontakları içeren örnek:

» simgesine tıklandığında veya tüm kontaklar atandıktan sonra gerekli olmayan kontaklar kaldırıldığında her kontak için tek bir giriş oluşturulur:

Exit	Operand1	Description	Param11	Param12
04		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
04	OR	Door opened unauthorised	06a, Timemgm	---
04	OR	Door opened unauthorised	03a, Entrance B:B	REVDOOR, Revolving Door

Aynı koşullar, örneğin optik bir sinyale ek olarak bir akustik sinyale de ihtiyacınız olursa ve aynı zamanda harici cihaza aynı anda bir mesaj gönderilmesi gerekirse birkaç çıkışa yüklenebilir:

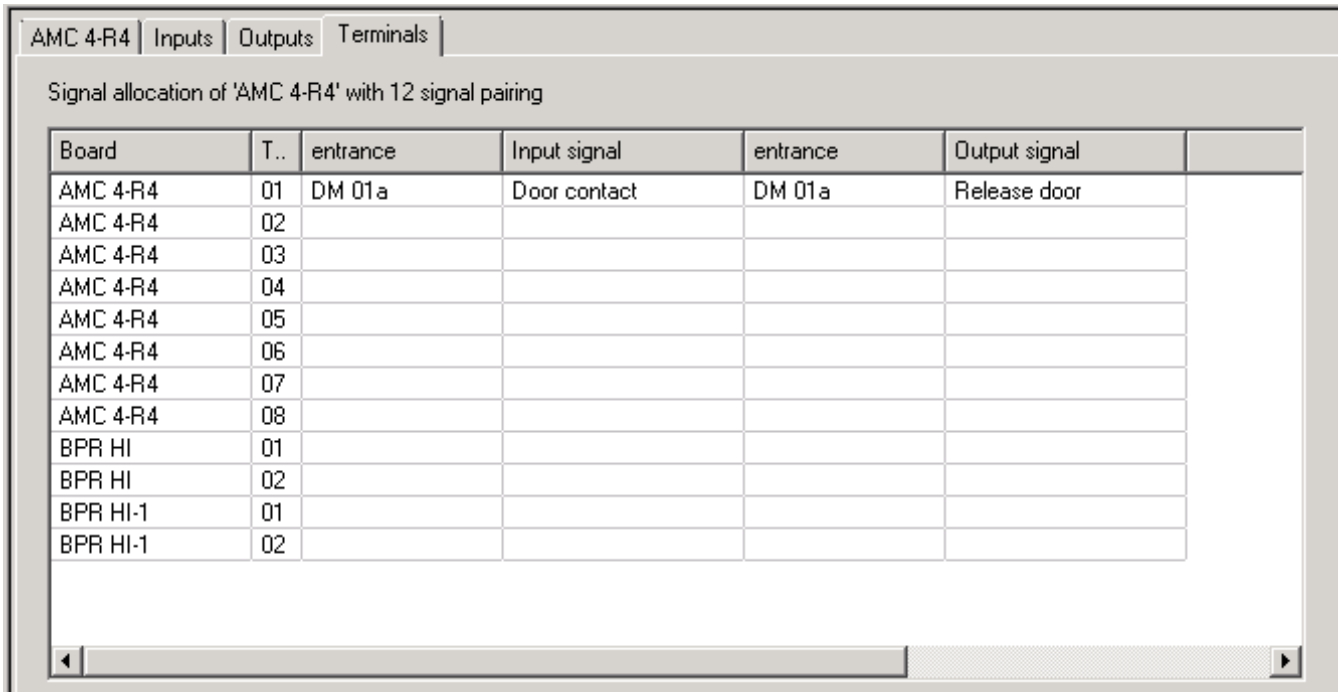
Exit	Operand1	Description	Param11	Param12
04		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 02, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 04, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 07, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 08, AMC 4-W-2
04	OR	Door opened unauthorised	06a, Timemgm	<< !!! >>
04	OR	Door opened unauthorised	03a, Entrance B:B	REVDOOR, Revolving Door
06		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 02, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 04, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 07, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 08, AMC 4-W-2
06	OR	Door opened unauthorised	06a, Timemgm	<< !!! >>
07		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 02, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 04, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 07, AMC 4-W-2

Parametre 11/21 ve 12/22 için varsayılan değerlerin bulunduğu tüm mevcut durumların listesi:

Description	Param11	Param12
Input activated	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input normal	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input open tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input enabled	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input disabled	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
Output reset	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
Door open	06a, Timemgm	<< !!! >>
Door closed	06a, Timemgm	<< !!! >>
Door opened unauthorised	06a, Timemgm	<< !!! >>
Door left open	06a, Timemgm	<< !!! >>
Reader shows access granted	---	TM-Reader IN
Reader shows access denied	---	TM-Reader IN
Time model active	---	000, <No time model>
Tamper reader	---	TM-Reader IN
Tamper AMC	---	---
Tamper I/O board	---	00, AMC, AMC 4-W-2
Power fail	---	---
Power good	---	---
Host communication ok	---	---
Host communication down	---	---

Terminaller sekmesindeki sinyalleri tanımlama

Terminals (Terminaller) sekmesinde bir AMC veya AMC-EXT'deki kontak tahsisi gösterilir. Girişler oluşturulduktan sonra, sinyal atamaları seçilen kapı modeline göre gösterilir. Kontrol cihazının ve genişletme kartlarının **Terminals** (Terminaller) sekmesinde değişiklik yapamazsınız. Düzenlemeler yalnızca giriş sayfasının terminaller sekmesinde yapılabilir. Bu nedenle terminal ayarları gri bir arka plan üzerinde görüntülenir. Kırmızı renkte görüntülenen girişler, ilgili çıkışların sinyal yapılandırmalarını gösterir.

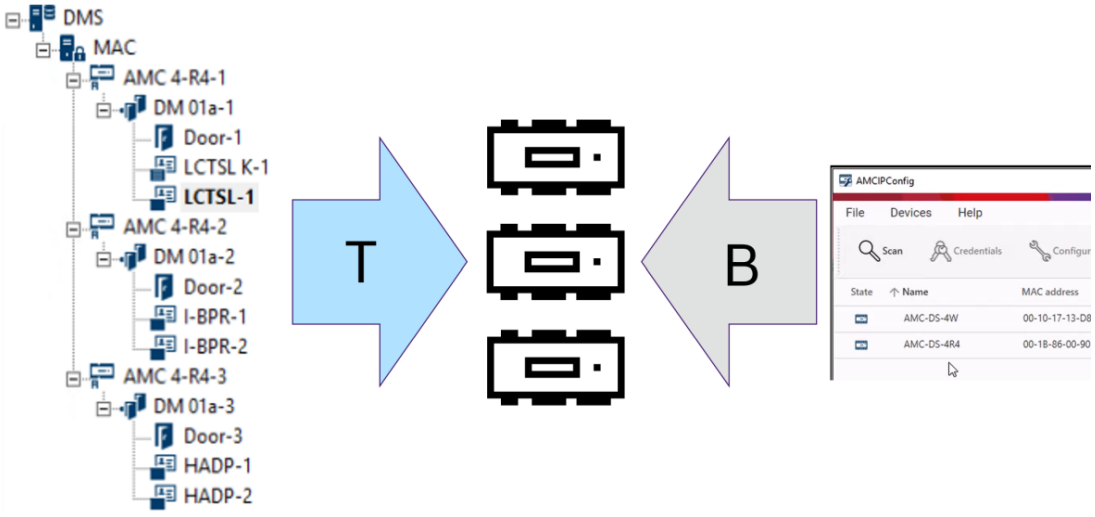


Board	T..	entrance	Input signal	entrance	Output signal
AMC 4-R4	01	DM 01a	Door contact	DM 01a	Release door
AMC 4-R4	02				
AMC 4-R4	03				
AMC 4-R4	04				
AMC 4-R4	05				
AMC 4-R4	06				
AMC 4-R4	07				
AMC 4-R4	08				
BPR HI	01				
BPR HI	02				
BPR HI-1	01				
BPR HI-1	02				

15 DTLS'yi güvenli iletişim için yapılandırma

Giriş

Kartlı geçiş sistemi (ACS), DTLS tarafından korunan son derece güvenli cihaz iletişimi sağlar. DTLS iletişimini ACS'deki cihazlar arasında dağıtmanın iki ana yolu vardır:
Yukarıdan aşağıya doğru dağıtım (T), ACS 'nin cihaz düzenleyicisinde yapılır.
Aşağıdan yukarıya doğru dağıtım (B) genellikle AMCIPConfig aracında yapılır ancak tamamlamak için cihaz düzenleyicisi gereklidir.



- (T) Yukarıdan aşağıya doğru dağıtım cihaz düzenleyicisinde iki farklı şekilde yapılabilir:
  - Tüm AMC'ler için DMS seviyesinde tek bir cihaz iletişim şifresi (DCP) kullanarak,
  - Cihaz ağacının farklı dalları için ilgili MAC'ler veya bir AMC'lerde başlayan birden fazla DCP kullanarak.
- (B) Aşağıdan yukarıya doğru dağıtım da AMCIPConfig aracında iki alternatif şekilde başlatılabilir:
  - AMC donanım anahtarı kullanarak
  - Rastgele bir LCD anahtarı kullanarak

Uyarı!
Aşağıdan yukarıya dağıtım için yine cihaz düzenleyicisinde DCP'lerin ayarlanması gerekir. Aşağıdan yukarıya dağıtım, AMC cihazında bir DCP ayarlamanızı sağlar. Ayrıca, MAC ve AMC arasında tam DTLS iletişimi sağlamak için aynı AMC'de aynı DCP'yi de ayarlamanız gerekir.

DTLS dağıtım seçeneklerinin özeti

	Kısa açıklama	Avantajlar	Dezavantajlar
Yukarıdan aşağıya	Sistem yöneticisi **Cihaz Düzenleyicisi**'nde güçlü bir şifre girer. Sistem, bu şifreden DMS'den MAC'lere ve AMC kapı kontrol cihazlarına kadar kartlı geçiş cihazları ağacı aracılığıyla yukarıdan aşağıya doğru yaydığı bir **Ana anahtar** oluşturur.	Hızlı, basit dağıtım.	Ana anahtarın AMC kapı kontrol cihazlarına yayılması sırasında cihazın iletişimi DTLS tarafından korunmaz.

	Kısa açıklama	Avantajlar	Dezavantajlar
	Cihaz ağacının tamamı için bir şifre ya da cihaz ağacının farklı dallarına ait farklı şifreler belirleyebilirsiniz.		
AMC donanım anahtarı kullanılarak aşağıdan yukarıya	Sistem yöneticisi, DTLS'yi AMC kapı kontrol cihazı seviyesinde dağıtmak için **AMC IPConfig** aracını kullanır.	Daha fazla dağıtım ayrımı ve esnekliği. Bu yöntem, yukarıdan aşağıya doğru dağıtımın ana dezavantajını, yani bir ana anahtarın ara sıra gerçekleşen korumasız iletişimini önler. Yine de DCP'yi ayarlarken AMCIPConfig aracından AMC'ye bağlantının güvenli olmasını gerektirir.	IPConfig aracı AMC'deki DCP'yi ayarlarken, güvenli iletişimi başka yollarla sağlamanız gerekir. Örneğin, AMC'yi doğrudan IPConfig'in çalıştığı bilgisayara bağlayın. IPConfig aracında ayarladığınız DCP'ler, cihaz düzenleyicisi aracılığıyla aynı AMC'de de ayarlanmalıdır.
Rasgele LCD tuşu kullanılarak aşağıdan yukarıya		Daha fazla dağıtım ayrımı ve esnekliği. En yüksek güvenliktir, çünkü LCD anahtarı ağ üzerinden hiçbir şekilde iletilmez. Bu nedenle, kimlik bilgilerinin yayılması her zaman koruma altındadır.	Daha karmaşık ve zaman alan dağıtım. 27 simgeli rastgele LCD anahtarını ağ dışındaki bazı yollarla IPConfig aracına aktarmanız gerekir.
Ayrıntılar ve yönergeleri bu bölümün sonraki kısımlarında bulabilirsiniz.			

DTLS terminolojisi

DCP (Cihaz İletişim Şifresi)	ACS'nin dahili bir ana anahtar oluşturduğu tek bir güçlü şifre. Şifre, ACS'de saklanmadığından güvenli halde tutulmalıdır.
Ana anahtar	Sistemin DCP'den ürettiği ve giriş kontrol cihazlarını korumak için kullandığı kod. Ana anahtar hiçbir zaman herhangi bir kullanıcıya görünmez.
Rastgele LCD anahtarı	AMC'nin her yeniden başlatıldığında yeniden oluşturduğu geçici alfa sayısal kod. Anahtar AMC'nin sıvı kristal ekranında (LCD) görüntülenebilir ve ağ iletişiminin kimliğini doğrulamak için yazılım araçları tarafından istenebilir.

AMC donanım anahtarı.	AMC'nin belirli donanım parametrelerinden oluşturduğu dahili kimlik doğrulama kodu. Kullanıcıya gösterilmez.

15.1 Yukarıdan aşağıya doğru DTLS dağıtımı

Ön koşullar

- AMS 4.0 veya BIS-ACE 4.9.1 ya da sonrası.
- DMS'den AMC'ye kartlı geçiş cihazları ağacı fiziksel olarak kurulmuş ve ağa bağlanmıştır ancak AMC'ler etkinleştirilmemiştir. Etkin, AMC'lerin **Communication to host enabled** (Ana bilgisayar ile iletişim etkin) onay kutularının seçildiği anlamına gelir.
- DTLS, AMC'lerde aşağıdan yukarıya doğru yöntemlerden biri ile zaten bir IPConfig aracı aracılığıyla yapılandırılmamıştır.

Prosedür: Tümü için bir DCP

1. ACS'de Cihaz Düzenleyici'ni başlatın
   - AMS Main menu (AMS Ana menü) > **Configuration** (Yapılandırma) > **Device data** (Cihaz verileri) > **Device tree** (Cihaz ağacı) 
   - Sizi Güçlü bir Cihaz İletişim Şifresi (DCP) girmeye davet eden bir iletişim kutusu penceresi görüntülenir.
2. Cihaz ağacındaki tüm AMC'ler için tek bir DCP ayarlamak üzere yerel şifre ilkelerinize göre güçlü bir şifre girin ve onaylayın.
   - İletişim kutusu şifre entropisine bağlı olarak şifre gücü ile ilgili geri bildirimde bulunur.
3. Şifre ACS'de saklanmadığından şifreyi dikkatlice not edin.
4. İletişim kutusunu kapatmak için **OK**'e (Tamam) tıklayın.

Alternatif prosedür: Cihaz ağacının farklı dalları için birden fazla DCP

1. ACS'de Cihaz Düzenleyici'ni başlatın
   - AMS Main menu (AMS Ana menü) > **Configuration** (Yapılandırma) > **Device data** (Cihaz verileri) > **Device tree** (Cihaz ağacı) 
   - Sizi Güçlü bir Cihaz İletişim Şifresi (DCP) girmeye davet eden bir iletişim kutusu penceresi görüntülenir.
2. Cihaz ağacının farklı dallarındaki (MAC'ler ve AMC'ler) farklı DCP'leri ayarlamak için **Cancel**'a (İptal) tıklayın.
   - Bir açılır iletişim kutusu, sistemdeki kaç AMC'de hala DCP olmadığını bildirir.
   - Cihaz ağacı Cihaz Düzenleyicisi'nde açılır.
3. DCP ayarlamak istediğiniz MAC veya AMC'yi seçmek için cihaz ağacını açın.
   - DCP'yi bir MAC seviyesinde ayarlarsanız tüm MAC'nin alt AMC'leri için de ayarlanır.
   - DCP'yi bir AMC düzeyinde ayarlarsanız bu, yalnızca bu AMC için ayarlanır.
4. **Device communication password:** (Cihaz iletişim şifresi:) metin alanının yanındaki üç nokta  düğmesine tıklayın.
5. Yerel şifre ilkelerinize göre güçlü bir şifre girin ve onaylayın.
6. ACS'de saklanmadığından şifreyi ve geçerli olduğu dikkatlice not edin.
7. Ayrı bir DCP ayarlamak istediğiniz her MAC veya AMC için bu prosedürü tekrarlayın.
8. İletişim kutusunu kapatmak için **OK**'e (Tamam) tıklayın.

Yukarıdan aşağıya dağıtımın sonucu

ACS, seçilen DMS veya MAC'nin altındaki tüm AMC'ler için dahili anahtarlar oluşturmak amacıyla DCP veya DCP'leri kullanır.

AMC IPConfig aracını kullanarak sonrasında DCP'yi bir veya daha fazla AMC'de değiştirmediğiniz sürece bu prosedürü yinelemeniz gerekmez (bkz. "aşağıdan yukarıya doğru" dağıtım). Bu durumda derhal aynı DCP'yi cihaz düzenleyicisinde aynı AMC'de ayarlamanız gerekir.

Daha sonra zaten DCP'leri bulunan DMS'ler ve MAC'lere alt cihaz ağacında cihaz eklerseniz yeni cihazlar aynı DCP'yi üst cihazlarından otomatik olarak devralır.

16 Girişleri Yapılandırma

16.1 Girişler - giriş

Giriş terimi bütünüyle bir giriş noktasındaki kartlı geçiş mekanizmasını belirtir:
Girişin öğeleri şunlardır:

- Giriş okuyucuları - 1 ile 4 arasında
- Örneğin bir kapı, turnike, tuzak veya bomlu bariyer gibi bir tür bariyer.
- Donanım elemanları arasında önceden belirlenmiş elektronik sinyal dizileri tarafından tanımlanan giriş prosedürü.

Bir Kapı modeli belirli bir giriş türüne ilişkin bir şablondur. Mevcut kapı elemanlarını (okuyucuların sayısı ve tipi, kapı veya bariyer tipi vb.) açıklar ve önceden tanımlanmış sinyal dizileriyle belirli bir kartlı geçiş işlemi uygular.
Kapı modelleri, bir kartlı geçiş sisteminin yapılandırmasını büyük ölçüde kolaylaştırır.

Kapı modeli 1	basit veya ortak kapı
Kapı modeli 3	giriş ve çıkış için ters çevrilebilir turnike
Kapı modeli 5	otopark girişi veya çıkışı
Kapı modeli 6	Zaman ve devam için gelen/giden okuyucuları
Kapı modeli 7	asansör kontrolü
Kapı modeli 9	bomlu araç bariyeri ve kayar kapı
Kapı modeli 10	IDS ile kurma/devre dışı bırakma özelliğine sahip basit kapı
Kapı modeli 14	IDS ile kurma/devre dışı bırakma özelliğine ve özel erişim haklarına sahip basit kapı
Kapı modeli 15	bağımsız giriş ve çıkış sinyalleri

- Kapı modelleri 1, 3, 5, 9 ve 10 gelen veya giden tarafta ek kart okuyucular için bir seçenek içerir.
- Kapı modeli 05 (otopark) veya 07 (asansör) içinde kullanılan yerel bir giriş kontrol cihazı başka bir kapı modeliyle paylaşılamaz.
- Bir giriş bir kapı modeli ile yapılandırılıp kaydedildiğinde, kapı modeli artık bir başka bir modelle değiştirilemez. Farklı bir kapı modeli gerekiyorsa giriş silinerek ve en baştan yeniden yapılandırılmalıdır.

Bazı kapı modellerinin aşağıdaki özelliklere sahip çeşitleri (a, b, c, r) vardır:

a	gelen **ve** giden okuyucuları
b	gelen okuyucusu ve giden basmalı düğmesi
c	gelen **VEYA** giden okuyucusu (ikisi de değil - **a** çeşidi olacak)
r	(Sadece kapı modeli 1). Örneğin, bir tahliye durumunda bir toplanma noktasında yalnızca kişileri kaydetmek amacıyla tek okuyucu. Bu kapı modelinde hiçbir fiziksel engel yoktur.

Yapılandırmayı sona erdirecek **OK** (Tamam) düğmesi yalnızca tüm zorunlu değerler girildiğinde etkin hale gelir. Örneğin, çeşidin (a) kapı modelleri için gelen **ve** giden okuyucuları gereklidir. İki okuyucu için de bir tip seçilinceye kadar kayıtlar kaydedilemez.

16.2 Giriş oluşturma

Seçim için sunulan okuyucu listesi seçtiğiniz kontrol cihazı tipine göre uyarlanır.

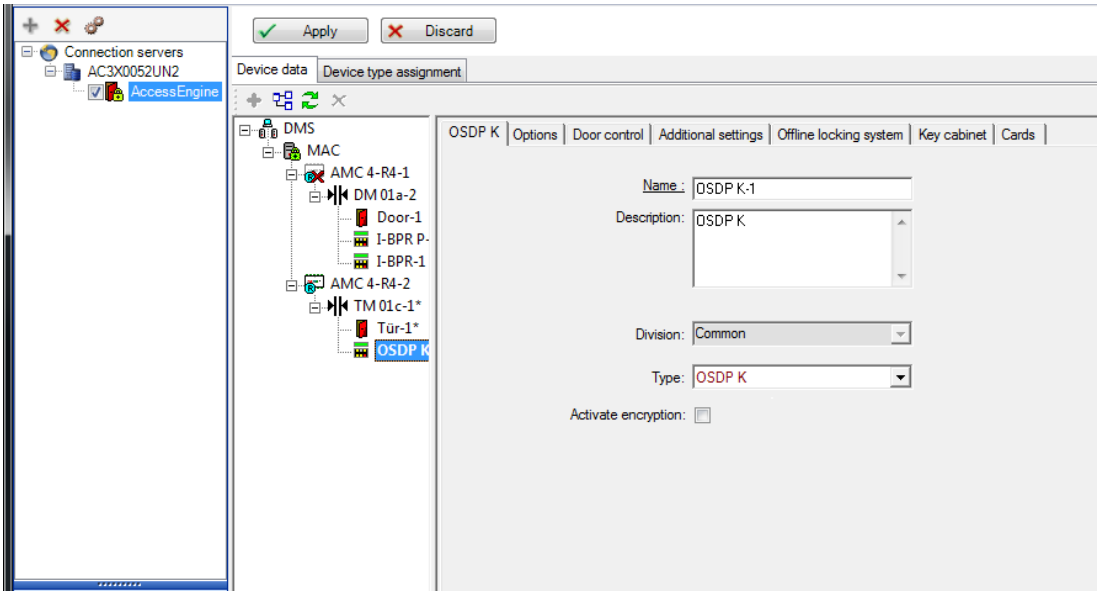
– **AMC 4W** tipleri için yalnızca hem klavyeli hem de klavyesiz Wiegand okuyucular kullanılabilir.
– **AMC 4R4** için ise aşağıdaki tabloda bulunan okuyucular kullanılabilir. Protokolleri aynı kontrol cihazında birlikte kullanmayın.

Okuyucu adı	Wiegand Protokolü	BPR Protokolü (*)	I-BPR Protokolü	HADP Protokolü	OSDP Protokolü
WIE1	X				
WIE1K (Klavye)	X				
BPR MF		X			
BPR MF Klavye		X			
BPR LE		X			
BPR LE Klavye		X			
BPR HI		X			
BPR HI Klavye		X			
TA40 LE		X			
TB15 HI1		X			
TB30 LE		X			
INTUS 1600			X		
I-BPR			X		
I-BPR K (Klavye)			X		
DT 7020			X		
OSDP					X
OSDP K (Klavye)					X
OSDP KD (Klavye + Ekran)					X
HADP				X	
HADP K (Klavye)				X	
HADP KD (Klavye + Ekran)				X	
RKL 55 (Klavye + LCD)				X	
RK40 (Klavye)				X	
R15				X	
R30				X	

R40				X	
RK40				X	
RKL55				X	

(*) BPR Protokolü kullanımdan kaldırılmış olup ve buraya yalnızca uyumluluk nedeniyle eklenmiştir.

Bir **OSDP okuyucusu** durumunda, iletişim kutusu aşağıdaki gibi görünür:



OSDP ile güvenli iletişim

Varsayılan olarak, **Activate encryption** (Şifrelemeyi etkinleştir) onay kutusu temizlenmiştir.

OSDPv2 güvenli destek bulunan okuyucular kullanıyorsanız bunu seçin.

Daha sonra onay kutusunun işaretini kaldırarak şifrelemeyi devre dışı bırakırsanız okuyucu donanımını üreticinin talimatlarına göre sıfırlayın.

Ek bir güvenlik önlemi olarak, farklı bir OSDP okuyucu birimiyle yapılandırılmış bir OSDP okuyucu birimini her değiştirme girişiminde kartlı geçiş sisteminde bir alarm oluşturulur. Operatör istemcideki alarmı kabul edebilir ve aynı anda değişim için izin verebilir.

Alarm mesajı: **Exchange of OSDP reader refused** (OSDP okuyucusu değişimi reddedildi)

Komut: **Allow exchanging the OSDP reader** (OSDP okuyucusunu değiştirmeye izin ver)

Aşağıdaki OSDP okuyucusu tipleri mevcuttur:

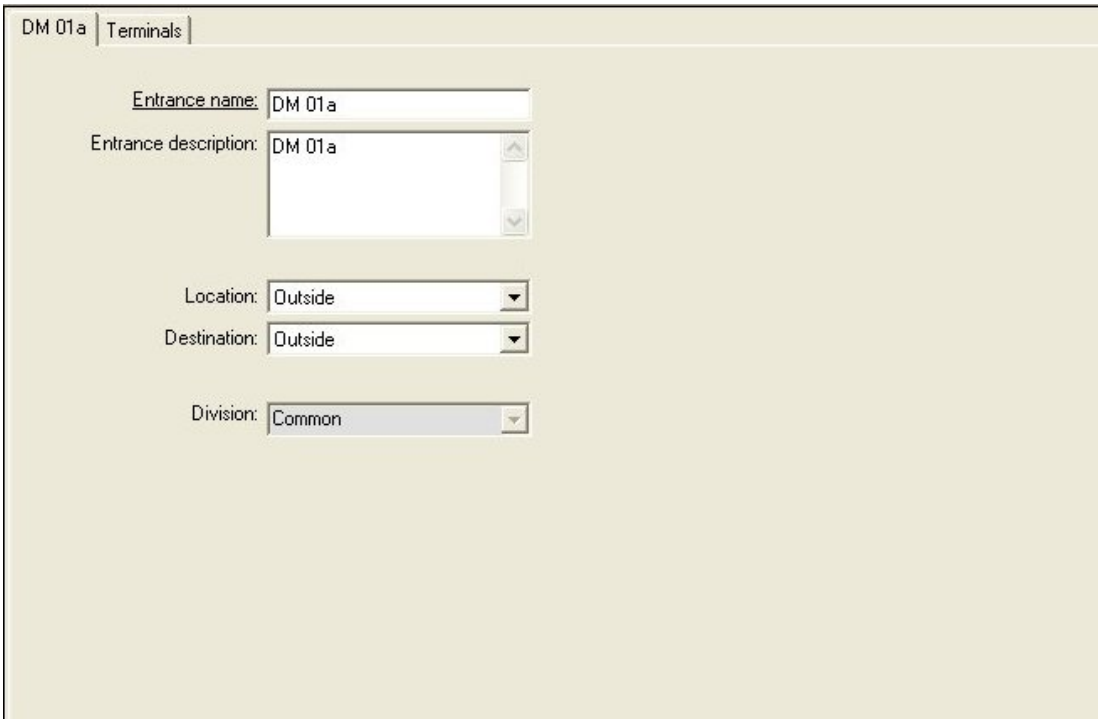
OSDP	Standart OSDP okuyucusu
OSDP Klavyesi	Klavyeli OSDP okuyucusu
OSDP Klavyesi + Ekranı	Klavyeli ve ekranlı OSDP okuyucusu

Aşağıdaki OSDP okuyucuları test edilmiştir:

OSDPv1 - güvenli olmayan mod	LECTUS duo 3000 C - MIFARE classic LECTUS duo 3000 CK - MIFARE classic LECTUS duo 3000 E - MIFARE Desfire EV1 LECTUS duo 3000 EK - MIFARE Desfire EV1

OSDPv2 - güvenli olmayan ve güvenli mod	LECTUS secure 2000 RO LECTUS secure 4000 RO LECTUS secure 5000 RO

Uyarı!
OSDP Uyarıları
Ürün ailelerini örneğin **LECTUS duo** ve **LECTUS secure**'u aynı OSDP veri yolunda birlikte kullanmayın.
Müşteriye özel bir anahtar oluşturulur ve OSDP okuyucusuna şifreli veri iletimi için kullanılır. Sistemin uygun şekilde yedeklendiğinden emin olun.
Anahtarları güvende tutun. Kayıp anahtarlar kurtarılamaz; okuyucu sadece fabrika ayarlarına döndürülebilir.
Güvenlik nedeniyle şifrelenmiş ve şifrelenmemiş modları aynı OSDP veri yolunda birlikte kullanmayın.
Cihaz Düzenleyicisi'nde okuyucunun OSDP sekmesindeki onay kutusunu temizleyerek şifrelemeyi devre dışı bırakırsanız okuyucu donanımını üreticinin talimatlarına göre sıfırlayın.

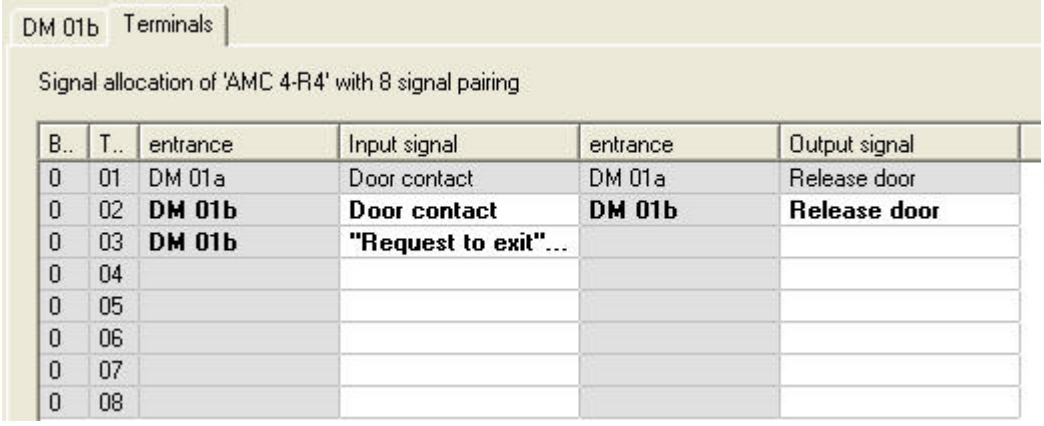


Parametre	Olası değerler	Açıklama
Entrance name (Giriş adı)	Alfa sayısal, 1 ile 16 karakter arasında	İletişim kutusu, giriş için benzersiz bir isim oluşturur, ancak istenirse girişi yapılandıran operatör tarafından bu adın üzerine yazılabilir.
Entrance description (Giriş açıklaması)	alfa sayısal: 0-255 karakter	Sistemde görüntüleme için rastgele bir açıklayıcı metin.

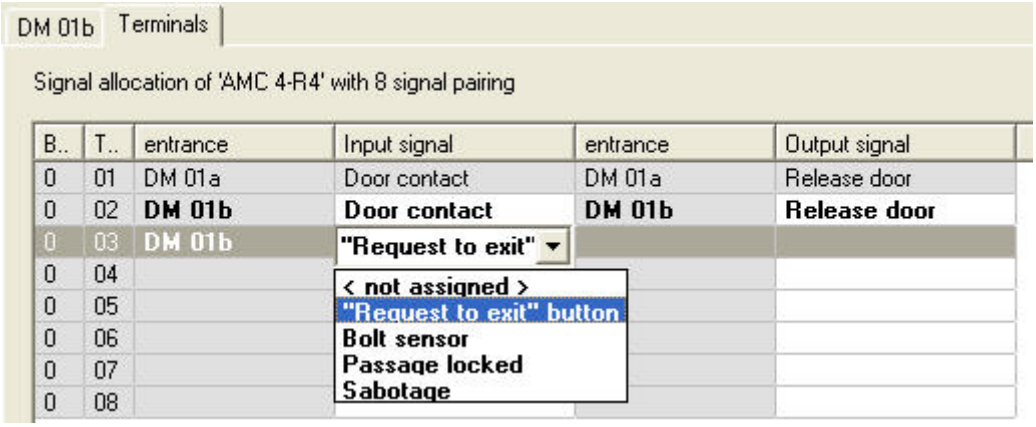
Location (Konum)	Herhangi bir tanımlanmış alan (otopark yok)	Okuyucunun bulunduğu adlandırılmış alan (sistemde tanımlandığı gibi). Bu bilgi giriş sırası kontrolü için kullanılır: Bir kişi bu okuyucuyu kullanmaya çalışırsa ancak o kişinin o anki konumu (sistem tarafından izlendiği gibi) okuyucununkinden farklıysa okuyucu kişinin girişini reddeder.
Destination (Hedef)	Herhangi bir tanımlanmış alan (otopark yok)	Okuyucunun girişe izin verdiği sistemde tanımlandığı gibi adlandırılmış alan. Bu bilgi giriş sırası kontrolü için kullanılır: Bir kişi bu okuyucuyu kullanırsa konumu **Destination** (Hedef) değeriyle güncellenir.
Waiting time external access decision (Bekleme süresi harici giriş kararı)	Saniyenin onda biri değerinde birim sayısı	Bir kartlı geçiş kontrol cihazının girişlerine bağlı harici bir sistemden veya cihazdan alacağı bir kararı beklediği süre.
Division (Bölüm)	Okuyucunun ait olduğu bölüm. Varsayılan değer **Common**'dır (Ortak)	Yalnızca **Divisions** (Bölümler) özelliği lisanslandığında geçerlidir.
Arming Area (Kurma Alanı) (sadece giriş modeli 14 için)	Bir harf: A'dan Z'ye kadar	Bir IDS grubunun girişleri, alanın okuyucularının etkinleştirilmesiyle birlikte aktif hale getirilir.

16.3 AMC terminallerini yapılandırma

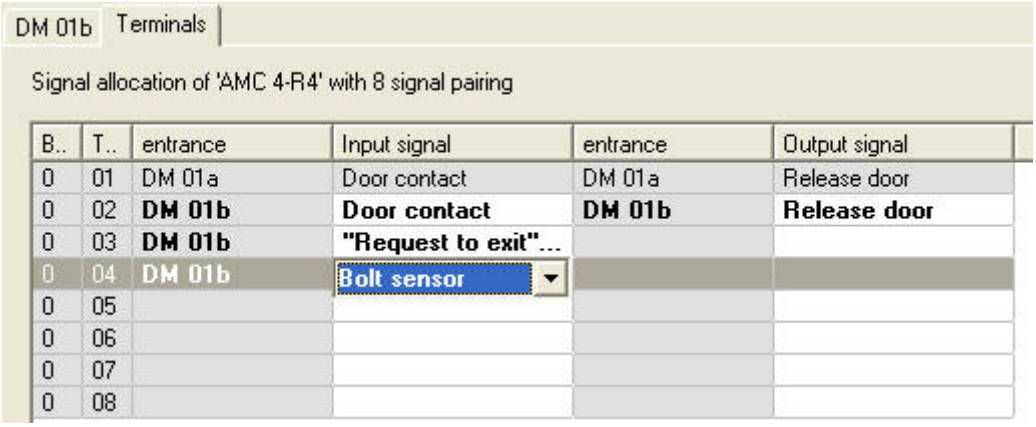
İçeriğinde ve yapısında, bu sekme AMC **Terminals** (Terminaller) sekmesiyle aynıdır.



Bununla birlikte, burada seçilen giriş modeli için sinyal atamasında değişiklik yapmak mümkündür. **Output signal** (Çıkış sinyali) veya **Input signal** (Giriş sinyali) sütunlarına çift tıklandığında birleşik kutular açılır.



Benzer şekilde ilgili giriş için ek sinyaller oluşturmak mümkündür. Boş bir satıra çift tıklandığında, ilgili birleşik kutu açılır:

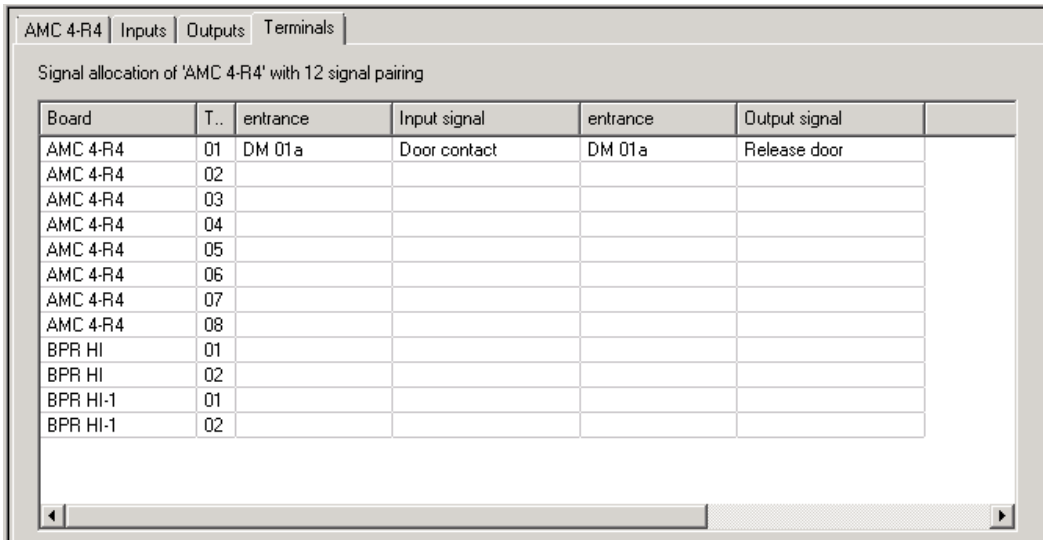


Düzenlemekte olduğunuz giriş için uygun olmayan sinyal atamaları gri bir arka planla salt okunurdur. Bunlar sadece ilgili giriş seçildiğinde düzenlenebilir.
AMC'nin **Outputs** (Çıkışlar) sekmesinde parametreleri belirtilen bu çıkışlara benzer bir arka plan ve soluk bir ön plan rengi verilir.

Uyarı!
Birleşik kutular %100 bağlama duyarlı değildir, bu nedenle gerçek hayatta çalışmayacak sinyalleri seçmek mümkündür. **Terminals** (Terminaller) sekmesinde sinyal ekleyip çıkarırsanız, bunları mantıksal ve fiziksel olarak girişle uyumlu olduklarından emin olmak için test edin.

Terminal Atama
Her AMC ve her giriş için bir **Terminal** sekmesi, 8 ayrı satırda AMC'ye ait 8 sinyalin tümünü gösterir. Kullanılmayan sinyaller beyaz, kullanılmış olanlar ise mavi renkte işaretlenmiştir. Liste aşağıdaki yapıya sahiptir:

- **Board** (Kart): AMC Wiegand Uzantısı (0) veya G/Ç genişletme kartının numaralandırılması (1-3)
- **Terminal**: AMC'deki (01-08) veya Wiegand genişletme kartındaki (09-16) kontak sayısı.
- **Entrance** (Giriş): Girişin adı
- **Output signal** (Çıkış sinyali): Çıkış sinyalinin adı
- **Entrance** (Giriş): Girişin adı
- **Input signal** (Giriş sinyali): Giriş sinyalinin adı



–

Sinyal atamasını değiştirme

Kontrol cihazlarının terminal sekmelerinde, ayrı sinyallerin atanması sadece görüntülenir (salt okunurdur). Bununla birlikte, ilgili girişlerin terminal sekmelerinde, seçilen girişlerin sinyallerini değiştirmek ya da yeniden konumlandırmak mümkündür.

Output signal (Çıkış sinyali) veya **Input signal** (Giriş sinyali) sütunundaki değiştirilecek girişe çift tıklandığında, bir açılır liste etkinleştirilir, böylece giriş modeli için sinyal olarak farklı bir değer seçilebilir. **Not Assigned**'ı (Atanmadı) seçerseniz sinyal serbest bırakılır ve diğer girişler için kullanılabilir.

Böylece yalnızca sinyalleri değiştirememekle kalmaz, aynı zamanda mevcut gerilimin kullanımını optimize etmek için diğer kontaklara da sinyal atayabilirsiniz. Herhangi bir serbest veya serbest bırakılmış kontak daha sonra yeni sinyaller için veya mevcut sinyaller için yeni konumlar olarak kullanılabilir.

Uyarı!

İlke olarak tüm giriş ve çıkış sinyalleri serbestçe seçilebilir, ancak tüm seçimler tüm kapı modelleri için mantıklı değildir. Örneğin, IDS sinyallerini IDS'yi desteklemeyen bir kapı modeline (ör. 01 veya 03) atamak mantıklı değildir. Daha fazla bilgi için Kapı Modellerine Sinyal Atama bölümündeki tabloya bakın.

Kapı modellerine sinyal atama

Sinyalleri kapı modellerine atamak için kullanılan açılır menülerde yanlış parametrelendirmeyi önlemek için, menüler yalnızca seçilen kapı modeliyle uyumlu olan sinyalleri sunar.

Giriş sinyalleri tablosu

Giriş Sinyalleri	Açıklama
Door contact (Kapı kontağı)	
"Çıkış talebi" düğmesi	Kapıyı açma düğmesi.
Cıvata sensörü	Yalnızca mesajlar için kullanılır. Kontrol işlevi yoktur.

Giriş kilitlendi	Karşıt kapıyı geçitlerde geçici olarak kilitlemek için kullanılır. Ancak aynı zamanda uzun süreli kilitleme için de kullanılabilir.
Dış Müdahale	Harici bir denetleyicinin dış müdahale sinyali.
Turnike normal konumda	Turnike kapalı.
Geçiş tamamlandı	Bir geçiş başarıyla tamamlandı. Bu, harici bir denetleyicinin darbesidir.
IDS: Kurulmaya hazır	Tüm dedektörler beklemedeyse ve IDS kurulabiliyorsa IDS tarafından ayarlanır.
IDS: Kuruldu	IDS kurulmuştur.
IDS: Kurma talebi düğmesi	IDS'yi kurma düğmesi.
Yetkisiz açılma sebebiyle alarmı bastırma	Bir kapı boşluğu düzeni AMC'yi dahil etmeden kapıyı açarsa kullanılır. AMC, hırsız alarmı mesajı göndermiyor, ancak "kapı yerel olarak açık".
Harici giriş kararı kabul edildi	Harici bir sistem girişi kabul ediyorsa sinyal ayarlanır
External access decision denied (Harici giriş kararı reddedildi)	Harici bir sistem girişi kabul reddederse sinyal ayarlanır

Çıkış sinyalleri tablosu

Çıkış Sinyalleri	**Açıklama**
Release door (Kapıyı serbest bırak)	
Geçit: Ters yönü kilitle	Tuzağın diğer tarafını kilitler. Bu sinyal, kapı açıldığında gönderilir.
Alarm bastırma	...IDS'ye. IDS'nin bir hırsız alarmı mesajı oluşturmasını önlemek için kapı açık olduğu sürece ayarlanır.
Stoplight green (Yeşil ışık)	Gösterge lambası: Kapı açık olduğu sürece kontrol edilir.
Max. door open time elapsed (Kapının maksimum açık kalma süresi geçti) veya Door security compromised (Kapı güvenliği tehlikeye girdi)	Kapı açık tutuluyorsa veya çok uzun süredir açıksa
Camera connecting (Kamera bağlanıyor)	Kamera, bir geçişin başında etkinleştirilir.

Release turnstile inbound (Turnike gelişini serbest bırak)	
Release turnstile outbound (Turnike çıkışını serbest bırak)	
Door is unlocked (Kapının kilidi açıldı)	Bir kapının kilidini uzun bir süreyle açma sinyali.
IDS: Kurma	IDS'yi kurma sinyali.
IDS: Devre dışı bırakma	IDS'yi devre dışı bırakma sinyali.
Harici giriş kararı etkin	Sinyal, harici kartlı geçiş sistemini etkinleştirmek için ayarlanmalıdır

Kapı modellerini giriş ve çıkış sinyallerine eşleme tablosu

Aşağıdaki tabloda anlamlı sinyal ve kapı modelleri atamaları gösterilmektedir.

Kapı Modeli	**Açıklama**	**Giriş Sinyalleri**	**Çıkış Sinyalleri**
01	Giriş ve çıkış okuyuculu basit kapı Zaman ve devam okuyucuları Harici giriş kararı mevcut	- Door contact (Kapı kontağı) - "Çıkış talebi" düğmesi - Cıvata sensörü - Giriş kilitlendi - Dış Müdahale - Yerel açma etkin - Harici giriş kararı kabul edildi - External access decision denied (Harici giriş kararı reddedildi)	- Release door (Kapıyı serbest bırak) - Geçit: ters yönü kilitle - Alarm bastırma - Stoplight green (Yeşil ışık) - Camera connecting (Kamera bağlanıyor) - Max. door open time elapsed (Kapının maksimum açık kalma süresi geçti) veya Door security compromised (Kapı güvenliği tehlikeye girdi) - Harici giriş kararı etkin
03	Giriş ve çıkış okuyuculu döner kapı Zaman ve devam okuyucuları Harici giriş kararı mevcut	- Turnike bekleme konumunda - "Çıkış talebi" düğmesi - Giriş kilitlendi - Dış Müdahale - Harici giriş kararı kabul edildi - External access decision denied (Harici giriş kararı reddedildi)	- Geçit: ters yönü kilitle - Release turnstile inbound (Turnike gelişini serbest bırak) - Release turnstile outbound (Turnike çıkışını serbest bırak) - Alarm bastırma - Camera connecting (Kamera bağlanıyor) - Max. door open time elapsed (Kapının maksimum açık kalma

			süresi geçti) veya - Door security compromised (Kapı güvenliği tehlikeye girdi) - Harici giriş kararı etkin
05	Otopark girişi veya çıkışı - maksimum 24 park bölgesi Zaman ve devam okuyucuları Harici giriş kararı mevcut	- Door contact (Kapı kontağı) - "Çıkış talebi" düğmesi - Giriş kilitlendi - Geçiş tamamlandı - Harici giriş kararı kabul edildi - External access decision denied (Harici giriş kararı reddedildi)	- Release door (Kapıyı serbest bırak) - Alarm bastırma - Stoplight green (Yeşil ışık) - Max. door open time elapsed (Kapının maksimum açık kalma süresi geçti) veya - Door security compromised (Kapı güvenliği tehlikeye girdi) - Door is unlocked (Kapının kilidi açıldı) - Harici giriş kararı etkin
06	Zaman ve devam okuyucuları		
07	Asansör - maksimum 56 kat		
09	Araç girişi veya giden okuyucu ve basmalı düğme Zaman ve devam okuyucuları Harici giriş kararı mevcut	- Door contact (Kapı kontağı) - "Çıkış talebi" düğmesi - Giriş kilitlendi - Geçiş tamamlandı - Harici giriş kararı kabul edildi - External access decision denied (Harici giriş kararı reddedildi)	- Release door (Kapıyı serbest bırak) - Alarm bastırma - Stoplight green (Yeşil ışık) - Max. door open time elapsed (Kapının maksimum açık kalma süresi geçti) veya - Door security compromised (Kapı güvenliği tehlikeye girdi) - Door is unlocked (Kapının kilidi açıldı) - Harici giriş kararı etkin
10	Giriş ve çıkış okuyucusu ile IDS kurma/devre dışı bırakma özelliğine sahip basit kapı Zaman ve devam okuyucuları	- Door contact (Kapı kontağı) - "Çıkış talebi" düğmesi - IDS: Kurulmaya hazır - IDS: Kuruldu - Dış Müdahale - IDS: Kurma isteği - Harici giriş kararı kabul edildi	- Release door (Kapıyı serbest bırak) - Camera connecting (Kamera bağlanıyor) - IDS: Kurma - IDS: Devre dışı bırakma

	Harici giriş kararı mevcut	- External access decision denied (Harici giriş kararı reddedildi)	- Max. door open time elapsed (Kapının maksimum açık kalma süresi geçti) veya - Door security compromised (Kapı güvenliği tehlikeye girdi) - Harici giriş kararı etkin
14	Giriş ve çıkış okuyucusu ile IDS kurma/devre dışı bırakma özelliğine sahip basit kapı Zaman ve devam okuyucuları	- Door contact (Kapı kontağı) - "Çıkış talebi" düğmesi - IDS: Kurulmaya hazır - IDS: Kuruldu - Dış Müdahale - IDS: Kurma isteği	- Release door (Kapıyı serbest bırak) - Camera connecting (Kamera bağlanıyor) - IDS: Kurma - Max. door open time elapsed (Kapının maksimum açık kalma süresi geçti) veya - Door security compromised (Kapı güvenliği tehlikeye girdi)
15	Dijital kontaklar		

Okuyuculara sinyal atama

Seri okuyucular (yani bir AMC2 4R4'teki okuyucular) ve OSDP okuyucuları yerel G/Ç sinyalleri ile geliştirilebilir. Bu şekilde ek sinyaller kullanılabilir hale getirilebilir ve kapı kontaklarına giden elektrik yolları kısalır.

Bir seri okuyucu oluşturulduğunda, ilgili girişin **Terminals** (Terminaller) sekmesi, kontrol cihazının ve genişletme kartı (varsa) sinyallerinin altındaki her okuyucu için iki giriş ile iki çıkış sinyali gösterir.

Uyarı!

Bu liste girişleri, yerel G/Ç'leri olup olmadığına bakılmaksızın her seri okuyucu için oluşturulur.

Bu okuyucu yerel sinyalleri, işlevlere atanamaz ve parametreleri kontrol cihazları ve kartlarınki gibi belirlenemez. Bunlar **Input signal** (Giriş sinyali) ve **Output signal** (Çıkış sinyali) sekmelerinde görünmez ya da asansörler (örneğin 56 kat sınırını aşmak için) için kullanılamaz. Bu nedenle, kapıların doğrudan kontrolü için en uygun (ör. kapı kilidi karşılığı veya serbest bırakma) sinyallerdir. Ancak bu, daha karmaşık parametreli işlevler için kontrol cihazının sinyallerini serbest bırakır.

Sinyalleri düzenleme

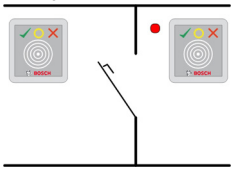
Bir giriş oluşturulduğunda, ilgili girişin **Terminals** (Terminaller) sekmesi, kontrol cihazının altındaki her okuyucu için iki giriş ve iki çıkış sinyali gösterir. Board (Kart) sütunu, okuyucunun adını görüntüler. Giriş için standart sinyaller, varsayılan olarak kontrol cihazındaki ilk serbest sinyallere atanır. Bunları okuyucunun kendi sinyallerine taşımak için öncelikle başlangıçtaki konumlarından silinmeleri gerekir. Bunu yapmak için **<Not assigned>** (Atanmadı) liste girişini seçin

Seçilen kapı modeli için olası sinyallerin bir listesini görmek ve böylece sinyali yeniden konumlandırmak için okuyucunun **Input signal** (Giriş sinyali) veya **Output signal** (Çıkış sinyali) sütununa çift tıklayın. Tüm sinyaller gibi bunlar da kontrol cihazının **Terminals** (Terminaller) sekmesinde görüntülenebilir, ancak burada düzenlenmez.

Uyarı!
Okuyucu sinyallerinin durumu izlenemez.
Bunlar sadece okuyucunun ait olduğu kapı için kullanılabilir.

16.4 Kapı modelleri için önceden tanımlanan sinyaller

Giriş Modeli 01



Model çeşitleri:

01a	Giriş **ve** çıkış okuyuculu normal kapı
01b	Giriş okuyuculu ve basmalı düğmeli normal kapı
01c	Giriş **veya** çıkış okuyuculu normal kapı

Olası sinyaller:

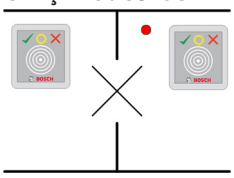
Giriş sinyalleri	**Çıkış sinyalleri**
Door contact (Kapı kontağı)	Release door (Kapıyı serbest bırak)
"Çıkış talebi" düğmesi	Geçit: Ters yönü kilitle
Dış Müdahale	Stoplight green (Yeşil ışık)
Yetkisiz açılma sebebiyle alarmı bastırma	Camera connecting (Kamera bağlanıyor)
	Max. door open time elapsed (Kapının maksimum açık kalma süresi geçti) veya Door security compromised (Kapı güvenliği tehlikeye girdi)

Uyarı!
Özellikle karşı taraftaki kilit olmak üzere tekleme işlevleri sadece DM 03 ile parametrelendirilebilir.

Alarm bastırma sadece kapı açılmadan önce alarm bastırma süresi 0'dan büyük olduğunda etkinleştirilir.

Bu giriş modeli, araç girişleri için de avantajlı olabilir; bu durumda kamyonlar ve arabalar için ikinci bir okuyucu da tavsiye edilir.

Giriş Modeli 03



Model çeşitleri:

03a	Giriş **ve** çıkış okuyuculu ters çevrilebilir turnike
03b	Giriş okuyuculu ve basmalı düğmeli ters çevrilebilir turnike
03c	Giriş **veya**çıkış okuyuculu turnike

Olası sinyaller:

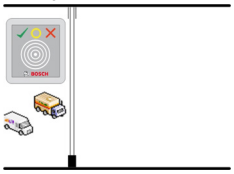
Giriş sinyali	**Çıkış sinyalleri**
Turnike normal konumda	Release turnstile inbound (Turnike gelişini serbest bırak)
"Çıkış talebi" düğmesi	Release turnstile outbound (Turnike çıkışını serbest bırak)
Dış Müdahale	Giriş kilitlendi
Yetkisiz açılma sebebiyle alarmı bastırma	Camera connecting (Kamera bağlanıyor)
	Max. door open time elapsed (Kapının maksimum açık kalma süresi geçti) veya Door security compromised (Kapı güvenliği tehlikeye girdi)
Mantrap (Tuzak) seçeneği kullanılan ek sinyaller:	
Giriş kilitlendi	Geçit: Ters yönü kilitle
	Alarm bastırma

Tuzaklara ilişkin yapılandırma notları:
Turnike normal konumdayken, bağlı olan tüm okuyucuların ilk giriş sinyali açılır. Bir kart gösterilir ve sahibin bu giriş için giriş hakları varsa:

- Giriş okuyucusunda ilk çıkış sinyali, etkinleştirme süresi boyunca giriş okuyucusunda ayarlanır.
- Çıkış okuyucusunda ikinci çıkış sinyali etkinleştirme süresi boyunca çıkış okuyucusuna ayarlanır.

Çıkış Talebi (REX) düğmesine basıldığında, ikinci giriş sinyali ve ikinci çıkış sinyali ayarlanır. Bu süre zarfında döner kapı etkin yönde kullanılabilir.

Giriş Modeli 05c



Model çeşidi:

05c	Otopark girişi çıkış **veya** giriş okuyucusu

Bu giriş modeli için olası sinyaller:

Giriş sinyalleri	**Çıkış sinyalleri**
Door contact (Kapı kontağı)	Release door (Kapıyı serbest bırak)
"Çıkış talebi" düğmesi	Door is unlocked (Kapının kilidi açıldı)
Giriş kilitlendi	Stoplight green (Yeşil ışık)
Geçiş tamamlandı	Alarm bastırma
	Max. door open time elapsed (Kapının maksimum açık kalma süresi geçti) veya Door security compromised (Kapı güvenliği tehlikeye girdi)

Otoparkın hem girişi hem de çıkışı aynı kontrol cihazında yapılandırılmalıdır. Otopark girişi bir kontrol cihazına atanmışsa söz konusu kontrol cihazı başka kapı modellerini düzenleyemez. Otoparka giriş için sadece bir giriş okuyucusu (çıkış okuyucusu yok) atanabilir. Giriş atandıktan sonra kapı modelini tekrar seçmek sadece çıkış okuyucusunu tanımlamanızı sağlar. Kartın çalışabilmesi için kartın yetkilerinde yer alması gereken her park yerine 24 adede kadar alt alan tanımlayabilirsiniz.

Giriş Modeli 06

Model çeşitleri

06a	Zaman ve devam için giriş **ve** çıkış okuyucusu
06c	Zaman ve devam için giriş **veya** çıkış okuyucusu

Bu kapı modeliyle oluşturulan okuyucular kapı ve engelleri kontrol etmez, ancak kart verilerini bir zaman ve devamlılık sistemine iletir. Bu okuyucular genellikle erişimin zaten kontrollü olduğu yerlerde bulunur.
Bu nedenle hiçbir sinyal tanımlanmaz.

Uyarı!
Geçerli ayırma çiftlerinin (giriş zamanı artı çıkış süresi) zaman ve devam sisteminde oluşturulabilmesi için, kapı modeli 06 olan iki ayrı okuyucuyu parametrelendirmek gerekir: Biri gelen, biri giden saati için

Giriş ve çıkış ayrı olmadığında **a** çeşidini kullanın. Giriş ve çıkış uzamsal olarak ayrıysa veya okuyucuları aynı kontrol cihazına takamıyorsanız **c** çeşidini kullanın. Okuyucudan birini gelen okuyucusu, birini ise giden okuyucusu olarak tanımladığınızdan emin olun.
Her girişte olduğu gibi, yetkiler oluşturmak ve atamak gereklidir. **Access Authorizations** (Giriş Yetkileri) ve **Area/Time Authorizations** (Alan/Zaman Yetkileri) iletişim kutularındaki **Time Management** sekmesi tanımlanan tüm saat ve devam okuyucularını gösterir. Gelen yönde en az bir okuyucuyu ve giden yönde bir okuyucuyu etkinleştirin. Zaman ve devam okuyucular için yetkiler, diğer giriş yetkileriyle birlikte veya ayrı yetkiler olarak atanabilir. Belirli bir yön için birden fazla zaman ve devam okuyucusu varsa belirli kart sahiplerini belirli okuyuculara atamak mümkündür. Sadece atanmış ve yetkili kullanıcıların devam süreleri okuyucu tarafından kaydedilip saklanır.

Uyarı!
Diğer kartlı geçiş özellikleri de zaman ve devam okuyucularının davranışını etkiler. Bu nedenle, kara listeler, zaman modelleri veya son kullanma tarihleri, bir zaman ve devam okuyucusunun giriş zamanlarını kaydetmesini engelleyebilir.

Kayıtlı giriş ve çıkış saatleri `<SW_installation_folder>\AccessEngine\AC\TAExchange\` dizininde `TAccExc_EXP.tx`t adı altında bir metin dosyasında saklanır ve bir zaman ve devam sistemine dışa aktarma bekler durumda tutulur.
Rezervasyon verileri şu biçimde iletilir:
`ddMMyyyy;hhmm[s];Direction [0,1]; AbsenceReason; Personnel-Nr.`
d=gün, M=ay, y=yıl, s=saat, m=dakika, s=yaz saati (gün ışığından yararlanma), 0=giden, 1=gelen
Dışa aktarma dosyası tüm ayırma işlemlerini kronolojik sırada içerir. Dosyanın içindeki alan ayracı noktalı virgüldür.

Giriş Modeli 07 çeşitleri

Model çeşitleri:

07a	Maks. 56 katlı asansör
07c	Maks. 56 kata sahip asansör ve zaman modeli

Giriş Modeli 07a
Sinyaller:

Giriş sinyali	Çıkış sinyalleri
	<Katın adı> adlı katı serbest bırakma
	Tanımlanan kat başına maksimum 56 adet olmak üzere bir çıkış sinyali.

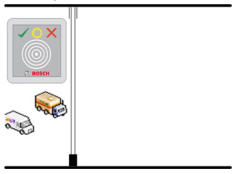
Asansörü çağırdıktan sonra kart sahibi sadece kartının yetkilendirildiği katları seçebilir. Asansör kapısı modelleri aynı kontrol cihazındaki diğer kapı modelleriyle birlikte kullanılamaz. AMC'deki her asansör için 56 kata kadar genişletme kartları kullanımı tanımlanabilir. Kartın yetkileri asansörün kendisini ve en az bir katını içermelidir.

Giriş Modeli 07c
Sinyaller:

Giriş Sinyali	Çıkış Sinyali
Giriş tuşu <katın adı>	<Katın adı> adlı katı serbest bırakma
Her tanımlanan kat için bir çıkış ve giriş vardır: 56'ya kadar.	

Asansörü çağırıp bir kat seçici düğmesine bastıktan sonra (bu yüzden giriş sinyallerine ihtiyaç duyulur) kartın yetkileri, seçilen katın dahil olup olmadığını anlamak üzere kontrol edilir.
Ayrıca bu kapı modeli ile **genel giriş** olarak görev yapan tüm katları tanımlamak mümkündür, yani bu kat için herhangi bir yetki kontrolü yapılmaz ve herhangi bir kişi asansörle bu kata gidebilir. Bununla birlikte, genel girişin kendisi, bunu günün belirli saatleriyle sınırlayan bir **zaman modeli** ile düzenlenebilir. Bu saatler dışında yetki kontrolleri her zamanki gibi yapılır.
Asansör kapısı modelleri aynı kontrol cihazındaki diğer kapı modelleriyle birlikte kullanılamaz. AMC'deki her asansör için 56 kata kadar genişletme kartları kullanımı tanımlanabilir. Kartın yetkileri asansörün kendisini ve en az bir katını içermelidir.

Giriş Modeli 09

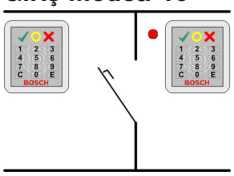


Olası sinyaller:

Giriş sinyalleri	Çıkış sinyalleri
Door contact (Kapı kontağı)	Release door (Kapıyı serbest bırak)
"Çıkış talebi" düğmesi	Kapı uzun süredir açık
Giriş kilitlendi	Trafik ışığı yeşil
Geçiş tamamlandı	Alarm bastırma
	Max. door open time elapsed (Kapının maksimum açık kalma süresi geçti) veya Door security compromised (Kapı güvenliği tehlikeye girdi)

Bariyer kontrolü için altta yatan bir kontrol (SPS) varsayılır. **Kapı modeli 5c**'nin aksine, bu girişi yapılandırabilir ve farklı AMC'lerden çıkabilirsiniz. Üstelik herhangi bir alt bölge yoktur, ancak park alanı için sadece genel bir yetki vardır.

Giriş Modeli 10



Model çeşitleri:

10a	Giriş **ve** çıkış okuyucusu **ile** IDS (hırsız algılama sistemi) kurma/devre dışı bırakma özelliğine sahip normal kapı
10b	Giriş, REX (çıkış talebi) düğmesi ve IDS kurma/devre dışı bırakma özelliğine sahip normal kapı
10e	Giriş, REX düğmesi ve merkezi olmayan IDS kurma/devre dışı bırakma özelliğine sahip normal kapı

Olası sinyaller:

Giriş sinyalleri	**Çıkış sinyalleri**
Door contact (Kapı kontağı)	Release door (Kapıyı serbest bırak)
IDS: Kuruldu	IDS: Kurma
IDS: Kurulmaya hazır	IDS: Devre dışı bırakma [sadece DM 10e]
"Çıkış talebi" düğmesi	Camera connecting (Kamera bağlanıyor)
Cıvata sensörü	Max. door open time elapsed (Kapının maksimum açık kalma süresi geçti) veya Door security compromised (Kapı güvenliği tehlikeye girdi)
Dış Müdahale	
Yetkisiz açılma sebebiyle alarmı bastırma	
IDS: Kurma talebi düğmesi	

Uyarı!
Bu kapı modeli için tuş takımı okuyucuları gereklidir. Kart sahiplerinin IDS'yi kurmaları/devre dışı bırakmaları için **PIN kodları** gereklidir.

Hangi okuyucuların kurulu olduğuna bağlı olarak farklı prosedürler gereklidir.

Seri okuyucular (I-BPR, HADP ve OSDP dahil)
7 tuşuna basıp Enter (#) ile onaylayarak kurun. Ardından kartı gösterin, PIN kodunu girin ve tekrar Enter (#) tuşu ile onaylayın.
Kartı gösterip PIN kodunu girerek ve Enter (#) ile onaylayarak devre dışı bırakın.

Wiegand okuyucular (seri BPR protokolü dahil)
7'ye basıp kartı göstererek ve PIN kodunu girerek kurun. Enter tuşunu kullanarak onaylamaya gerek yoktur.

Kartı gösterip PIN kodunu girerek devre dışı bırakın. Devre dışı bırakma ve kapı açma aynı anda gerçekleşir.

DM 10e'nin özel özellikleri:
Kapı modelleri 10a ve 10b ile her giriş kendi güvenlik alanı olduğu halde, 10e ile birden çok giriş birimler halinde gruplandırılabilir. Bu gruptaki herhangi bir okuyucu birimin tamamını kurma veya devre dışı bırakma özelliğine sahiptir. Durumu gruptaki okuyucuların herhangi biriyle sıfırlamak için bir **Disarm IDS** (IDS'yi devre dışı bırak) çıkış sinyali gereklidir.
Sinyaller:
- Kapı modelleri 10a ve 10b:
  - - Kurma, sabit bir sinyalle tetiklenir
  - - Devre dışı bırakma, sabit sinyalin kesilmesiyle tetiklenir.
- Kapı modeli 10e:
  - - Kurma ve devre dışı bırakma, 1 saniye süreli bir sinyal darbesiyle tetiklenir.

[İki durumlu bir röle kullanarak IDS'yi birden çok kapıdan kontrol etmek mümkündür. Bunu yapmak üzere tüm kapıların sinyalleri için rölede bir VEYA çalışması gereklidir. **IDS armed** (IDS kurulu) ve **IDS ready to arm** (IDS kurulmaya hazır) sinyalleri katılan tüm kapılarda çoğaltılmalıdır.]

Özel girişler
Aşağıdakiler gibi özel özelliklere sahip giriş modelleri için:
- Asansörler
- Hırsız algılama
- Genel dijital veya ikili anahtarlar
- Tuzaklar

Özel girişlere ayrılmış bölüme bakın.

Bkz.
- *Özel girişler, sayfa 91*

16.5 Özel girişler

16.5.1 Asansörler (DM07)

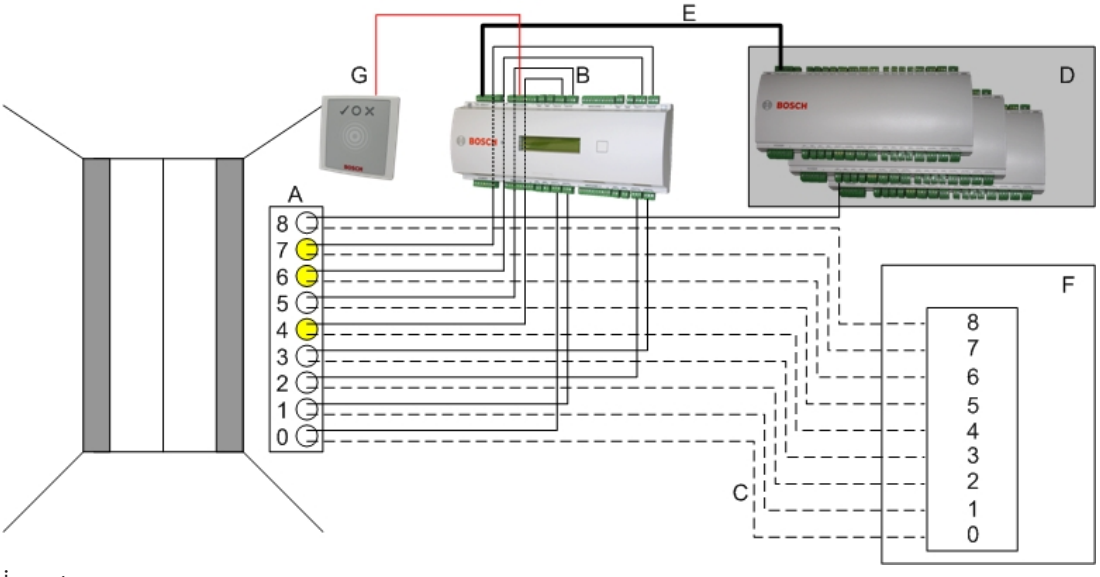
Asansörlerle ilgili genel notlar (Giriş Modeli 07)
Asansörler aynı AMC kontrol cihazındaki diğer kapı modelleriyle birleştirilemez.
Asansörler **Group access** (Grup girişi) veya **Attendant required** (Eşlik eden gerekli) okuyucu seçenekleriyle kullanılamaz.
Bir AMC'de en fazla 8 kat tanımlanabilir. Bir AMC genişletme kartı, genişletme kartı başına 8 veya 16 ek çıkış sunar.
Bu nedenle, en büyük genişletme kartlarından maksimum sayıda kullanarak RS485 okuyucular ile en fazla 56 katı, ek olarak özel bir Wiegand genişletme kartı kullanıldıysa Wiegand okuyucular ile 64 katı yapılandırmak mümkündür.

Giriş modelleri 07a ve 07c arasındaki farklar
Kartlı geçiş yetkilendirme iletişim kutularında, bir kişinin yetkisine belirli katları atayabilirsiniz.
Asansör **07a** giriş modeli kullanılarak oluşturulduysa bir kart sahibi kimlik kartını gösterir ve izin aldığı katlar kullanılabilir hale gelir.

Sistem, **07c** giriş modeliyle kişi bunu seçtikten sonra seçilen kat için yetkiyi kontrol eder. İşaretlenen **genel** katlar yetkiden bağımsız olarak her kişi tarafından kullanılabilir. Bir zaman modeli ile birlikte, genel işlev belirtilen zaman modeliyle sınırlandırılabilir. Bu süre dışında seçilen kat için yetki kontrol edilir.

Asansörler için kablolama şeması:

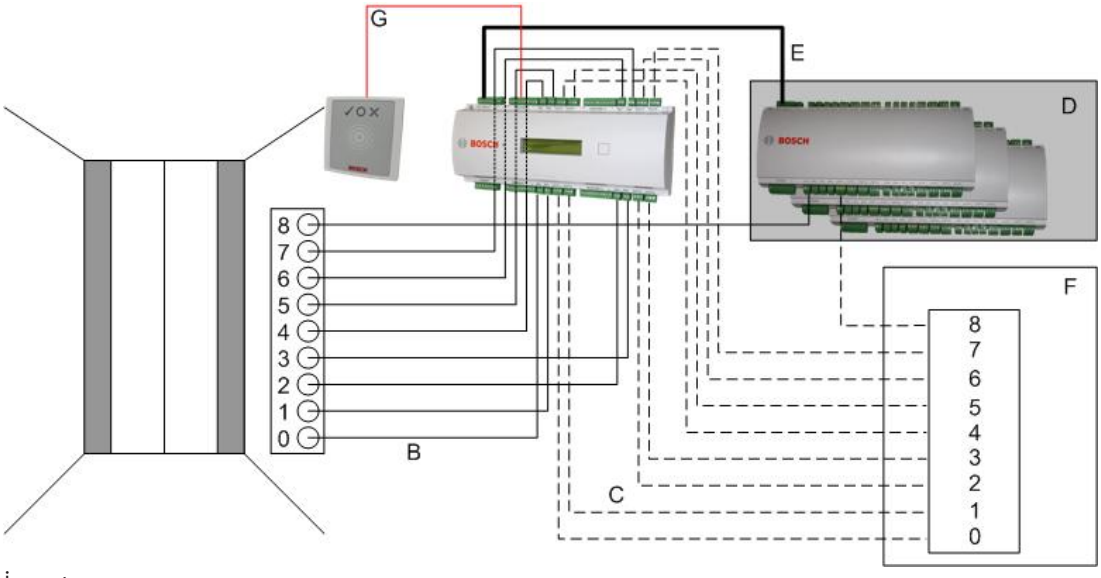
Aşağıdaki görüntüde, 07a kapı modeli kullanılan bir asansörün bağlantı şeması gösterilmektedir.



İşaret:

- A = Asansörün anahtar kartı
- B = (düz çizgi) AMC-Çıkış sinyalleri
- C = (kesik çizgi) Asansör kontrollerine bağlantı
- D = Kendi sekiz girişi ve çıkışı yeterli değilse bir AMC'ye en fazla üç G/Ç Kartı bağlanabilir.
- E = AMC'den G/Ç Kartlarına Veri ve Güç beslemesi
- F = Asansörün yer seçicisi
- G = Okuyucu. Her asansör için iki okuyucu yapılandırılabilir.

Aşağıdaki görüntüde, 07c kapı modeli kullanılan bir asansörün bağlantı şeması gösterilmektedir.

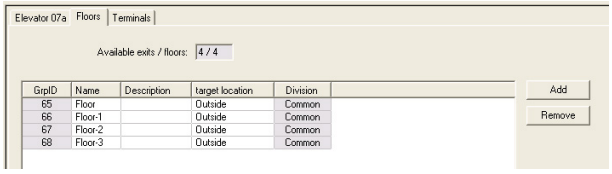


İşaret:

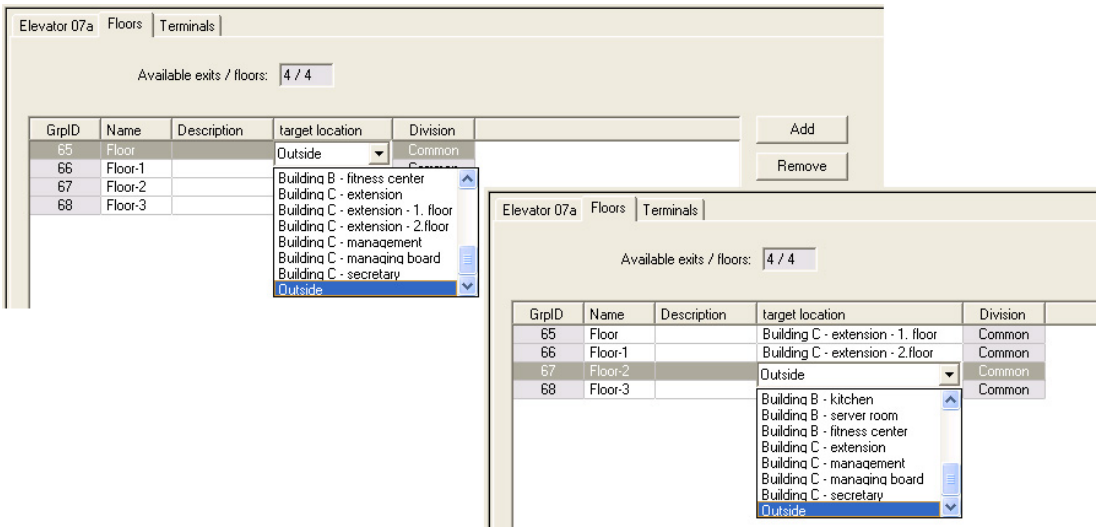
- B = (düz çizgi) AMC-Çıkış sinyalleri
- C = (kesik çizgi) Asansör kontrollerine bağlantı
- D = Kendi sekiz girişi ve çıkışı yeterli değilse bir AMC'ye en fazla üç G/Ç Kartı bağlanabilir.
- E = AMC'den G/Ç Kartlarına Veri ve Güç beslemesi
- F = Asansörün yer seçicisi
- G = Okuyucu. Her asansör için iki okuyucu yapılandırılabilir.

Otoparklar gibi asansörlerde de **Genel parametresi bulunur.** Bu parametre her kat için ayrı ayrı ayarlanabilir. **Public** (Genel) parametresi etkinse giriş yetkileri kontrol edilmez, böylece asansördeki herhangi bir kart sahibi katı seçebilir.
İsterseniz, giriş modeli için bir zaman modeli ayarlayın: Tanımlanan saat dilimlerinin dışında yetkiler kontrol edilir.

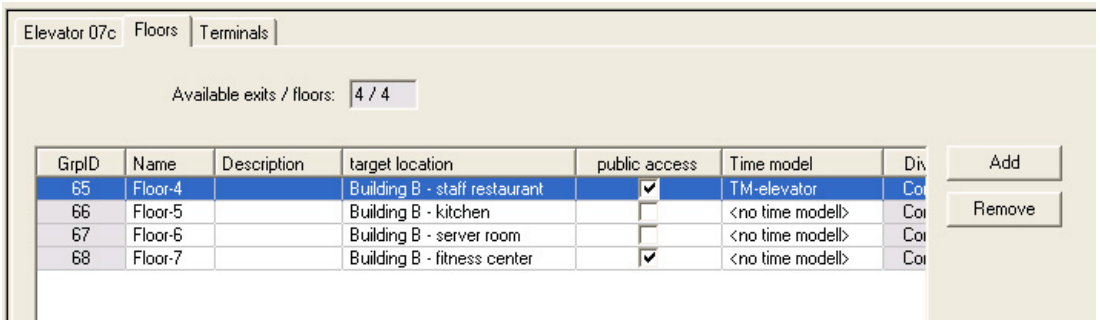
Giriş modeli 07 için katlar
Add (Ekle) ve **Remove** (Kaldır) düğmelerini kullanarak asansör için kat eklemek veya kaldırmak üzere **Floors** (Katlar) sekmesini kullanın.



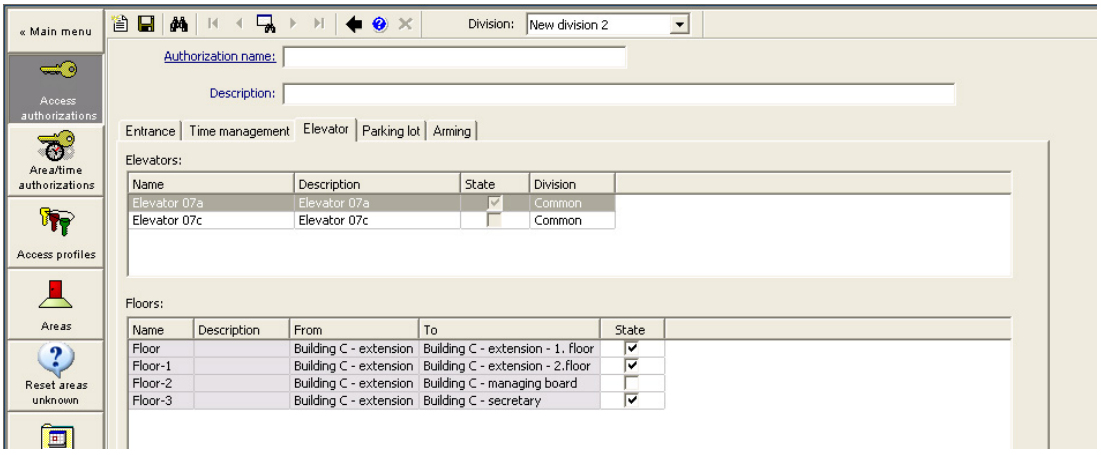
Bir kat için hedef konumları, otoparklar ve park bölgeleri hariç herhangi bir **Area** (Alan) olabilir.
Tek bir kata sadece bir Alan atanabilir. Bu nedenle birleşik kutularda sunulan alanların seçimi her atamadan sonra azalır, böylece istem dışı çift atamalar önlenir.



Giriş modeli 07a kullanılırken **Public access** (Genel giriş) kutusu işaretlenerek tek katları genel girişe açmak mümkündür. Bu durumda yetkilerin kontrolü yapılmaz. Bununla birlikte ek bir **Time model** (Zaman modeli) ataması önceden tanımlanan sürelere erişimi kısıtlar.



Access authorizations (Giriş yetkileri) ve **Area/time authorizations** (Alan/zaman yetkileri) iletişim kutularındaki üst liste kutusunun üstünde yer alan **Elevator** (Asansör) sekmesinde, önce gerekli asansörü ve ardından aşağıdan kart sahibine giriş izni verilen katları seçin.



16.5.2 Hırsız alarmlı kapı modelleri (DM14)

Giriş

Giriş modeli 10'un (DM10) tersine, **DM14** bir hırsız alarm sistemini ya da belirli bir Kurma alanı için IDS'yi kurabilir ve devre dışı bırakabilir. Kart sahibinin gerekli tüm diğer giriş izinlerine sahip olması kaydıyla, bir DM14 girişi de onu devre dışı bırakan kart sahibine giriş izni verecek şekilde yapılandırılabilir.

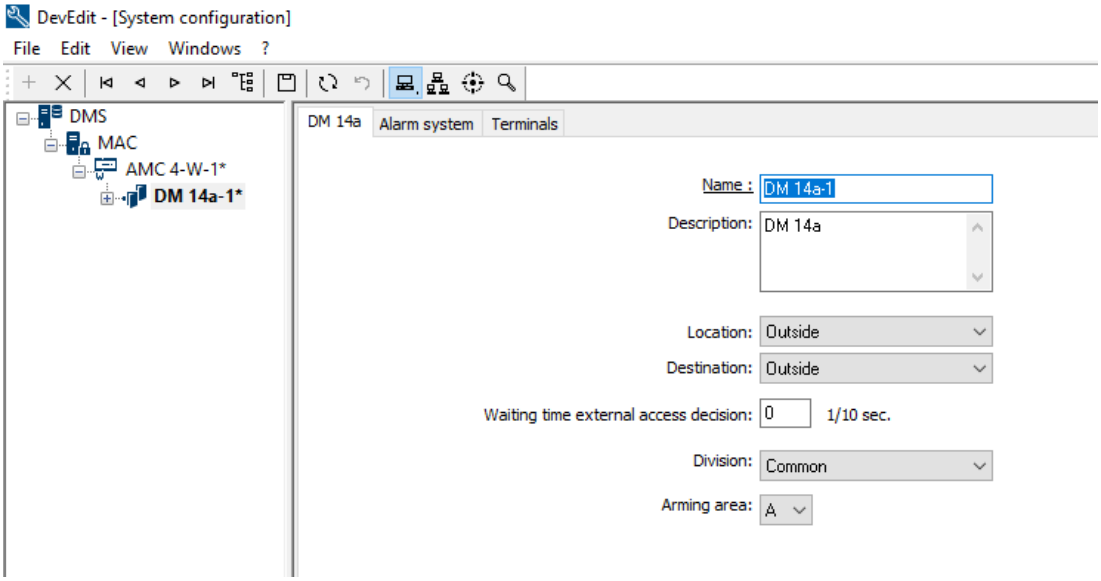
Cihaz düzenleyici ve iletişim yöneticisindeki DM14 yapılandırma prosedürü şu görevleri içerir:

1. Giriş ve kurma alanını tanımlamak için genel parametreleri ayarlama.
2. Alanı devre dışı bırakmak için tam prosedürü ayarlamak için belirli parametreler belirleme.
3. Girişteki kapı kontol cihazının terminallerinde IDS'ye özel giriş ve çıkış sinyallerini tanımlayın.
4. Kurma/devre dışı bırakma izinlerini, DM 14 girişlerini çalıştırmak için söz konusu kart sahiplerinin giriş yetkilerine ekleyin.

Görevler aşağıdaki bölümlerde açıklanmaktadır.

Genel parametreler

İlk sekme olan **DM14a** veya **DM14b**'de aşağıdaki parametreleri ayarlayın.

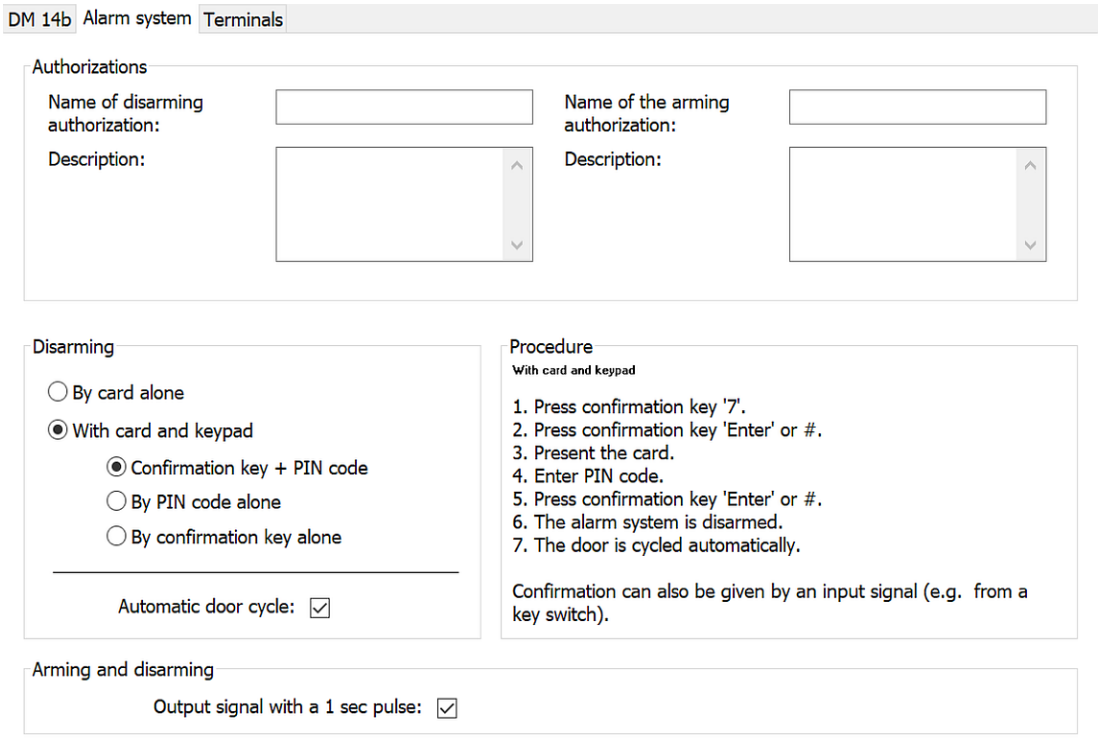


Parametre	Değer tipi	Açıklama
Name (Ad)	Serbest metin	Girişin adı.
Açıklama	Serbest metin, isteğe bağlı	Girişin açıklaması.
Location (Konum)	Kullanılıyorsa tanımlanan alanların listesi	Girişinin bulunduğu giriş alanı.

Parametre	Değer tipi	Açıklama
Destination (Hedef)	Kullanılıyorsa tanımlanan alanların listesi	Girişin ait olduğu giriş alanı.
Division (Bölüm)	Kullanılıyorsa tanımlanan bölümlerin listesi	Girişin ait olduğu kartlı geçiş sistemi içindeki bölüm veya kiracı.
Waiting time external access decision (Bekleme süresi harici giriş kararı)	Saniyenin onda biri	Onun adına giriş kararları vermek için AMC'nin terminallerine harici bir sistem bağladıysanız bu parametre harici sistemden yanıt bekleme süresini sınırlar. Not: Giriş kararı, örneğin giriş yetkileri, zaman modelleri ve bölümler (kullanılıyorsa) gibi kartlı geçiş sisteminde tanımlanan **tüm** koşulların yerine getirilmesini gerektirir. Varsayılan değer 0'dır, yani parametre yok sayılır.
Arming area (Kurma alanı)	Büyük harf listesi A...Z	DM14 girişlerini Kurma alanları olarak gruplandırmak için bir harf.

Alarm sistem parametreleri

İkinci sekme olan **Alarm system** (Alarm sistemi) sekmesinde aşağıdaki parametreleri ayarlayın. Bu parametreler, kimlik bilgilerini ve IDS'yi devre dışı bırakma prosedürünü düzenler ve devre dışı bırakma işlemi ilk sekmede tanımlandığı gibi aynı kurma alanındaki tüm girişleri etkiler.



Parametre	Değer tipi	Açıklama
Yetki bölmesi		
Devre dışı bırakma yetkisinin adı	Serbest metin	Bir kart sahibi bu girişte IDS'yi devreden çıkardığında protokollerde ve raporlarda görünecek ad.
Kurma yetkisi adı	Serbest metin	Bir kart sahibi bu girişte IDS'yi kurduğunda protokollerde ve raporlarda görünecek ad.
Açıklama (her yetki için bir adet)	Serbest metin, isteğe bağlı	Kurma yetkilerinin açıklamaları
Devre dışı bırakma bölmesi		
Yalnızca kart ile	Radyo düğmesi	Başka bir kimlik doğrulama olmadan okuyucuya bir kart gösterilerek IDS'nin devre dışı bırakılmasını sağlamak için bu seçeneği seçin.
Kart ve tuş takımı ile	Radyo düğmesi	IDS'nin okuyucuya kart gösterip okuyucu tuş takımı aracılığıyla fazladan kimlik denetimi sağlayarak devre dışı bırakılmasını sağlamak için bu seçeneği seçin. Tam kimlik doğrulama ve devre dışı bırakma prosedürü aşağıdaki alt parametreler tarafından belirlenir:
Onay anahtarı + PIN kodu	Radyo düğmesi	Kart sahiplerinin bir kart, onay anahtarı ve PIN kodu ile kendi kimlik denetimlerini yapmaları gerekir.

Parametre	Değer tipi	Açıklama
Yalnızca PIN koduyla	Radyo düğmesi	Kart sahiplerinin bir kart ve PIN kodu kullanarak kendi kimlik denetimlerini yapmaları gerekir.
Yalnızca onay anahtarıyla	Radyo düğmesi	Kart sahiplerinin bir kart ve onay anahtarı ile kendi kimlik denetimlerini yapmaları gerekir.
Otomatik kapı çevrimi	Onay kutusu	Kart sahibinin aynı anda devre dışı bırakarak giriş yapmasını sağlamak için, devre dışı bıraktıktan sonra kapı kilidini kapatıp açmak istiyorsanız bu onay kutusunu seçin. **Not:** Kilit yalnızca kart sahibinin bu kapı için de giriş izni varsa kapatılıp açılır.
Prosedür bölmesi		
Disarming (Devre dışı bırakma) bölmesinde ayarlanan parametrelere bağlı olarak, bu bölmede IDS'yi devre dışı bırakmak için standart bir prosedür gösterilir. Bu prosedürü, bu Kurma alanındaki DM14 girişlerini kullanacak kart sahiplerine iletin.		
Kurma ve devre dışı bırakma bölmesi		
1 sn. darbeye sahip çıkış sinyali	Onay kutusu	**Bosch veya G Series** hırsız alarm paneli kullanıyorsanız bu onay kutusunu seçin. Sonuç olarak, sinyali sabit bir 1 (kur) veya 0 (devre dışı bırak) olarak ayarlamak yerine, girişin hırsız alarmı alanının kurma durumu olarak değiştirmek için tek bir darbe sinyali gönderilir.

Kapı kontrol cihazı terminalleri

Bir DM14 girişiyle kurmayı ve devre dışı bırakmayı mümkün hale getirmek için, girişin kapı kontrol cihazının terminallerinde kullanmak istediğiniz IDS girişini ve çıkış sinyallerini tanımlamanız gerekir.

Bu adımın, DM14 girişleri bulunan her kontrol cihazı için bir kez gerçekleştirilmesi gerekir. Aynı kontrol cihazı ve genişletme kartlarında tanımladığınız tüm sonraki DM14 girişleri, sinyalleri paylaşılan kontrol cihazından devralır.

Varsayılan sinyaller aşağıdaki tabloda açıklanmaktadır.

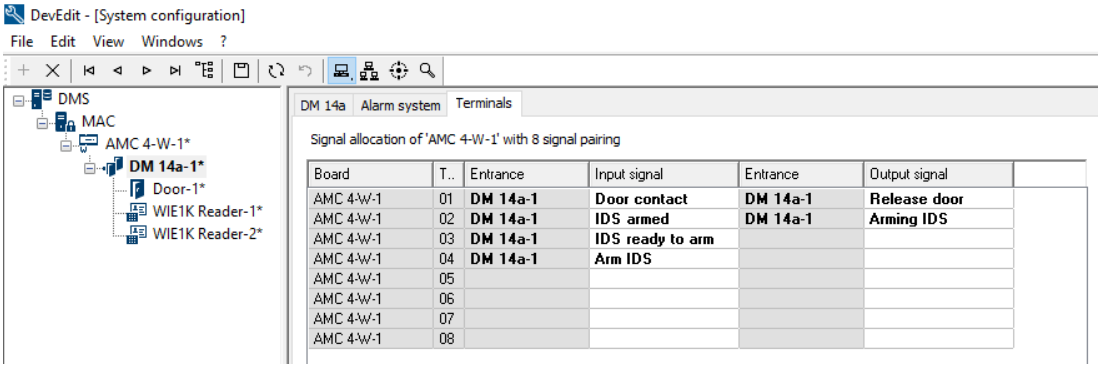
Sinyal	Giriş/ Çıkış	Açıklama
IDS kuruldu	Giriş	IDS bu hırsız alarmı alanı için kuruldu.
IDS kurulmaya hazır	Giriş	Hiçbir IDS noktası arızalı (açık veya hazır değil) durumda değil.
Arm IDS (IDS'yi kur)	Giriş	IDS'yi kurma isteği.
"Çıkış talebi" düğmesi (REX)	Giriş	
Cıvata sensörü	Giriş	Bir sensör kapı sürgüsünü izliyor.
Dış Müdahale	Giriş	Dış müdahale algılandı.

Sinyal	Giriş/ Çıkış	Açıklama
Yetkisiz açılma sebebiyle alarmı bastırma	Giriş	Bir hareket dedektörü tarafından REX sinyali verildiyse, yapılandırılan fazladan süre boyunca alarmı bastırın. Ayrıntılar için REX aktarma özelliğine bakın.
Release door (Kapıyı serbest bırak)	Çıkış	Giriş izni vermek için kapının mekanizmasını kilit açılacak ve yeniden kilitlenecek şekilde kapatıp açın.
Arming IDS (IDS kuruluyor)	Çıkış	IDS'yi geçerli durumuna (iki konumlu) bağlı olarak kurun veya devre dışı bırakın.
Camera connecting (Kamera bağlanıyor)	Çıkış	Girişe bağlı bir kamerayı etkinleştirin.
Max. door open time elapsed (Kapının maksimum açık kalma süresi geçti) veya **Door security compromised** (Kapı güvenliği tehlikeye girdi)	Çıkış	Kapı açık tutuluyor veya sistem kapıda güvenlik ihlali olduğundan şüpheleniyor.

Sinyalleri terminallere atama prosedürü

1. 3. sekme olan **Terminals**'ı (Terminaller) açın.

– Bu girişin kapı kontrol cihazının terminalleri ile sahip olabileceği tüm genişletme kartları bir tabloda görüntülenir.



2. Giriş sinyali için kullanmak istediğiniz terminale karşılık gelen satırı seçin.
3. İlgili hücrede, **Giriş sinyali** sütununda, açılır listeden istediğiniz sinyali seçin. Listede yalnızca o ana kadar atanmamış sinyallerin göründüğünü unutmayın.
4. Bu giriş için ihtiyaç duyduğunuz diğer giriş sinyallerini eklemek için önceki adımları tekrarlayın.

5. **Output signal** (Çıkış sinyali) sütununa ihtiyaç duyduğunuz tüm çıkış sinyallerini eklemek için prosedürü gerektiği ölçüde tekrarlayın.

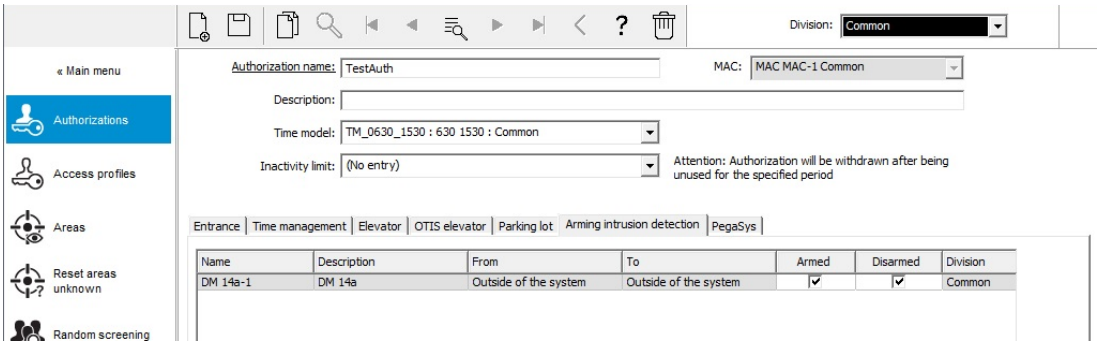
DM14 girişlerini kurma ve devre dışı bırakma yetkilerini tanımlama

Siz cihaz düzenleyicide bir DM14 girişi oluşturduktan sonra giriş, giriş yetkilerinin eklenmesi için kullanılabilir hale gelir.

1. İletişim kutusu yöneticisinde, şuraya gidin:

– Main menu (Ana menü) > **System data** (Sistem verileri) > **Authorizations** (Yetkiler) > sekme: **Arming Intrusion detection** (Hırsız algılamayı kurma)

2. İletişim kutusunda mevcut bir giriş yetkisini yükleyin veya yeni bir tane oluşturmak için (Yeni) simgesine tıklayın.
3. Listeden istendiğiniz DM14 girişini bulun ve **Armed** (Kuruldu) ve/veya **Disarmed** (Devre dışı bırakıldı) onay kutularını seçin.

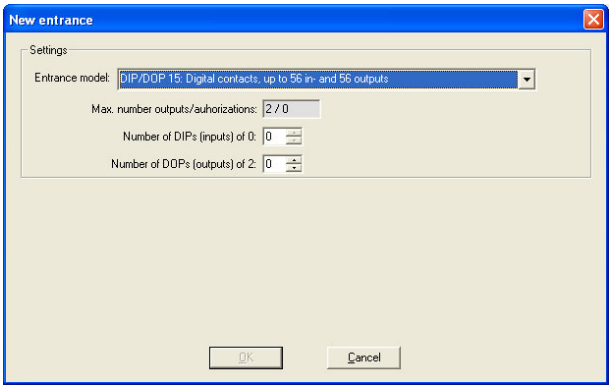


4. Giriş yetkisini seçilen izinlerle kaydetmek için (Kaydet) simgesine tıklayın.
5. Bu giriş yetkisini DM 14 girişlerini çalıştırmak için söz konusu kart sahiplerine atayın.

16.5.3 DIP'ler ve DOP'lar (DM15)

Giriş Modeli 15'i oluşturma:

Bu giriş modeli bağımsız giriş ve çıkış sinyalleri sunar.



Tüm okuyucu arayüzleri alınırsa sadece bu giriş modeli kullanılabilir hale gelir. Bu giriş modelini en az iki sinyal serbest olduğu sürece tanımlayabilirsiniz.

Asansörler (model 07) veya otoparklar (model 05c) bulunan AMC'lere bu giriş modeli atanamaz.

Giriş Modeli 15

Olası sinyaller: Bu varsayılan adların üzerine yazılabilir.

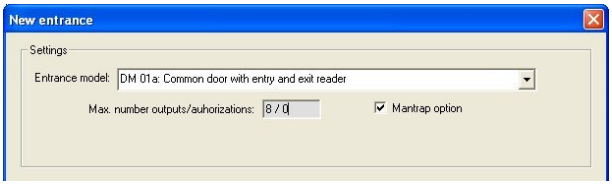
Giriş Sinyali	Çıkış Sinyali
DIP	DOP
DIP-1	DOP-1
...	...
DIP-63	DOP-63

Diğer kapı modellerinden farklı olarak, giriş modeli 15 hala serbest olan bir kontrol cihazının giriş ve çıkışlarını yönetir ve bunları tüm sistemin kullanımına yönelik genel girişler ve gerilimsiz çıkışlar olarak yerleştirir.
Diğer kapı modellerinin çıkış kontaklarından farklı olarak, giriş modeli 15'in çıkış kontaklarına cihaz düzenleyicide tek tek göz atılabilir.

Yeniden başlatma işlemlerinden sonra DOP'leri eski haline getirme
Bir MAC veya AMC yeniden başlatıldığında, normalde kendi alt DOP'lerinin durum değerlerini varsayılan değer olan 0'a (sıfır) ayarlar.
Bir yeniden başlatma işleminin her zaman DOP'nin buna manuel olarak atanan son duruma sıfırlanmasını sağlamak için, cihaz ağacında DOP'yi seçin ve ana penceredeki **Keep state** (Durumu koru) onay kutusunu seçin.

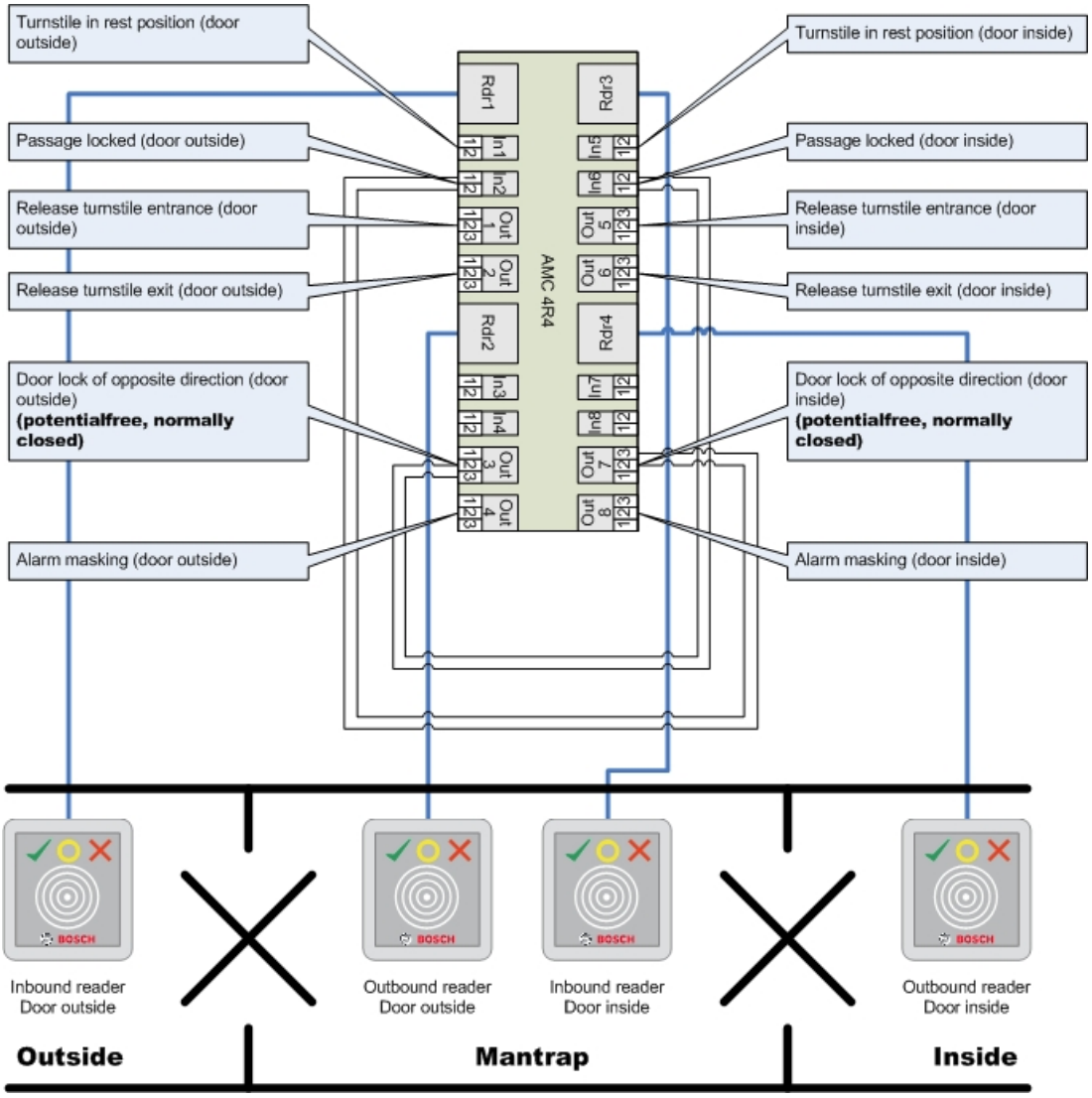
16.5.4 Tuzak kapı modelleri

Tuzak oluşturma
Giriş modeli 01 ve 03, kart sahibi girişlerinin tekilleştirilmesi için "tuzaklar" olarak kullanılabilir. Gerekli ek sinyalleri kullanılabilir hale getirmek için **Mantrap option** (Tuzak seçeneği) onay kutusunu kullanın.



01 ve 03 numaralı tüm model tiplerini birleştirebilirsiniz, ancak bu seçeneği tuzağa ait iki girişte de ayarlayabilirsiniz.
Kapı modeli için alışıldık sinyal atamalarıyla birlikte, tuzak seçeneği kendi başına ek sinyal atamaları gerektirir.

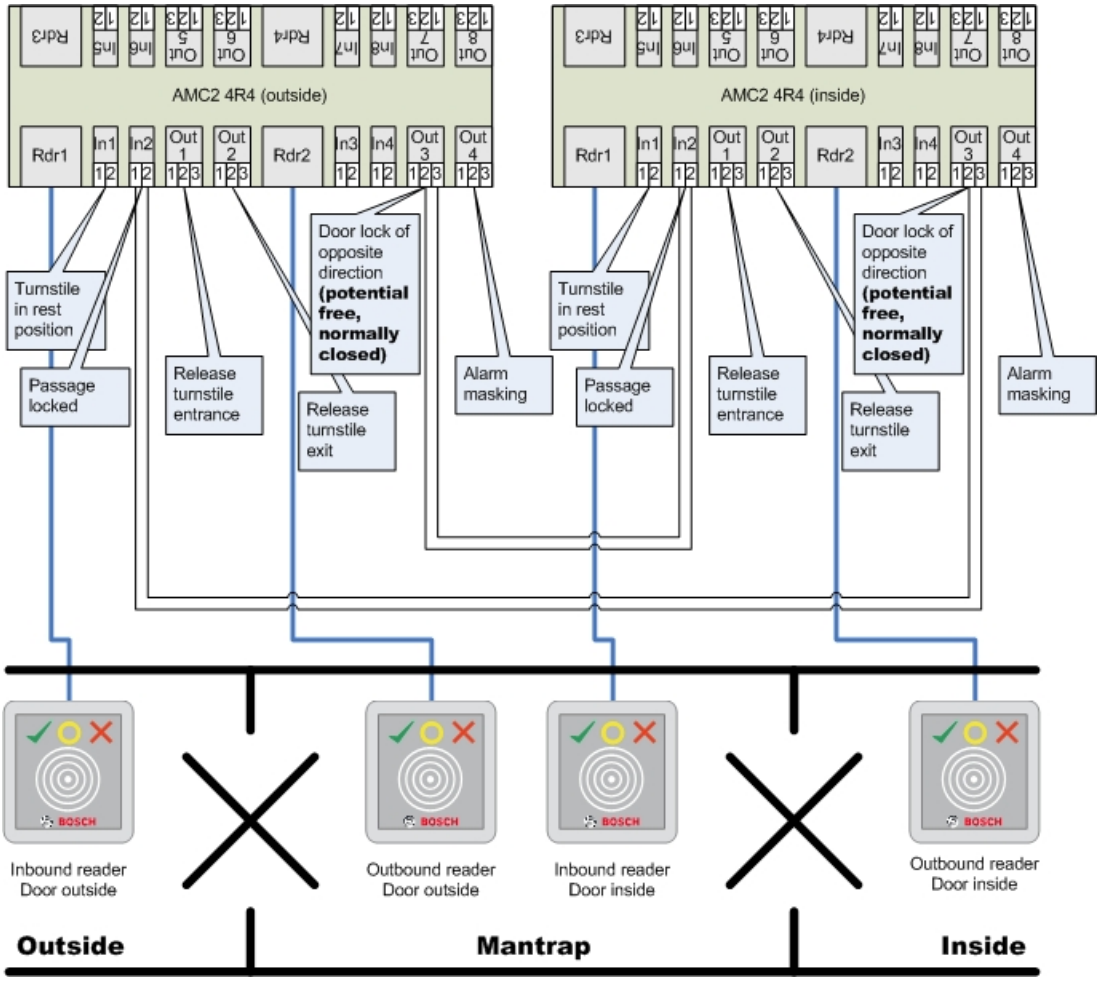
Örnek: Bir kontrol cihazındaki tuzak
Turnikeler, kart sahipleri tarafından yapılan tekil erişiminin en yaygın aracıdır. Bu nedenle aşağıdaki örneklerde, kapı model 3a'yı (giriş ve çıkış okuyuculu turnike) kullandık.
İki turnikeli tuzak yapılandırması (DM 03a):



Ters yön için kapı kilitlerine yapılan bağlantılar, turnikelerin yalnızca bir tanesinin herhangi bir zamanda açılmasını sağlar.

Uyarı!
Çıkış sinyalleri (Çıkış) 3 ve 7 potansiyelsiz (kuru mod) olarak ayarlanmalıdır
"Ters yön kapı kilidi" sinyali 0'da etkindir. "Normalde kapalı" çıkış 3 ve 7 için kullanılacaktır.

Örnek: İki kontrol cihazında tuzak
İki kontrol cihazında dağıtılan iki turnikeli (DM 03a) tuzak yapılandırması:



Ters yön için kapı kilitlerine yapılan bağlantılar, turnikelerin yalnızca bir tanesinin herhangi bir zamanda açılmasını sağlar.

Uyarı!
Çıkış sinyali (Çıkış) 3 potansiyelsiz (kuru mod) olarak ayarlanmalıdır.
"Ters yön kapı kilidi" sinyali 0'da etkindir. "Normalde kapalı" çıkış 3 için kullanılacaktır.

16.6 Kapılar

Sekme: Kapı

Parametre	Olası değerler	Açıklama
Name (Ad)	Alfa sayısal, en çok 16 karakter	Oluşturulan varsayılan değer isteğe bağlı olarak benzersiz bir adla değiştirilebilir.
Açıklama	Alfa sayısal, en çok 255 karakter	
Division (Bölüm)	Varsayılan bölüm "Common"dır (Ortak).	Yalnızca **Divisions** (Bölümler) özelliği lisanslandığında geçerlidir.
Bir tuzak yapılandırıldıysa yalnızca kapı modelleri 01 ve 03 için:		

Tuzak seçeneği	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	İki birleşik kapının kapı modeli 01 veya 03'ü kullandığı bir tuzak vardır. **İki** kapı için de tuzak seçeneğini etkinleştirin. Kapılar ayrıca özel fiziksel kablo bağlantısı da gerektirir.

Sekme: Seçenekler

Parametre	**Olası değerler**	**Açıklamalar**
Açık/kapalı mesajı oluştur	0 = onay kutusu işaretli değil 1 = onay kutusu işaretli.	0 = Kapı açıldığında (kapı, çerçeveyle bir açı oluşturuyor) veya kapalı olduğunda (kapı, çerçevesine tamamen oturmuş) mesaj oluşturulmaz. 1 = İlgili mesajlar olay kaydında oluşturulur.
Door set to manual (Kapı manuele ayarlandı)	0 = onay kutusu işaretli değil 1 = onay kutusu işaretli.	0 = kapı normal modda (varsayılan), yani, genel sistem tarafından giriş kontrolüne tabi. 1 = kapı kartlı geçiş sisteminden çıkarıldı. Kapı kontrol edilmez ve mesaj üretmez. Sadece manuel olarak kilitlenebilir veya kilidi açılabilir. Bu kapı için diğer tüm parametreler kapalıdır. Bu parametre kapı ve okuyucu için ayrı olarak ayarlanmalıdır.
Kapı modu	0 = Kapı normal modda 1 = Kapının kilidi açıldı 2 = Kapının kilidi zaman modeline göre açıldı 3 = Kapı ilk geçişten sonra zaman modeline göre açık 5 = Kapı uzun süreli olarak engellendi 6 = Kapı zaman modeline göre engellendi	0 = normal mod (varsayılan) - kapı kimlik bilgilerinin giriş haklarına bağlı olarak kilitlenir veya kilidi açılır. 1 = uzun süreliğine kilitle - süre için giriş kontrolü askıya alınır. 2 = zaman modeliyle tanımlanan bir süre için kilidi açın. Kartlı geçiş süre boyunca askıya alınır. 3 = ilk kişinin erişimi olana kadar zaman modeli etkin olduğu sürece kilitlidir - ardından zaman modeli etkin olduğu sürece açıktır. 5 = engel manuel olarak kaldırılana kadar engellendi (kartlı geçiş sisteminden çıkarılır). 6 = zaman modeli etkin olduğu sürece engellenmiştir (kartlı geçiş sisteminden çıkarılmış), kapı kontrolü yoktur, kapı zaman modeli etkinken kullanılamaz.
Time model (Zaman modeli)	mevcut zaman modellerinden biri	Kapı açma sürelerine yönelik zaman modeli. Kapı modları 2, 3, 4, 6 ve 7 seçiliyse zaman modellerine ait liste kutusu kullanılabilir. Bir zaman modeli seçmek gereklidir.

Kapı çarpma sinyaline kadar geçen maks. süre:	0 - 9999	Kilit açma sinyalinin maksimum süresi. Birim 1/10 sn. Varsayılan değerler: Kapılar için 50, döner kapılar (kapı modeli 03) için 10 ve bariyerler (kapı modelleri 05c veya 09c) için 200.
Kapı çarpma sinyaline kadar geçen min. süre:	0 - 9999	1/10 sn. içinde kilit açma sinyalinin minimum süresi. Varsayılan: 10.
Ön ekli alarm bastırma	0 - 9999	Kapı çarpma sinyalinden **önce** ek alarm bastırma. (`$PARAMETER_WAITEMA`) Kapı çarpmasının hırsız alarmından daha yavaş tepki verdiği çok nadir durumlarda, kapıya kilit açma sinyali göndermeden önce alarmı geçici olarak bastırmak mümkündür. Birim: 1/10 sn. Varsayılan 0. 20 değeri (yani 2 sn.) normalde çok yavaş kapılar için bile yeterlidir.
Son ekli alarm bastırma	0 - 9999	Kapı çarpma sinyalinden **sonra** ek alarm bastırma. (`$PARAMETER_OPENINRT`) Kapı çarpma sinyali (kilit açma sinyali) geçtikten sonra, belirtilen zaman aralığında kapı alarmı tetiklemeden açılabilir. Birim: 1/10 sn. Varsayılan: 0.
Door strike mode (Kapı kilidi karşılığı modu)	Liste kutusu girişi	0 = Etkinleştirme zamanından sonra REX (çıkış talebi) düğmesi devre dışı 1 = REX (çıkış talebi) düğmesi hemen devre dışı bırakıldı (= varsayılan)
Kapı çerçeve sensörü bulunuyor	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	0 = kapının çerçeve kontağı yok 1 = kapının çerçeve kontağı var. Kapalı bir kontak genellikle kapının kapalı olduğu anlamına gelir. (=varsayılan)
Sürgü sensörü bulunuyor	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	0 (varsayılan) = kapının sürgüsü sensörü yok 1 = kapının sürgüsü sensörü var. Kapı sürgülendiğinde veya sürgüsü açıldığında bir mesaj gönderilir.
Uzatılmış kapı açılma süresi (engelli kişiler)	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	0 = Kilit açma sinyali, bir **kapı** parametresi olan "Maks. kilit etkinleştirme süresi"nden ayarlanan standart süreye, yani kapı çarpması sinyaline kadar olan süreye sahiptir.

		1 (varsayılan) = kilit açma sinyalinin süresi, bir **MAC** parametresi olan "**Engelli kişiler için zaman faktörü**"nde ayarlanan faktör ile çarpılır (sekme: **Genel erişim ayarları**). Bu MAC parametresindeki 0 değeri, uzatılmış kapı açık kalma sürelerini devre dışı bırakır.

Sekme: Kapı güvenliği

Parametre	Olası değerler	Açıklamalar
"Kapı zorlanarak açıldı" mesajı oluştur	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	0 = hırsız alarmı mesajı yok. Bu, bir kapı içeriden serbestçe açılabiliyorsa faydalıdır. 1 = (varsayılan) Kapı yetkisiz olarak açıldığında bir mesaj verilir, ardından kapı kapandığında başka bir mesaj gelir.
"Kapı açık tutuluyor" için aşağıdakilerden sonra mesaj oluştur:	0 - 9999	Bu süreden sonra kapı açık kalırsa, kapının çok uzun süre açık kaldığına dair bir uyarı mesajı verilir. Birim: 1/10 sn. Varsayılan: 300. 0 = Zaman aşımı yok, mesaj yok.
"Kapı zorlanarak açıldı" için alarm bastırma uzantısı	0 - 9999	"REX aktarma" özelliğinde kullanılır: Birim = 1/10 sn. Varsayılan 0. Bir hareket dedektöründen gelen REX sinyalinden sonra, kapı bu süre içinde tekrar kapanırsa, normal `Unauthorized opening of door N` mesajının yerini şu mesaj alır: `Door N opened (in alarm suppression mode)` Burada N kapının numarasıdır.
"Kapı zorlanarak açıldı" için yerel alarm oluştur	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	Ön koşul: Bu iletişim kutusundaki **"Kapı zorlanarak açıldı" mesajı oluştur** onay kutusu seçilidir (yukarıya bakın). 0 = (varsayılan) Bu kapıya bağlı okuyucularda yerel alarm çalmaz. 1 = Kapı zorla açılırsa bu kapıya bağlı okuyucularda yerel alarm çalar.
"Kapı açık tutuluyor" için aşağıdakilerden sonra yerel alarm oluştur:	0 - 9999	Bu süreden sonra kapı açık kalırsa, bu kapıya bağlı okuyucularda yerel alarm çalar. Birim: 1/10 sn. 0 = (varsayılan) Yerel alarm yok.

16.6.1 REX aktarma

Giriş

Kapıyı içerden manuel olarak açmanın güvenlik riski oluşturmadığı girişlerde kapının kilidini açmak için REX düğmesinin yerini genellikle bir hareket dedektörü alır. Bu yaygın senaryo için ACS, `Door forced open` alarmını eşzamanlı olarak aktarırken (askıya alırken) hareket dedektöründen gelen REX sinyalinin süresini uzatmanın basit bir yolunu sunar.
Bu özellik "REX aktarma" olarak bilinir.
Özellik çalışırken, aktarma süresi içinde kapıdan ayrılan kart sahipleri,
`Unauthorized opening of door N` olayı yerine
`Door N opened (in alarm suppression mode)` giriş olayını oluşturacaktır.

Uyarı!
Kurulu hırsız alarmı sistemleriyle REX aktarma.
REX aktarma özelliği, parametrede ayarlanan süre boyunca alarmları askıya alır:
Cihaz Düzenleyici >... > **Kapı** > sekmesi: **Kapı güvenliği** > **"Kapı zorlanarak açıldı" için alarm bastırma uzantısı**
Kapının zaten hırsız alarmı sisteminin bir parçası olarak kurulu olup olmadığına bakılmaksızın.

Ön koşullar

- Aşağıdaki tiplerde yapılandırılmış kapılar: 01a, 01b, 01c, 03a, 03b, 03c, 10a, 10b, 10e, 14a, 14b
- Fiziksel kapı, kapının kilidini açmak için bir REX düğmesi yerine bir hareket dedektörü ile donatılmıştır. Hareket dedektöründen gelen sinyalin süresini en az 1 saniye olarak ayarlayın.

İletişim yolu

- **Main menu** (Ana menü) >**Configuration** (Yapılandırma) > **Device data** (Cihaz verileri)

Prosedür

1. Aygıt düzenleyicisinde istenen girişe (bir kapı kontrol cihazının doğrudan alt düğümü) gidin.
2. Girişin **Terminaller** sekmesinde şu türe sahip yeni bir giriş sinyali oluşturun:
   `Suppress alarm from unauthorized opening`
3. Değişiklikleri kaydetmek için  (Kaydet) simgesine tıklayın.
4. İstediğiniz girişte bulunan kapıyı seçin
5. Kapının **Kapı güvenliği** sekmesinde
   "Kapı zorla açıldı" için alarm bastırma uzantısı'na bir değer ayarlayın.
- Değer saniyenin onda biri cinsindendir.
- Varsayılan değer `0`'dır. Varsayılan olarak, kart sahibi hareket dedektörün hassas alanını terk ettikten sonra alarm bastırma uzantısı yoktur.

6. Değişiklikleri kaydetmek için  (Kaydet) simgesine tıklayın.

16.6.2 Kapıları yerel alarm çalacak şekilde ayarlama

Giriş

Aşağıdaki kapı durumları için ACS, kapıya bağlı tüm okuyucularda alarm çalar.

Durum	Yerel alarm yanıtı
Kapı zorlanarak açıldı	Alarm, 17 saniye boyunca veya kapı kapanıncaya kadar çalar.
Kapı açık tutuluyor	Alarm, kapı kapanıncaya kadar çalar.

Ön koşullar

– Okuyucular OSDP veya Wiegand protokolünü kullanır
– Okuyucularda alarm sesli uyarı cihazları bulunur ve kapı kontrol ünitesine elektriksel olarak bağlıdır.
– AMC üretici yazılımı sürümü 02.38 ya da sonraki sürümler.

Aşağıdaki okuyucu türleri **desteklenmemektedir**:

– IDEMIA okuyucular
– Wiegand protokollü Suprema okuyucuları
– LBUS okuyucuları
– BG900 okuyucuları

İletişim yolu

– **Main menu** (Ana menü) >**Configuration** (Yapılandırma) > **Device data** (Cihaz verileri)

Kapı zorlanarak açıldı prosedürü

1. Yapılandırmak istediğiniz kapıyı cihaz ağacından seçin.
2. Kapının **Kapı güvenliği** sekmesinde
   "kapı zorlanarak açıldı" mesajı oluştur onay kutusunu seçin.
3. **"Kapı zorlanarak açıldı" mesajı oluştur**
   onay kutusunu seçin. Varsayılan değer `0` 'dır (onay kutusu seçili değildir). Bu, varsayılan olarak hiçbir yerel alarmın çalmayacağı anlamına gelir.
4. Değişiklikleri kaydetmek için  (Kaydet) simgesine tıklayın.

Kapı açık tutuluyor prosedürü

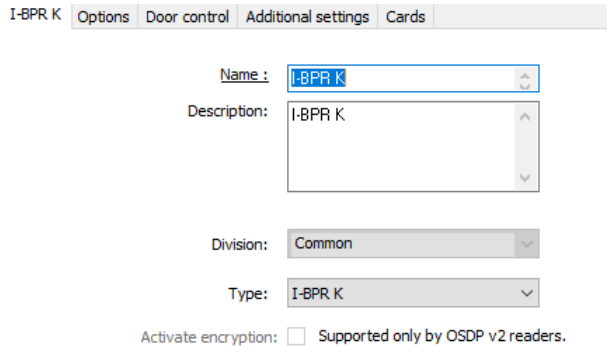
1. Yapılandırmak istediğiniz kapıyı cihaz ağacından seçin.
2. Kapının **Kapı güvenliği** sekmesinde, aşağıdakilerden sonra
   "Kapı açık tutuluyor" için yerel alarm oluştur amacıyla sıfır olmayan bir değer ayarlayın:

– Değer saniyenin onda biri cinsindendir.
– Varsayılan değer `0`'dır. Bu, varsayılan olarak hiçbir yerel alarmın çalmayacağı anlamına gelir.

3. Değişiklikleri kaydetmek için  (Kaydet) simgesine tıklayın.

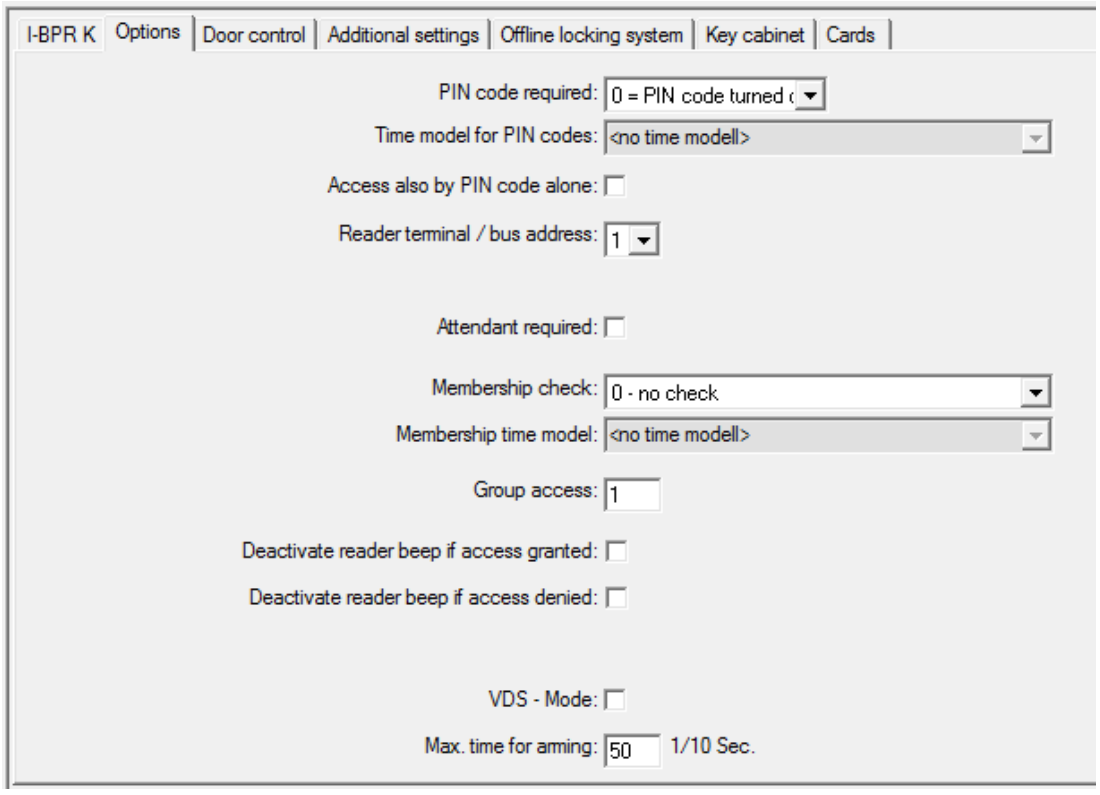
16.7 Readers (Okuyucular)

Okuyucu Yapılandırma: Genel Parametreler



Parametre	Olası Değerler	Açıklama
Reader name (Okuyucu adı)	alfa sayısal, 1 ile 16 karakter arasında kısıtlanmış	Varsayılan değer, benzersiz bir ad ile değiştirilebilir.
Reader description (Okuyucu açıklaması)	alfa sayısal: 0-255 karakter	Bir serbest metin açıklaması.
Division (Bölüm)	Varsayılan "Common" (Ortak) bölümü.	Sadece Bölümler lisanslı ve kullanımdaysa geçerlidir.
Type (Tip)	alfa sayısal, 1 ile 16 karakter arasında kısıtlanmış	Okuyucu türü veya okuyucu grubu

Okuyucu Yapılandırma: Seçenekler



Parametre	Olası değerler	Açıklama
PIN code required (PIN kodu gerekiyor)	0 = PIN kodu kapalı - gerekli giriş yok (varsayılan) 1 = PIN kodu açık - giriş her zaman gerekli 2 = Zaman modeline göre kontrol edilen PIN kodu - giriş sadece zaman modelinin dışındaysa gerekli	Bu alan sadece okuyucu bir giriş cihazına sahipse etkindir. Karttaki yetkiler ve giriş sırası (etkinse) gibi kontrollerin PIN'in doğruluğuna göre öncelikli olduğunu unutmayın.
Time model for PIN codes (PIN kodlarına ilişkin zaman modeli)	mevcut zaman modellerinden biri	**PIN code required** (PIN kodu gerekli) parametresi 2 olarak ayarlanmışsa burada bir zaman modeli seçimi zorunludur.
Access also by PIN code alone (Yalnızca PIN koduyla da eriş)	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	Bu okuyucunun, kartlı geçiş sistemi bu şekilde yapılandırıldıysa kartsız, tek bir PIN'e bağlı olarak girişe izin verip veremeyeceğini belirler. Bkz.

Reader terminal / bus address (Okuyucu terminali / veri yolu adresi)	1 - 4	AMC 4W için: Wiegand Arayüzlerine göre numaralandırılmış. AMC 4R4 için: Okuyucunun atlanmış adresi gibi numaralandırılmış.
Attendant required (Eşlik eden gerekli)	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	0 = ziyaretçinin hiçbir eşlik edene ihtiyacı yok (varsayılan) 1 = eşlik eden okuyucuyu da kullanmalıdır
Membership check (Üyelik kontrolü)	Liste kutusu girişi	Membership check (Üyelik kontrolü) genellikle bir kartlı geçiş sistemi canlı hale gelmeden önce erken aşamalarda kullanılır. Burada giriş, benzersiz kişisel kimliği yerine kimlik bilgisinin genel şirket kimliğine göre verilir. **ÖNEMLİ** Membership check (Üyelik kontrolü) yalnızca özelleştirilmiş tanımlar veya biyometrik kimlik bilgileri ile **değil** kart tanımlarının sistemde (gri arka plan) önceden tanımlandığı fiziksel kimlik bilgileriyle çalışır. **0 - kontrol yok** Membership check (Üyelik kontrolü) kapalıdır, ancak kart yetkiler için normal olarak kontrol edilir (varsayılan) **1 - kontrol** Kart sadece şirket kimliği için kontrol edilir, yani sistem üyeliğine yöneliktir. **2 - zaman modeline bağlı olarak** Kart, şirket kimliği (üyelik) için, ancak sadece üyelik zamanı modelinde tanımlanan süre boyunca kontrol edilir.
Membership time model (Üyelik zaman modeli)	mevcut zaman modellerinden biri	Zaman modeli, üyelik kontrolünü etkinleştirir/devre dışı bırakır. **Membership check** (Üyelik kontrolü) seçenek 2 için bir zaman modelinin seçimi zorunludur.
Group access (Grup girişi)	1 - 10	**Tuş takımlı okuyucular için:** Kapı açılmadan önce kart okuyucusuna gösterilmesi gereken minimum geçerli kart sayısı. Grup, bu sayıdan daha fazla karttan oluşabilir; bu durumda, grubun tamamlandığını göstermek için ENTER/# tuşu kullanılır. Bunun üzerine kapı açılır. **Tuş takımsız okuyucular için:**

		Kapı açılmadan önce kart okuyucusuna gösterilmesi gereken tam geçerli kart sayısı. Varsayılan değer 1'dir.
Deactivate reader beep if access granted (Giriş izni verilirse okuyucu bip sesini devre dışı bırak)	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	Etkinleştirilirse (1), yetkili bir kullanıcıya erişim izni verilirse okuyucu sessiz kalır.
Deactivate reader beep if access not granted (Giriş izni verilmezse okuyucu bip sesini devre dışı bırak)	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	Etkinse (1), yetkisiz bir kullanıcının giriş izni reddedildiğinde okuyucu sessiz kalır.
 "Deactivate Reader Beep" (Okuyucu Bip Sesini Devre Dışı Bırak) işlevleri ilgili okuyucu üretici yazılımına bağlıdır. Bazı okuyucuların üretici yazılımı bu işlevi desteklemeyebilir.		
VDS mode (VDS modu)	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	Etkinse (1) okuyucunun sinyalizasyonu kapatılır.
Max. time for arming (Maks. kurma süresi)	1 - 100 [1/sn.]	Kurulumun yapıldığı hırsız alarm panelinden alınan geri bildirim için gereken maksimum süre.

Ağ ve Çalışma modları

Bu sekme sadece ağa bağlı biyometrik okuyucular için görüntülenir.

Şablonlar depolanmış modellerdir. Kart verileri veya biyometrik veriler olabilirler.

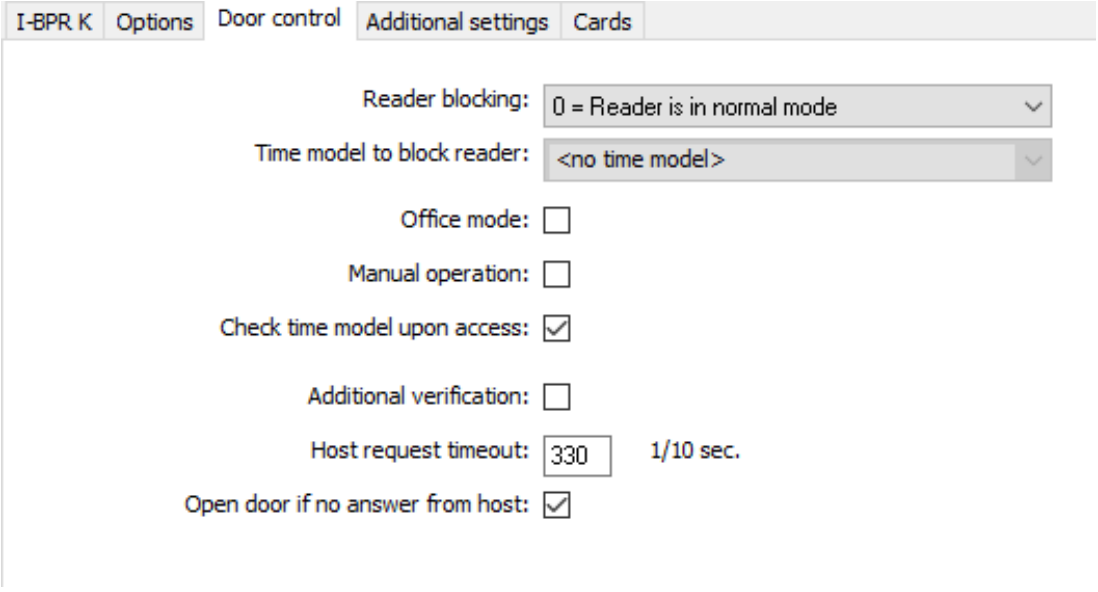
Şablonlar hem cihaz ağacındaki okuyucunun üzerindeki cihazlarda hem de okuyucunun kendisinde saklanabilir. Okuyucudaki veriler, üstündeki cihazlar tarafından düzenli olarak güncellenir.

Okuyucu, giriş kararları verirken kendi şablonlarını kullanacak veya yalnızca şablonları yukarıdaki cihazlardan kullanacak şekilde yapılandırılabilir.

Parametre	**Açıklama**
IP address (IP adresi):	Bu ağa bağlı okuyucunun IP adresi
Port:	Varsayılan port `51211`'dir

Parametre	Açıklama
Sunucudaki şablonlar	
Card only (Yalnızca kart)	Okuyucu sadece kart verilerini okur. Bunları sistem genelinden gelen verilere göre doğrular.
Card and fingerprint (Kart ve parmak izi)	Okuyucu hem kart verilerini hem de parmak izi verilerini okur. Bunları sistem genelinden gelen verilere göre doğrular.
Cihazdaki şablonlar	
Person dependent verification (Kişiye bağlı doğrulama)	Okuyucu, tek kart sahibinin ayarlarının hangi **Identification mode**'u (Kimlik modu) kullandığını belirlemesini sağlar. Personel verileri aşağıdaki seçenekleri sunar: – Fingerprint only (Yalnızca parmak izi) – Card only (Yalnızca kart) – Card and fingerprint (Kart ve parmak izi) Bunlar bu tablonun ilerleyen kısımlarında açıklanmaktadır.
Fingerprint only (Yalnızca parmak izi)	Okuyucu sadece parmak izi verilerini okur. Bunları kendi depolanmış verilerine göre doğrular.
Card only (Yalnızca kart)	Okuyucu sadece kart verilerini okur. Bunları kendi depolanmış verilerine göre doğrular.
Card and fingerprint (Kart ve parmak izi)	Okuyucu hem kart verilerini hem de parmak izi verilerini okur. Bunları kendi depolanmış verilerine göre doğrular.
Card or fingerprint (Kart veya parmak izi)	Okuyucu, kart sahibinin hangisini daha önce gösterdiğine bağlı olarak kart verilerini veya parmak izi verilerini okur. Bunları kendi depolanmış verilerine göre doğrular.

Okuyucu Yapılandırma: Kapı Kontrolü

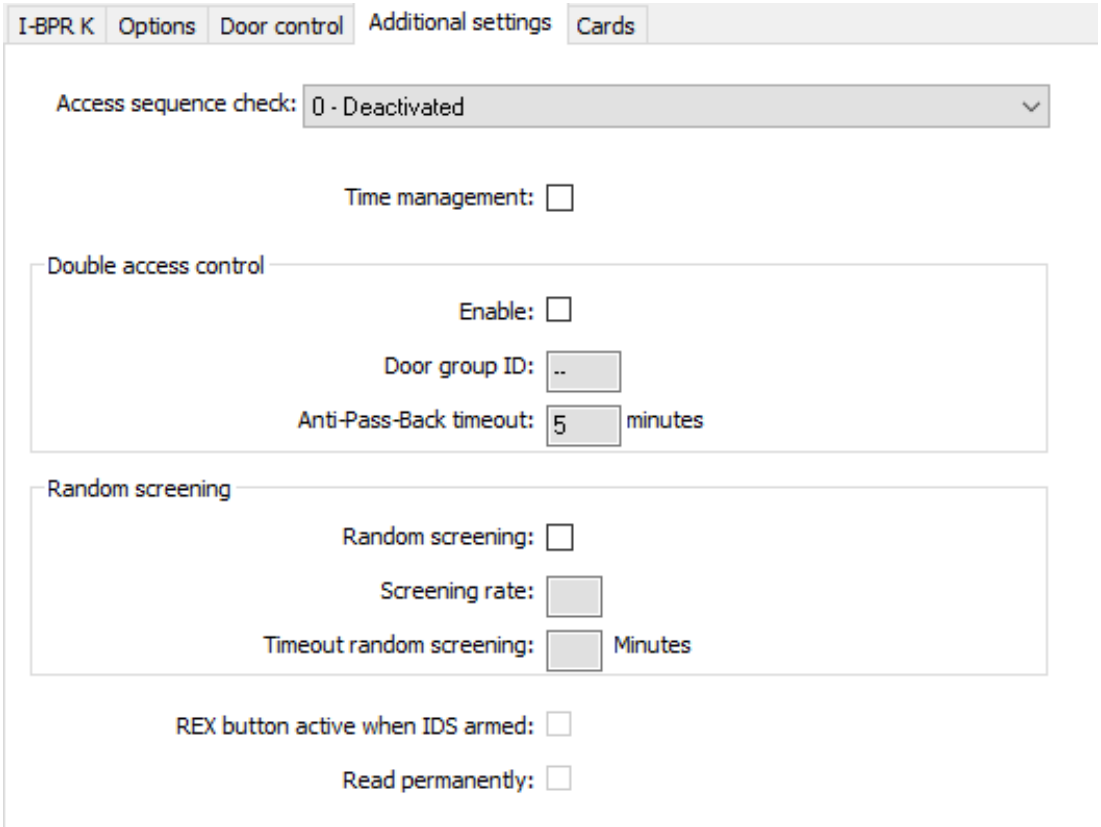


Parametre	Olası değerler	Açıklamalar

Reader blocking (Okuyucu engelleme)	Liste kutusu girişi	0 = Okuyucu normal modda - engelleme yok (= varsayılan) 1 = Okuyucu kalıcı olarak engellendi - kalıcı engelleme 2 = Okuyucu, zaman modeline bağlı olarak engellenir - *Time model to block reader* (Okuyucuyu engellemek için zaman modeli) ile ayarlanan zaman modeline göre engelleme
Time model to block reader (Okuyucuyu engellemek için zaman modeli)	sistemde tanımlanan zaman modellerinden biri.	Okuyucuyu seçilen zaman modeline göre engeller.
Office mode (Ofis modu)	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	Bu okuyucunun girişi Office mode'a (Office modu) ayarlamasına olanak tanır. Okuyucunun tuş takımlı olması gerekir. Bu parametre etkinleştirildiğinde, uygun şekilde yetkilendirilmiş bir kart sahibi, kartını göstermeden önce 3 tuşuna basarak ofis modunu açar ve kapatır. Bkz. *Kişilere Ofis modunu ayarlama yetkisi verme, sayfa 199*
Manuel çalıştırma	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	0 = okuyucu normal modda (= varsayılan) 1 = okuyucu, kartlı geçiş sisteminden etkin bir şekilde kaldırıldı, yani "bozuk". Hiçbir komut alınmadı. Bu okuyucu için diğer tüm parametreler kapalıdır. Parametre, hem okuyucu hem de kapı için bağımsız olarak ayarlanmalıdır.
Check time models upon access (Girişten sonra zaman modellerini kontrol et)	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	0 = Zaman modelleri kontrol edilmez. Giriş için zaman kısıtlaması yoktur. 1 = Kart sahibine doğrudan veya alan-zaman yetkisi olarak atanmış bir zaman modeli varsa zaman modeli kontrol edilir. (=varsayılan)
Additional verification (Ek doğrulama)	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	0 = ana bilgisayar doğrulaması gerekli değil 1 = ana bilgisayar doğrulaması gerekli (varsayılan) (**ÖNEMLİ**: Bu seçeneğin etkinleştirilmesi, bir Bosch BVMS veya Bosch kartlı geçiş sisteminin operatörü tarafından yapılan ek video doğrulaması için gereklidir.)

Host request timeout (Ana bilgisayar isteği zaman aşımı)	0 = devre dışı	0 = AMC, ana bilgisayar doğrulaması olmadan çalışır (*Area Change* (Alan Değişikliği) veya *Person Countings* (Kişi Sayımı) ile çalışmaz). Bu kontrol sadece Ana bilgisayar doğrulaması devre dışıysa (0) ve *Open door if no answer from host* (Ana bilgisayardan yanıt alınamazsa kapıyı aç) etkinse (1) devrededir. 1-9999 x saniyenin 1/10'u. (Varsayılan = 330 = 33 saniye). Okuyucu kartlı geçiş sisteminden onay ister. Onay bu süre içinde alınmıyorsa AMC, **Open door if no answer from host** (Ana bilgisayardan yanıt yoksa kapıyı aç) parametresini kontrol eder veya buna göre geçişi reddeder.
Open door if no answer from host (Ana bilgisayardan yanıt alınamazsa kapıyı aç)	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (varsayılan) (onay kutusu işaretli)	Bu kontrol, sadece **Host verification** (Ana makine doğrulaması) ayarlandıysa etkindir. 0 = ana bilgisayar sistemi zaman aşımından önce hata verirse kapıyı açmaz. 1 (varsayılan) = ana bilgisayar sistemi zaman aşımından önce hata verirse kapıyı zaman aşımından sonra açar.

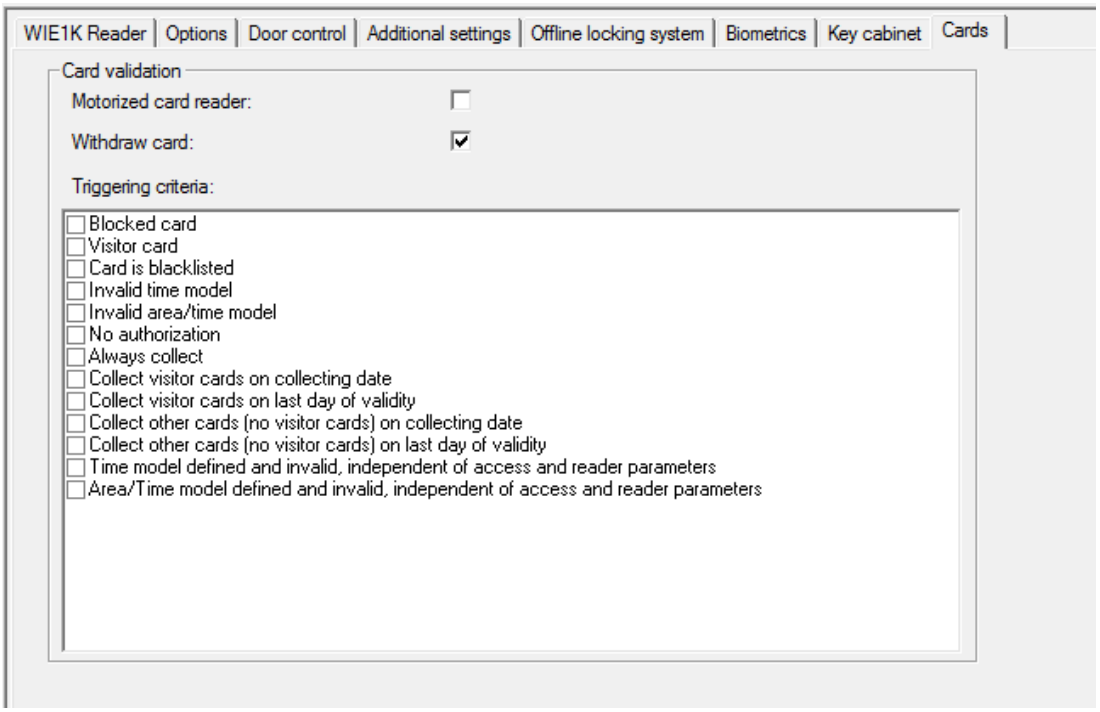
Okuyucu Yapılandırma: Ek Ayarlar



Parametre	Olası değerler	Açıklamalar
Giriş sırası kontrolü	0 - Devre dışı 1 - Etkin; LAC arızasından sonra devre dışı bırak 2 - Etkin; LAC arızasından sonra etkin bırak 3 - Etkin; LAC arızalandığında bile sıkı sıra kontrolü kullan (not: Kişinin konumunu manuel olarak güncelle)	0 = okuyucu giriş sırası kontrolünde yer almaz (= varsayılan) Etkin bir sıra kontrolü, UNKNOWN (BİLİNMİYOR) olarak ayarlanmış kişileri aşağıdaki şekillerde ele alabilir: 1 = Kartın ilk değeri, konumu kontrol etmeden aşağı olacaktır. Tüm kontrol cihazları çevrimiçi olmalıdır. 2 = Kartın ilk değeri, konumu kontrol etmeden bozuk olacaktır. 3 = LAC arızası sırasında her kart değeri için konum kontrolü bozuk olacaktır.
Genel olarak tüm giriş sıralamasını kontrol etmek veya devre dışı bırakmak için bir MAC komutu vardır. Bir süre boyunca giriş sırası kontrolünü devre dışı bırakmak için, maksimum değer olarak 2880 (= 48 saat) ile dakika cinsinden bir değer verilir. "0" değerini ayarlamak, erişim sıralamasını tamamen devre dışı bırakır. **Not:** Bu komut, sadece **Enable access sequence** (Giriş sırasını etkinleştir) parametresinin ayarlandığı okuyucular için erişim sırasını değiştirebilir. *Tüm* okuyucular için giriş sırası kontrolünü devre dışı bırakmaz/etkinleştirmez.		
Time Management (Zaman Yönetimi)	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	Bu seçilirse kartlı geçiş sistemi Zaman ve Katılım yönetimi için veri toplar.
Çift giriş kontrolü (anti-passback kontrolü)		
Enable (Etkinleştir)	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	0 = çift giriş kontrolsüz (= varsayılan) 1 = çift giriş kontrollü **Duration** (Süre) tarafından belirlenen süre içinde bu okuyucu ve gruptaki diğer okuyucular aynı kartla kullanılamaz. Bu parametre etkinse sadece bir okuyucu kullanılsa bile bir kapı grubu kimliği kullanılmalıdır.
Door group ID (Kapı grubu kimliği)	Harfler A - Z ve a - z ile "-" 2 karakter	Okuyucular, bir Kapı grubu kimliği kullanılarak gruplandırılabilir. Bir okuyucuda bir kart göstermek, kapı grubundaki

		(Varsayılan = **--**) tüm okuyucularda zaman aşımına kadar sonraki ayırma işlemlerini engeller.
Anti-passback time out (Anti-passback zaman aşımı)	1 - 120	Okuyucu, bu süre geçtikten sonra aynı kartla kullanılabilir. Kart, grup dışındaki bir okuyucuda kullanılır kullanılmaz engelleme hemen kaldırılır. Değerler dakikadır - varsayılan = 5.
Random screening (Rastgele tarama)	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	0 = rastgele tarama yok 1 = faktöre göre rastgele tarama **Blocking** (Engelleme) iletişim kutusu tarafından engeli kaldırılana kadar kabul edilmez.
Screening rate (Tarama oranı)	1 - 100	Genişletilmiş bir kontrol için rastgele tarama yüzdesi. Rastgele tarama etkinse kullanılabilir.
Timeout random screening (Zaman aşımı rastgele taraması)	1 - 120	Ayarlanan zaman içinde kullanıcı rastgele taramaya tabidir. Değerler dakikadır - varsayılan = 5.
REX button active when IDS armed (IDS kuruluyken REX düğmesi etkin)	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	Yalnızca **DM10** ve **DM14** için: IDS kuruluyken REX basmalı düğmeleri varsayılan olarak devre dışıdır. Bu, izlenen alandan çıkmayı imkansız hale getirir. Bu yeni okuyucu parametresi, IDS devredeyken bile REX düğmesini etkinleştirir.
Read permanently (Kalıcı olarak oku)	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	Okuyucu, üreticinin ilgili yazılımına sahipse kalıcı olarak okur.

Okuyucu Yapılandırma: Kartlar



Parametre	Olası değerler	Açıklamalar
Motorized card reader (Motorlu kart okuyucu)	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	Motorlu kart okuyucusu kullanılıyorsa bu onay kutusunu seçin
Withdraw card (Kartı geri al)	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	Motorlu kart okuyucusu varsa Withdraw (Geri al), karta fiziksel olarak el koymak anlamına gelir. Başka kart okuyucular varsa Withdraw (Geri al), sistemin kartı geçersiz kıldığı anlamına gelir.
Triggering criteria (Tetikleme kriterleri)	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	Bu listeden **Withdraw card** (Kartı geri al) işlemini tetiklemesi gereken tüm kriterleri seçin.

Uyarı!
Motorlu kart okuyucular sadece IBPR okuyucuları ile kullanılabilir.

Bkz.

– *Kişilere Ofis modunu ayarlama yetkisi verme, sayfa 199*

16.7.1 Rastgele taramayı yapılandırma

Rastgele tarama, ek güvenlik kontrolleri için personeli rastgele seçerek saha güvenliğini artırmanın yaygın kullanılan bir yöntemidir.

Ön gereksinimler:

– Bir kişinin kendi kimlik kartını göstermeden başka bir kişiyi takip etmesini engellemek için giriş tuzak veya turnike tipinde olmalıdır.
– Geçiş yönlerinden en az biri için bir kart okuyucu bulunmalıdır.
– Okuyucular normal giriş kontrolü için yapılandırılmış olmalıdır.
– Karıştırıcı her okuyucu için ayrı biçimde yapılandırılabilir.
– Sistem tarafından ayarlanan her türlü engellemeyi kaldırmak için yakın çevrede bir iş istasyonu bulunmalıdır.

Prosedür

1. Cihaz düzenleyici DevEdit'te istediğiniz okuyucuyu bulun
2. **Settings** (Ayarlar) sekmesinde, **Random screening** (Rastgele tarama) onay kutusunu seçin.
3. **Screening percentage** (Tarama yüzdesi) kutusuna taranacak kişi yüzdesini girin.
4. Yaptığınız ayarları kaydedin.

16.8 Yalnızca PIN'le giriş

Arka plan

Tuş takımlı okuyucular yalnızca PIN'le girişe izin verecek şekilde yapılandırılabilir. Okuyucular bu şekilde yapılandırıldığında, kartlı geçiş operatörü seçilen personele ayrı ayrı PIN'ler atayabilir. Uygulamada, bu personel yalnızca bir PIN'den oluşan bir "sanal kart" alır. Bu Tanıma PIN'i olarak adlandırılır. Bunun tersine Doğrulama PIN'i daha yüksek güvenlik uygulamak üzere bir kartla birlikte kullanılan bir PIN'dir.

Operatör personelin PIN'lerini manuel olarak girebilir veya personele sistem tarafından oluşturulan PIN'ler atayabilir.
Aynı personelin aynı zamanda onlara atanmış olan herhangi bir fiziksel kartı kullanarak giriş yapmaya devam edebileceğini unutmayın.

Operatörler için ön koşul niteliğindeki yetki

Kart sahibinin yalnızca PIN ile erişim yetkisi, yalnızca sanal kartlar atamak için özel yetkiye sahip operatörler tarafından verilebilir. Bir operatöre bu yetkiyi vermek için aşağıdaki gibi ilerleyin.

1. Main menu (Ana menü) > **Configuration** (Yapılandırma) > **Operators and workstations** (Operatörler ve iş istasyonları) > **User profiles** (Kullanıcı profilleri) bölümüne gidin.
2. Yetkiyi alacak Kullanıcı profilini seçin:
   Profile name (Profil adı) metin alanına girin veya istediğiniz profili bulmak için arama özelliğini kullanın.
3. İletişim kutuları listesinde, **Cards**
   'ı (Kartlar) içeren hücreye tıklayın Ana pencere bölmesinin altına yakın bir yerde **Special functions** (Özel işlevler) adına bir açılır pencere görünür.

4. Special functions (Özel işlevler) bölmesinde, **Assign virtual cards (PIN)** (Sanal kart (PIN) ata) onay kutusunu seçin.
5. Yaptığınız değişiklikleri kaydetmek için simgesine veya **Apply**'a (Uygula) tıklayın

Desteklenen okuyucu türleri için Kimlik PIN'inin uzunluğunu ayarlama

Elle girilen veya sistem tarafından oluşturulan PIN'lerin uzunluğu, sistem yapılandırmasında ayarlanan parametreyle düzenlenir.

– Main menu (Ana menü)> **Configuration** (Yapılandırma) > **Options** (Seçenekler) > **PIN codes** (PIN kodları) > **PIN code length** (PIN kodu uzunluğu)

Bir okuyucuyu yalnızca PIN'le giriş için yapılandırma

1. Main menu (Ana menü) > **Configuration** (Yapılandırma) > **Device data** (Cihaz verileri) > **Workstations** (İş istasyonları) ağacına gidin
2. **Workstation** (İş istasyonu) bölmesinde, okuyucunun fiziksel olarak bağlı olduğu iş istasyonunu seçin.
3. İş istasyonuna sağ tıklayın ve bir **Dialog Enter PIN** (İletişim Kutusuyla PIN Girme) veya **Dialog Generate PIN** (İletişim Kutusuyla PIN Oluşturma) okuyucu tipi ekleyin.
4. **Workstations** bölmesinden okuyucuyu seçin.
   Workstations (İş istasyonları) bölmesinin sağında özel bir okuyucu yapılandırma bölmesi görünür.
5. **Card usage default** (Kart kullanım varsayılanı) açılır listesinin **Virtual Card (Sanal Kart) varsayılan değerini içerdiğinden emin olun. PIN'i kart olarak kullanın**.
6. Yaptığınız değişiklikleri kaydetmek için simgesine veya **Apply**'a (Uygula) tıklayın
7. Cihaz düzenleyici DevEdit'te, **Device configuration** (Cihaz yapılandırması) ağacına gidin
8. Yalnızca PIN ile girişi yapılandırmak istediğiniz girişteki okuyucuyu seçin.
9. **Options** (Seçenekler) sekmesinde **Access also by PIN code alone** (Yalnızca PIN koduyla da eriş) onay kutusunu seçin.
10. Yaptığınız değişiklikleri kaydetmek için simgesine veya **Apply**'a (Uygula) tıklayın

16.9 AMC genişletme kartları

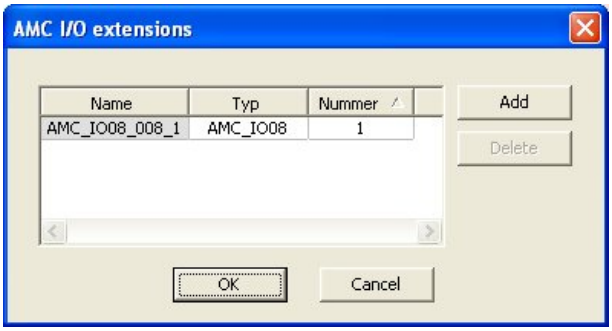
AMC-G/Ç-EXT (G/Ç Genişleme Kartı) oluşturma

Genişletme kartları, AMC'de bulunan sekiz kontak gerekli kontakların (örneğin asansörlerdeki) bağlantısı için yeterli değilse ek giriş ve çıkış sinyalleri sağlar.
Bu genişletmeler, ilgili AMC'ye fiziksel olarak bağlanır ve yalnızca Cihaz Düzenleyici'deki ilgili AMC'lerin altına takılabilir. Bir AMC-EXT oluşturmak için gezginde ilgili AMC girişi ve **New Object** (Yeni Nesne) bağlam menüsünde **New Extension Board** (Yeni Genişletme Kartı) girişi seçilir.

Uyarı!

+düğmesine  tıklamak yalnızca Cihaz Düzenleyici'deki araç çubuğunda yeni girişler oluşturur. Genişletme kartları, bağlam menüsü kullanılarak seçilebilir.

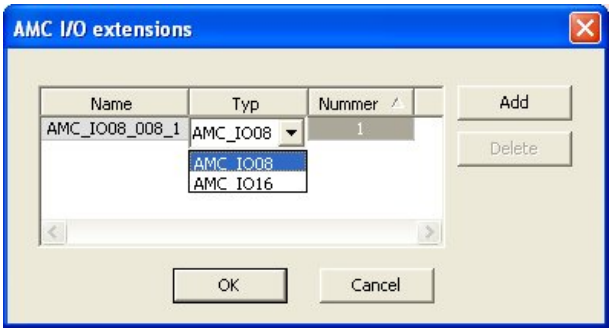
Genişletmelerin oluşturulması için bir seçim iletişim kutusu görüntülenir.



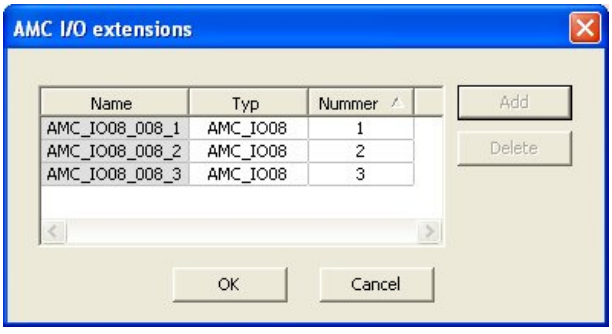
AMC-EXT'nin iki çeşidi vardır:

- AMC_IO08: 8 girişli ve 8 çıkışlı
- AMC_IO16: 16 girişli ve 16 çıkışlı
- AMC_4W genişletme: 8 girişli ve 8 çıkışlı

Seçim iletişim kutusu AMC_IO08'e sahip bir giriş içerir. **Type** (Tip) sütunundaki liste kutusuna çift tıklayarak, bir AMC_IO16 da yerleştirebilirsiniz.



Bir AMC'ye en fazla üç genişletme bağlayabilirsiniz. İki çeşidin bir karışımı mümkündür. Daha fazla liste girişi oluşturmak için **Add**'e (Ekle) tıklayın. Tüm bu sütun girişleri özelleştirilebilir.



Genişletme kartları, oluşturulduğu gibi 1, 2 veya 3 olarak numaralandırılır. Sinyallerin numaralandırılması her kart için 01'den başlar. Sinyal numarası ile kart numarasıyla birlikte benzersiz bir kimlik sağlar. Genişletmek kartlarının sinyalleri, ait oldukları AMC'nin sekmesinde de görülebilir.

Böylece AMC'deki giriş ve çıkış sinyalleriyle birlikte 56'ya kadar sinyal çifti sağlanabilir. Genişletme kartları, gerektiği gibi tek tek veya ileri bir tarihte maksimum sayıya (AMC başına 3) kadar eklenebilir.

AMC2 4W-EXT oluşturma

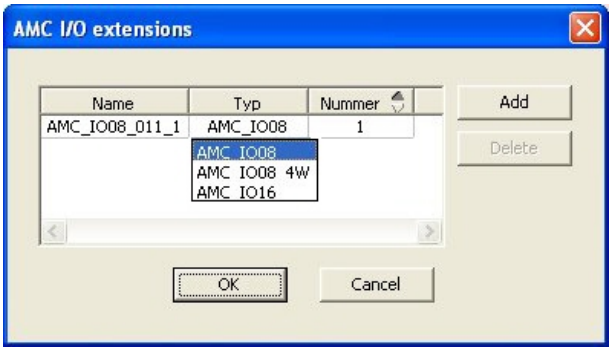
Wiegand okuyucu arayüzlerine (AMC2 4W) sahip kontrol cihazları için özel genişletme kartları (AMC2 4W-EXT) yapılandırmak mümkündür. Bu modüller, her biri 8 giriş ve 8 çıkış kontağı olacak şekilde ek 4 Wiegand okuyucu bağlantısı sağlar. Böylece, AMC2 4W başına bağlanabilen maksimum okuyucu ve kapı sayısı ikiye katlanarak 8'e ulaşır.

Uyarı!
AMC2 4W-EXT, tek başına bir kontrol cihazı olarak kullanılamaz, ancak sadece AMC2-4W'ye bir genişletme olarak kullanılabilir. Kapılar kontrollüdür ve giriş kontrolü kararları sadece AMC2 4W tarafından verilir.

AMC2 4W-EXT sadece bir AMC2 4W ile bağlantılı olarak kullanılabilir. Sadece Wiegand okuyucu arayüzleri bulunduğundan, AMC çeşidi AMC2 4R4 ile birlikte kullanılamaz.
G/Ç genişletme kartları (AMC2 8I-8O-EXT ve AMC2 16I-16O-EXT) gibi, AMC2 4W-EXT, AMC2 4W'nin genişletme arayüzü aracılığıyla bağlanır. Genişletme kartının kendi belleği ya da ekranı yoktur, ancak tamamen AMC2 4W tarafından kontrol edilir.
Bir AMC2 4W-EXT ve maksimum üç G/Ç genişletmesi, her AMC2-4W'ye bağlanabilir.
Sistemde bir AMC2 4W-EXT oluşturmak için Gezgin'de istediğiniz ana AMC2 4W'ye sağ tıklayın ve bağlam menüsünden **New object** (Yeni nesne) > **New extension board**'u (Yeni genişletme kartı) seçin.

Uyarı!
Cihaz verileri düzenleyicinin araç çubuğundaki ✚ düğmesi sadece giriş eklemek için kullanılabilir. Genişletme kartları sadece bağlam menüsü aracılığıyla eklenebilir.

Bir AMC2 4W listesinin AMC_IO08_4W ek elemanını içermesi dışında, G/Ç uzantıları oluşturmak için olanla aynı seçim iletişim kutusu görüntülenir.



AMC2 4W liste girişi sadece bir kez eklenebilir, bununla birlikte en çok üç G/Ç Genişletmesi eklenebilir.
Add (Ekle) düğmesi yeni liste girişleri ekler. Bir AMC2 4W varsa maksimum sayı 4'tür, dördüncü giriş ise bir AMC2 4W-EXT kartı olarak oluşturulur.

Genişletme kartları, 1, 2 veya 3 oluşturma sırasına göre numaralandırılır. AMC2 4W-EXT, 0 (sıfır) değerini alır. AMC2 4W-EXT'nin sinyallerinin numaralandırılması, kontrol cihazınınkinden, yani 09'dan 16'ya kadar devam ederken, her G/Ç kartının numaralandırması 01 ile başlar. Tüm genişletme kartlarının sinyalleri ilgili AMC2 4W sekmesinde de gösterilir. Böylece AMC2 4W'nin giriş ve çıkış sinyalleriyle birlikte 64'e kadar sinyal çifti sağlanabilir.

Genişletme kartlarını değiştirme ve silme

İlk sekme, genişletme kartlarını yapılandırmak için aşağıdaki kontrolleri içerir.

Parametre	Olası değerler	Açıklama
Board name (Kart adı)	Sınırlandırılmış alfa sayısal: 1-16 basamak	Varsayılan kimlik benzersiz bir adı garanti eder, ancak manuel olarak geçersiz kılınabilir. Lütfen kimliğin benzersiz olduğundan emin olun. DHCP sunucularıyla ağ bağlantılarında ağ adı kullanılmalıdır.
Board description (Kart açıklaması)	alfa sayısal: 0 - 255 basamak	Bu metin OPC dalında görüntülenir.
Board number (Kart numarası)	1 - 3	AMC'ye bağlı kart sayısı. Sadece görüntüleme alanı.
Power supply (Güç kaynağı)	0 = devre dışı (onay kutusu işaretli) 1 = etkin (onay kutusu işaretli)	Besleme geriliminin denetlenmesi. Gerilim kesintileri ile gecikmenin sonunda bir mesaj üretilir. Denetim işlevi bir USV kullanıldığını varsayar, böylece bir mesaj oluşturulabilir. 0 = denetim yok 1 = denetim etkin
Division (Bölüm)	Varsayılan değer **Common** (Ortak)	Yalnızca **Divisions** (Bölümler) özelliği lisanslandığında geçerlidir.

Inputs (Girişler), Outputs (Çıkışlar) ve Signal Settings (Sinyal Ayarları) sekmeleri, kontrol cihazların ait ilgili sekmelerle aynı düzene ve işleve sahiptir.

Genişletme kartlarını silme

Bir genişletme kartı yalnızca arayüzlerinden hiçbiri meşgul olmadığında silinebilir. İlişkili sinyaller öncelikle  sil düğmesi ve **Delete object** (bağlam menüsü seçeceği) kullanılabilir hale gelmeden önce farklı bir kartta yapılandırılmalıdır.

AMC2 4W-EXT

Genişletme kartlarını meşgul eden okuyucular tek tek kaldırılamadığından ya da yeniden yapılandırılamadığından, ilgili girişlerle birlikte silinmeleri gerekir. O zamana kadar AMC2 4W-EXT de kaldırılamaz.

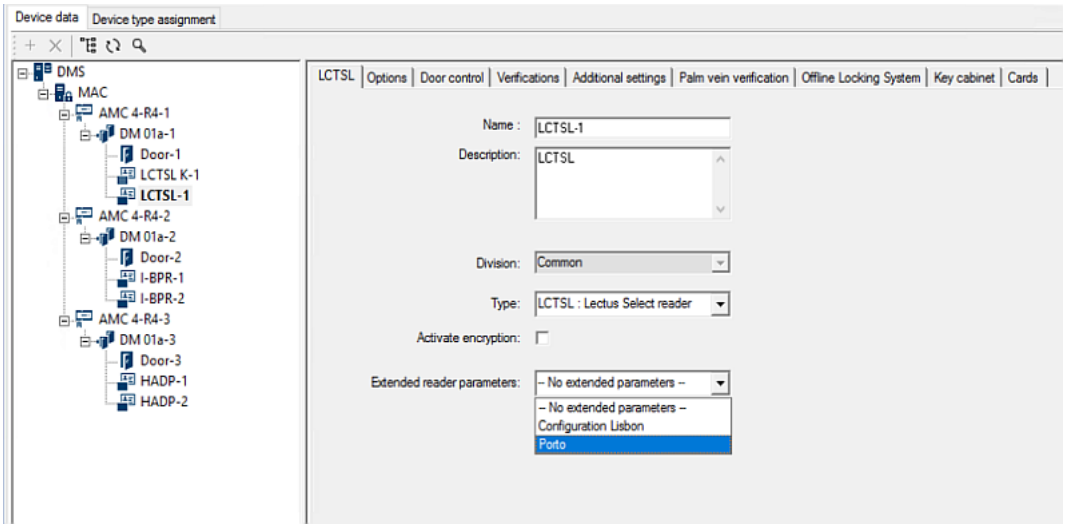
17 Özel okuyucu yapılandırmaları

17.1 Giriş

BIS 4.9 ve AMS 4.0 itibarıyla Bosch kartlı geçiş sistemleri özelleştirilmiş MIFARE DESFire ayarlarının kullanılmasına izin vermektedir. `Bosch.ReaderConfigTool.exe`. yardımcı aracını kullanarak şifrelenmiş parametre dosyaları oluşturabilirsiniz. Bu araç BIS ACE 4.9, AMS 4.0 ve sonraki sürümler için kendi belgelerine göre kurulumlara dahil edilmiştir. Uyumlu okuyucuların geçerli listesi için belgelere başvurun
Aşağıdaki bölümlerde, şifrelenmiş bir parametre dosyasını içe aktarmak ve bu dosyayı giriş kontrol cihazları hiyerarşisindeki uyumlu herhangi bir okuyucuya veya tüm okuyuculara uygulamak için Cihaz Düzenleyicisi'nin nasıl kullanılacağı açıklanmaktadır.

17.2 Okuyucu özelliği: Genişletilmiş okuyucu parametreleri

Uyumlu okuyucular için mevcut genişletilmiş parametre grupları, **Extended reader parameters** (Genişletilmiş okuyucu parametreleri) etiketinin altındaki cihaz düzenleyicisinin özellik sayfalarında görüntülenir.



Şekil 17.1: Genişletilmiş okuyucu parametreleri

Açılır listenin varsayılan değeri şudur: `No extended parameters`. Bu, ek parametre gruplarını içe aktarmadığınız sürece mümkün olan tek olası değerdir.

Prosedür

İçe aktarılmış bir parametre grubunu uyumlu bir okuyucuya uygulamak için:

1. Cihaz Düzenleyici'sinde, cihaz ağacından okuyucuyu seçin
2. İlk özellik sekmesini seçin
3. **Extended reader parameters** (Genişletilmiş okuyucu parametreleri) listesinden gerekli parametre grubunu seçin
4. **Apply**'a (Uygula) veya simgesine tıklayın

17.3 Bir okuyucu parametre grubunu içe aktarma

Yalnızca cihaz hiyerarşisinin DMS seviyesindeki parametre dosyalarını içe aktarıp silebilirsiniz.

Ön koşullar

Kartlı geçiş sistemi için onaylanan bir parametre dosyasına gidin. Varsayılan olarak dosya türü şudur: `.ReaderConfigSave`

Prosedür

1. Cihaz Düzenleyicisi'nde DMS düğümüne sağ tıklayın ve bağlam menüsünden **Import reader parameter sets**'i (Okuyucu parametre kümelerini içe aktar) seçin.
   Import reader parameter sets (Okuyucu parametre kümelerini içe aktar) açılır penceresi görünür.
2. Dosya gezginini kullanarak **File**'a (Dosya) tıklayın ve parametre dosyasını bulun.
3. İstendiğinde, parametre dosyasının şifresini girin.
   Şifre doğruysa açılır pencerenin alt yarısı aşağıdaki bilgilerle doldurulur:

– Parametre grubunun uygulandığı okuyucu türlerinin listesi.
– Parametre kümesinin adı. Bu iletişim kutusunda düzenleyebilirsiniz.
– Parametre grubunu oluşturan sağladıysa serbest metin açıklama. Bu iletişim kutusuna açıklama ekleyebilir veya açıklamayı düzenleyebilirsiniz.

4. Kartlı geçiş sistemi tarafından olası gelecekte kullanılmak üzere ayarlanan parametreyi içe aktarmak için **Import**'a (İçe aktar) tıklayın.

– Parametre grubu içe aktarılır ve kartlı geçiş sisteminde saklanır.
– Bu, açılır pencerenin en üst kısmındaki mevcut parametre grupları listesine eklenir.

5. **Import reader parameter sets** (Okuyucu parametre gruplarını içe aktar) açılır penceresinden çıkmak için **Exit**'e (Çıkış) tıklayın.

17.4 Bir parametre grubunu okuyuculara uygulama

Giriş

Bir parametre grubunu kartlı geçiş sistemine aktarmak onun daha sonra kullanmak üzere depolanmasını sağlar, ancak bunu sistemdeki okuyuculara uygulamaz. Parametre grubunu uygulamak cihaz hiyerarşisindeki farklı seviyelerde gerçekleştirebileceğiniz fazladan bir adımdır:

– DMS
– MAC
– AMC

DMS, MAC veya AMC seviyesine bir parametre grubu uyguladığınızda bu grup, yalnızca grubun oluşturulduğu okuyucu türlerinin alt okuyucularına uygulanabilir. Başka hiçbir alt okuyucu etkilenmez.

Ön koşullar

Bir okuyucu parametre grubunu başarıyla içe aktardınız.

Prosedür

1. Cihaz Düzenleyicisi'nde, okuyucularının parametrelerini belirlemek istediğiniz bir okuyucuyu ya da cihaza (DMS, MAC veya AMC) sağ tıklayın.
2. Bağlam menüsünden **Manage reader parameter sets**'i (Okuyucu parametre gruplarını yönet) seçin.
3. Üstteki **Parameter sets for reader types** (Okuyucu türleri için parametre grupları) liste bölmesinde, uygulamak istediğiniz parametre grubunu seçin.
   İlgili okuyucular sol alt bölmede gösterilir: **Readers parametrizable with this parameter set** (Bu parametre grubuyla parametreleri belirlenebilen okuyucular).
4. **Readers parametrizable with this parameter set** (Bu parametre grubuyla parametreleri belirlenebilen okuyucular) listesinde, seçilen parametre grubunu uygulamak istediğiniz okuyucuları seçin.

– Okuyucu sayısı büyükse ekranı belirli bir MAC veya AMC'nin alt öğeleriyle sınırlamak için açılır listeleri kullanın.

5. Seçilen okuyucuları sağ alttaki **All readers parametrized with the selected parameter set** (Parametreleri seçilen parametre grubuyla belirlenen tüm okuyucular) bölmesine taşımak için ok düğmelerini kullanın.

Uyarı!
Uyumlu okuyucuları görüntüleme
Yalnızca parametre kümesiyle uyumlu olan okuyucular listelenir. **Show all readers** (Tüm okuyucuları göster) onay kutusunu işaretlerseniz başka parametre gruplarına sahip okuyucular da görüntülenir. Bunlar seçilen parametre grubu için salt okunur olarak işaretlenmeleri amacıyla gri bir arka plana sahiptir.

6. Açılır pencereyi kapatmak için **OK**'e (Tamam) tıklayın.

7. Geride, Cihaz Düzenleyicisi'nde **Apply**'a (Uygula) veya simgesine tıklayın.
Bu parametre açılır penceredeki **All readers parametrized with the selected parameter set** (Parametreleri seçilen parametre grubuyla belirlenen tüm okuyucular) listesinde bıraktığınız tüm okuyuculara uygulanır.

17.5 Okuyucu parametre gruplarını yönetme

Giriş
Cihaz hiyerarşisindeki farklı seviyelerde parametre gruplarının uygulamasını değiştirebilirsiniz:
– DMS
– MAC
– AMC
DMS, MAC veya AMC seviyesindeki değişiklikler yalnızca grubun oluşturulduğu okuyucu türlerine ait alt okuyuculara uygulanabilir. Başka hiçbir alt okuyucu etkilenmez.

Ön koşul
Bir okuyucu parametre grubunu başarıyla içe aktardınız.

Prosedür
1. Cihaz Düzenleyicisi'nde bir okuyucuya veya cihaza (DMS, MAC veya AMC) sağ tıklayın.
2. Bağlam menüsünden **Manage reader parameter sets**'i (Okuyucu parametre gruplarını yönet) seçin.
3. Üstteki **Parameter sets for reader types** (Okuyucu türleri için parametre grupları) liste bölmesinde, uygulamak istediğiniz parametre grubunu seçin.
– İlgili okuyucular sol alt bölmede listelenir: **Readers parametrizable with this parameter set** (Bu parametre grubuyla parametreleri belirlenebilen okuyucular).
– Parametre dosyasının daha önce uygulandığı okuyucular sağ alt bölmede listelenir: **All readers parametrized with the selected parameter set** (Parametreleri seçilen parametre grubuyla belirlenen tüm okuyucular).
4. İki listeden de okuyucular seçin. Okuyucuları sağ alttaki **All readers parametrized with the selected parameter set** (Parametreleri seçilen parametre grubuyla belirlenen tüm okuyucular) listesine taşımak ve buradan kaldırmak için ok tuşlarını kullanın.
– ÖNEMLİ: Bu prosedürdeki son adım için listeden çıkardığınız okuyucuları dikkatli bir şekilde not edin.
5. Yaptığınız değişiklikleri tamamladığınızda, açılır pencereyi kapatmak için **OK**'e (Tamam) tıklayın.

6. Yeniden Cihaz Düzenleyicisi'nde, **Apply**'a veya  simgesine tıklayın.

– Parametre grubu **All readers parametrized with the selected parameter set** (Parametreleri seçilen parametre grubuyla belirlenen tüm okuyucular) listesinde bıraktığınız tüm okuyuculara uygulanır.
– Listeden çıkardığınız okuyuculardan kaldırılır.

7. Listeden çıkardığınız tüm okuyucular için aşağıdakilerden birini yapın:

– Okuyucu donanımındaki DIP anahtarlarını kullanarak fabrika varsayılanlarına sıfırlayın.
– Bunlara farklı bir parametre grubu uygulayın.

Uyarı!
Bir parametre grubunun silinmesi onu kullanan okuyucuları yeniden yapılandırmaz. Silinen okuyucu yapılandırması, siz okuyucu donanımını sıfırlayana veya farklı bir parametre grubu uygulayana kadar kullanılan okuyucularda kalır.

17.6 Okuyucu parametre gruplarını silme

Yalnızca cihaz hiyerarşisinin DMS seviyesindeki parametre dosyalarını içe aktarıp silebilirsiniz.

Ön koşullar
En az bir parametre dosyası daha önce kartlı geçiş sisteminize aktarılmalıdır.

Prosedür

1. Cihaz Düzenleyicisi'nde DMS düğümüne sağ tıklayın ve bağlam menüsünden **Delete reader parameter sets**'i (Okuyucu parametre kümelerini sil) seçin.
   Delete reader parameter sets (Okuyucu parametre kümelerini sil) açılır penceresi görünür.
2. **Parameter sets for reader types** (Okuyucu türleri için parametre grupları) listesinden silmek istediğiniz parametre grubunu seçin.

– Açılır pencerenin sağ alt kısmında, o anda parametreleri seçilen parametre grubuyla belirlenen (yapılandırılan) tüm okuyucuların listesi görünür.
– Bu okuyucuları dikkatlice not edin, parametre grubunu sildikten sonra sıfırlanmaları veya yeniden yapılandırılmaları gerekecektir. Ayrıntılar için bu prosedürün son adımına bakın.

3. **Delete**'e (Sil) tıklayın
4. **Exit**'e (Çık) tıklayın
5. Yeniden Cihaz Düzenleyicisi'nde, **Apply**'a veya  simgesine tıklayın.
6. Silinen parametre grubunu kullanan tüm okuyuculara aşağıdakilerden birini yapın:

– Okuyucu donanımındaki DIP anahtarlarını kullanarak fabrika varsayılanlarına sıfırlayın.
– Bunlara farklı bir parametre grubu uygulayın.

Uyarı!
Bir parametre grubunun silinmesi onu kullanan okuyucuları yeniden yapılandırmaz. Silinen okuyucu yapılandırması, siz okuyucu donanımını sıfırlayana veya farklı bir parametre grubu uygulayana kadar kullanılan okuyucularda kalır.

18 Personel verileri için Özel Alanlar

Giriş

Personel için veri alanları birçok şekilde özelleştirilebilir:

- **Visible** (Görünür) olup olmadıkları, yani istemcide görüntülenip görüntülenmedikleri
- **Required** (Gerekli) olup olmadıkları, yani bir veri kaydının alandaki geçerli veriler olmadan depolanıp depolanmayacağı
- İçerdikleri değerlerin sistem içinde **Unique** (Benzersiz) olarak tutulması gerekip gerekmediği
- İçerdikleri veri türü (metin, tarih-saat, tam sayı vb.)
- İstemcide nerede (hangi sütunda, hangi satırda ve hangi sırada) görünecekleri
- Ne kadar büyük görünecekleri
- Verilerin standart raporlarda kullanılıp kullanılmayacağı ve nerede kullanılacağı

Elbette, yine de burada belirtilen tüm özelliklerle tamamen yeni veri alanları tanımlamak mümkündür.

18.1 Özel alanlara ön izleme yapma ve bunları düzenleme

İletişim yolu

- Main menu (Ana Menü) > **Configuration** (Yapılandırma) > **Options** (Seçenekler) > **Custom fields** (Özel alanlar)

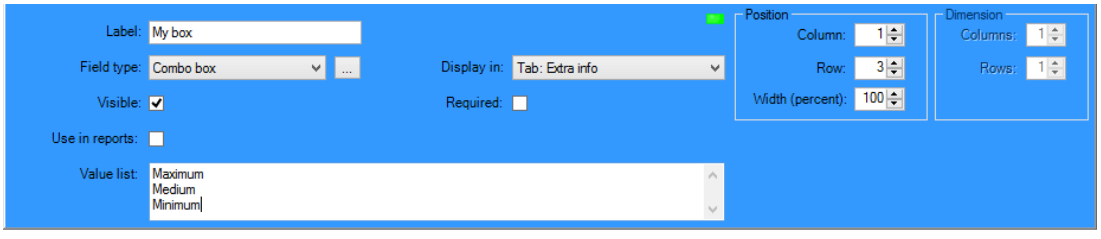
Ana pencere iki sekmeye ayrılmıştır

Genel bilgiler	Bu sekme ve alt sekmeleri (**Address (Adres), Contact (İletişim), Additional person data (Ek kişi verileri), Additional Company data (Ek Şirket verileri), Remarks (Açıklamalar), Card Control (Kart Kontrolü)** ve**Extra Info** (Ekstra Bilgiler) salt okunurdur ve verilerin istemci yazılımındaki hangi sekmelerde görüneceğine ilişkin kabaca bir WYSIWYG genel bakışı içerir.
Details (Ayrıntılar)	Bu sekmede, her önceden tanımlanmış veya kullanıcı tanımlı veri alanı için bir düzenleyici bulunur.

Mevcut veri alanlarını düzenleme

Custom fields (Özel alanlar) > **Details** (Ayrıntılar) sekmesindeki önceden veya kullanıcı tarafından tanımlanan her veri alanının niteliklerinin değiştirilebileceği kendi düzenleyici penceresi vardır.

Değiştirmek istediğiniz alanın düzenleyicisine tıklayın. Etkin düzenleyici vurgulanacaktır.



Özel alanların düzenlenebilir özellikleri aşağıdaki tabloda açıklanmıştır.

Etiket metni	Açıklama
Label (Etiket)	**Label** (Etiket) veri alanının istemcide görünen etiketidir. Sitenizde kullanılan terminolojiyi yansıtacak şekilde serbestçe yazılabilir.

Etiket metni	Açıklama
Field type (Alan tipi)	**Field type** (Alan tipi) verilerin tipidir ve operatörün istemcide giriş yapmak için kullanacağı iletişim kutusu kontrolünü belirler. Her alan tipi, geçerli tarihler, saatler, metin uzunlukları ve sayısal sınırları sağlamak amacıyla belirli giriş değerleri için tutarlılık kontrolleri sağlar. – **Text field** (Metin alanı) – İzin verilen karakter sayısını belirtmek için yanındaki üç nokta düğmesine tıklayın. – **Check box** (Onay kutusu) – **Date field** (Tarih alanı) – **Time** (Saat) – **Date-time field** (Tarih saat alanı) – **Combo box** (Birleşik kutu) – Sunulan metin alanındaki birleşik kutunuz için geçerli değerleri girin. Bunları virgül veya satır başı karakterleriyle ayırın. – **Numerical input** (Sayısal giriş) – Sunulan döndürme kutularındaki sayısal giriş için minimum ve maksimum değerlerinizi girin. – **Building control 1** (Bina kontrolü 1) ve **Building control 2** (Bina kontrolü 2) – Bunlar, burada yeniden etiketlenebilen (**Label** (Etiket) alanı) ve istemci kullanıcı arayüzündeki komutlara bağlanabilen özel kontrollerdir. Böylece, belirli kullanıcıların saha içerisinde kartlarıyla özel işlemler gerçekleştirmesine izin verebilirsiniz. Bu tür işlemlere, projektörlerin açılması veya özel ekipman kontrolü örnek verilebilir.
Visible (Görünür)	Veri alanının istemcide görünmesini önlemek için bu onay kutusunu temizleyin.
Unique (Benzersiz)	Bu alana girilen değerlerin benzersiz olduğundan emin olmak için bu onay kutusunu seçin. Ardından sistem veritabanında bu alan için zaten depolanmış olan değerin girişini reddeder. Örneğin personel numaralarının kişiler ve araç plakaları için benzersiz olması gerekir.
	Yeşil ışık, veri alanının o anda veritabanında **kullanılmadığı** anlamına gelir. Kırmızı ışık ise veri alanının o anda veritabanında kullanıldığını gösterir.
Display in (Şurada görüntüle)	Veri alanının görünmesi gereken istemci sekmesini seçmek için bu açılır listeyi kullanın.
Required (Gerekli)	Veri alanını zorunlu hale getirmek için bu onay kutusunu seçin. Örneğin, her personel kaydı için bir soyadı gereklidir. Soyadı olmadan veri kaydı saklanamaz. Düzenleyicinin, **Visible** (Görünür) onay kutusuyla gerekli bir veri alanının görünmez olarak ayarlanmasına izin vermeyeceğini unutmayın. İstemcide kullanım kolaylığı için, tüm gerekli alanların ilk sekmeye yerleştirilmesi kesinlikle tavsiye edilir.

Etiket metni	Açıklama
Position (Konum)	**Display in** (Şurada görüntüle) açılır listesinde adlandırılan sekmede yer alan veri alanını konumlandırmak için **Column** (Sütun) ve **Row** (Satır) döndürme kutularını kullanın. Düzenleyicinin, zaten kullanımda olan bir konumu seçmenize veya mevcut veri alanlarını çakıştırmanıza izin vermeyeceğini unutmayın. Metin alanları gibi belirli yeniden boyutlandırılabilir kontrollerin boyutunu ayarlamak için **Width (percent)** (Genişlik (yüzde)) döndürme kutusunu kullanın. %100 kontrolün, veri alanı etiketiyle henüz doldurulmamış olan yuvanın tamamını kaplayacağı anlamına gelir.
Dimension (Boyut)	**Display in** (Şurada görüntüle) açılır listesinde adlandırılan sekmede doldurulacak sütun ve satır sayısını belirtmek için **Column** (Sütun) ve **Row** (Satır) döndürme kutularını kullanın. Düzenleyicinin mevcut veri alanlarını çakıştırmanıza izin vermeyeceğini unutmayın.

Yeni veri alanları oluşturma ve düzenleme

Custom fields (Özel alanlar) > **Details** (Ayrıntılar) sekmesindeki önceden veya kullanıcı tarafından tanımlanan her veri alanının niteliklerinin değiştirilebileceği kendi düzenleyici bölmesi vardır.

New field'a (Yeni alan) tıklayarak kendi editörüyle yeni bir özel alan oluşturun. Etkin düzenleyici bölmesi vurgulanır.

Düzenleyici, mevcut veri alanlarını düzenlemek için aynı iletişim kontrollerine sahiptir, yukarıdaki tabloya bakın. Ayrıca fazladan iki öğe şunlardır:

Use in reports (Raporlarda kullan) (onay kutusu)	Yeni veri alanının standart raporlarda görünmesini sağlamak için bu onay kutusunu seçin.
Sequence number (Sıra numarası) (döndürme kutusu)	Sıra numarası, veri alanının standart raporlarda dolduracağı sütunu belirler.

Uyarı!

Sadece sıralama numaraları 1..10 o anda **Badge Designer** (Kimlik Kartı Tasarımcısı) ve **Reports** (Raporlar) ile adreslenebilir.

18.2 Veri alanlarına ilişkin kurallar

- Veri alanlarının konumu
  - Her alan sadece bir sekmede görünebilir.
  - Her özel alan herhangi bir seçilebilir sekmede görünebilir.
  - Alanlar, girişi **Display in** (Şurada görüntüle) açılır listesinde değiştirerek diğer sekmelere taşınabilir.
- Etiket herhangi bir metin içerebilir: Maksimum uzunluk 20 karakterdir.
- Özel metin alanları herhangi bir metin içerebilir: Maksimum uzunluk 2000 karakterdir.
- Herhangi bir alan gerekli bir alan haline getirilebilir, ancak **Visible** (Görünür) onay kutusu seçilmelidir.

Uyarı!
Verimli kullanabilmek için acil öneriler
Kişilerin verilerini depolamak için kullanmadan önce alan türlerini ve kullanım alanlarını kabul edip sonuçlandırın:
Her veri giriş alanı, belirli bir veritabanı alanına atanır, böylece veriler hem manuel olarak hem de rapor üreteçleri tarafından bulunabilir. Veritabanında özel alanlardaki veri kayıtları saklandıktan sonra, bu alanlar artık veri kaybı riski olmadan taşınamaz veya değiştirilemez.

19 Tehdit Seviyesi Yönetimini Yapılandırma

Giriş

Tehdit seviyesi yönetiminin amacı, etkilenen alan boyunca giriş davranışlarında acil bir değişiklik yaparak acil durumlara etkili bir şekilde müdahale etmektir.

19.1 Tehdit Seviyesi Yönetimine İlişkin Kavramlar

- **Threat** (Tehdit), bir kartlı geçiş sistemindeki girişlerin bazılarından veya tümünden hemen ve aynı anda müdahale gerektiren kritik bir durumdur.
- **Threat level** (Tehdit seviyesi), sistemin öngörülen bir duruma verdiği yanıttır. Her tehdit seviyesinin MAC girişlerinin her biri nasıl yanıt vereceğini bilecek şekilde dikkatlice yapılandırılması gerekir.
  Tehdit seviyeleri tamamen özelleştirilebilir, örneğin, tipik yüksek tehdit seviyeleri şu şekilde yapılandırılabilir:
  - **Lockout** (Dışarıda Bırakma): Yalnızca yüksek güvenlik seviyelerine sahip ilk müdahale edenler giriş yapabilir.
  - **Lockdown** (Kilitleme): Tüm kapılar kilitlenir. Yapılandırılan güvenlik seviyesinin altındaki tüm kimlik bilgileri için hem giriş hem de çıkış reddedilir.
  - **Evacuation** (Tahliye): Tüm çıkış kapılarının kilidi açılır.
- Tipik düşük tehdit seviyeleri şu şekilde yapılandırılabilir:
  - **Sports event** (Spor etkinliği): Spor sahalarının kapılarının kilidi açılır, diğer tüm alanların güvenliği sağlanır.
  - **Parents' evening** (Veli toplantısı): Yalnızca seçilen sınıflara ve ana girişe erişilebilir.
- **Threat alert** (Tehdit uyarısı), bir tehdit seviyesini tetikleyen bir alarmdır. Uygun yetkiye sahip kişiler ani bir eylemle, örneğin operatör kullanıcı arayüzü, donanım sinyali (ör. basmalı düğme) ile veya herhangi bir okuyucuya özel bir uyarı kartı göstererek bir tehdit uyarısı tetikleyebilir.
- **Security level** (Güvenlik seviyesi) kart sahipleri ve okuyucuların 0..100 arasında bir tam sayı olarak ifade edilen **Security profiles**'ının (Güvenlik profilleri) bir özniteliğidir. Her tehdit seviyesi Ana Giriş Kontrol Cihazı'nın (MAC) okuyucularını atanan güvenlik seviyelerine ayarlar. Ardından, bu okuyucular yalnızca güvenlik profillerinde eşit veya daha yüksek güvenlik seviyesine sahip kişilerin kimlik bilgilerine giriş izni verir.
- **Security profile** (Güvenlik profili) **Person type**'a (Kişi türü) (**Kişi güvenlik profili**), bir kapıya (**Kapı güvenlik profili**) veya bir okuyucuya (**Okuyucu güvenlik profili**) atanabilecek bir öznitelik koleksiyonudur. Güvenlik profilleri aşağıdaki kartlı geçiş davranışlarını düzenler:
  - Yukarıda tanımlandığı gibi kişi türü, kapı veya okuyucuya ilişkin **Security level** (Güvenlik seviyesi)
  - **Screening rate** (Tarama oranı). Rastgele taramanın bu kişi türü veya okuyucu tarafından tetiklenme olasılığının yüzdesi.

19.2 Yapılandırma işlemine genel bakış

Tehdit Seviyesi Yönetimi için, bu genel bilgilerden sonra ayrıntılı olarak açıklanan aşağıdaki yapılandırma adımları gereklidir

1. Cihaz Düzenleyici'de
   - Tehdit seviyelerini tanımlama
   - Kapı güvenlik profillerini tanımlama
   - Okuyucu güvenlik profillerini tanımlama
   - Kapı güvenlik profillerini girişlere atama
2. Sistem veri iletişim kutularında

- Kişi güvenlik profillerini tanımlama
- Kişi güvenlik profillerini kişi türlerine atama

3. Personel verileri iletişim kutularında
   - Kişi türlerini kişilere atama
   - Kişi türlerini kişi gruplarına atama

Tehdit seviyesi yönetimi başarılı bir şekilde yapılandırıldığında, alarmlar ve MAC'in cihaz durumları, Harita görünümü uygulamasından izlenerek kontrol edilebilir. Ayrıntılar için Harita görünümü için çevrimiçi yardım bölümüne bakın.

19.3 Cihaz düzenleyicideki yapılandırma adımları

Bu bölümde cihaz düzenleyicide gerekli olan ön koşul yapılandırma adımları açıklanmaktadır.

Uyarı!
Cihaz verileri bir tehdit seviyesi devredeyken cihaz düzenleyicisinde değiştirilemez.

19.3.1 Tehdit seviyesi oluşturma

Bu bölümde, sitenizde kullanılmak üzere tehdit seviyeleri oluşturma açıklanmaktadır. En fazla 15 adet oluşturulabilir.

İletişim yolu

- **Main menu** (Ana menü) >**Configuration** (Yapılandırma) > **Device data** (Cihaz verileri)

Prosedür

1. **Threat levels** (Tehdit seviyeleri) alt sekmesini seçin
   - Threat levels (Tehdit seviyeleri) tablosu görünür. Bu tablo, her biri bir ada, açıklamaya ve yapılandırıldıktan sonra tehdit seviyesini etkinleştirmek için kullanılan bir onay kutusuna sahip en fazla 15 tehdit seviyesi içerebilir.
2. **Please enter a name for the threat level** (Tehdit seviyesi için lütfen ad girin) ifadesini içeren satıra tıklayın
3. Sistem operatörlerine anlamlı gelecek bir ad girin.
4. (isteğe bağlı) **Description** (Açıklama) sütununa, bu tehdit seviyesi devredeyken girişlerin nasıl davranacağını belirten daha ayrıntılı bir açıklama girin.
5. Bu noktada **Active** (Etkin) onay kutusunu **seçmeyin**. Aşağıdaki bölümlerde açıklandığı gibi, bu tehdit seviyesine ait tüm diğer yapılandırma adımlarını tamamlayın.
6. Yeni tehdit seviyesini kaydetmek için (Kaydet) düğmesine tıklayın.

19.3.2 Kapı güvenlik profili oluşturma

Bu bölümde farklı kapı türleri için güvenlik profilleri oluşturma ve bir tehdit seviyesi girdiğinde bu profildeki tüm kapılar için durumu tanımlama konuları açıklanmaktadır.

İletişim yolu

- **Main menu** (Ana menü) >**Configuration** (Yapılandırma) > **Device data** (Cihaz verileri)

Ön koşullar

- En az bir tehdit seviyesi tanımlanmış olmalıdır
- Cihaz ağacında en az bir giriş yapılandırılmış olmalıdır.

Prosedür

1. **Door security profiles** (Kapı güvenlik profilleri) alt sekmesini seçin
   - Ana iletişim kutusu penceresi 2 bölmeye bölünür: **Selection** (Seçim) ve **Door security profile** (Kapı güvenlik profili) (varsayılan ad)
2. **New**'a (Yeni) tıklayın
   - Varsayılan bir ada sahip yeni bir kapı güvenlik profili oluşturulur
   - **Door security profile** (Kapı güvenliği profili) bölmesindeki **Threat level** (Tehdit seviyesi) bölmesi **State** (Durum) sütunundaki **undefined** (tanımlanmadı) değeriyle birlikte daha önce oluşturulan tehdit seviyeleriyle doldurulur.
3. **Door security profile** (Kapı güvenliği profili) bölmesinde, bu profilin atanacağı kapı türü için bir ad girin.
   - Yeni profil adı **Selection** (Seçim) bölmesinde görünür. İstenirse bu, söz konusu bölmede **Delete**'e tıklanarak yapılandırmadan silinebilir.
4. (İsteğe Bağlı) Operatörlerin profili doğru olarak atamasına yardımcı olmak için profile ait bir açıklama girin.
5. Bu profil turnikelere atanacaksa **Turnstile** (Turnike) onay kutusunu seçin.
   - Bu, farklı tehdit seviyelerindeki kapının hedef durumu (örneğin, tek başına girişe veya çıkışa izin verme veya ikisi birden) için ek seçenekler sağlar.
6. **Threat level** (Tehdit seviyesi) tablosunun **State** (Durum) sütununda, her tehdit seviyesi için söz konusu tehdit seviyesinin tetiklendiği bu profile ait tüm kapılarda uygun bir hedef durumu seçin.
7. Değişiklikleri kaydetmek için  (Kaydet) simgesine tıklayın.

Yapılandırmanızda bulunan kapı türleri kadar kapı güvenlik profili oluşturmak için prosedürü tekrarlayın. Tipik kapı türleri şunlar olabilir:
- Ana genel kapı
- Dışarıya tahliye erişimi
- Sınıflara giriş
- Spor sahasına genel giriş

19.3.3 Okuyucu güvenlik profili oluşturma

Bu bölümde farklı okuyucu türleri için güvenlik profillerinin nasıl oluşturulacağı açıklanmaktadır. Okuyucu güvenlik profilleri **her tehdit seviyesi** için aşağıdaki okuyucu özniteliklerini tanımlar:
- Bir kimlik bilgisinin okuyucuya erişebilmesi için gereken minimum güvenlik seviyesi.
- Tarama hızı, yani daha fazla güvenlik taraması için rastgele seçilecek kart sahiplerinin yüzdesi.
  - **Not**: Bir okuyucu güvenlik profilinde ayarlanan tarama hızı, okuyucunun kendisinde ayarlanan tarama hızını geçersiz kılar.

İletişim yolu

- **Main menu** (Ana menü) >**Configuration** (Yapılandırma) > **Device data** (Cihaz verileri)

Ön koşullar

- En az bir tehdit seviyesi tanımlanmış olmalıdır
- Cihaz ağacında en az bir giriş yapılandırılmış olmalıdır.

Prosedür

1. **Reader security profiles** (Okuyucu güvenlik profilleri) alt sekmesini seçin

- Ana iletişim kutusu penceresi 2 bölmeye bölünür: **Selection** (Seçim) ve **Reader security profile** (Okuyucu güvenlik profili) (varsayılan ad)

2. **New**'a (Yeni) tıklayın
   - Varsayılan bir ada sahip yeni bir okuyucu güvenlik profili oluşturulur
   - **Reader security profile**'daki (Okuyucu güvenlik profili) **Threat level** (Tehdit seviyesi) bölmesi **Security level** (Güvenlik seviyesi) ve **Screening rate** (Tarama hızı) sütunlarında her biri için **0** varsayılan değeriyle birlikte daha önce oluşturulan tehdit seviyeleriyle doldurulur.
3. **Reader security profile** (Okuyucu güvenliği profili) bölmesinde, bu profilin atanacağı okuyucu türü için bir ad girin.
   - Yeni profil adı **Selection** (Seçim) bölmesinde görünür. İstenirse bu, söz konusu bölmede **Delete**'e tıklanarak yapılandırmadan silinebilir.
4. (İsteğe Bağlı) Operatörlerin profili doğru olarak atamasına yardımcı olmak için profile ait bir açıklama girin.
5. **Threat level** (Tehdit seviyesi) tablosunun **Security level** (Güvenlik seviyesi) sütununda, her tehdit seviyesinde bir operatörün söz konusu tehdit seviyesi her tetiklendiğinde bu profile ait bir okuyucuyu çalıştırmak için sahip olması gereken minimum bir güvenlik seviyesi (0..100 arasında bir tam sayı) seçin.
6. **Threat level** (Tehdit seviyesi) tablosunun **Screening rate** (Tarama hızı) tablosunda her tehdit seviyesi için söz konusu tehdit seviyesi her tetiklendiğinde fazladan yapılan güvenlik kontrolleri için okuyucu tarafından rastgele seçilecek kart sahiplerinin yüzdesini seçin.
7. Değişiklikleri kaydetmek için  (Kaydet) simgesine tıklayın.

19.3.4 Kapı ve okuyucu güvenlik profillerini girişlere atama

Bu bölümde, kapı ve okuyucu güvenlik profillerinin belirli girişlerdeki kapılara ve okuyuculara nasıl atanacağı açıklanmaktadır.
İlk alt prosedür, atamak istediğiniz giriş kümesini tanımlamak ve filtrelemek, ikinci alt prosedür ise atamaları yapmaktır.
Ayrıca tanımladığınız çeşitli tehdit seviyeleriyle ayarlanacaklarından seçilen girişlerin durumları, güvenlik seviyeleri ve tarama hızlarına ön izleme yapabilirsiniz.

İletişim yolu

- **Main menu** (Ana menü) >**Configuration** (Yapılandırma) > **Device data** (Cihaz verileri)

Ön koşullar

- En az bir tehdit seviyesi tanımlanmış olmalıdır
- Cihaz ağacında en az bir giriş yapılandırılmış olmalıdır.

Prosedür

1. Cihaz ağacında **DMS**'i (cihaz ağacının kökü) seçin
2. Ana iletişim kutusunda, **Threat level management**'ı (Tehdit seviyesi yönetimi) seçin.
   - Ana iletişim kutusu bölmesinde birkaç alt sekme yer alır.

1. alt prosedür: Atama için girişleri seçme

1. **Entrances** (Girişler) alt sekmesini seçin
   - Ana iletişim penceresi 2 bölmeye ayrılır: **Filter conditions** (Filtre koşulları) ve o ana kadar sistemde oluşturulan tüm girişlerden oluşan bir tablo.
2. (İsteğe Bağlı) **Filtre koşulları** bölmesinde, iletişim kutusunun alt yarısında yer alan tabloda görünen giriş kümesini daraltmak için kriterler girin, örneğin;

- Tabloda **Inbound readers** mı (Gelen okuyucular), **Outbound readers** mı (Giden okuyucular) ve/veya **Doors**'un (Kapılar) mu göründüğünü belirleyen onay kutularını seçin veya temizleyin.
- Tabloda belirtilen tüm girişler, alanlar, profil adları veya okuyucu adlarının adında görünmesi gereken karakter dizelerini girin.
- Henüz yapılandırılmayan kapıların ve okuyucuların da tabloda görünmesi gerekip gerekmediğini belirleyen onay kutusunu seçin veya temizleyin

3. Entrances (Girişler) listesini filtrelemek için **Apply filter**'a (Filtre uygula), filtre kontrollerini yeniden varsayılan değerlerine ayarlamak için **Reset filter**'a (Filtreyi sıfırla) tıklayın.

2. alt prosedür: Seçilen girişlere güvenlik profilleri atama

Ön koşul: Atanacak girişlerin tanımlanmış olması ve iletişim kutusunun alt yarısındaki tabloda görünmesi gerekir.

Her girişin genellikle bir kapı veya bariyer ile bir veya daha fazla kart okuyucudan oluştuğunu unutmayın. Ancak **Assembly points** (Montaj noktaları) gibi bazı uzmanlara yönelik giriş türlerinde bunlar bulunmayabilir.

1. **Door or reader security profile** (Kapı veya okuyucu güvenlik profili), atamak istediğiniz kapıya veya okuyucuya karşılık gelen hücreye tıklayın.
2. Hücrenin açılır listesinden bir kapı veya okuyucu güvenlik profili seçin.

(İsteğe Bağlı) Tehdit seviyelerinde kapı ve okuyucuların davranışına ön izleme yapma

Tablonun sağ tarafındaki sütunlar salt okunurdur. **Select threat level for details** (Ayrıntılar için tehdit seviyesi seçin) listesinden seçilen tehdit seviyesi devredeyse tablodaki kapılar ve okuyucuların kilit durumunu (**Mode** (Mod)), **Security level**'ını (Tehdit seviyesi) ve **Screening rate**'ini (Tarama hızı) gösterirler.

Ön koşul: Ön izleme yapmak istediğiniz girişlerin tanımlanmış olması ve iletişim kutusunun alt yarısındaki tabloda görüntülenmesi gerekir.

- **Select threat level for details** (Ayrıntılar için tehdit seviyesi seçin) listesinden ön izleme yapmak istediğiniz tehdit seviyesini seçin.

⇨ Tabloda kapıların kilitlenme durumu (**Mode** (Mod)), **Security level** (Güvenlik seviyesi) ve **Screening rates** (Tarama hızları) seçilen tehdit seviyesi devredeyken olacağı gibi görüntülenir.

19.3.5 Bir donanım sinyaline tehdit seviyesi atama

Bu bölümde, bir tehdit uyarısını tetiklemek veya iptal etmek için bir donanım giriş sinyalinin nasıl atanacağı açıklanmaktadır.

İletişim yolu

– **Main menu** (Ana menü) >**Configuration** (Yapılandırma) > **Device data** (Cihaz verileri)

Ön koşullar

– En az bir tehdit seviyesi tanımlanmış olmalıdır
– Cihaz ağacında en az bir giriş yapılandırılmış olmalıdır.

Prosedür

1. Cihaz ağacında, giriş sinyallerini atamak istediğiniz AMC kontrol cihazının altından bir **giriş** seçin.
2. Ana iletişim penceresinde **Terminals** (Terminaller) sekmesini seçin.
   – Girişler ve sinyaller tablosu görüntülenir.
3. Atamak istediğiniz sinyalin satırında **Input signal** (Giriş sinyali) hücresine tıklayın.

- Açılır liste **Threat level: Deactivate** (Tehdit seviyesi: Devre dışı bırak) komutunun yanı sıra
  daha önce tanımladığınız her tehdit seviyesi için bir **Threat level:** `<name>` (Tehdit seviyesi) içerir.
- **Threat level: Deactivate** (Tehdit seviyesi: Devre dışı bırak) komutu o anda devrede olan her türlü tehdit seviyesini iptal eder.

4. Komutları istediğiniz giriş sinyallerine atayın.
5. Değişiklikleri kaydetmek için  (Kaydet) simgesine tıklayın.

Uyarı!
DM 15 kısıtlaması
Kapı modeli 15 (DIP/DOP) şu anda bir tehdit seviyesi tetiklemek için kullanılamaz.

19.4 Sistem verileri iletişim kutularındaki yapılandırma adımları

Bu bölümde, **Person security profiles**'ın (Kişi güvenlik profilleri) nasıl oluşturulacağı ve bunların **Person types**'a (Kişi türleri) nasıl atanacağı açıklanmaktadır.

19.4.1 Kişi güvenlik profili oluşturma

İletişim yolu

- **Main menu** (Ana menü) > **System data** (Sistem verileri) > **Person security profile** (Kişi güvenlik profili)

Ön koşullar

Kişi güvenlik profilleri, sistemin kritik durumlarda çalışması bakımından önemli sonuçlara sahip olacaklarından dikkatli planlama ve belirtim gerektirir.

Prosedür

1. İletişim kutusu zaten veri içeriyorsa temizlemek için  (Yeni) simgesine tıklayın.
2. Security profile name (Güvenlik profili adı) metin alanındaki yeni profil için bir ad girin:
3. (İsteğe Bağlı) Operatörlerin profili doğru olarak atamasına yardımcı olmak için profile ait bir açıklama girin.
4. **Security level** (Güvenlik seviyesi) kutusuna 0 ile 100 arasında bir tam sayı girin.
   - Kart sahibinin bir girişi kullanmak için yetkilendirilmesi kaydıyla, güvenlik seviyesi o anda 100 olarak ayarlanmış olsa da, 100 herhangi bir okuyucuda giriş hakkı kazanmak için yeterlidir
   - Aksi takdirde bir kart sahibinin kişi güvenlik profilindeki güvenlik seviyesi okuyucunun geçerli güvenlik seviyesine eşit veya bundan büyük olmalıdır.
5. **Screening rate** (Tarama hızı) kutusuna 0 ile 100 arasında bir tam sayı girin.
   - **Not**: Kişi profilinin tarama hızı, okuyucu profilinin tarama hızına göre ikinci derecededir. Aşağıdaki tabloda iki profil tarama hızı arasındaki etkileşim açıklanmaktadır.
6. Değişiklikleri kaydetmek için  (Kaydet) simgesine tıklayın.

Kişi ve okuyucu güvenlik profilleri için tarama hızları arasındaki etkileşim

Reader security profile R'deki (Okuyucu güvenlik profili) tarama hızı (%)	Person security profile P'deki (Kişi güvenlik profili) tarama hızı (%)	Ek güvenlik kontrolleri için kişi seçildi mi?
0	Herhangi bir	**No** (Hayır)
100	Herhangi bir	**Yes** (Evet)
1..99	0	**No** (Hayır)
1..99	100	**Yes** (Evet)
1..99	1..99	**Possibly** (Olabilir) Olasılık = MAX(R,P)

19.4.2 Kişi türüne kişi güvenlik profili atama

İletişim yolu

– **Main menu** (Ana menü) > **System data** > **Person Type** (Kişi Türü)

Prosedür

Not: Geçmişteki nedenlerle buradaki **Employee ID** (Çalışan Kimliği) **Person type** (Kişi türü) ile eş anlamlıdır.

1. **Predefined employee IDs** (Önceden tanımlanan çalışan kimlikleri) veya **User-defined employee IDs** (Kullanıcı tarafından tanımlanan çalışan kimlikleri) tablosunda istediğiniz kişi türüne denk gelen **Security profile name**'i (Güvenlik profili adı) seçin.
2. Açılır listeden bir kişi güvenlik profili seçin.
   – Kişi güvenlik profili gerektiren tüm kişi türleri için bu prosedürü tekrarlayın
3. Atamalarınızı kaydetmek için  (Kaydet) simgesine tıklayın

19.5 Personel verileri iletişim kutularındaki yapılandırma adımları

Bu bölümde, sistemde oluşturulan yeni **Person** (Kişi) kayıtlarının nasıl oluşturulduğu ve nasıl **Person type**'ları (Kişi türleri) aracılığıyla **Person security profile** (Kişi güvenlik profili) aldıkları açıklanmaktadır.

İletişim yolları

– **Main menu** (Ana menü) > **Personnel data** (Personel verileri) > **Persons** (Kişiler)
– **Main menu** (Ana menü) > **Personnel data** (Personel verileri) > **Group of Persons** (Kişi Grubu)

Not: Geçmişteki nedenlerle buradaki **Employee ID** (Çalışan Kimliği) **Person type** (Kişi türü) ile eş anlamlıdır.

Prosedür

Sistemde oluşturan tüm **Person** (Kişi) kayıtlarında bir **Person type** (Kişi türü) olması gerekir.

1. Sistemin yalnızca **Main menu** (Ana menü) > **System data** (Sistem verileri) > **Person Type** (Kişi Türü) iletişim kutusunda yer alan **Person security profile** (Kişi güvenlik profili) ile ilişkilendirilen **Person types** (Kişi türleri) atamasını sağlayın.
2. **Person security profiles**'ın (Kişi güvenlik profilleri) ilişkilendirilmesi ve **Person** (Kişi) kayıtlarının oluşturulması hakkındaki ayrıntılar için aşağıdaki bağlantılara tıklayın.

Bkz.

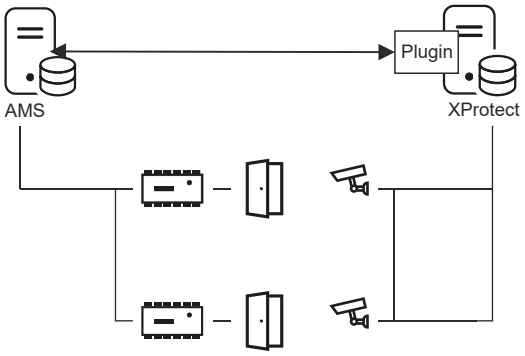
- *Kişi türüne kişi güvenlik profili atama, sayfa 138*
- *Personel verilerini oluşturma ve yönetme, sayfa 188*

20 Milestone XProtect'i AMS'yi kullanacak şekilde yapılandırma

Giriş

Bu bölümde, AMS'nin kartlı geçiş özelliklerini kullanmak için Milestone XProtect'in nasıl yapılandırılacağı açıklanmaktadır.

AMS tarafından sağlanan ancak XProtect sunucusuna kurulan bir eklenti olayları ve komutları AMS'ye iletir ve sonuçları yeniden XProtect'e gönderir.



Bu yapılandırma aşağıdaki bölümlerde açıklanan 3 aşamaya sahiptir:

- AMS genel sertifikasını XProtect sunucusuna kurma.
- AMS eklentisini XProtect sunucusuna kurma.
- AMS'yi XProtect uygulamasında yapılandırma.

Uyarı!

Farklı kaynaklardan gelen eklentilerin potansiyel uyumsuzluğu

Milestone XProtect eklentileri korumalı değildir, diğer bir deyişle birbirinden tamamen yalıtılmış değildir. Bu nedenle, aynı XProtect sunucusunda farklı .NET sürümlerine ait birden çok eklentiyi ve bunların bağlılıklarını çalıştırırsanız yazılım hataları oluşabilir. BOSCH, yalnızca kurulu olan tek eklenti AMS eklentisiyse eklentinin doğru çalışmasını garanti edebilir.

Ön koşullar

- AMS kurulmuş ve lisanslanmış olmalıdır.
- XProtect, aynı bilgisayarda veya kendi bilgisayarında kurulmuş ve lisanslanmış olmalıdır.
- İki sistem arasında bir ağ bağlantısı bulunmalıdır.

AMS genel sertifikasını XProtect sunucusuna kurma

Bu prosedürün yalnızca AMS farklı bir bilgisayarda çalışıyorsa gerekli olduğunu unutmayın.

1. Sertifikayı AMS sunucusundan
   `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Certificates\Access Management System Internal CA.cer`
   XProtect sunucusuna kopyalayın.
2. XProtect sunucusunda sertifika dosyasına çift tıklayın.
   Sertifika sihirbazı görünür.
3. **Install Certificate...**'a (Sertifikayı Yükle) tıklayın
   Sertifika İçe Aktarma Sihirbazı görünür.

4. **Local Machine**'i (Yerel Makine) **Store Location** (Saklama Konumu) olarak seçin ve **Next**'e (İleri) tıklayın
5. **Place all certificates...**'ı (Tüm sertifikaları yerleştir) seçin
6. **Browse...**'a (Göz At) tıklayın
7. **Trusted Root Certification Authorities**'i (Güvenilir Kök Sertifika Yetkilileri) seçin ve **OK**'e (Tamam) tıklayın
8. **Next**'e (İleri) tıklayın
9. Ayarların özetini gözden geçirin ve **Finish**'e (Bitir) tıklayın

AMS eklentisini XProtect sunucusuna kurma

1. Kurulum dosyasını
   `AMS XProtect Plugin Setup.exe`
   AMS kurulum ortamından XProtect sunucusuna kopyalayın.
2. Dosyayı, XProtect sunucusunda çalıştırın.
   Kurulum sihirbazı görünür.
3. Kurulum sihirbazında, AMS XProtect Eklentisi'nin kurulum için işaretlendiğinden emin olun ve **Next**'e (İleri) tıklayın.
   Son Kullanıcı Lisans Sözleşmesi görüntülenir. Devam etmek istiyorsanız sözleşmeyi kabul etmek için **Accept**'e (Kabul et) tıklayın.
4. Sihirbaz, eklenti için varsayılan kurulum yolunu görüntüler. Varsayılan yolu kabul etmek için **Next**'e (İleri) veya **Next**'e (İleri) tıklamadan önce değiştirmek için **Browse**'a (Göz at) tıklayın.
   Sihirbaz, AMS XProtect eklentisini yüklemek üzere olduğunu onaylar.
5. **Install**'a (Kur) tıklayın
6. Kurulumun tamamlandığına ilişkin onayı bekleyin ve **Finish**'e (Bitir) tıklayın.
7. **Milestone XProtect Event Server** adındaki Windows hizmetini yeniden başlatın.

AMS'yi XProtect uygulamasında yapılandırma

1. XProtect Management uygulamasında **Advanced Configuration** (Gelişmiş Yapılandırma) > **Access Control**'e (Kartlı Geçiş) gidin
2. **Access Control**'a (Kartlı Geçiş) sağ tıklayın ve **Create new...**
   'ı (Yeni oluştur) seçin. Eklenti sihirbazı görünür.
3. Eklenti sihirbazına aşağıdaki bilgileri girin:
   - **Name** (Ad): Bu AMS-XProtect entegrasyonunu XProtect sistemindeki diğer entegrasyonlardan ayırt etmek için bu entegrasyona ilişkin açıklama
   - **Integration plug-in** (Entegrasyon eklentisi): `AMS - XProtect Plugin` (Bu ad, eklenti başarıyla kurulduktan sonra açılır listede yer alır)
   - **AMS API discovery endpoint** (AMS API bulma uç noktası): `44347`'nin AMS API'sı kurulurken seçilen varsayılan port olduğu `https://<hostname of the AMS system>:44347/`
     .
   - **Operator name** (Operatör adı): XProtect kameraların eşleneceği kapıları çalıştırmak için en düşük izinlere sahip bir AMS operatörünün kullanıcı adı.
   - **Operator password** (Operatör şifresi): Söz konusu operatörün AMS şifresi.
4. **Next**'e (İleri) tıklayın
   AMS eklentisi belirttiğiniz AMS sunucusuna bağlanır ve bulduğu kartlı geçiş öğelerini (kapılar, birimler, sunucular, olaylar, komutlar ve durumlar) gösterir.

5. İlerleme çubuğunun sonuna gelindiğinde, **Next**
   'e (İleri) tıklayınAssociate cameras (Kameraları ilişkilendir) sihirbazı sayfası görüntülenir.
6. Kameraları kapılarla ilişkilendirmek için, kameraları **Cameras** (Kameralar) listesinden **Doors** (Kapılar) listesindeki giriş noktalarına sürükleyin.
7. Tamamladığınızda **Next**'e (İleri) tıklayın.
   XProtect yapılandırmayı kaydeder ve ne zaman başarıyla kaydettiğini onaylar.

21 Otis Compass'i Entegre Etme

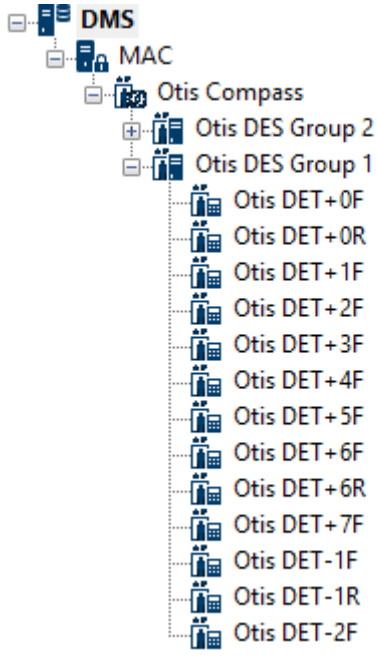
Giriş

Compass, Otis Elevator Company'nin Hedef Yönetim Sistemidir. İşlevi, hedeflerine mümkün olduğunca verimli bir şekilde ulaşabilmeleri için asansörleri yolculara göndererek birden fazla asansör grubunu yönetmektir. Gerekli verileri sağlamak için yolcuların artık **Yukarı** veya **Aşağı** tuşlarına basması gerekmeyecek ancak kart okuyucu, dokunmatik ekran veya tuş takımı terminallerinde hedeflerini isteyeceklerdir.

Bosch kartlı geçiş sistemleriyle entegrasyon güvenliğe katkıda bulunur. Yolcular, çalışma sırasındaki kimlik bilgilerine ve zaman modellerine bağlı olarak kendi evlerinin bulunduğu katlar ve diğer yetkili hedeflere verimli bir şekilde ulaştırılır. Sistem, yolcunun yetki profillerinde bulunmayan katlara yönelik veya geçerli zaman modeli dışındaki bir saatteki istekleri kabul etmez.

Compass sisteminin donanım topolojisi

Bir Compass sisteminin donanımı, Cihaz Düzenleyicisi'nde tek bir MAC'in altında 3 katmanlı bir hiyerarşi olarak yukarıdan aşağıya doğru yapılandırılır.



Yukarıdaki hiyerarşi şunları gösterir:
Özel bir MAC'teki bir **Otis Compass** sistemi
Bir **DES** ile yönetilen tek bir asansör grubu
Her biri -2 ila +7 arasında kat numarasına ve ön veya arka kapıları ifade eden F veya R harfine sahip bir dizi terminal (**DET**).

Birinci katman: (Otis Compass)
Hedef yönetim sistemi. Her **Compass** sistemi en fazla 8 asansör grubunu yönetebilir.
Parametreler: Kat aralığı,
ağ adresleri,
port numaraları ve zaman aşımları.

İkinci katman: (Otis DES/DER)
Her biri 1 veya 2 fiziksel cihazdan oluşan mantıksal bir Hedef Giriş Sunucusu (DES) tarafından yönetilen en fazla 8 asansör grubu.
Ayrıca Hedef Giriş Yeniden Yönlendiricileri (DER) olarak da bilinen optimizasyon için bu katmanda en fazla 2 adet isteğe bağlı cihaz bulunabilir.
Parametreler: Asansör grubu başına 1 grup kimliği.
Cihaz başına 1 IP adresi.
Asansör kapıları bulunan katlar ve bunlara herkesin erişip erişemeyeceği.

Üçüncü katman: Otis DET
Hedef Giriş Terminalleri (DET)
Parametreler: Terminal başına 1 IP adresi.
Her terminal için asansör kapıları bulunan erişilebilir katlar.

Kartlı geçiş sisteminde entegrasyona genel bakış

Kartlı geçiş sisteminin yöneticileri, daha sonra şu bölümde ayrıntılı olarak açıklanan aşağıdaki aşamalarda Compass'i entegre edebilir:

1. Cihaz Düzenleyicisi'nde tek bir MAC'te Compass donanımını yapılandırın.
2. Ana kat gibi OTIS'e özel kart sahibi özellikleri için özelleştirilmiş alanları yapılandırın.
3. Belirli asansör hedeflerine erişimi yöneten yetki profilleri oluşturun.
4. Yetki profillerini ilgili kart sahiplerine atayın

21.1 Bir Compass sistemini Cihaz Düzenleyicisi'nde yapılandırma

Bu bölümde, Cihaz Düzenleyicisi'nde bir Otis Compass sistemini yapılandırma adımları açıklanmaktadır.

İletişim yolu

– **Main menu** (Ana menü) >**Configuration** (Yapılandırma) > **Device data** (Cihaz verileri)

21.1.1 1. Katman: Compass sistemini ayarlama

1. Katman prosedürü: Compass sistemini ayarlam

1. Cihaz Düzenleyicisi ağaç görünümünde istediğiniz MAC'i seçin
2. Sağ tıklayın ve **New Otis Compass**'i (Yeni Otis Compass) seçin. Özellikler sayfasında 2 sekme bulunur.
   – **Otis Compass**
   – **Floors** (Katlar)
3. **Otis Compass** sekmesinde ayarlanacak en önemli parametreler şunlardır:
   – **Name** (Ad) (cihaz ağacında görünmesi gereken ad)
   – **MAC IP-Address** (MAC IP adresi) (Compass sisteminin MAC ile iletişim kurduğu özel bir ağ kartında Compass sistemine ait geri çağırma IP adresi).
   NOT: Bu, MAC'in kendi IP adresi **değildir**.
   – **Division** (Bölüm) (yalnızca bölümler lisanslandırılmış ve kurulumunuzda kullanılıyorsa)

Uzman teknik destek ekibi tarafından değiştirilmesi söylenmedikçe, kalan parametreleri varsayılan değerlerinde bırakın. Bunlar, aşağıdaki tabloda kısaca açıklanmaktadır:

Parametre	Varsayılan değer	Açıklama
MC grup adresi	234.46.30.7	Çok noktaya yayın grubunun IP adresi
Uzak DES/DER için MC portu Yerel DES/DER için MC portu	48307 47307	Çok noktaya yayın portları
Uzak DES/DER için UDP portu Yerel DES/DER için UDP portu	46303 45303	DES ve DER cihazları için UDP portu
Uzak DET için UDP portu Yerel DET için UDP portu	45308 46308	DET cihazları için UDP portları
Çoklu yayın canlı yayına geçme süresi (TTL)	5 saniye	

Parametre	Varsayılan değer	Açıklama
Sinyal aralığı	1 saniye	Sinyaller arasındaki süre. Bu sinyaller bir cihazın "canlı", çalışır durumda olduğu diğer cihazları gösterir
Maks. kaçırılan sinyal sayısı	3	Bir cihaz "ölü" (artık çalışmıyor) kabul edilmeden önce kaçırabilecek sinyal sayısı
Mesaj zaman aşımı	1 saniye	
Mesaj yeniden deneme sayısı	3	

1. **Floors** (Katlar) sekmesinde, **Change floor range**'e (Kat aralığını değiştir) tıklayın
2. Otis Compass sisteminin tüm asansör gruplarının hizmet vereceği en alt ve en üst katların numaralarını girin.
   – Maksimum aralık -127 ile +127 arasındadır.
3. Değişiklikleri kaydetmek için  (Kaydet) simgesine tıklayın.

21.1.2 2. Katman: Asansör grupları, DES ve DER cihazları

2. Katman prosedürü: Asansör gruplarını (DES/DER cihazları) ayarlama
Giriş
DES (Hedef Giriş Sunucusu), asansör grubunu yöneten bilgisayardır. İstenirse, ayrı IP adreslerine sahip iki fiziksel DES cihazı yük devri özelliğine sahip mantıksal bir DES'te birleştirilebilir.
DER (Hedef Girişi Yeniden Yönlendiricisi) asansör gruplarını bağlar ve DET'lerin binadaki ortak bir giriş noktasında, örneğin lobide binadaki her kat için hedef isteklerini kabul etmesini sağlar. DER, yük devri modunda çalışacak şekilde yapılandırılmamıştır.

Cihaz ağacında DES cihazları oluşturma:
1. Cihaz Düzenleyicisi ağaç görünümünde istediğiniz Otis Compass'i seçin
2. Sağ tıklayın ve **New Otis DES**'i (Yeni Otis DES) seçin. Özellikler sayfasında 2 sekme bulunur:
   – **Otis DES**
   – **Floors** (Katlar)
3. **Otis DES** sekmesinde aşağıdaki parametreleri ayarlayın:
   – **Name** (Ad): Cihaz ağacında görünmesi gereken ad.
   Daha sonra yapılandırma işleminde DES ve DET cihazlarını yapılandıranlar için net yön sağlayacak sistematik bir adlandırma şeması kullanın.
   – **Description:** (Açıklama) (isteğe bağlı) cihazın serbest metin açıklaması.
   – **Group:** (Grup) 1-10 arasında bir tam sayıdır**.** Bu tam sayının tüm asansör grupları (DES/DER cihazları tarafından atanır) arasında bu Otis Compass sistemi içinde benzersiz olmasını sağlayın. Aynı **Group** (Grup) numarasını birden fazla kez kullanıyorsanız cihaz düzenlemelerinizi kaydedemezsiniz.
   – **1st IP address:** (1. IP adresi) Bu DES cihazının IP adresi.

- **2nd IP address:** (2. IP adresi) Bu DES'in yedek bir ikizi varsa IP adresini buraya girin.
- **Division** (Bölüm) (yalnızca bölümler lisanslandırılmış ve kurulumunuzda kullanılıyorsa)

Floors (Katlar) sekmesinde, 1. Katman (Compass sistemi) için tanımlanan katlar düzenlenebilir hücrelerden oluşan bir tablo olarak sunulur.

Cihaz ağacında DER cihazları oluşturma:
DER cihazları DES cihazlarıyla neredeyse aynı şekilde oluşturulur. Tek fark, bir DER'nin hiçbir yük devri cihazına ihtiyacı olmamasıdır, böylece **2nd IP address** (2. IP adresi) için bir parametreye sahip olmaz.

Örnek asansör grubu.
Aşağıdaki örnekte, ön ve arka kapıları olan 10 katlı bir asansör grubu için genel olarak erişilebilen zemin ve 6. katlar gösterilmektedir.

OTIS DES | Floors

Highest floor: 7

Lowest floor: -2

Change floor range

Floor number	Name	Description	Front door	Front door publicly accessible	Rear door	Rear door publicly accessible
7	VIP	CxO floor	☑	☐	☐	☐
6	Restaurant	Public	☑	☑	☑	☑
5	Offices-4	Staff	☑	☐	☐	☐
4	Offices-3	Staff	☑	☐	☐	☐
3	Offices-2	Staff	☑	☐	☐	☐
2	Offices-1	Staff	☑	☐	☐	☐
1	Conference	Invited visitors	☑	☐	☐	☐
0	Lobby	Public	☑	☑	☑	☑
-1	Maintenance	Restricted	☑	☐	☑	☐
-2	Servers	Restricted	☑	☐	☐	☐

1. **Front door** (Ön kapı) sütununda, asansörün ön kapısının kullanımını sunduğu tüm katların onay kutularını seçin.
2. Mümkünse **Rear door** (Arka kapı) sütunu için de benzer onay kutularını seçin.
3. **Genel olarak erişilebilen Front door** (Ön kapı) sütunu, kısıtlamasız olarak tüm asansör yolcularının erişebildiği katların onay kutularını seçin.
4. Mümkünse **genel olarak erişilebilen Rear door** (Arka kapı) sütunu için onay kutularını benzer şekilde seçin.
5. (isteğe bağlı) **Otis Compass** seviyesinde ayarlanan kat aralığını daha da kısıtlamak için bu sekmedeki **Change floor range**'e (Kat aralığını değiştir) tıklayın.
6. **Name** (Ad) ve **Description** (Açıklama) sütunlarındaki varsayılan adların üzerine anlamlı alternatifler yazdırın.
7. Değişiklikleri kaydetmek için (Kaydet) simgesine tıklayın.

21.1.3 3. Katman: DET cihazları

3. Katman prosedürü: Terminalleri ayarlama (DET cihazları)
Giriş:
Bir DET (DEC (Hedef Giriş Bilgisayarı) olarak da bilinir) fiziksel kimlik bilgilerini veya PIN kodlarını okur. Bir DET, bir asansörün ön ceya arka kapısının dışında veya asansör kabininin içinde belirli bir kata yerleştirilebilir.

Cihaz ağacında DET cihazları oluşturma:
1. Cihaz Düzenleyicisi ağaç görünümünde istediğiniz Otis DES/DER cihazını seçin.
2. Sağ tıklayın ve **New Otis terminal**'i (Yeni Otis terminali) seçin.
   – **Create Otis terminals** (Otis terminalleri oluştur) açılır penceresi görünür
3. Bu DES/DER'de yapılandırmak istediğiniz terminallerin sayısını girin.
4. Varsayılan değerleri kabul edin veya IP adresinin dört sekizli değeri için yeni başlangıç değerleri girin.
   – Herhangi bir sekizli ancak genllikle 4. için sekizli değerini artırarak sistemin her terminal için benzersiz bir IP adresi yapılandırmasını istiyorsanız **Automatic increment** (Otomatik artış) onay kutusunu seçin.
5. **OK**'e (Tamam) tıklayın.
   – Cihaz ağacında istediğiniz sayıda DET cihazı oluşturulur.
   – IP adresleri önceki adımda belirlenen şekilde artırılır.

DET cihazlarını yapılandırma
Her DET'e ilişkin özellikler sayfasında 2 sekme bulunur:
– **Otis terminal** (Otis terminali)
– **Floors** (Katlar)
1. **Otis terminal** (Otis terminali) sekmesinde aşağıdaki parametreleri ayarlayın:
   – **Name:** (Ad) Cihaz ağacında görünmesi gereken ad
   – **Description** (Açıklama) (isteğe bağlı) Cihazın serbest metin açıklaması.
   – **IP address** (IP adresi) Bu DET cihazının IP adresi
   – **Operational mode:** (Çalışma modu) `1..4`
   Bu, terminalin asansör yolcusundan hedefleri nasıl istediğini belirler ve istekleri doğrulama için DES/DER'e geçirir. Aşağıdaki tabloda ayrıntılar verilmiştir:

Op. modu	Açıklama	Davranış
1	Varsayılan kat	(Varsayılan çalışma modu) Yolcu kendi kimlik bilgilerini sunar veya bir PIN kodu girer. Kimlik bilgileri veya PIN geçerliyse ve yolcu başka giriş yapmazsa DET, DES'den, yolcunun varsayılan veya "ana" katını ister. Yolcu farklı bir hedef kat girerse DET söz konusu hedefi DES'ten ister.
2	Yetki verilen katlara giriş	Yolcu kendi kimlik bilgilerini sunar veya bir PIN kodu girdikten sonra bir hedef kat girer. DET, DES'ten söz konusu hedefi ister. Kartlı geçiş sistemi istenen hedefe giriş izni verir veya vermez.
3	Hedef katın kullanıcı tarafından girilmesi	Yolcu bir hedef kat girer. Hedefe genel olarak erişilebiliyorsa DET, hedefi DES'ten ister. Aksi takdirde DET, yolcudan kimlik bilgilerini doğrulama için sunmasını ister.

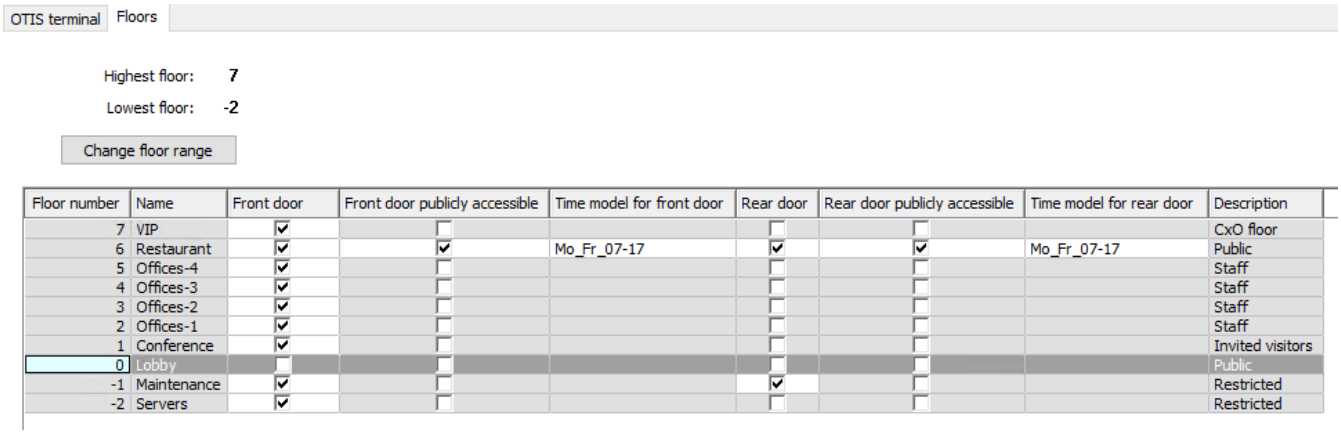
Op. modu	Açıklama	Davranış
4	Varsayılan kat veya hedef katın kullanıcı tarafından girilmesi.	Yolcu kendi kimlik bilgilerini sunar veya bir PIN kodu girer. Kimlik bilgileri veya PIN geçerliyse DET, DES'den yolcunun varsayılan veya "ana" katını ister. Yolcu, ayarlı bir zaman aşımı süresi içinde varsayılan katın seçimini geçersiz kılabilir ve farklı bir hedef seçebilir.

- **Audit records:** (Kayıtları denetle) Olay günlüğü için bu terminalde yolcu girişlerini kaydetmek üzere bu onay kutusunu seçin.
- **PIN code:** (PIN kodu) Bu terminalde, fiziksel kimlik bilgilerine alternatif olarak bir kimlik PIN kodu kullanılmasına izin vermek için bu onay kutusunu seçin.
  Not: Otis terminallerinde kullanım için PIN kodlarını kaydetmek üzere **Dialog PIN card (enter)** (İletişim kutusu PIN kartı (gir)) tipi kayıt okuyucuları kullanın.
- **Time models:** (Zaman modelleri) Zaman modellerinin bu terminalin kullanılabileceği zamanları kısıtlamasına izin vermek için bu onay kutusunu seçin.
- **Division** (Bölüm) (yalnızca bölümler lisanslandırılmış ve kurulumunuzda kullanılıyorsa)

Otis terminal (Otis terminali) özellikler sayfasının **Floors** (Katlar) sekmesinde 2. Katman için tanımladığınız katlar düzenlenebilir hücrelerden oluşan bir tablo olarak gösterilir.
Not: Yukarıdaki 2. Katman için tanımlanan adlandırma şeması yeterli yönlendirme sağlamalıdır. Sağlamazsa çalışmanızı kaydetmenizi ve ad şemasını tamamlamak için 2. Katman'a geri dönmenizi öneririz.

1. Cihaz ağacında yeni oluşturduğunuz her DET'i sırayla seçin ve **Floors** (Katlar) sekmesini açın.
   - **Floors** (Katlar) tablosu görünür
2. **Front door** (Ön kapı) sütununda, geçerli DET'ten ulaşılabilecek her katın onay kutusunu seçin.
3. **Front door publicly accessible** (Ön kapı genel olarak erişilebilir) sütununda, genel olarak, yani açık yetki olmadan erişilebilen her ön kapının onay kutusunu seçin.
4. (isteğe bağlı) **Time model for front door** (Ön kapı için zaman modeli) sütununda, gerekirse bu katta ön kapıya genel erişimi kısıtlamak için bir zaman modeli seçin. Örneğin, restoran katına günün yalnızca belirli saatlerinde erişilebilir.
5. Gerekirse **Rear door** (Arka kapı), **Rear door publicly accessible** (Arka kapı genel olarak erişilebilir) ve **Time model for rear door** (Arka kapı için zaman modeli) sütunları için önceki adımları tekrarlayın.
6. Değişiklikleri kaydetmek için  (Kaydet) simgesine tıklayın.

Örnek:
Aşağıdaki örnekte, 10 katlı bir asansör grubunun katları, lobide bulunan asansör ön kapısından erişilebilen katlar ve kapılarla birlikte gösterilmiştir. Restoran katına hem ön hem de arka asansör kapılarında giriş bir zaman modeliyle kısıtlanmıştır.



Floor number	Name	Front door	Front door publicly accessible	Time model for front door	Rear door	Rear door publicly accessible	Time model for rear door	Description
7	VIP	☑	☐		☐	☐		CxO floor
6	Restaurant	☑	☑	Mo_Fr_07-17	☑	☑	Mo_Fr_07-17	Public
5	Offices-4	☑	☐		☐	☐		Staff
4	Offices-3	☑	☐		☐	☐		Staff
3	Offices-2	☑	☐		☐	☐		Staff
2	Offices-1	☑	☐		☐	☐		Staff
1	Conference	☑	☐		☐	☐		Invited visitors
0	Lobby	☐	☐		☐	☐		Public
-1	Maintenance	☑	☐		☑	☐		Restricted
-2	Servers	☑	☐		☐	☐		Restricted

21.2 Kart sahiplerinin Otis'e özel özellikleri için özelleştirilmiş alanları yapılandırma

Giriş

Bu bölümde, bir operatörün bir kart sahibi için Otise özel özellikleri, özellikle kart sahibinin "evi" veya varsayılan hedefini girebileceği özel alanların nasıl oluşturulacağı açıklanmaktadır.

Bu "ev" **üç koordinatla** tanımlanmalıdır:

1. Asansör grubu,
2. Kat
3. Kapı

Kartlı geçiş sistemi istemcisinde bir kart sahibi için bir ana kat belirtirken bir operatörün verileri aynı sırada girmesi gerekir: asansör grubu, kat, kapı. Bu nedenle üç özel alan tercihen yukarıdan aşağıya olacak şekilde okuma düzeninde konumlandırılmalıdır.

Üç koordinat oluşturmanız gerektiğine ilişkin tüm açılır hatırlatmaları onaylamak için **OK**'e (Tamam) tıklayın.

Gerekli 3 özel alanın yanı sıra kartlı geçiş istemci arayüzünün **Elevators** (Asansör) sekmesinde görünmesini istediğiniz özel alanları tanımlayın.

Özel alanları yapılandırma hakkında genel bilgi için **Custom fields for personnel data** (Personel verileri için özel alanlar) için ACE/AMS Yapılandırma yardımına bakın.

İletişim yolu

Main menu (Ana Menü) > **Configuration** (Yapılandırma) > **Options** (Seçenekler) > **Custom fields** (Özel alanlar)

Prosedür

Custom fields (Özel alanlar) özellik sayfasında **Elevators** (Özellikler) sekmesini seçin.

İlk koordinat: Asansör grubu

1. Sekmedeki bir hücreye çift tıklayın ve yeni bir giriş alanı oluşturmak için **Yes**'e tıklayın.
2. **Field type** (Alan tipi) listesinden **Otis DES selection**'ı (Otis DES seçimi) seçin.
3. **Label** (Etiket) alanına `Elevator Group` ifadesini girin
4. **Display in** (Şurada görüntüle:) listesinden `Tab:Elevators`'ı seçin
5. **Position** (Konum) grubunda **Elevators** (Asansörler) sekmesinde bu özel alanın görüneceği benzersiz bir konum seçin.

İkinci koordinat: Ana kat

1. Yeni bir özel alan oluşturmak için **New field**'a (Yeni alan) tıklayın.

2. **Field type** (Alan tipi) listesinden **Home floor**'u (Ana kat) seçin.
3. **Label** (Etiket) alanına `Home floor` ifadesini girin
4. **Display in** (Şurada görüntüle:) listesinden `Tab:Elevators`'ı seçin
5. **Position** (Konum) grubunda **Elevators** (Asansörler) sekmesinde bu özel alanın görüneceği benzersiz bir konum seçin. Sistemin operatörler tarafından kolayca kullanılması için önceki koordinatın altında olmalıdır.

Üçüncü koordinat: Çıkış kapısı

1. Yeni bir özel alan oluşturmak için **New field**'a (Yeni alan) tıklayın.
2. **Field type** (Alan tipi) listesinden **Exit door**'u (Çıkış kapısı) seçin.
3. **Label** (Etiket) alanına `Exit door` ifadesini girin
4. **Display in** (Şurada görüntüle:) listesinden `Tab:Elevators`'ı seçin
5. **Position** (Konum) grubunda **Elevators** (Asansörler) sekmesinde bu özel alanın görüneceği benzersiz bir konum seçin. Sistemin operatörler tarafından kolayca kullanılması için önceki koordinatın altında olmalıdır.

Kart sahiplerine yönelik özel Otis seçenekleri

Giriş

Standart Otis işlevlerine uygun olarak sekiz Otis'e özel ikili seçenek sunulur. **Elevators** (Asansör) sekmesinde özel alanlar olarak tanımlandıysa **Persons** (Kişiler) iletişim kutusundaki kart sahiplerinin (Main menu (Ana menü) > **Personnel data** (Personel verileri) > **Persons** (Kişiler)) **Elevator data** (Asansör verileri) sekmesinde onay kutuları olarak görünürler. Bunlar daha sonra kartlı geçiş sisteminin operatörleri tarafından seçilip temizlenebilir.

Bu seçenekleri yalnızca Otis temsilciniz tarafından belirtildiği gibi yapılandırın.

Prosedür

1. Yeni bir özel alan oluşturmak için **New field**'a (Yeni alan) tıklayın.
2. **Field type** (Alan tipi) listesinden, **Otis options**'ı (Otis seçenekleri) seçin.
3. **Label** (Etiket) alanına, örneğin `Otis flag 1` gibi veya Otis belgelerine göre kendi etiketinizi girin.
4. **Display in** (Şurada görüntüle:) listesinden `Tab:Elevators`'ı seçin
5. **Function type** (İşlev tipi) listesinden, `OTIS option 1`-`OTIS option 8` arasındaki seçeneklerden birini seçin.
6. **Position** (Konum) grubunda **Elevators** (Asansörler) sekmesinde bu onay kutusunun görüneceği benzersiz bir konum seçin.
7. Değişiklikleri kaydetmek için  (Kaydet) simgesine tıklayın.

21.3 Otis asansörler için yetki oluşturma ve yapılandırma

Giriş

Bu bölümde, Otis asansör grupları, katlar ve asansör kapılarının giriş haklarının bir **Authorization**'a (Yetki) nasıl ekleneceği açıklanmaktadır.

Yetkiler doğrudan kart sahiplerine veya daha yaygın olarak daha önce kart sahiplerine atanan diğer yetkilerle birlikte **giriş profillerine** atanır.

Ön koşullar

Cihaz Düzenleyicisi'nde bir MAC'te bir Otis Compass sistemi tanımlanmıştır. Bir asansör grubu (DES ile temsil edilen) ve kat + kapı çiftleri (onların DET'leriyle gösterilir) ile tamamlanır.

İletişim yolu

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

Prosedür

1. **Authorization name** (Yetki adı) alanına mevcut bir yetki adını girin veya yeni bir yetki oluşturmak için  (Yeni) simgesine tıklayın.
2. **MAC** listesinde, Otis Compass sisteminin oluşturulduğu MAC'in adını seçin.
3. **Otis elevator** (Otis asansör) sekmesine tıklayın
4. **Otis elevators** (Otis asansörler) listesinde, yetkiye eklemek istediğiniz asansör grubuna ait DES/DER'i seçin (Bir yetkinin yalnızca bir adet DES/DER içerebileceğini unutmayın).
   – Seçilen asansör grubunun katları **Floors** (katlar) bölmesinde görüntülenir.
5. **Floors** (Katlar) bölmesinin **Rear door** (Arka kapı) ve **Front door** (Ön kapı) sütunlarında bu yetkiye eklenebilecek katlardaki kapıları seçin.
   – Bu asansör grubu için **seçilmeyen** katlar ve kapıların Cihaz Düzenleyicisi'nde tanımlandığında, gri renkte olduğunu ve bu iletişim kutusunda seçilebilir olmadığını unutmayın.
6. Alternatif olarak tüm katları ve kapıları tek seferde seçmek veya temizlemek için **Assign all floors** (Tüm katları ata) ve **Remove all floors** (Tüm katları kaldır) düğmelerine tıklayın.
7. Yetkiyi kaydetmek için  (**Kaydet**) simgesine tıklayın.

22 IDEMIA Universal BioBridge'i Yapılandırma

Bu bölümde, IDEMIA biyometrik cihazlarının **MorphoManager** ve **BioBridge** aracılığıyla Bosch kartlı geçiş sistemleriyle çalışacak şekilde yapılandırması açıklanmaktadır.
Alt bölümlerde aşağıdaki alanlarda gerekli yapılandırma görevleri ele alınmaktadır:

- Bosch kartlı geçiş sistemi
- MorphoManager
- MorphoManager'daki BioBridge kayıt istemcisi
- Çeşitli kart teknolojileri ve biçimlerine yönelik uyarlamalar

22.1 Bosch kartlı geçiş sisteminde BioBridge'i ayarlama

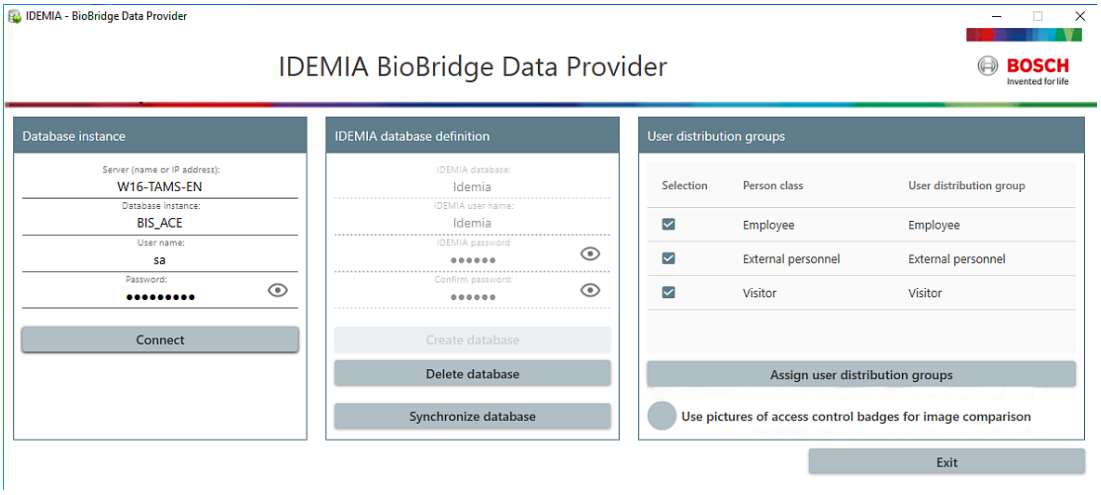
Aşağıdaki adımlar, IDEMIA biyometrik cihazlarını Bosch kartlı geçiş sistemine bağlayan veritabanını oluşturmak için ACS'de gerçekleştirilir. Veritabanı aşağıdaki veritabanı varlıklarını birbiriyle eşler:

- **Person class** (Kişi sınıfı) (Bosch) ve
- **User distribution group** (Kullanıcı dağıtım grubu) (IDEMIA).

İletişim yolu

- AMS main menu (AMS ana menüsü) > **Configuration** (Yapılandırma) > **Tools** (Araçlar) > **IDEMIA database configuration** (IDEMIA veritabanı yapılandırması)

1. **Configuration IDEMIA database**'e (Yapılandırma IDEMIA veritabanı) tıklayın.
   IDEMIA BioBridge Data Provider (IDEMIA BioBridge Veri Sağlayıcı) iletişim kutusu görünür.



2. **Database instance** (Veritabanı örneği) bölmesinde, aşağıdaki bilgileri girin:

- **Server** (Sunucu): ACS SQL Server veritabanı örneğinin çalıştığı bilgisayarın ana bilgisayar adı veya IP adresi. SQL sunucusu yerel olarak çalışıyorsa bu, yerel ana bilgisayar olabilir.
- **Database Instance** (Veritabanı örneği): ACS veritabanının örneği (varsayılan `ACE`).
- **Username** (Kullanıcı adı): ACS veritabanı örneğinin yönetici hesabının adı (varsayılan: `sa`)
- **Password** (Şifre): ACS kurulumu sırasında yapılandırıldığı şekilde yönetici hesabının şifresi.

3. **Connect**'e (Bağlan) tıklayın. Bunu yapıncaya kadar tüm diğer kontroller devre dışı bırakılır.

IDEMIA veritabanı tanım bölmesinde

İlk iki alan salt okunurdur:

– **Idemia database** (Idemia veritabanı): Bosch ve IDEMIA verilerini birleştiren veritabanının adı.

– **Idemia username** (Idemia kullanıcı adı): yazılımı veritabanında adına komut yürüttüğü veritabanı kullanıcısının adı.

1. **Idemia username** (Idemia username) için güçlü bir şifre girin ve onaylayın.
2. Şifreyi dikkatlice not edin. Gelecekteki yapılandırma görevlerinde gerekli olacaktır ve kaybolursa yeniden alınamaz.
3. **Create database**'e (Veritabanı oluştur) tıklayın.
   Oluşturma işleminin başarılı olup olmadığı bir mesaj kutusu tarafından onaylanır. **OK**'e (Tamam) tıklayın
4. Testler başarıyla tamamlandığında, iletişim kutusunu kapatmak için **Exit**'e (Çık) tıklayın.

User distribution groups (Kullanıcı dağıtım grupları) bölmesinde

Kullanıcı Dağıtım Grupları, kullanıcıları (kimlik bilgisi sahiplerini) biyometrik okuyucular veya MorphoManager istemcilerinden oluşan gruplarla eşleştiren MorphoManager nesneleridir. Bunları Bosch kartlı geçiş sistemlerinin **kişi sınıflarıyla** eşleştiriyoruz.

1. Select (Seç) sütununda, yüklemenizde kullanılan her ACE **Person Class**'ın (Kişi Sınıfı) onay kutusunu seçin.
2. Seçtiğiniz her satır için, ilgili kişi sınıfının adını **User distribution group** (Kullanıcı dağıtım grubu) sütunundaki ilgili hücreye kopyalayın.

– **Person class** (Kişi sınıfı) ve **User distribution group** (Kullanıcı dağıtım grubu) adlarının tam olarak eşleşmesi gerektiğini unutmayın.

3. Eşleştirme tamamlandığında **Assign user distribution groups**'a (Kullanıcı dağıtım gruplarını ata) tıklayın.

VisionPass yüz tanıma için kimlik fotoğrafları sunma

IDEMIA okuyucuların ACE veritabanındaki kart sahiplerinin fotoğraflarını kullanarak VisionPass yüz tanıma işlemi yapmasını sağlamak:

- **Use pictures of access control badges for image comparison** 'a (Resim karşılaştırması için erişim kontrolü kimlik kartlarının resimlerini kullan) tıklayın ve açılır pencerede onaylayın.
  IDEMIA BioBridge Data Provider (IDEMIA BioBridge Veri Sağlayıcısı) penceresi eşitlemenin devam ettiğini onaylar.
  İlgili görüntü verilerinin miktarına bağlı olarak, aktarım uzun sürebileceğini unutmayın.

22.2 Kart teknolojilerinin ve biçimlerinin seçilmesi

Giriş

Biyometrik tanımlamanın yanı sıra kartları da kullanmayı düşünüyorsanız, MorphoManager'da bu erişim kartlarının biçimini (veya biçimlerini) içeren bir profil (veya "Wiegand profili") oluşturmanız gerekir.

Aşağıdaki tablo desteklenen biçimlere ilişkin bir genel bakış sunar. MIFARE teknolojisi için yalnızca CSN tanımanın desteklendiğini unutmayın.

Card Family	HID Prox	HID Class	HID iClass Seos	MIFARE Classic	MIFARE DESFire EV0	MIFARE DESFire EV1
Card Variant	Prox	2k/2 16k/2 16k/16 32k(16k/2+16k/1) 32k(16k/16+16k/1)	Seos	1K 4-byte NUID 1k 7-byte UID 4k 4-byte NUID 4k 7byte UID	2k 4k 8k	2k 4k 8k

Şekil 22.1: IDEMIA kartları desteklenmektedir

Genel prosedür

1. MorphoManager'da **Administration** (Yönetim) > **Wiegand Profile**'a (Wiegand Profili) gidin
2. Özel bir Wiegand profili oluşturmak için **Add**'e (Ekle) tıklayın
3. İlgili iletişim kutularında, biçimlendirme bilgilerini ve sisteminizde kullanılan kart teknolojisini girin
4. Sistemde yeni tanımlanan Wiegand profilinizi kullanmak için adını aşağıdaki MorphoManager iletişim kutularındaki **Wiegand Profile** (Wiegand Profili) alanına girin:

– **Administration (Yönetim) > Biometric Device profile (Biyometrik cihaz profili)**
– **Administration (Yönetici) > User policy (Kullanıcı ilkesi)**

Mifare Classic CSN

1. `User CSN Element` Wiegand öğesini ekleyin ve şu ayrıntıları girin:

– **Name** (Ad): `CSN` (örneğin)
– **Length** (Uzunluk) `32`
– **Transformation mode (Dönüştürme modu):** `Reversed`

2. **Administration (Yönetim) > Biometric Device profile (Biyometrik cihaz profili)** bölümünde **Multi-Factor Mode Settings** (Çok Faktörlü Mod Ayarları) sayfasında **MIFARE Classic** onay kutusunu seçin

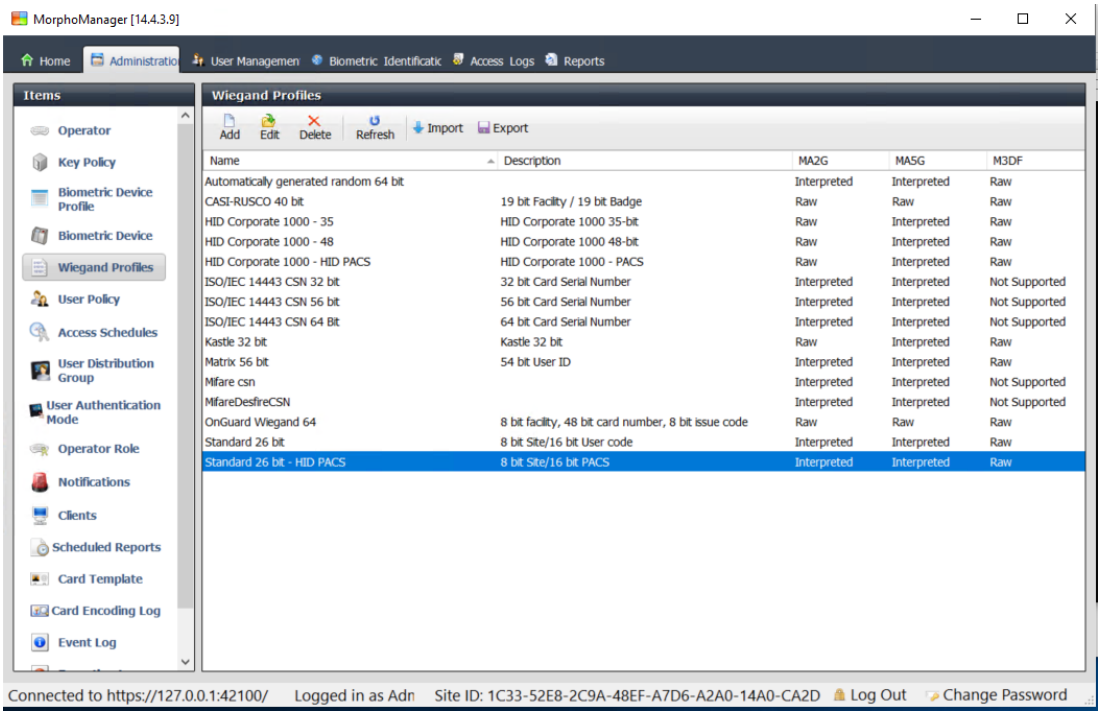
Mifare DESFire CSN

Yapılandırma aşağıdaki ayrıntılar hariç Mifare Classic ile aynıdır:

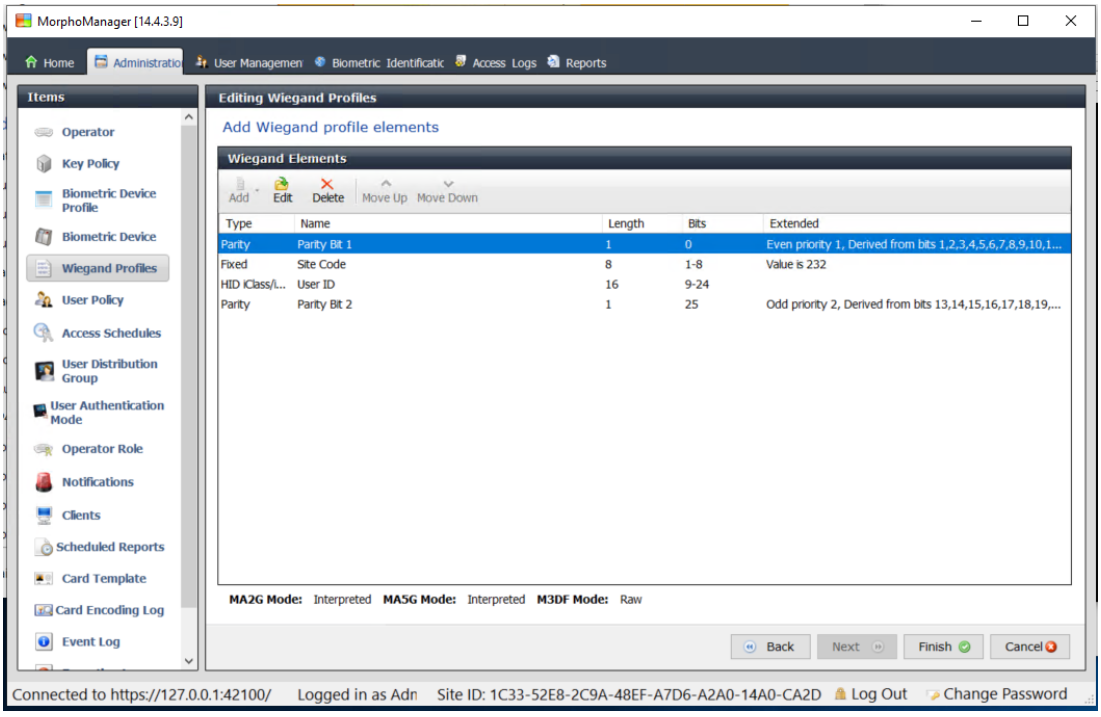
– **Length** (Uzunluk): `56`
– **User CSN Element** (Kullanıcı CSN Öğesi) Wiegand öğesini ekleyin
  – **Name:**'in (Ad:) altına ad girin
  – **Length** (Uzunluk) için 56 girin
  – **Transformation mode:** (Dönüştürme modu) için `Reversed` girin
– **Administration (Yönetim) > Biometric Device profile (Biyometrik cihaz profili)** bölümünde **Multi-Factor Mode Settings** (Çok Faktörlü Mod Ayarları) sayfasında **Mifare DESFire 3DES** onay kutusunu seçin

iClass 26 BIT

1. Önceden tanımlanan `Standard 26 bit-HID PACS` profilini seçin



2. **Edit**'e (Düzenle) tıklayın
3. **Next**'e (İleri) tıklayın



4. **Edit**'e (Düzenle) tıklayın
5. `Fixed Facility Code` satırını silin
6. `HID iClass SEP User ID` satırını seçin
7. **Edit**'e (Düzenle) tıklayın
8. `1..16` olan kullanıcı kimliği uzunluğunu `1..24` olarak değiştirin
9. **Administration (Yönetim) > Biometric Device profile**'ın (Biyometrik cihaz profili) altında, Biometric Device Settings (Biyometrik Cihaz Ayarları) sayfasında Wiegand Profili için `Standard 26 BIT-HID-PACS`'i seçin

10. **Administration (Yönetim) > Biometric Device profile**'ın (Biyometrik cihaz profili) altında, **Multi-Factor Mode Settings** (Çok Faktörlü Mod Ayarları) sayfasında, `HID iClass` onay kutusunu seçin
11. **Custom Parameters** (Özel Parametreler) sayfasına ulaşana kadar Next'e (İleri) tıklayın
12. **Add**'e (Ekle) tıklayın
13. `wiegand.site_code_propagation` özel parametresini (büyük/küçük harf duyarlı) ekleyin
14. Değerini `1` olarak ayarlayın
15. **Finish**'e (Bitir) tıklayın.
16. Bu tamamlanmış Wiegand profilini **Administration (Yönetim) > User policy (Kullanıcı ilkesi)** bölümünde girin

iClass 35 BIT

1. Önceden tanımlanan `HID Corporate 1000 35 BIT` profilini seçin
2. **Edit**'e (Düzenle) tıklayın
3. **Next**'e (İleri) tıklayın
4. `Fixed Company ID` öğe satırını seçin ve silin
5. `User Card ID Number` öğe satırını seçin ve silin
6. `HID iClass/iClass SE PACS Data` öğe satırını ekleyin ve öğe ayrıntılarında, aşağıdakileri ayarlayın:

– Name (Ad): `Card ID Number`
– Length (Uzunluk): `32`
– **Administration (Yönetim) > Biometric Device profile**'ın (Biyometrik cihaz profili) altında, **Multi-Factor Mode Settings** (Çok Faktörlü Mod Ayarları) sayfasında, `HID iClass` onay kutusunu seçin
– **Custom Parameters** (Özel Parametreler) sayfasına ulaşana kadar **Next**'e (İleri) tıklayın
– **Add**'e (Ekle) tıklayın
– `wiegand.site_code_propagation` özel parametresini (büyük/küçük harf duyarlı) ekleyin
– Değerini `1` olarak ayarlayın
– **Finish**'e (Bitir) tıklayın.
– Bu tamamlanmış Wiegand profilini **Administration (Yönetim) > User policy (Kullanıcı ilkesi)** bölümünde girin

iClass 37 BIT

– **Administration > Wiegand Profile** (Yönetim > Wiegand Profili)
– **Add new profile**'a (Yeni profil ekle) tıklayın
– **Length** (Uzunluk) `37`

1. Öğe eşliği ekleyin:

– **Name** (Ad): (örneğin) `EvenParityBit 1`
– **Priority** (Öncelik): `1`
– **Length** (Uzunluk): `18`
– **Mode** (Mod): `Even`
– **Basis bits** (Temel bitler): `1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18`
– **Next**'e (İleri) tıklayın

2. `User HID iClass/iClass SE PACS Data` öğesini ekleyin ve öğe ayrıntılarında, aşağıdakileri ayarlayın:

– **Name** (Ad)**:** `UserID`
– **Length** (Uzunluk): `35`

– **Next**'e (İleri) tıklayın
3. Öğe eşliği ekleyin:
– **Name** (Ad): (örneğin) `Parity Bits 2`
– **Priority** (Öncelik): `2`
– **Length** (Uzunluk): `19`
– **Mode** (Mod): `Odd`
– **Basis bits** (Temel bitler):
`19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37`
– **Next**'e (İleri) tıklayın
– **Administration (Yönetim) > Biometric Device profile**'ın (Biyometrik cihaz profili) altında, **Multi-Factor Mode Settings** (Çok Faktörlü Mod Ayarları) sayfasında, `HID iClass` onay kutusunu seçin
– **Custom Parameters** (Özel Parametreler) sayfasına ulaşana kadar **Next**'e (İleri) tıklayın
– **Add**'e (Ekle) tıklayın
– `wiegand.site_code_propagation` özel parametresini (büyük/küçük harf duyarlı) ekleyin
– Değerini `1` olarak ayarlayın
– **Finish**'e (Bitir) tıklayın.
– Bu tamamlanmış Wiegand profilini **Administration (Yönetim) > User policy (Kullanıcı ilkesi)** bölümünde girin

iClass 48BIT

1. Önceden tanımlanan `HID Corporate 1000 48 BIT` profilini seçin
2. **Edit**'e (Düzenle) tıklayın
3. **Next**'e (İleri) tıklayın
4. `Fixed Company ID` öğe satırını seçin ve silin
5. `User Card ID Number` öğe satırını seçin ve silin
6. `HID iClass/iClass SE PACS Data` öğe satırını ekleyin ve öğe ayrıntılarında, aşağıdakileri ayarlayın:
– Name (Ad): `User`
– Length (Uzunluk): `45`
7. **Administration (Yönetim) > Biometric Device profile**'ın (Biyometrik cihaz profili) altında, **Multi-Factor Mode Settings** (Çok Faktörlü Mod Ayarları) sayfasında, `HID iClass` onay kutusunu seçin
8. **Custom Parameters** (Özel Parametreler) sayfasına ulaşana kadar **Next**'e (İleri) tıklayın
9. **Add**'e (Ekle) tıklayın
10. `wiegand.site_code_propagation` özel parametresini (büyük/küçük harf duyarlı) ekleyin
– Değerini `1` olarak ayarlayın
11. **Finish**'e (Bitir) tıklayın.
12. Bu tamamlanmış Wiegand profilini **Administration** (Yönetim) > **User policy** (Kullanıcı ilkesi) bölümünde girin

HID Prox

1. Önceden tanımlanan `Standard 26 BIT` profilini seçin
2. **Edit**'e (Düzenle) tıklayın
3. **Next**'e (İleri) tıklayın
4. `Fixed Facility Code` satırını silin
5. **Edit**'e (Düzenle) tıklayın

6. `1..16` olan kullanıcı kimliği uzunluğunu `1..24` olarak değiştirin
7. **Administration (Yönetim) > Biometric Device profile**'ın (Biyometrik cihaz profili) altında, Biometric Device Settings (Biyometrik Cihaz Ayarları) sayfasında Wiegand Profili için `Standard 26 BIT`'i seçin
8. **Administration (Yönetim) > Biometric Device profile**'ın (Biyometrik cihaz profili) altında, **Multi-Factor Mode Settings** (Çok Faktörlü Mod Ayarları) sayfasında, şu onay kutularını seçin:
– **Biyometri**
– **Proximity kartı**
9. **Custom Parameters** (Özel Parametreler) sayfasına ulaşana kadar **Next**'e (İleri) tıklayın
10. **Add**'e (Ekle) tıklayın
11. `wiegand.site_code_propagation` özel parametresini (büyük/küçük harf duyarlı) ekleyin
– Değerini `1` olarak ayarlayın
12. **Finish**'e (Bitir) tıklayın.
13. Bu tamamlanmış Wiegand profilini **Administration** (Yönetim) > **User policy** (Kullanıcı ilkesi) bölümünde girin

22.3 Tanıma modunun seçilmesi

Giriş

Biyometrik okuyucular kimlik bilgisi sahiplerini farklı biçimlerde tanımlayabilir. Bu yollar, Identification (Tanıma) modları veya Authentication (Kimlik Doğrulama) modları olarak bilinir.

– Kimlik bilgisi sahibinin okuyucuya ne gösterdiğine bağlı olarak **kart VEYA biyometri** ile
– **Kart VE Biyometri** ile, yani kullanıcının, biyometrik kimlik bilgileri aracılığıyla kartın gerçek sahiplerini doğrulaması gerekir.
– **Yalnızca Biyometri** ile

Bu bölümde, MorphoManager'daki bu modların nasıl ayarlanacağı açıklanmaktadır.
Kart kimlik bilgilerinin söz konusu olduğu her yerde, uygun kart teknolojisi ve biçimi için bir profil oluşturulması gerektiğini unutmayın.

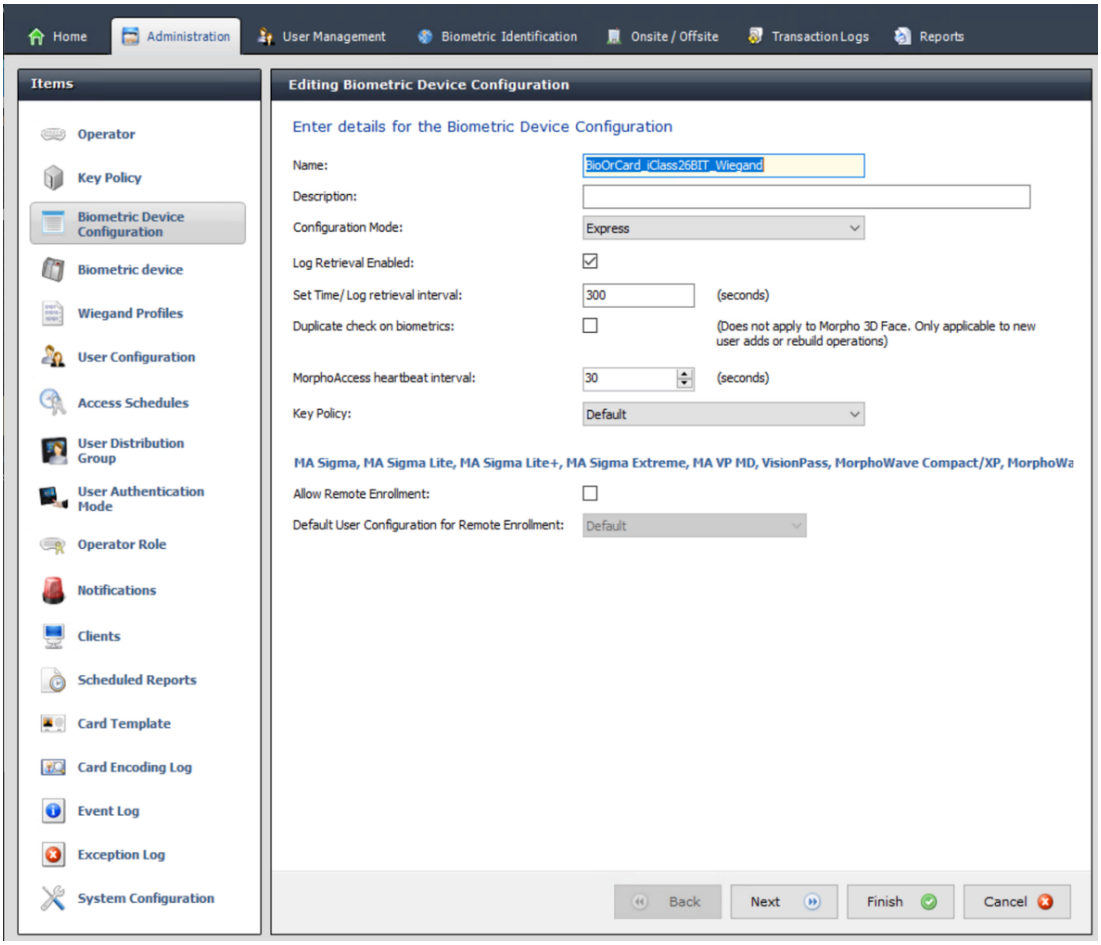
İletişim yolu

MorphoManager'da **Administration** (Yönetim) sekmesinde

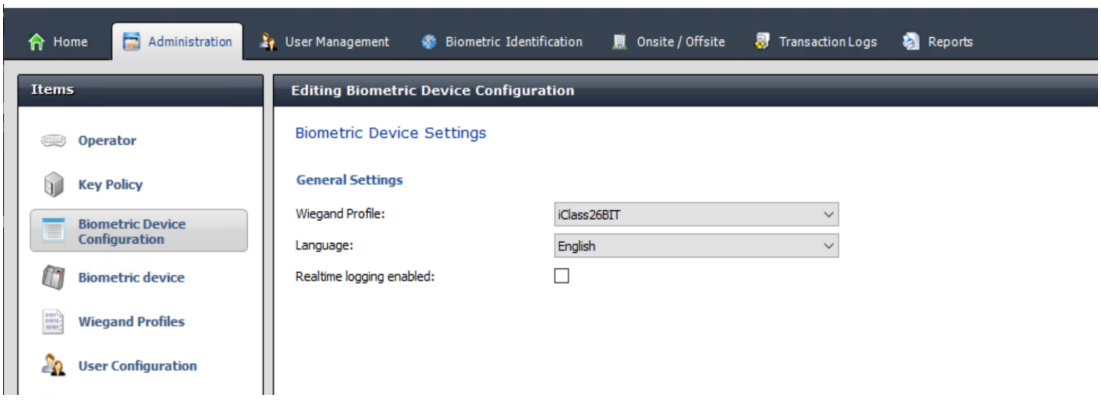
22.3.1 Kart veya biyometri

Bu özel kimlik doğrulama modunu, kullanıcılar kendilerini kartla VEYA biyometrik kimlik bilgileriyle tanımlayacaklarsa oluşturun.

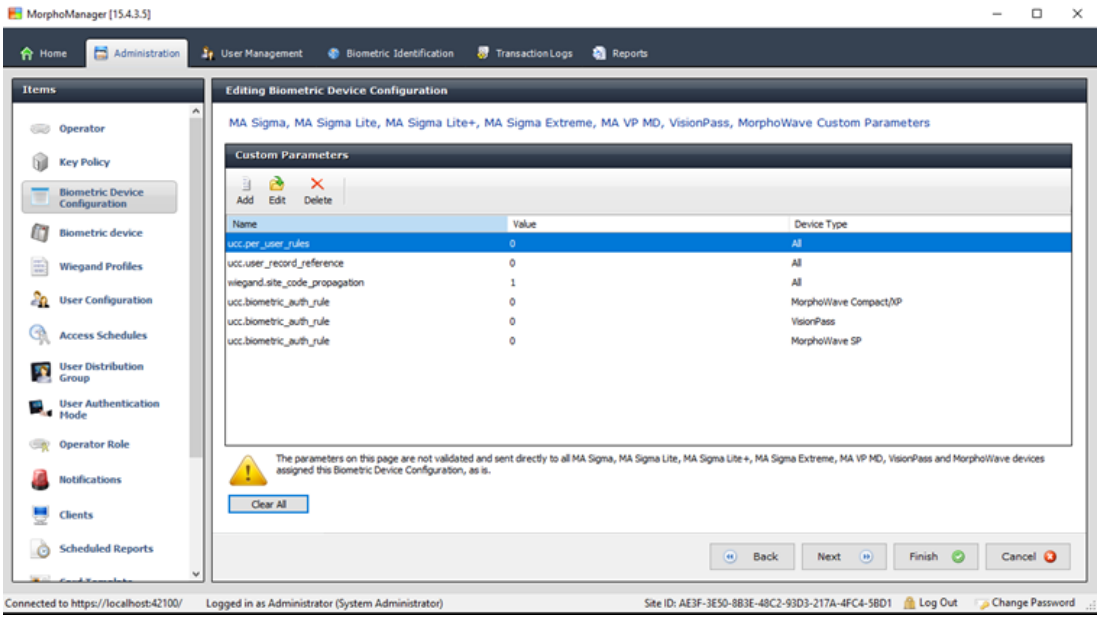
1. MorphoManager'da **Administration** (Yönetim) > **Biometric Device Yapılandırması**'na (Biyometrik Cihaz Yapılandırması) gidin
2. Biyometrik cihaz yapılandırması için bir ad girin, örneğin `CardORBiometric`



3. **Biometric Device Settings** (Biyometrik Cihaz Ayarları) başlıklı sayfaya ulaşana kadar **Next**'e (İleri) tıklayın



4. **Wiegand Profile** (Wiegand Profili) için BioBridge'i ayarlarken biyometrik cihazlarınız için tanımladığınızla aynı profili seçin.
5. **Biometric Threshold settings** (Biyometrik eşik ayarları) iletişim kutusuna ulaşana kadar **Next**'e (İleri) tıklayın.
6. **Biometric Threshold** (Biyometrik Eşik) değerlerini yerel koşullarınıza ve MorphoManager belgelerine göre ayarlayın. Varsayılan değer `Recommended`'dır
7. **Multi Factor Mode Settings**'e (Çok Faktörlü Mod Ayarları) ulaşıncaya kadar **Next**'e (İleri) tıklayın.
8. **Biometric** (Biyometrik) onay kutusunu, ayrıca yüklemenizde kullanılan kart teknolojisinin onay kutusunu seçin.
9. **Custom Parameters** (Özel Parametreler) ekranına ulaşana kadar **Next**'e (İleri) tıklayın



10. Kullandığınız her cihaz için:
    Add'e (Ekle) tıklayın ve iki özel parametre ekleyin.
    (Bu iki parametre ayarlanırsa okuyucu, kart verilerini doğrudan AMC'ye gönderir. Kullanıcının IDEMIA okuyucusuna kaydolması gerekmez)
- `ucc.per_user_rules`
- `ucc.user_record_reference`

11. WAVE ve VisionPass okuyucular için bir parametre daha ekleyin:
- `ucc.biometric_auth_rule=0`
- Bu durumda **Device Type** (Cihaz Tipi) için `MorphoWave Compact/XP`, `MorphoWave`, `SP` veya `VisionPass` seçin.

12. **Finish**'e (Bitir) tıklayın

Bu kullanıcı kimlik doğrulama modunu kullanıcılara atama

ACS 'de her kart sahibi için geçerli kart tanımına sahip bir kart atamanız gerekir.

1. MorphoManager'da **Administration** (Yönetim) > **User Authentication Mode**'a (Kullanıcı Kimlik Doğrulama Modu) gidin
2. Aşağıdaki nitelikleri ayarlayın**:**

- **Mode**'u (Mod) `Enabled` olarak ayarlayın
- **Template Location** (Şablonu Konumu) listesini `Download to Device` olarak ayarlayın
- **Allow Start by Biometric** (Biyometrik ile Başlatmaya İzin Ver) onay kutusunu seçili hale getirin
- **Allow Start by Contactless Card** (Temassız Kart ile Başlatmaya İzin Ver) onay kutusunu seçili hale getirin
- **Require Template Match**'i (Şablonların Aynı Olmasını Zorunlu Tut) devre dışı bırakın

3. **Administration** (Yönetim) > **User Configuration**'a (Kullanıcı Yapılandırması) gidin
4. **Add**'e (Ekle) tıklayın
5. **User Authentication Mode** (Kullanıcı Kimlik Doğrulama Modu) için, yukarıda Kart VE biometrisi için oluşturduğunuz modun adını seçin.
6. **Finish**'e (Bitir) tıklayın

Bkz.

– *Kart teknolojilerinin ve biçimlerinin seçilmesi, sayfa 153*

22.3.2 Kart VE Biyometri

Kullanıcıların, kart sahipleri olduklarını doğrulamak için kart ve biyometrik kimlik bilgileri kullanmaları gerekiyorsa aşağıdaki ayarları yapın.

1. MorphoManager'da **Administration** (Yönetim) > **Biometric Device Yapılandırması**'na (Biyometrik Cihaz Yapılandırması) gidin
2. **Biometric Device Settings** (Biyometrik Cihaz Ayarları) başlıklı sayfaya ulaşana kadar **Next**'e (İleri) tıklayın
3. **Wiegand Profile** (Wiegand Profili) için BioBridge'i ayarlarken biyometrik cihazlarınız için tanımladığınızla aynı profili seçin.
4. **Multi-Factor Mode Settings** (Çok Faktörlü Mod Ayarları) başlıklı sayfaya ulaşıncaya kadar **Next**'e (İleri) tıklayın
5. Yüklemenizde kullanılan kart teknolojisinin onay kutusunu seçin.
6. **Finish**'e (Bitir) tıklayın

Bu kullanıcı kimlik doğrulama modunu kullanıcılara atama

ACS 'de her kart sahibi için geçerli kart tanımına sahip bir kart atamanız gerekir.

1. MorphoManager'da **Administration** (Yönetim) > **User Configuration**'a (Kullanıcı Yapılandırması) gidin.
2. **User Authentication Mode** (Kullanıcı Kimlik Doğrulama Modu) için listeden `Contactless Card ID + Biometric` 'i seçin.
3. **Finish**'e (Bitir) tıklayın.

Bkz.

– *Kart teknolojilerinin ve biçimlerinin seçilmesi, sayfa 153*

22.3.3 Yalnızca biyometri

Kullanıcıların kendilerini yalnızca biyometrik kimlik bilgileriyle tanıtması gerekiyorsa aşağıdaki ayarları yapın.

1. MorphoManager'da **Administration** (Yönetim) > **Biometric Device Yapılandırması**'na (Biyometrik Cihaz Yapılandırması) gidin
2. **Editing Biometric Device Configuration** (Biyometrik Cihaz Yapılandırmasını Düzenleme) başlıklı sayfaya ulaşana kadar **Next**'e (İleri) tıklayın
3. **Wiegand Profile** (Wiegand Profili) için BioBridge'i ayarlarken biyometrik cihazlarınız için tanımladığınızla aynı profili seçin
4. **Multi-Factor Mode Settings** (Çok Faktörlü Mod Ayarları) başlıklı sayfaya ulaşıncaya kadar **Next**'e (İleri) tıklayın
5. **Multi-Factor Mode** (Çok Faktörlü Mod) için listeden `Biometric only`'yi seçin
6. **Finish**'e (Bitir) tıklayın

Bu kullanıcı kimlik doğrulama modunu kullanıcılara atama

ACS 'de her kart sahibi için geçerli kart tanımına sahip bir kart atamanız gerekir.

1. MorphoManager'da **Administration** (Yönetim) > **User Configuration**'a (Kullanıcı Yapılandırması) gidin.
2. **User Authentication Mode** (Kullanıcı Kimlik Doğrulama Modu) için listeden `Biometric(1:many)` 'i seçin.
3. **Finish**'e (Bitir) tıklayın.

22.4 MorphoManager'da BioBridge'i ayarlama

Ön koşullar

MorphoManager, ağınızdaki bir MorphoManager sunucusuna yüklenmiş olmalıdır.
MorphoManager'ın kendi kurulum kılavuzuna ve çevrimiçi yardımına bakın.

Genel bilgiler

Bosch kartlı geçiş sistemleri ve Morphomanager arasındaki BioBridge arayüzünü kullanmak için, aşağıdakileri MorphoManager'da yapılandırmanız gerekir:

- **Biyometrik Cihaz Yapılandırması**
- **Biyometrik Cihaz**
- **Wiegand Profilleri**
- **Kullanıcı Yapılandırması**
- **Kullanıcı Dağıtım Grubu**
- **Kullanıcı Kimlik Doğrulaması Modu**
- **Sistem Yapılandırması**

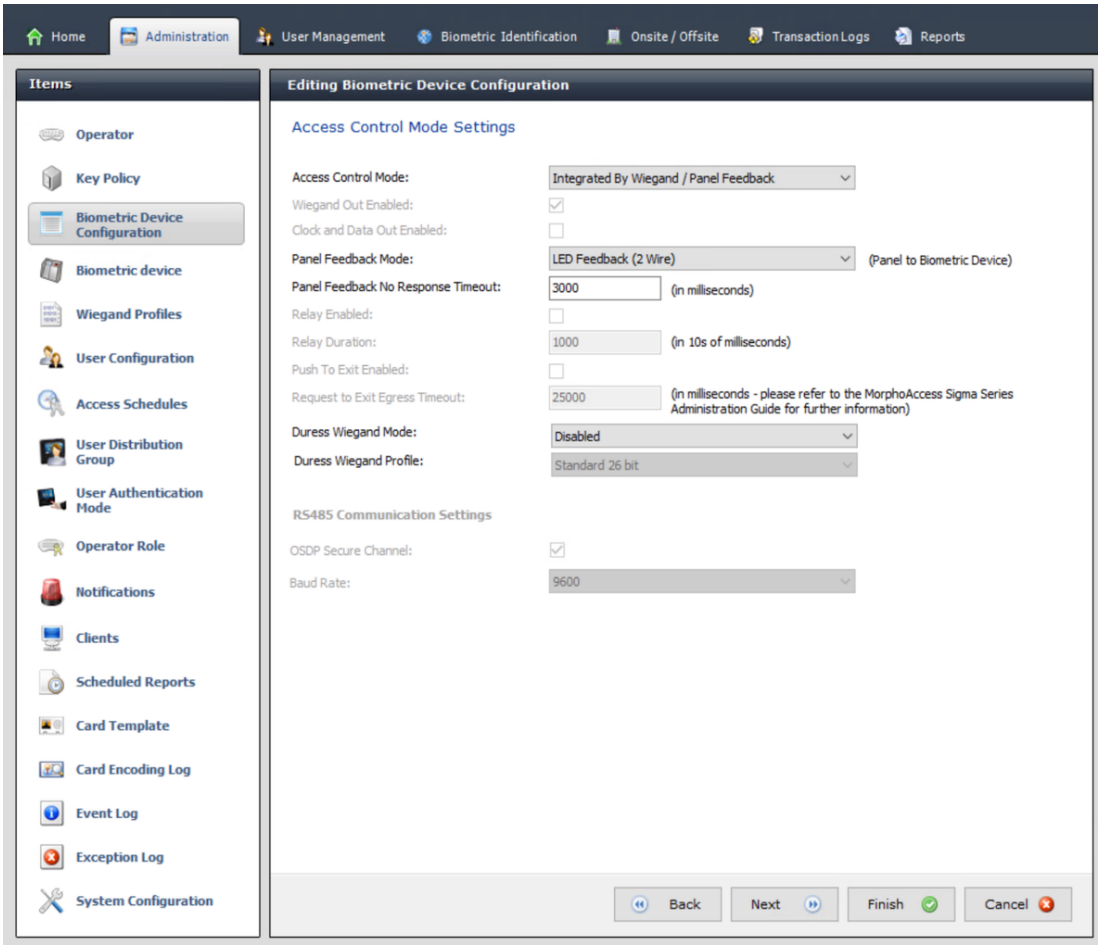
Ayrıca Morphomanager BioBridge ve ACS ile paylaştığı veritabanı arasındaki iletişim için Açık Veritabanı Bağlantısı (ODBC) kurulmalıdır.
Tüm bu yapılandırma görevleri aşağıdaki bölümlerde açıklanmaktadır.

22.4.1 Biyometrik Cihaz Yapılandırması

Biyometrik Cihaz Yapılandırması bir veya daha fazla biyometrik cihaz için ortak ayarları ve parametreleri tanımlar. Biyometrik cihazları sisteme daha sonra **Administration**'ın (Yönetim) **Biometric Device** (Biyometrik Cihaz) bölümünde eklediğinizde, bunlara bir Biyometrik Cihaz Yapılandırması uygulamış olursunuz.
Aşağıdaki prosedürde, biyometrik okuyucuları IDEMIA'dan ek kart okuma teknolojisiyle dağıttığınız varsayılmaktadır.

Prosedür:

1. MorphoManager'da **Yönetim** > **Biyometrik Cihaz Yapılandırması**'na gidin.
2. Yeni bir biyometrik cihaz yapılandırması oluşturmak için **Ekle**'ye tıklayın.
3. Sonraki ekranda profil için bir ad ve açıklama (isteğe bağlı) girin. Açıklama alanını kullanmazsanız okuyucu grubunun türünü ve tanımlama modlarını (biyometri ve/veya kart) açıklayan bir ad kullanmanızı öneririz.
4. **Biometric Device Settings**'na (Biyometrik Cihaz Ayarları) ulaşana kadar **Next**'e (İleri) tıklayın
   – Yüklemeniz için daha önce oluşturduğunuz Wiegand profilini seçin.
5. **Access Control Mode Settings** (Kartlı Geçiş Mod Ayarları) sayfasına ulaşana kadar **Next**'e (İleri) tıklayın.



Bu noktada, Wiegand ve OSDP AMC prosedürleri ayrılır. Aşağıda AMC kontrol cihazınızın tipine karşılık gelen prosedürü izleyin:

Wiegand AMC'ler için

1. **Access Control Mode**'u (Kartlı Geçiş Modu) `Integrated by Wiegand` olarak ayarlayın
2. **Panel Feedback Mode**'u (Panel Geri Besleme Modu) `LED Feedback (2 wire)` olarak ayarlayın
3. **Finish**'e (Bitir) tıklayın

OSDP AMC'ler için

1. **Access Control Mode**'u (Kartlı Geçiş Modu) `Integrated by OSDP` olarak ayarlayın
2. **Panel Feedback Mode**'u (Panel Geri Besleme Modu) `LED Feedback (2 wire)` olarak ayarlayın
3. **OSDP Secure Channel** (OSDP Güvenli Kanal) onay kutusunu seçin.
4. Baud hızını `9600` olarak ayarlayın
5. Daha fazla ayrıntı için **Biyometrik cihaz** bölümüne bakın
6. MorphoManager 'dan çıkmak için **Finish**'e (Bitir) tıklayın.

OSDP anahtarlarıyla ilgili sorun giderme

OSDP okuyucuyla güvenli bir bağlantı kuramıyorsanız, ana anahtarı aşağıdaki şekilde sıfırlamayı deneyin:

1. Ayrı bir program olan **MorphoBioToolBox (MBTB)** programını başlatın

2. MorphoBioToolBox programında **Device Settings** (Cihaz Ayarları) > **Reset**'e (Sıfırla) gidin
3. OSDP ana anahtarını seçin
4. **Reset cryptographic keys**'e (Şifreleme anahtarlarını sıfırla) tıklayın
5. MorphoBioToolBox'dan çıkın

Daha karmaşık durumlar için IDEMIA teknik destek ekibine başvurun.

Bkz.

– *Biyometrik cihaz, sayfa 164*

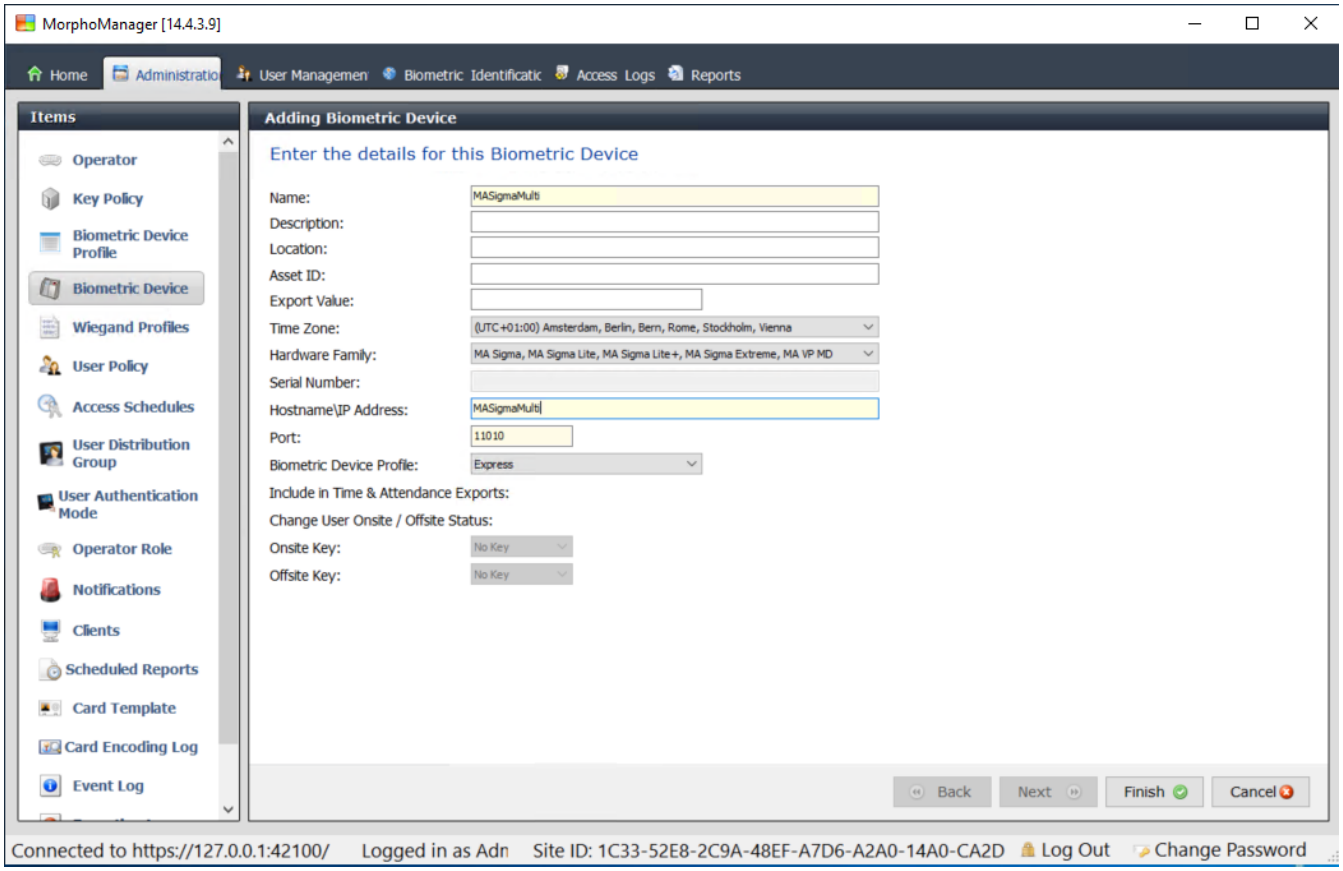
22.4.2 Biyometrik cihaz

Biyometrik cihazlar, okudukları biyometrik kimlik bilgilerinin veritabanındaki kayıtlarla eşleşip eşleşmediğini test eder. Ayrıca her kullanım olayının kaydını tutarlar.

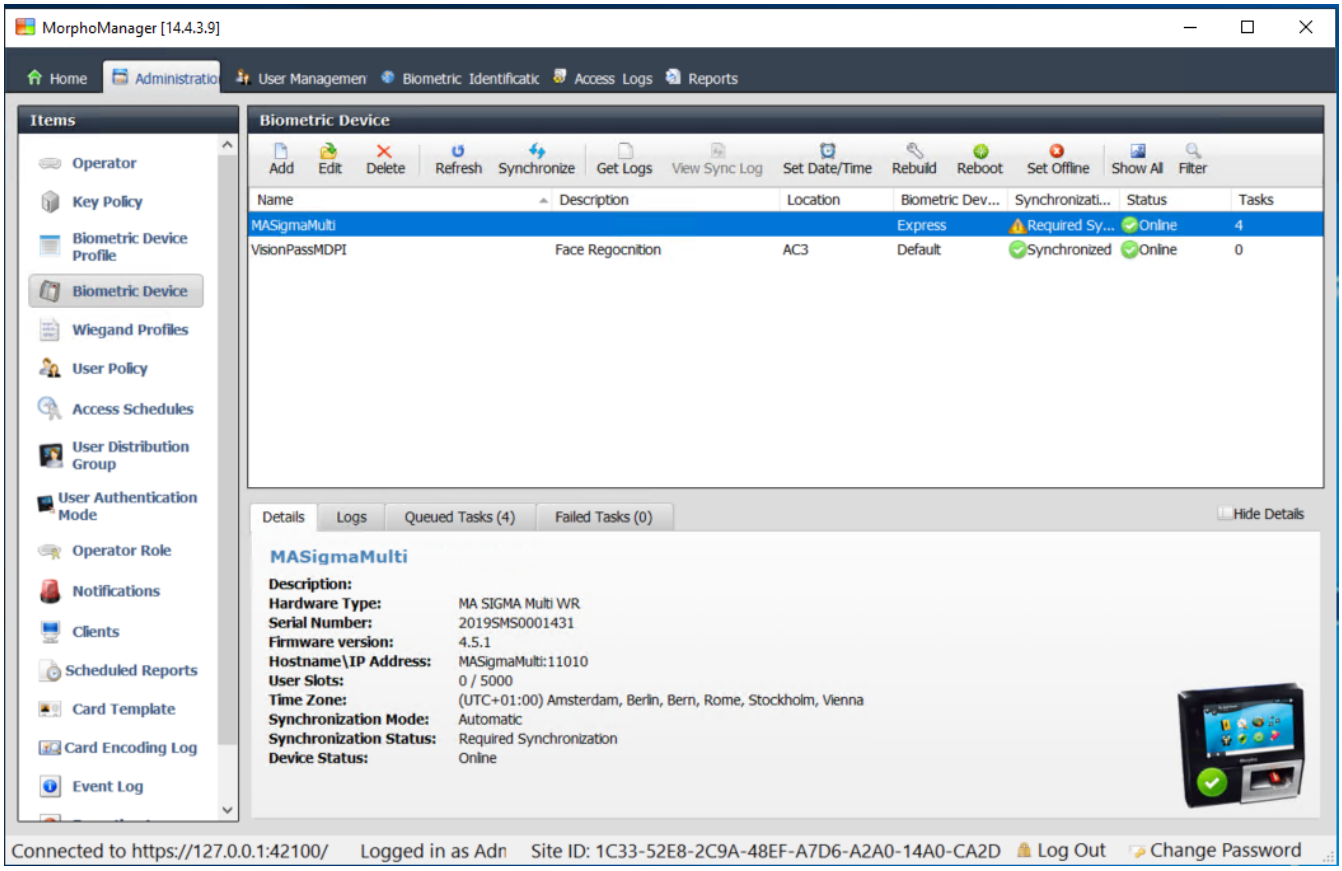
Prosedür:

1. MorphoManager'da **Administration** (Yönetim) > **Biometric device**'a (Biyometrik Cihaz) gidin.
2. Yeni bir biyometrik cihaz oluşturmak için **Add**'e (Ekle) tıklayın.
3. Cihaz için en azından temel ayrıntıları girin:

– (listeden) **Hardware Family** (Donanım Ailesi)
– **Hostname\IP address** (Ana bilgisayar adı\IP adresi)
– (listeden) daha önce tanımladığınız **Biometric Device Configuration** (Biyometrik Cihaz Yapılandırması)



4. **Finish**
'e (Bitir) tıklayın. Biometric Device (Biyometrik Cihaz) iletişim kutusu bu noktada daha önce yapılandırılmış olan cihazları listeler:

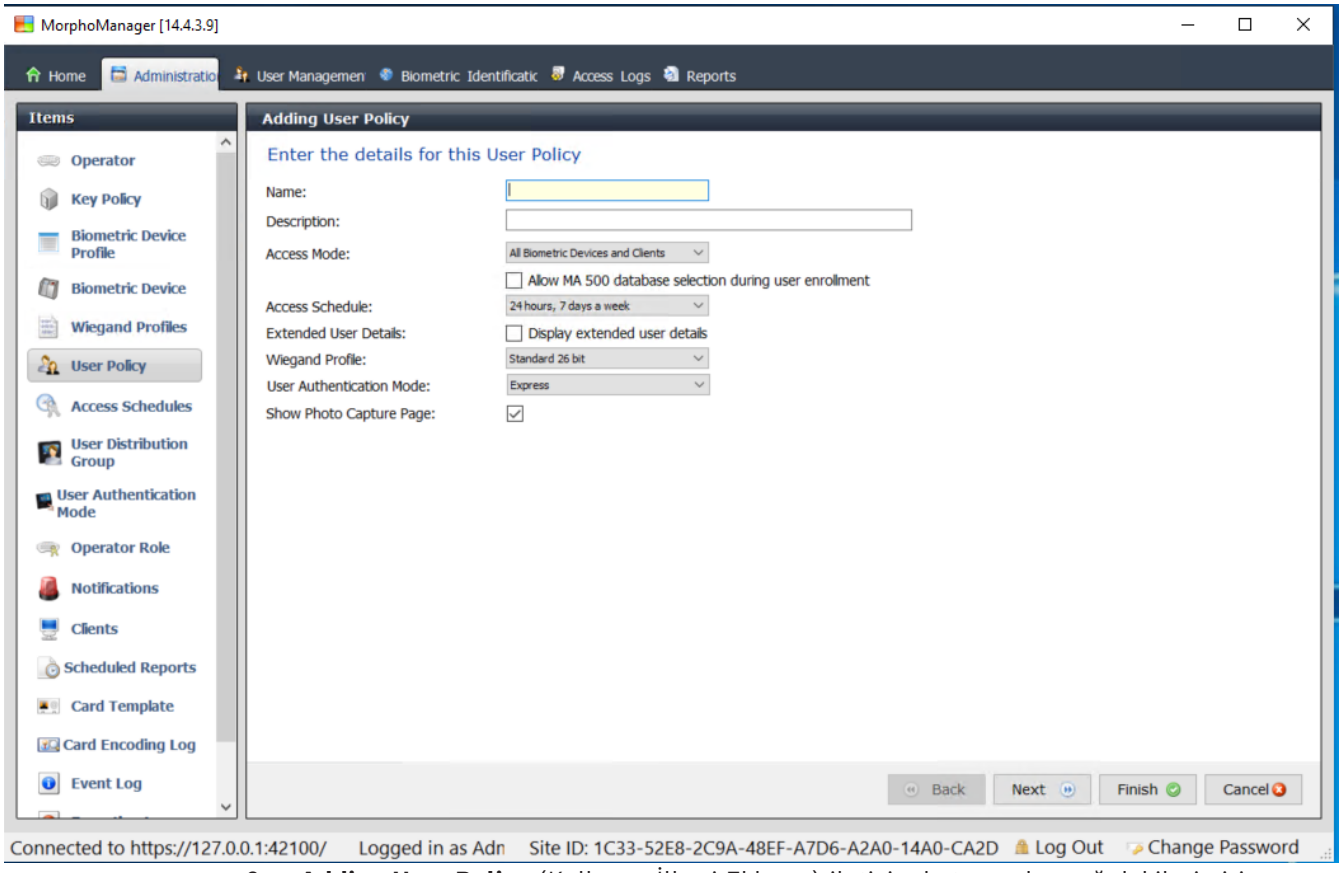


22.4.3 Kullanıcı Yapılandırması

Kullanıcı yapılandırmaları, aynı giriş gereksinimlerine sahip kullanıcılara atadığınız giriş haklarına, yani, biyometrik cihazların hangi modlarda ve hangi saatlerde kullanılmasına izin verildiğine ilişkin paketlerdir.

Prosedür:

1. MorphoManager'da **Administration** (Yönetim) > **User Configuration**'a (Kullanıcı Yapılandırması) gidin.
2. Yeni bir kullanıcı yapılandırması oluşturmak için **Add**'e (Ekle) tıklayın.



3. **Adding User Policy** (Kullanıcı İlkesi Ekleme) iletişim kutusunda aşağıdakileri girin:

– Kullanıcı ilkesi için **Name** (Ad) ve açıklama (isteğe bağlı)
– **Access Mode** (Giriş Modu) `Per User`
– Giriş izni verilen gün ve saatleri yöneten bir **Access Schedule** (Giriş Programı)
– **Biometric Device Profile** (Biyometrik Cihaz Profili) için tanımlayıp kullandığınız aynı **Wiegand Profile** (Wiegand Profili).
– Cihaz kullanıcılarının cihazları kullanma şekillerine (parmak izi, parmak, yüz, kart vb.) bağlı bir **User Authentication Mode** (Kullanıcı Kimlik Doğrulama Modu). Ayrıntılar için **Tanımlama modunun seçilmesi** bölümüne bakın.

4. **Finish**'e (Bitir) tıklayın

Varsayılan Kullanıcı İlkesi bir `(1: Many)` kullanıcı kimlik doğrulama moduna sahip olacaktır. Diğer kimlik doğrulama modlarını kullanmak için ek kullanıcı ilkeleri oluşturun. Bir kullanıcı ilkesine atanabilecek her türlü çeşitli özellikler hakkında daha fazla ayrıntı için MorphoManager Kullanım Kılavuzu'na başvurun.

Bkz.

– *Tanıma modunun seçilmesi, sayfa 158*

22.4.4 Kullanıcı Dağıtım Grupları

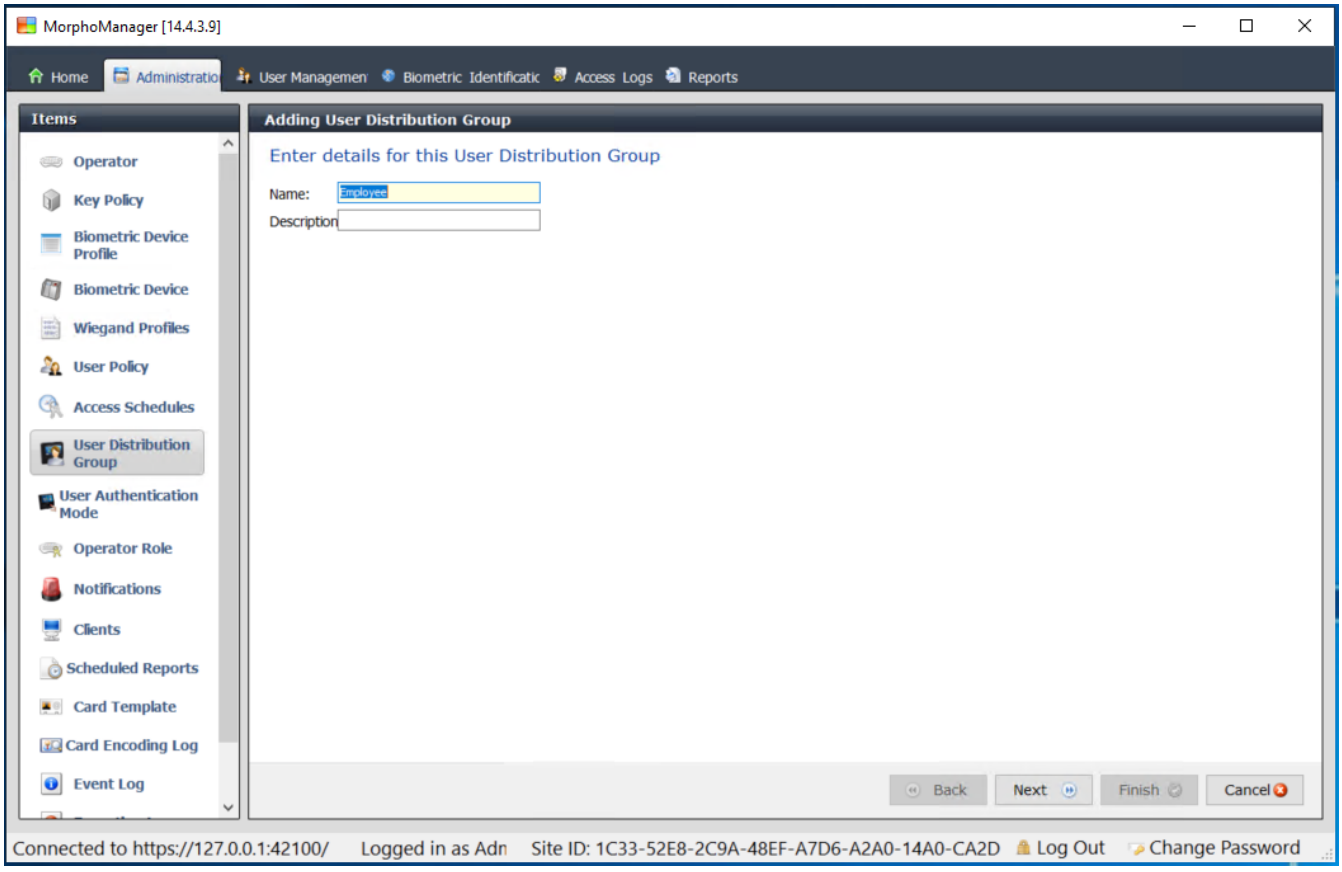
Kullanıcı Dağıtım Grupları, kullanıcıları biyometrik okuyucu veya MorphoManager istemci gruplarıyla eşleştirir.

Ön gereksinimler:

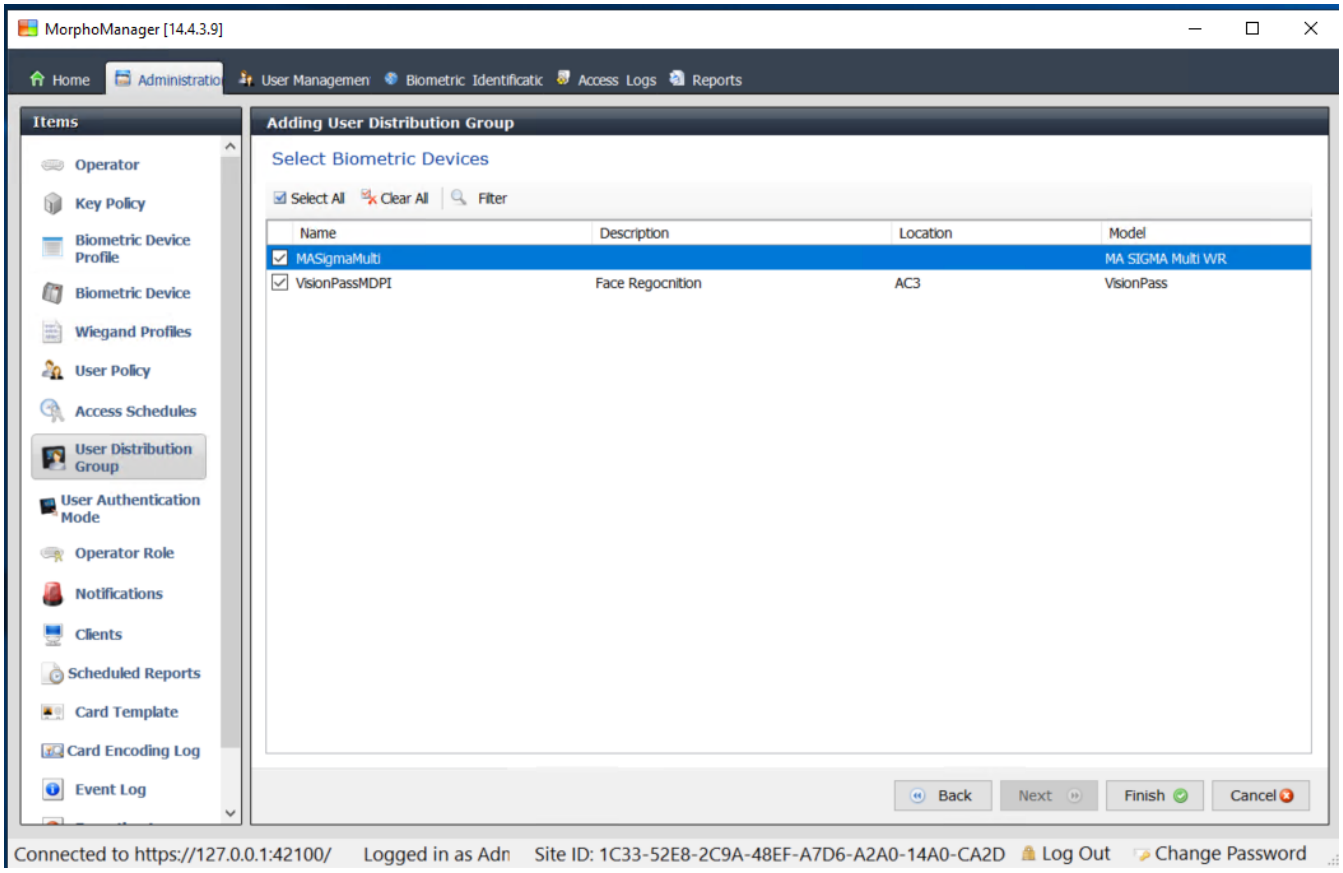
Her Kullanıcı Dağıtım Grubu ACS'de en az bir Kişi Sınıfı ile eşleştirilmelidir. Dolayısıyla kullandığınız her Kişi Sınıfı için en az bir Kullanıcı Dağıtım Grubu oluşturun.

Prosedür:

1. MorphoManager'da **Administration** (Yönetim) > **User Distribution Group**'a (Kullanıcı Dağıtım Grubu) gidin.
2. Yeni bir Kullanıcı Dağıtım Grubu oluşturmak için **Add**'e (Ekle) tıklayın.



3. **Select Biometric Devices** (Biyometrik Cihaz Seç) başlıklı sayfaya ulaşana kadar **Next**'e (İleri) tıklayın.
4. Bu Kullanıcı Dağıtım Grubundaki kişilerin kullanması gereken biyometrik cihazların onay kutularını seçin.



5. **Finish**'e (Bitir) tıklayın

22.4.5 BioBridge için ODBC ayarlama

Giriş

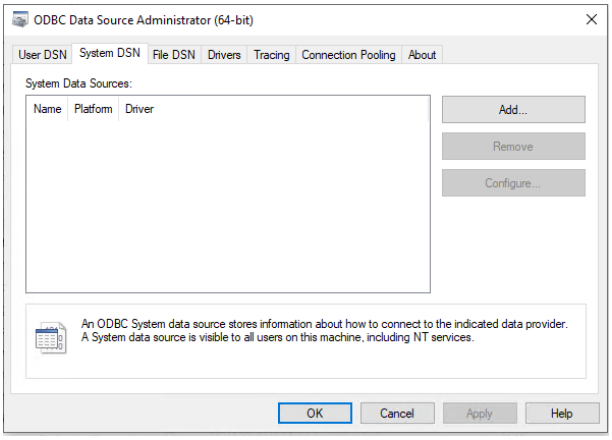
Açık Veritabanı Bağlantısı (ODBC), MorphoManager BioBridge'in kullanımı için bir ön koşuldur. ODBC farklı veritabanlarına erişmek için kullanılan standart bir programlama arayüzüdür. Önerilen sürücü: `OdbCDriver17SQLServer`

- BIS için sürücü, BIS kurulum medyasında `BIS\3rd_Party\OdbCDriver17SQLServer` adresinde bulunur.
- AMS için sürücüyü `www.microsoft.com` sayfasından indirin

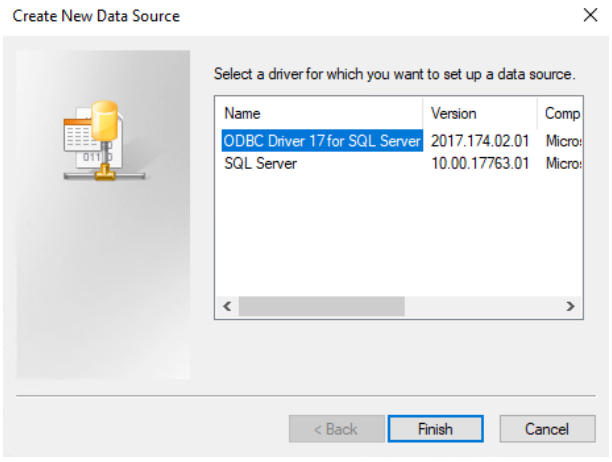
Veri Kaynağı Oluşturma

ODBC için Veri Kaynağı adı (DSN) oluşturma

1. Windows Denetim Masası'nda **Administrative Tools**'u (Yönetimsel Araçlar) seçin.
2. Listeden `ODBC Data Sources (64-bit)`'i seçin.
3. **System DSN** (Sistem DSN'si) sekmesini seçin.

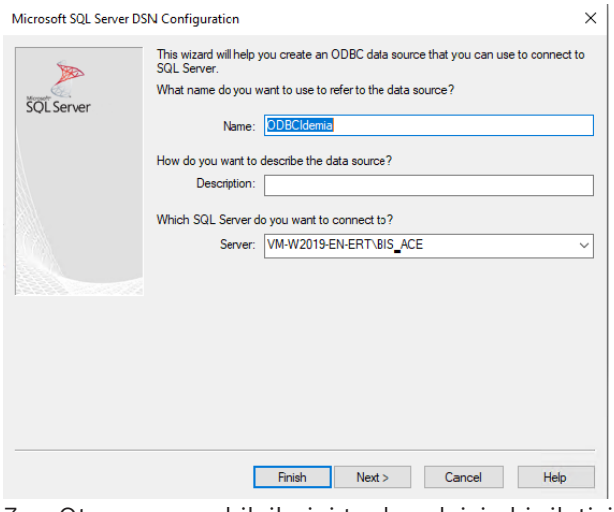


4. Sürücü seçmek için **Add**'e (Ekle) tıklayın.
5. Sürücü olarak `ODBC Driver 17 for SQL Server`'ı seçin ve **Finish**'e (Bitir) tıklayın.

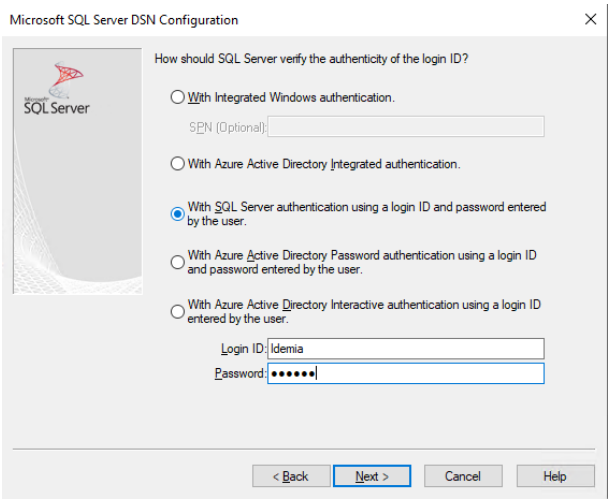


6. Veri kaynağı için aşağıdaki ayrıntıları girin.

– **Name** (Ad): Veri kaynağı için bir ad
– **Description** (Açıklama) (isteğe bağlı)
– **Server** (Sunucu): ACE veritabanının yüklü olduğu bilgisayarın adı ve veritabanının adı (varsayılan: <MyACS server>\`ACE`)



7. Oturum açma bilgilerini toplamak için bir iletişim kutusu görüntülendiğinde **Next> (İleri)** A 'ya tıklayın



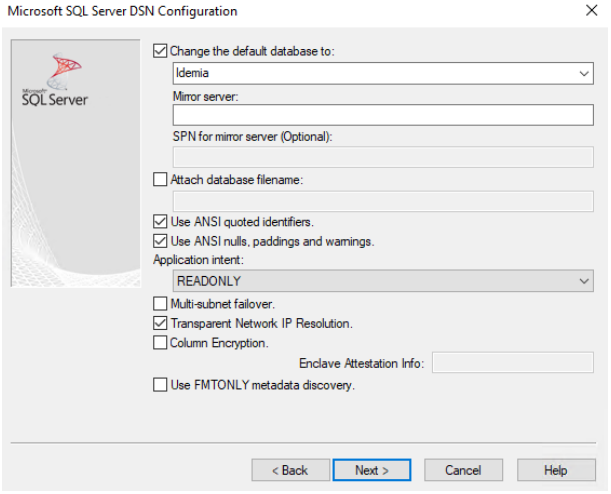
8. **With SQL Server authentication using a login ID...**'yi (Oturum açma kimliğiyle SQL Server kimlik doğrulaması ile) seçin
9. Aşağıdaki bilgileri girin:

– **Login ID** (Oturum açma kimliği): ACS'de yapılandırılan Idemia veritabanı kullanıcısının kullanıcı adı. Bu her zaman `Idemia`'dır.
– **Password** (Şifre): ACS'de yapılandırıldığında Idemia veritabanı kullanıcısı için ayarlanan şifredir

10. **Next>**'e (İleri) tıklayın
11. Sonraki iletişim kutusunda onay kutularını seçin:

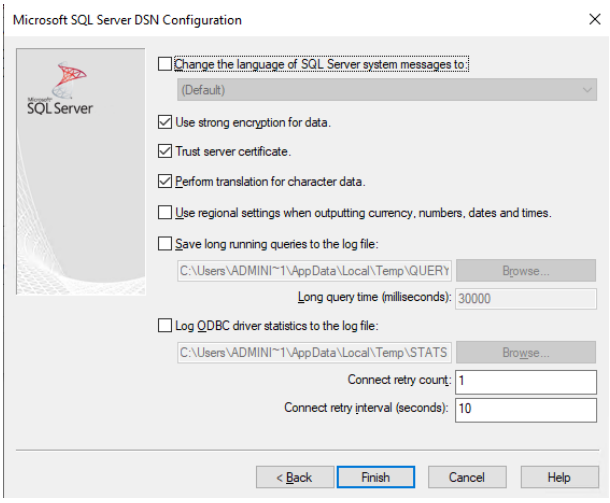
– **Varsayılan veri tabanını aşağıdakiler olarak değiştirin** ve `Idemia` 'yı seçin
– **Use ANSI quoted identifiers** (ANSI tırnak içinde tanımlayıcılar kullanın)
– **Use ANSI nulls, paddings and warnings** (ANSI null, dolgu ve uyarılarını kullanın)
– **Transparent Network IP Resolution** (Şeffaf Ağ IP Çözünürlüğü)

12. **Application intent**'i (Uygulama amacı) `READONLY` olarak ayarlayın

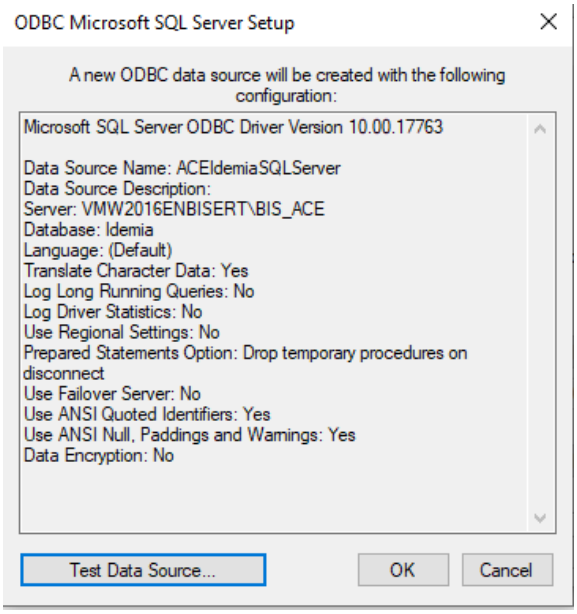


13. **Next>**'e (İleri) tıklayın
14. Sonraki iletişim kutusunda onay kutularını seçin

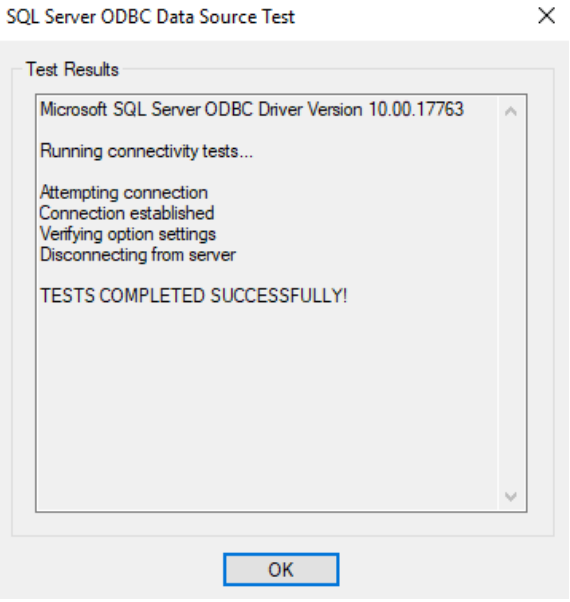
– **Use strong encryption for data** (Veriler için güçlü şifreleme kullan)
– **Perform translation for character data** (Karakter verileri için çeviri yap)
– **Trust server certificate** (Güvenli sunucu sertifikası)



15. **Finish**'e (Bitir) tıklayın
16. Sonraki iletişim kutusunda özet verileri gözden geçirin



17. **Test Data Source...**'a (Veri Kaynağını Test Et) tıklayın ve testlerin sorunsuz olarak tamamlandığından emin olun



18. Tüm değişiklikleri kaydedin ve ODBC kurulum sihirbazından çıkın.

22.4.6 BioBridge Sistem Yapılandırması

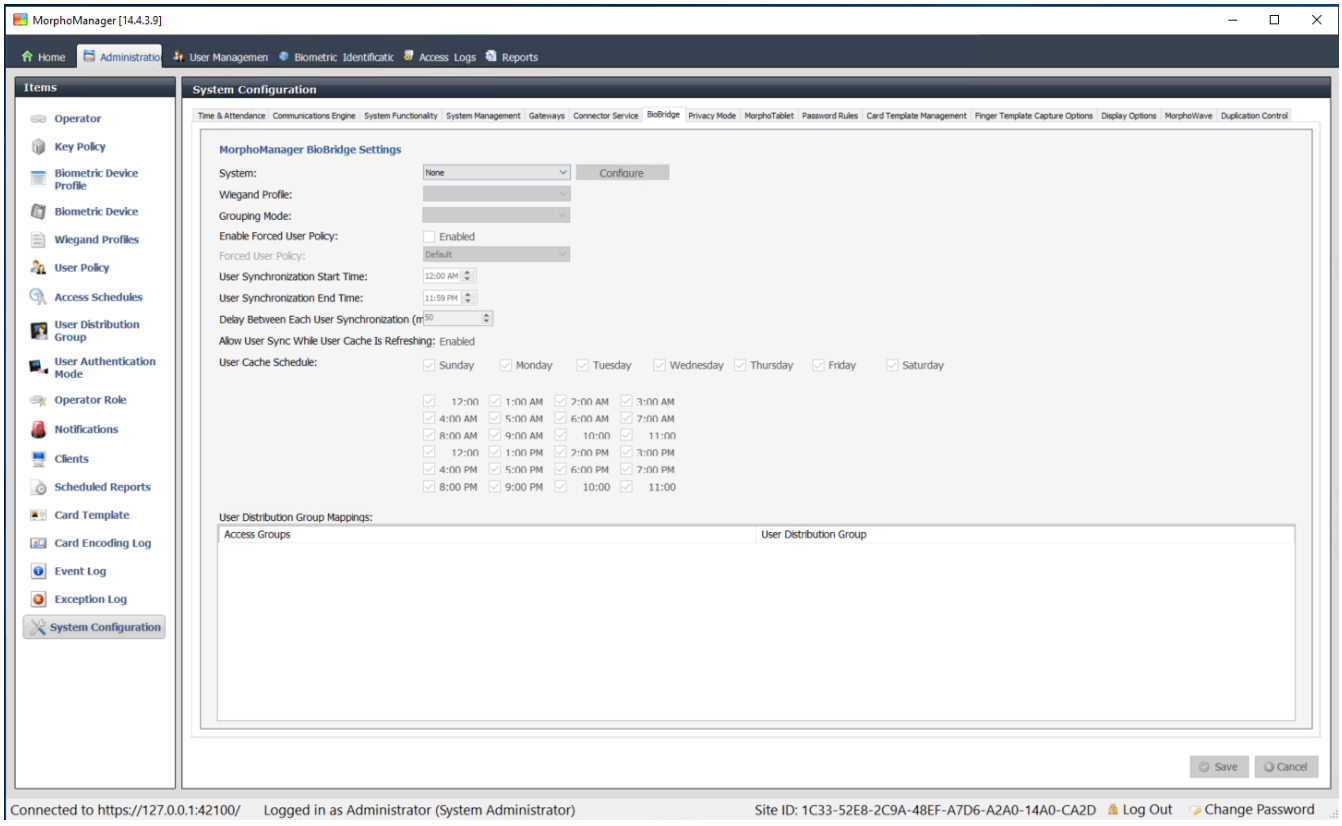
Bu bölümde, kartlı geçiş sistemleri için BioBridge arayüzünü kullanması için gereken kalan ayarlar açıklanmaktadır.

Ön koşul

ODBC, BioBridge için ayarlanmış olmalıdır. Bkz. *BioBridge için ODBC ayarlama, sayfa 168*

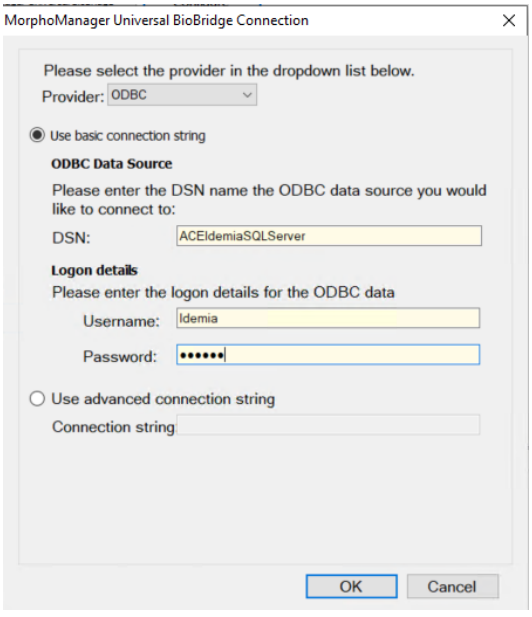
Prosedür:

1. MorphoManager'da **Administration** (Yönetim) > **System Configuration**'a (Sistem Yapılandırması) gidin.
2. **BioBridge** sekmesini seçin



3. **System** (Sistem) açılır listesinde, `MorphoManager Universal BioBridge`'i seçin
4. **Configure**

   'a (Yapılandır) tıklayın Bir açılır iletişim kutusu görünür.



Açılır penceredе

1. **Provider** (Sağlayıcı) açılır listesinde, `ODBC`'yi seçin
2. ODBC kurulumundan DSN'yi (Veri Kaynağı Adı) girin.
3. **Logon details**'in (Oturum açma ayrıntıları) altında, kullanıcı adı (`Idemia`) ve şifreyi ODBC kurulumunda tanımlandığı gibi girin.
4. **OK**'e (Tamam) tıklayarak **System Configuration** (Sistem Yapılandırması) iletişim kutusuna geri dönün.

System Configuration (Sistem Yapılandırması) iletişim kutusunda

1. **Wiegand Profile** (Wiegand Profili) için: Listeden daha önce tanımladığınız Wiegand profilini seçin.

Gruplandırma modu:

Bu ayar, MorphoManager'ın MM Universal BioBridge kullanıcılarını MorphoManager Kullanıcı Dağıtım Grupları ile eşleme yöntemini belirler. Aşağıdakilerden birini seçin:

– **Automatic** (Otomatik): Bu mod, aynı adlandırma kurallarına sahiplerse MM Universal BioBridge'deki **Erişim Seviyesi gruplarını** MorphoManager **Kullanıcı Dağıtım Grupları** ile otomatik olarak eşleştirir.
– **Manual** (Manuel): MM Universal BioBridge 'in **Access Level groups**'u (Giriş seviyesi grupları) ve MorphoManager'ın **User Distribution Group(s)**'u (Kullanıcı Dağıtım Grupları) aynı değilse **User Policy Mappings**'de (Kullanıcı İlkesi Eşlemeleri) eşlemeyi manuel olarak gerçekleştirebilirsiniz.

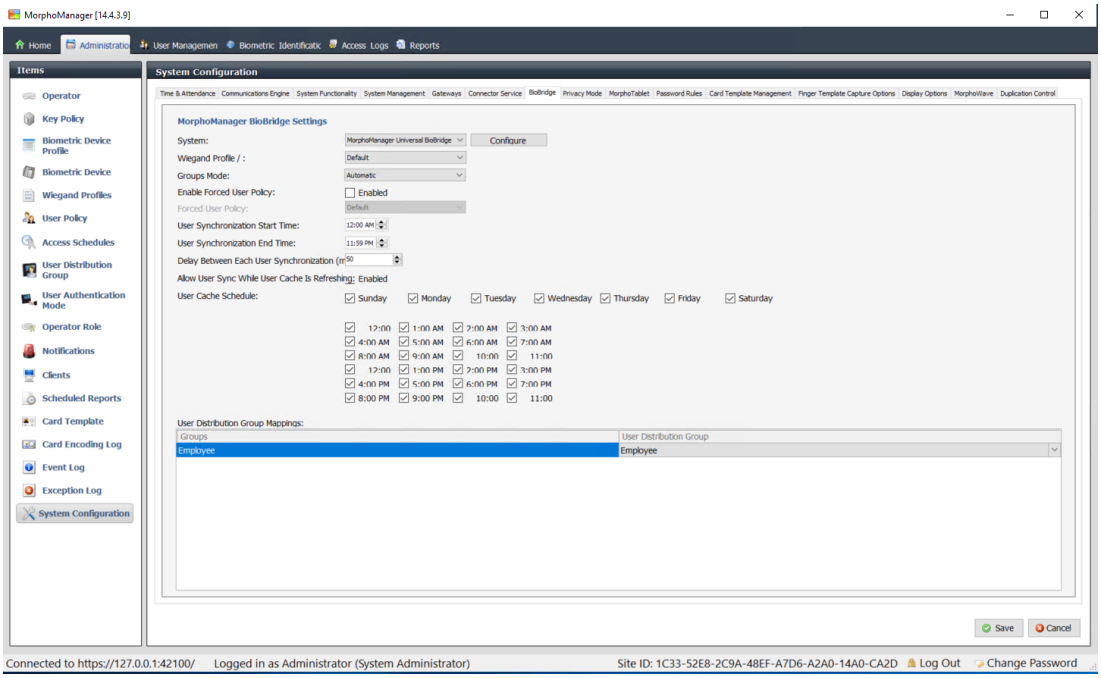
Diğer ayarlar

Çoğu durumda aşağıdaki ayarlar varsayılan değerlerinde bırakılabilir:

Enable Forced User Policy (Zorlanan Kullanıcı İlkesini Etkinleştir)	Seçildiğinde, BioBridge kayıt istemcisinde kayıtlı olan tüm kullanıcılar bitişik listeden seçilen kullanıcı ilkesini alır. Bu onay kutusunu işaretlerseniz her zaman `Per User` adlı kullanıcı ilkesini kullanın
User Synchronization Start Time and End Time (Kullanıcı Eşitleme Başlangıç ve Bitiş Saati)	Kullanıcı eşitleme altyapısının yalnızca bu iki zaman arasında çalışmasına izin verilir.
Delay between Each User Synchronization (Her Kullanıcı Eşitlemesi Arasındaki Gecikme)	Kullanıcı eşitlemeleri arasındaki zaman aralığı. Gecikmeyi artırmak sistem kaynaklarını kaydeder ancak tüm kullanıcıların güncelleştirilmesi için süreyi artırır.
Allow User Sync While User Cache Is Refreshing (Kullanıcı Önbelleği Yenilenirken Kullanıcı Eşitlemesine İzin Ver)	Etkinken, kullanıcı eşitleme altyapısı kullanıcı ön belleğini yenilemeye paralel olarak çalışır. Bu, sistem kaynakları bakımından çok zorludur. Büyük veritabanlarını kullanırken bu ayarı devre dışı bırakmanız önerilir.
User Cache Refresh Schedule (Kullanıcı Önbellek Yenileme Programı)	Kullanıcı önbelleğinin yenileneceği günler ve saatler. En yüksek doğruluk için bu, her zaman olmalıdır, ancak büyük veritabanlarına sahip sistemlerin performansı için bir ödün vermek gerekir.

Kullanıcı Dağıtım Grubu eşlemeleri

– Eşlemeler tablosunda tüm **Groups**'un (Gruplar) (ACS'de tanımlanan **Personnel classes** (Personel sınıfları)) **User Distribution groups** (Kullanıcı Dağıtım Grupları) ile (MorphoManager'da tanımlanır) eşlendiğinden emin olun.



22.5 BioBridge Kayıt İstemcisini Yapılandırma

Giriş

BioBridge kayıt istemcisi, kartlı geçiş sistemi kullanıcıları için biyometrik kayıtlar oluşturabileceğiniz bir bilgisayardır. BioBridge kayıt istemcisinin kurulumu 3 bölümden oluşur:

- MorphoManager'a bir kayıt operatörü ekleme
- Kaydolma görevleri için MorphoManager istemci bilgisayarlarını yapılandırma
- Kayıt istemcisini test etme

Ön koşullar

MorphoManager BioBridge, IDEMIA sistemleri için biyometrik kayıt yaptığınız her ACE iş istasyonuna yüklenmelidir.

22.5.1 MorphoManager'a kayıt operatörü ekleme

Prosedür

MorphoManager istemci yükleme kılavuzundaki talimatları izleyin.

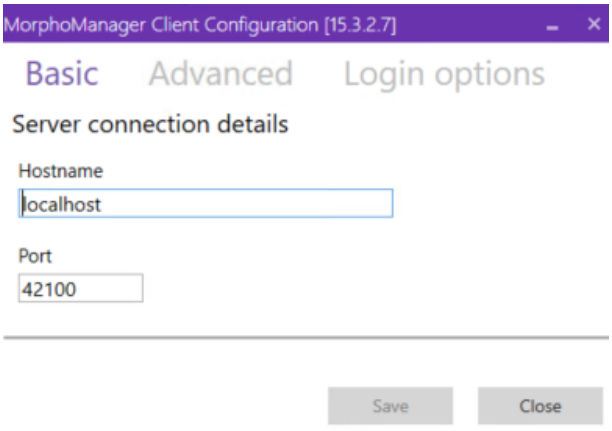
Not: Güvenlik nedeniyle, Active Directory kullanıcı hesapları önerilir.

22.5.2 Kaydolma görevleri için MorphoManager istemci bilgisayarlarını yapılandırma

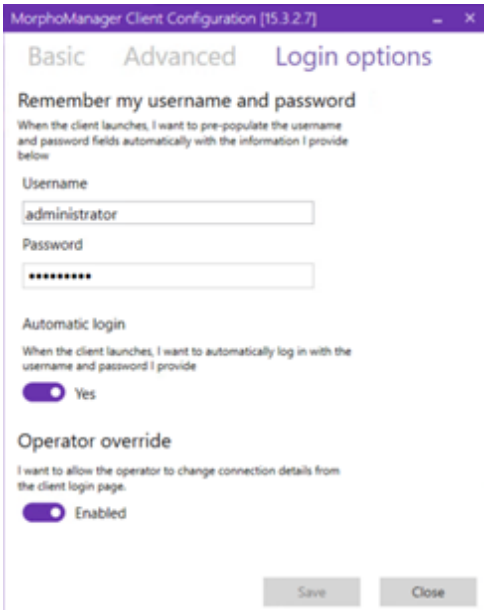
Biyometrik kayıt için kullanmak istediğiniz her bilgisayarda bu prosedürü gerçekleştirin.

Prosedür

1. MorphoManager yükleme dizininde (varsayılan: `C:\Program,Files(x86)\Morpho\MorphoManager\Client\ `) `ID1.ECP4.MorphoManager.AdvancedClientConfig.exe` dosyasını yönetici olarak yürütün

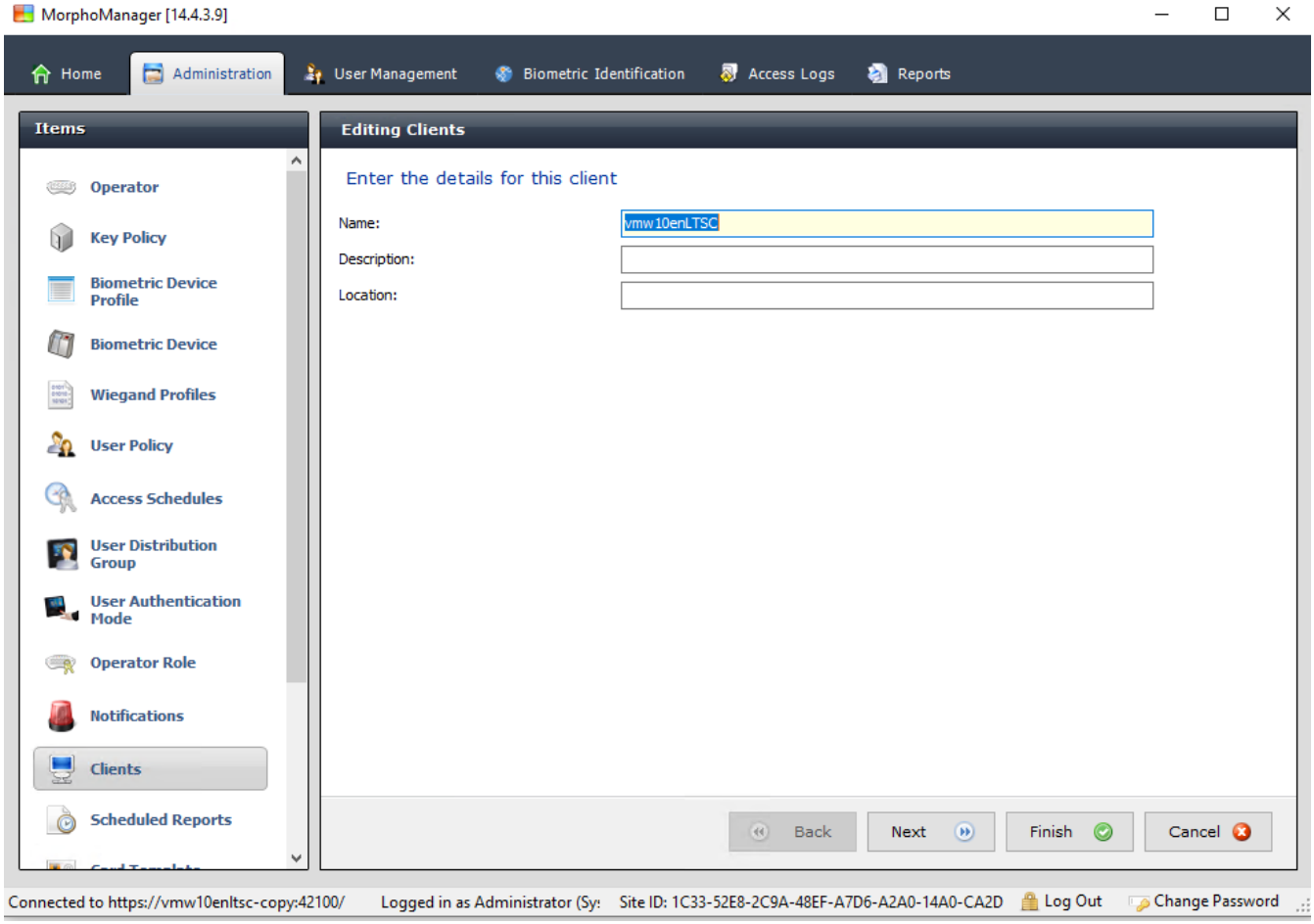


2. **Basic** (Temel) sekmesinde **Hostname**'in (Ana bilgisayar adı) altındaki Morpho sunucusunun ana bilgisayar adını girin.
3. Güvenli yüklemelerde, Morpho belgelerine göre Active Directory veya yerel kullanıcı adı ve parola kullanın.
4. Alternatif olarak, **Login options** (Oturum açma seçenekleri) sekmesinde [yüksek güvenlikli yüklemeler için ÖNERİLMEZ]

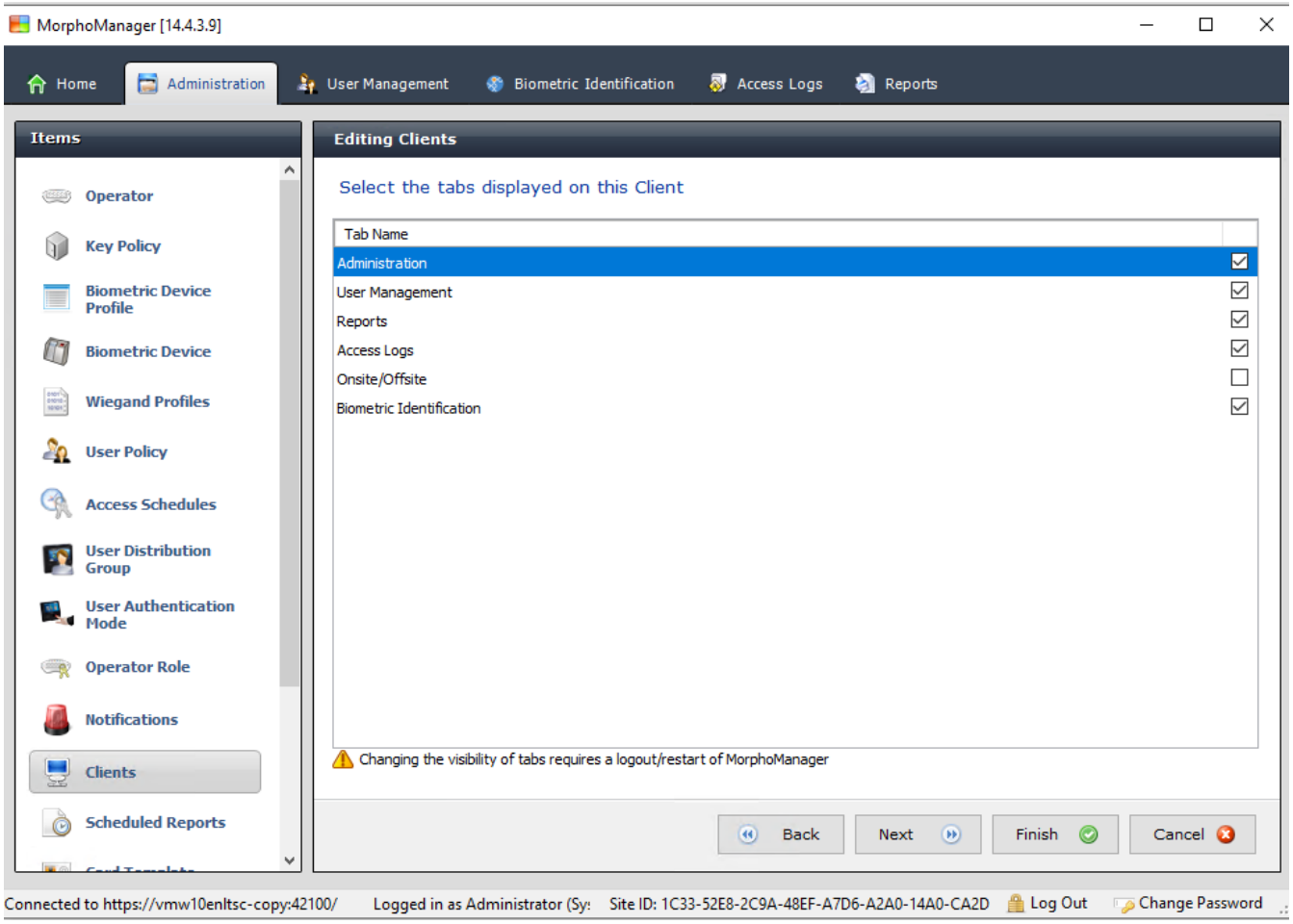


– Önceki bölümde, kayıt operatörü için girdiğiniz kullanıcı adını ve şifreyi girin
– **Automatic login**'i (Otomatik oturum açma) `Yes` olacak şekilde değiştirin.

1. MorphoManager yükleme dizininde (varsayılan: `C:\Program Files(x86)\Morpho\MorphoManager\Client\`) `Start ID1.ECP4.MorphoManager.Client.exe` dosyasını yönetici olarak yürütün
2. **Administration** (Yönetim) > **Clients**'a (İstemciler) gidin
3. Bir istemci bilgisayar seçin
4. **Edit**'e (Düzenle) tıklayın

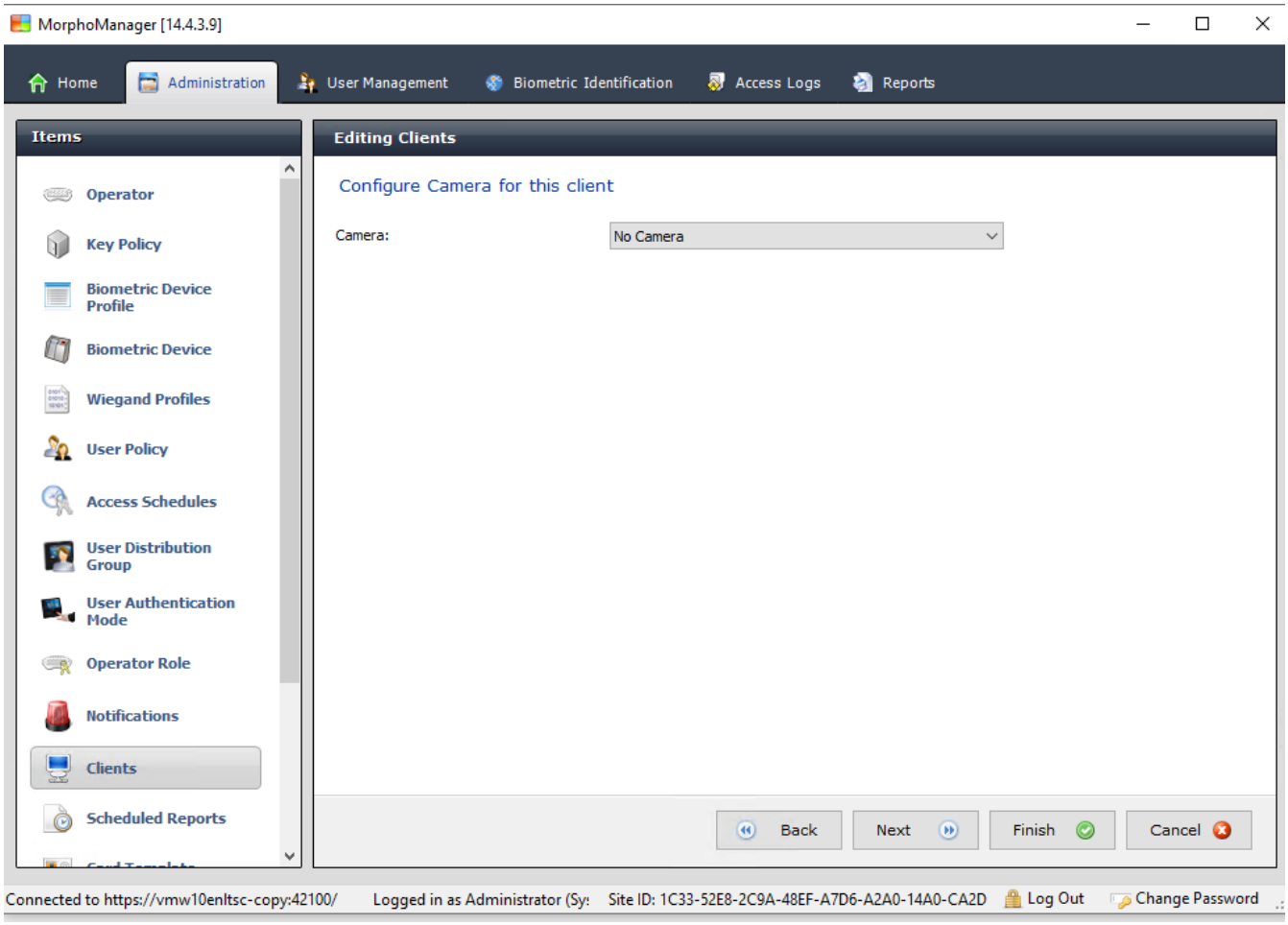


5. İstediğiniz kayıt istemcisinin adı ile isteğe bağlı olarak konumu ve açıklamayı girin.
6. **Next**'e (İleri) tıklayın

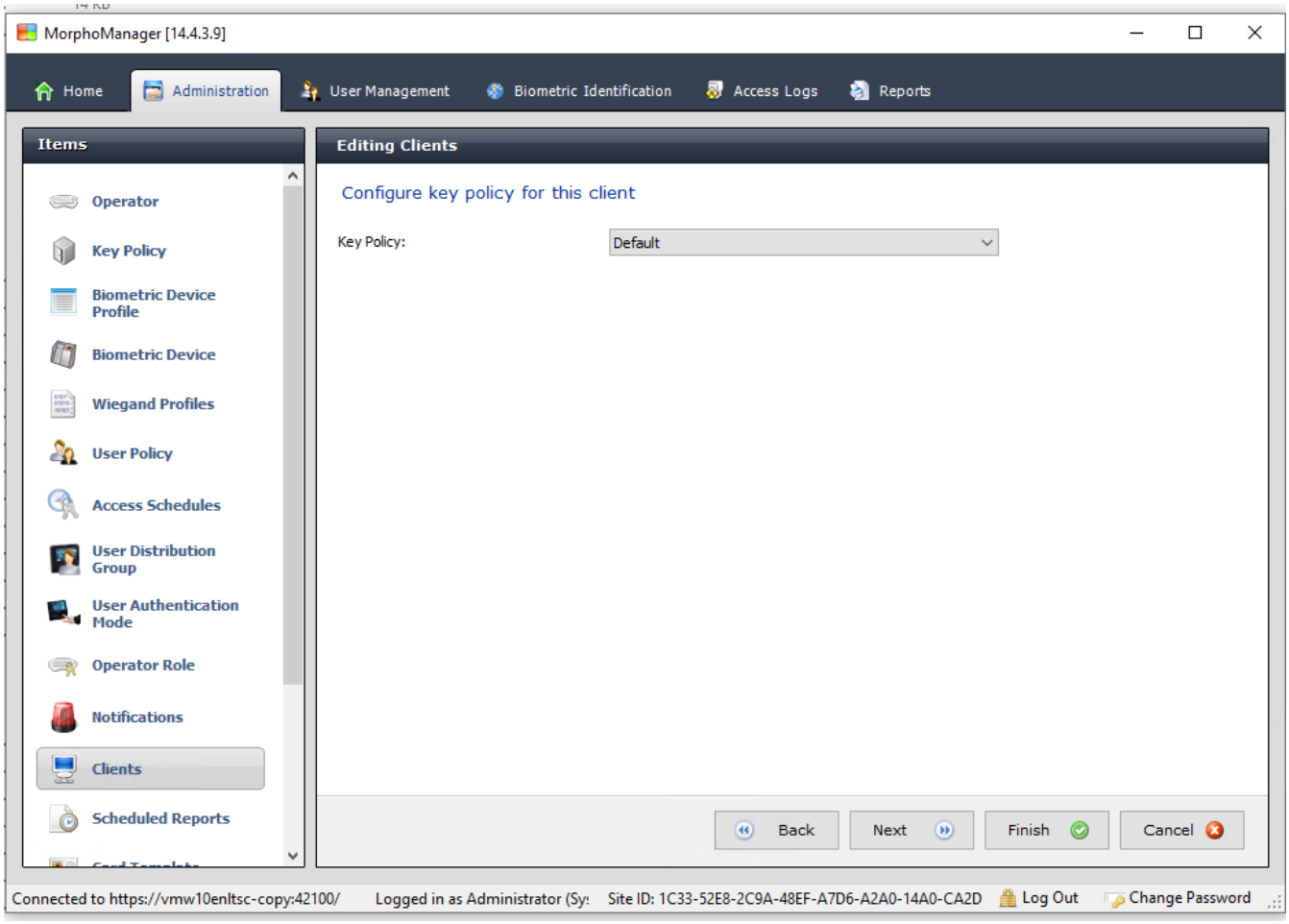


7. Kayıt istemcisinde görüntülemek istediğiniz sekmelerin onay kutularını seçin:
- **Administration (Yönetim),**
- **User Management (Kullanıcı Yönetimi),**
- **Reports (Raporlar),**
- **Access Logs (Giriş Günlükleri),**
- **Biometric Identification (Biyometrik Kimlik)**

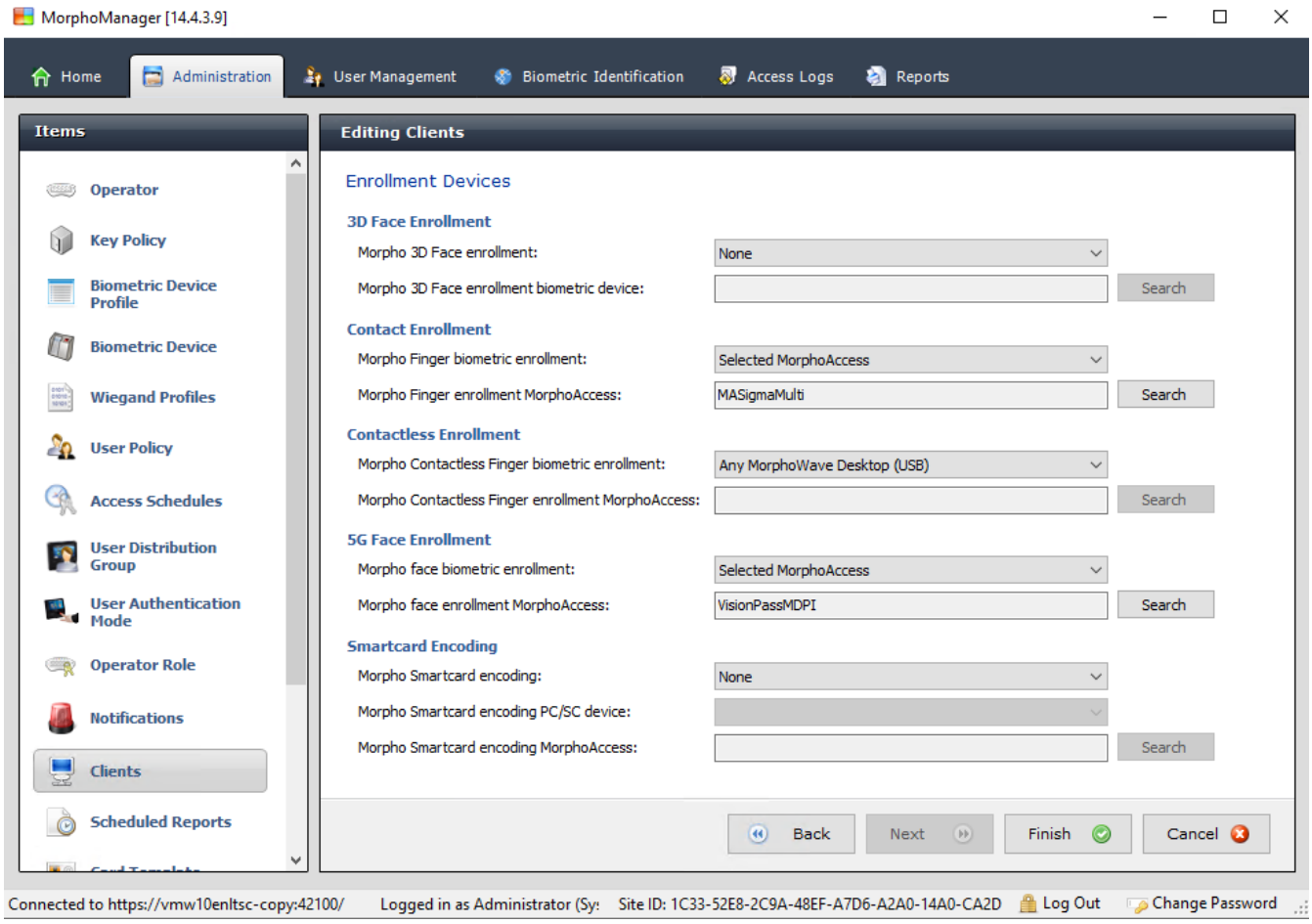
8. **Next**'e (İleri) tıklayın



9. **Camera** (Kamera) için listeden `No camera`'yı seçin
10. **Next**'e (İleri) tıklayın



11. **Key Policy** (Anahtar İlkesi) için listeden `Default`'u seçin
12. **Next**'e (İleri) tıklayın



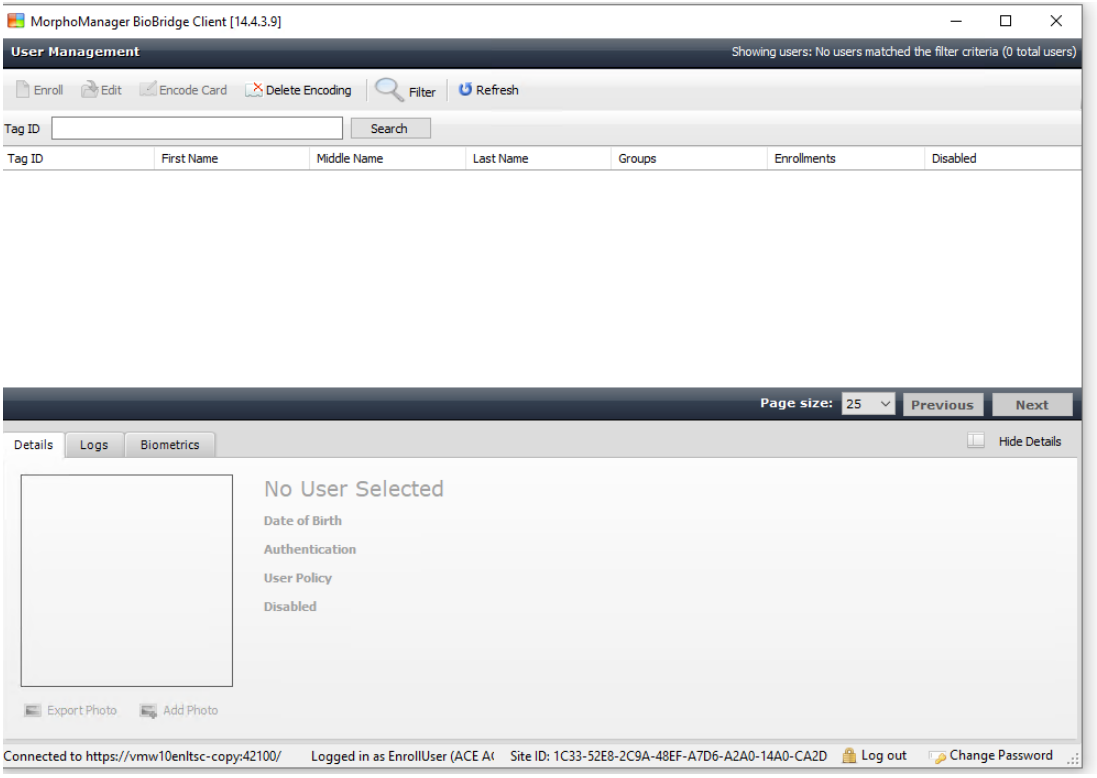
13. Kayıt iş istasyonunda kullanmak istediğiniz biyometrik kayıt okuyucusunu seçin
14. **Finish**'e (Bitir) tıklayın
15. MorphoManager uygulamasını kapatın

Bkz.

– *BioBridge Kayıt İstemcisini Yapılandırma, sayfa 175*

22.5.3 Kayıt istemcisini test etme

1. Morphomanager yükleme dizininde (varsayılan: `C:\Program,Files(x86)\Morpho\MorphoManager\Client\ `) `ID1.ECP4.MorphoManager.BioBridgeEnrollmentClient.exe` dosyasını yürütün



1. Kayıt operatörünün kullanıcı adını ve şifresini girmek zorunda kalmadan kayıt ekranını açabildiğinden emin olun.

22.6 Teknik notlar ve sınırlar

Resmi olarak desteklenen Windows işletim sistemleri
IDEMIA, Bosch ACS ile aynı Windows 10 sürümlerini destekler.

Microsoft SQL Server'ın resmi olarak desteklenen sürümü
Destek sürümü SQL Server 2017'dir

Kartlı geçiş sistemi başına bir adet IDEMIA sistemi
Bosch kartlı geçiş sistemi yalnızca bir adet IDEMIA sistemini destekleyebilir.

Kart sahibi başına bir adet IDEMIA kartı.
Bosch kartlı geçiş sistemleri kart sahibi başına birden fazla kartı desteklerken, IDEMIA yalnızca bir adet kartı destekler. Bu nedenle, kayıt sırasında ve BIS ile eşitleme yaparken, "Giriş", "Geçici" veya "Otopark" türündeki ilk geçerli kart (durum = 1) IDEMIA'ya atanır. Kart daha sonra engellenirse numarası hala iletilir ve olay günlüğüne kaydedilir.

Maksimum IDEMIA kart sahibi sayısı
BioBridge MorphoManager, 100.000 adede kadar kart sahibini işleyebilir.

Maksimum giriş grubu sayısı
IDEMIA 5000 adede kadar giriş grubunu (kullanıcı dağıtım grupları) destekler. Bunlar Bosch kartlı geçiş sistemindeki **Person classes**'la (Kişi sınıfları) eşleştirilir.

Şablon indirme performansı
- 1 cihaza 1000 şablon: İndirme işlemi 1 dakika sonra sürer.
- 100 cihaza 1000 şablon: Birkaç dakika içinde indirilir.

IDEMIA, bölümleri desteklemez
Bir IDEMIA sistemi entegre edildiğinde, ACS sistemi bir bölümün kart sahiplerini başka bir bölümün kartlı operatörlerinden güvenli bir şekilde tarayamaz. Bölümler arasında mutlak gizlilik zorunluysa IDEMIA sistemini entegre etmeyin.

Sanal Kartlar/Yalnızca PIN koduna göre giriş.
IDEMIA yalnızca PIN koduna göre girişi desteklemez. Fiziksel bir kart gereklidir.

IDEMIA baskı parmak işlevi
IDEMIA baskı parmak işlevi şu anda AMC denetleyicileri tarafından desteklenmemektedir.

Minimum tanıma kriterleri grubu.
IDEMIA sisteminde kayıt için en az aşağıdaki tanıma kriterleri gereklidir:
- First name (Ad),
- Soyadı,
- Kişi sınıfı
- Kart sahibine atanmış bir adet fiziksel kart.

Okuyucularda görüntülenen durumlar
Wiegand ve OSDP okuyucularında okuyucu durumu (ör. "Device Blocked" (Cihaz Engellendi)) görüntülenmez.

Yedekleme ve Geri Yükleme
IDEMIA ile bir yedeği geri yüklemeden önce, IDEMIA DataBridge sağlayıcı aracını kullanarak IDEMIA veritabanını silin ve yeniden oluşturun.
Biometric device (Biyometrik cihaz) iletişim kutusunda tüm yapılandırmaların IDEMIA okuyucularına doğru şekilde gönderildiğinden emin olun. Senkronizasyon görevlerinden biri başarısız olursa, okuyucu yapılandırmasını yeniden oluşturun:
1. MorphoManager'da **Biometric device**'a (Biyometrik cihaz) gidin.
2. Etkilenen cihazı seçin.
3. **Rebuild**'i (Yeniden oluştur) tıklayın.

ACS kartı işlevlerinin IDEMIA kimlik doğrulama modlarıyla uyumluluğu:

İşlevler	Mod: Kart VE Bio	Mod: Kart VEYA Bio
Giriş kartları: Ekleme	Tamam	Tamam
Giriş kartları: Güncelleme	Tamam	Tamam
Giriş kartları: Silme	Tamam	Tamam
Giriş kartları: Birden fazla kart	Yalnızca ilk kart	Biometri için kullanılan ilk kart.
Yedek kart	Tamam	Tamam

Geçici kart	Tamam	Tamam
Geçici kart: Yalnızca süre	Tamam	Tamam
Geçici kart: tüm kartları hemen devre dışı bırakma süresi	Tamam	Tamam
Geçici kart: Belirlenen süreden sonra kartları otomatik olarak etkinleştir	Tamam	Tamam
Geçici kart: Kartları devre dışı bırak ve otomatik olarak etkinleştir	Tamam	Tamam
Alarm kartları	Desteklenmiyor	Tamam
Office mode (Ofis modu)	Desteklenmiyor (*)	Desteklenmiyor (*)
Ziyaretçi	Muhtemelen ilk ziyaretçinin biyometrik verileri karta atanmış olarak kalmıştır.	Muhtemelen ilk ziyaretçinin biyometrik verileri karta atanmış olarak kalmıştır.
Güvenlik görevlisi	Desteklenmiyor	Biometri desteklenmiyor. Kart çalışıyor.
Otopark Kartı	Tamam	Tamam
PIN kodu	Desteklenmiyor (*)	Desteklenmiyor (*)
3. taraf doğrulama	PIN kodu yok (*)	PIN kodu yok (*)
(*) IDEMIA okuyucu tuş takımı okuyucusu olarak kullanılamaz		

23 EN 60839 elde etmek

Giriş

EN 60839, aşağıdakilere ait donanım ve yazılımları için bir Avrupa uluslararası standartlar ailesidir:

- Alarm ve elektronik güvenlik sistemleri
- Elektronik kartlı geçiş sistemleri

Giriş kontrol sisteminizin bu standarda uygunluğunu sağlamak üzere yapılandırmanın bazı bölümlerinin uyarlanması gerekebilir. Aşağıdaki listede en önemli kısımlar bulunmaktadır. Tam bir liste için lütfen kendi ülkenizde kabul edilen standarda bakın.

AMS 4.0'ı EN 60839, sınıf 2 sertifikalı sistem olarak kullanmak üzere gerekenler

- Sistem, her MAC başına bir bölge kullanımı açısından Genel anti-passback gereksinimlerini karşılamalıdır.
- AMS sisteminin kullanılabilen farklı zaman dilimleri, MAC'lerin sayısına bağlı olmalıdır. Her MAC için ayrı bir saat dilimi kullanılabilmelidir.
- Kapı kontaklarının kabloları, yangın veya hırsızlık önleme sistemi tarafından tetiklenen bir acil tahliyede kapının açılmasını engellememelidir.
- RS485 arabiriminde yalnızca OSDP okuyucuları şifreleme kullanmalıdır.
- Yapılandırma moduna erişim sıkı bir şekilde kontrol edilmelidir. Bu, örneğin bilgisayarları güvenli alanlara yerleştirerek ve oturum açma oturumlarındaki zaman aşımları aracılığıyla, özellikle uygulama ve işletim sistemi düzeyindeki hareketsiz kalma zaman aşımları aracılığıyla sağlanabilir.
- Ağ ve elektrik kabloları güvenli bir alana döşenmeli veya boruların içinde tamamen kapalı durumda olmalıdır.
- Güvenli olmayan alana yalnızca kart okuyucular monte edilebilir, diğer tüm cihazlar güvenli alanlarda bulunmalıdır.
- Biyometrik veya fiziksel kimlik bilgileri için minimum doğrulama PIN uzunluğu en az `4` olarak ayarlanmalıdır.
- Kimlik PIN'lerinin minimum uzunluğu en az `8` olarak ayarlanmalıdır.
- Ana sunucu bilgisayarı, bağlantı sunucuları, MAC sunucuları ve istemciler bir ağ zaman sunucusuyla senkronize edilmelidir.
- Yerel giriş kontrol cihazlarında (örneğin AMC'ler) güç izleme etkinleştirilmelidir.
- Yerel giriş kontrol cihazlarının (örneğin AMC'ler) çevrimdışı çalışmasına yalnızca ağ arızaları sırasında izin verilmelidir. Örneğin, AMC parametresi olan **Host timeout** (Ana bilgisayar zaman aşımı) `0` olarak ayarlanmamalıdır.

Şifre gücü için kurallar

- Şifre minimum uzunluğu en az `5` karakter olmalıdır.

24 Giriş yetkilerini ve profillerini tanımlama

24.1 Giriş yetkileri oluşturma

İletişim yolu

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

Prosedür

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.
   Bu, 14-365 gün arasında belirlenen bir süredir. Bu yetkinin atandığı bir kişi, belirlenen süre içinde kullanılamazsa yetkiyi kaybeder. Atanan kişi yetkiyi her kullandığında, zamanlayıcı yeniden sıfırdan başlatılır.
6. (Zorunlu) En az bir **Entrance** (Giriş) atayın.
   Kapı modellerine bağlı olarak mevcut girişler farklı sekmelerde gösterilir.
   (Genel) **Entrance** (Giriş), **Time management** (Zaman yönetimi), **Elevator** (Asansör), **Parking lot** (Otopark), **Arming Intrusion detection** (Hırsız algılamayı kurma).
   Aşağıda açıklandığı gibi çeşitli sekmelerdeki listelerden girişleri tek tek seçin.
   Alternatif olarak, her sekmedeki **Assign all** (Tümünü ata) ve **Remove all** (Tümünü kaldır) düğmelerini kullanın.
   - **Entrance** (Giriş) sekmesinde, **In** (Giriş) veya **Out** (Çıkış) onay kutularından birini veya ikisini birden seçerek bir giriş tercih edin.
   - **Time management** (Zaman yönetimi) sekmesinde (zaman ve devam okuyucuları için) **In** (Giriş) veya **Out** (Çıkış) onay kutularından birini veya ikisini birden seçin
   - **Elevator** (Asansör) sekmesinde farklı katları seçin
   - **Parking lot** (Otopark) sekmesinde bir otopark ve bir park bölgesi seçin
   - **Arming Intrusion detection** (Hırsız alarmı algılamayı kurma) sekmesinde **Armed**'ı (Kurulu) veya **Disarmed**'ı (Devre Dışı) seçin.
7. Listeden uygun MAC'i seçin
8. Yetkiyi kaydetmek için Save'e (Kaydet)  tıklayın

Uyarı!

Düzenleyen profil kilitlenmedikçe, yetkilerde sonradan yapılan değişiklikler mevcut atananları etkiler.

Örnek: 60 günlük bir Hareketsizlik sınırı 14 güne indirilirse söz konusu yetkiyi son 14 günde kullanmayan herkes yetkiyi kaybeder.

İstisna: Bir yetki, bir Çalışan Kimliğine (Kişi tipi) **kilitlenen** bir giriş profilinin parçasıysa , bu tür kişilerin yetkideki hareketsizlik sınırlarından etkilenmez. Profil kilitleri aşağıdaki onay kutusu ile ayarlanabilir.

Main menu (Ana menü) > **System data** (Sistem verileri) > **Person Types** (Kişi Tipleri) > tablo: **Predefined Employee IDs** (Önceden Tanımlanan Çalışan Kimlikleri) > onay kutusu: **Profile locked** (Profil kilitli)

24.2 Giriş profilleri oluşturma

Not: Yetkileri paket haline getirmek için giriş profillerini kullanma
Tutarlılık ve kolaylık için giriş yetkileri tek olarak atanmaz, ancak genellikle **Giriş profilleri** halinde paketlenerek bu şekilde atanır.

– Main menu (Ana menü): **> System data (Sistem verileri)** > **Access profiles** (Giriş profilleri)

Ön gereksinimler
Giriş Yetkileri sistemde zaten tanımlanmıştır.

Prosedür

1. Araç çubuğundaki **New**'a (Yeni)  tıklayarak giriş alanlarını temizleyin.
   Alternatif olarak, mevcut olana göre yeni bir profil oluşturmak için **Copy**'ye (Kopyala)  tıklayın.
2. Profil için benzersiz bir ad girin
3. (İsteğe bağlı) Bir açıklama girin
4. (İsteğe bağlı) Bu profili ziyaretçilerle sınırlamak için **Visitor profile** (Ziyaret profili) onay kutusunu seçin
5. (İsteğe bağlı) **Standard duration of validity** (Standart geçerlilik süresi) için bir değer ayarlayın.
   – Değer ayarlanmamışsa profil süresiz olarak atanır.
   – Bir değer ayarlanmışsa bu değer daha sonra profilin sonraki atamasının son kullanma tarihini hesaplamak için kullanılır.
6. (Zorunlu) En az bir **Authorization** (Yetki) atayın:
   Atama için kullanılabilen yetkiler sağda belirtilir.
   Zaten atanmış olan yetkiler solda gösterilir.
   Öğeleri seçin ve ardından öğeleri bir listeden diğerine taşımak için listeler arasındaki düğmelere tıklayın.
   –  seçilen öğeyi atar.
   –  seçilen öğenin atamasını kaldırır.
7. Profili kaydetmek için Kaydet'e  tıklayın.

25 Personel verilerini oluşturma ve yönetme

İletişim yolu

Main menu (Ana menü) > **Personnel data** (Personel verileri) > <alt iletişim kutuları>

Genel Prosedür

1. **Persons** (Kişiler) alt iletişim kutusuna kişinin kimlik verilerini girin.
2. **Cards** (Kartlar) alt iletişim kutusunda:
   - Giriş profillerini veya tek giriş yetkilerini atayın.
   - Gerekirse bir zaman modeli atayın.
   - Kartı atayın.
3. **PIN-Code** (PIN Kodu) alt iletişim kutusunda: Gerekirse bir PIN Kodu atayın.
4. **Print Badges** (Kimlik Kartlarını Yazdır) alt iletişim kutusunda kartı yazdırın.

Visitors (Ziyaretçiler) için, aşağıdaki işlemleri yapın:

- **Visitors** (Ziyaretçiler) menüsünün **Visitors** (Ziyaretçiler) iletişim kutusuna kişisel verileri girin ve gerekirse bir eşlik eden atayın.

Uyarı!

Kimlik kartları ile giriş yetkilerinin aynı anda atanması gerekmez. Bu nedenle kimlik kartları kişilere giriş yetkileri atanmadan atanabilir. Bunun tersi de mümkündür. Ancak, iki durumda da bu kişilere tüm giriş reddedilir.

Kartları tarama işlemi.

Kartlar okuyucularda tarandığında, okuyucu bir dizi kontrol gerçekleştirir:

- Kart geçerli ve sistemde kayıtlı mı?
- Kart sahibi şu anda engellenmiş (sistemde devre dışı bırakılmış) durumda mı?
- Kart sahibi bu yönde giriş için giriş yetkisine sahip mi?
- Giriş yetkisi bir alan-zaman yetkisi mi? Öyleyse, tarama süresi zaman modeli tarafından belirlenen süreler içinde mi?
- Giriş yetkisi etkin mi (**süresi dolmuş** mu yoksa **engellenmiş** (devre dışı) mi)?
- Kart sahibi bir zaman modeline tabi mi? Tabiyse tarama süresi tanımlanan aralıklar içinde mi?
  Ön koşul: Zaman modeli kontrollerinin ilgili okuyucuda etkinleştirilmesi gerekir.
- Kart sahibi Giriş sırası izlemeye göre doğru konumda mı?
  Ön koşul: Giriş sırası izleme, ilgili okuyucuda etkindir.
- Bu okuyucunun hedef alanı için maksimum kişi sayısı tanımlandı mı ve bu sayıya zaten ulaşıldı mı?
- Giriş sırası izleme söz konusu olduğunda, anti-passback dahil: Bu kart, anti-passback tarafından belirlenen engelleme zamanı dolmadan önce bir okuyucuda taranıyor mu?
- Ek bir PIN kodu gerekli mi? **Ön koşul**: Okuyucunun klavyesi olmalıdır.
- Bir tehdit seviyesi devredeyse kart sahibinin **Kişi güvenlik profili** en azından bu tehdit seviyesindeki okuyucunun güvenlik seviyesine eşit **güvenlik seviyesine** sahip mi?

25.1 Kişiler

Aşağıdaki tabloda **Persons** (Kişiler) iletişim kutularında *varsayılan olarak* görüntülenen veriler listelenmektedir. İletişim kutuları son derece özelleştirilebilirdir. **Custom fields for personnel data** (Personel verileri için özel alanlar) bölümüne bakın.
Neredeyse tüm alanlar isteğe bağlıdır. Zorunlu alanlar kullanıcı arayüzünde altı çizili etiketlerle açıkça işaretlenir.

Sekme	Alan adı

İletişim kutusu başlığı	Name (Ad)
	First name (Ad)
	Birth name (Kızlık soyadı) (bazı kültürlerde doğum adı olarak anılır)
	Personnel no. (Personel no.)
	Date of birth (Doğum tarihi)
	Employee ID (Çalışan kimliği) (Kişi türü olarak da bilinir)
	Gender (Cinsiyet)
	Company (Şirket)
	Title (Başlık)
	ID card no. (Kimlik kartı no.)
	Car license no. (Araba ruhsatı no.)
Address (Adres)	Zip code (Posta kodu) (bazı kültürlerde zip kodu olarak anılır)
	Cadde, no.
	Ülke, eyalet
	Milliyet
İletişim	Diğer telefon
	Şirket telefonu
	Şirket faksı
	Cep telefonu
	Telefon
	E-Posta
	Web sayfası adresi
Ek Kişi Verileri	Lakap (bazı kültürlerde diğer ad olarak kullanılır)
	Doğum yeri
	Medeni durum
	Resmi kimlik kartı
	Kimlik kartı no.
	Geçerlilik bitişi
	Yükseklik
Ek Şirket Verileri	Departman
	Konum
	Maliyet merkezi
	İş unvanı

	Eşlik eden (Eskort)
	Ziyaret nedeni
	Açıklamalar
Açıklamalar	(Kişi hakkında notlar ve açıklamalar için serbest biçimli bir metin alanı sağlar.
Fazladan Bilgi	Kullanıcı tanımlı 10 alan
İmza	İmzaları al, yeniden kaydet veya sil
Parmak izleri	Parmak izlerini biyometrik kimlik bilgileri olarak alın, yeniden kaydedin, silin ve test edin. Baskıyı işaret etmek için belirli parmak izlerini atayın.

Bkz.

– *Personel verileri için Özel Alanlar, sayfa 128*

25.1.1 Kart kontrolü veya Bina kontrolü seçenekleri

Genel bilgiler

Kart sahiplerinin 1 veya 2 genel giriş kontrol cihazı kartıyla kartlarını etkinleştirebilmelerini sağlamak için **Card control** (Kart kontrolü) sekmesini kullanın. **Persons** (Kişiler) iletişim kutusunda bir **Building control** (Bina kontrolü) onay kutusunu seçerek özelliği bir kart sahibine atayabilirsiniz. **Building control** (Bina kontrolü) (veya **Card control** (Kart kontrolü)) onay kutuları varsayılan olarak Kişinin **Card control** (Kart Kontrolü) sekmesinde görünen ancak başka herhangi bir yere konumlandırılabilen önceden tanımlanmış özel alanlardır.
Bir Bina kontrol seçeneği için iki ana görev vardır. Bunlar aşağıda açıklanmıştır:

– Onay kutusunu yapılandırma: Uygun bir etiket ekleyin ve (isterseniz) **Persons** (Kişiler) iletişim kutusunun farklı bir sekmesine konumlandırın.
– İşlevi bir AMC kartlı giriş kontrol cihazındaki bir çıkışa ve bir onay kutusuna atayın.

Ön koşullar

– Kartlı geçiş cihazı çıkışı kart tarafından etkinleştirilecek cihaza elektriksel olarak bağlıdır.

İletişim yolu

– AMS Ana menüsü > **Configuration** (Yapılandırma) > **Options** (Seçenekler) > **Custom fields** (Özel alanlar) > **Card control** (Kart kontrolü) sekmesi

Onay kutularını yapılandırma

1. **Custom fields** (Özel alanlar) sayfasında üstteki bölmede **Details** (Ayrıntılar) sekmesini seçin.
2. 1 veya 2 olmak üzere kullanmak istediğiniz **Building control** (Bina kontrolü) işlevini seçin.
3. Uygun bir adı etiketin üzerine yazdırın (önerilir). İsterseniz onay kutusunu **Card control**(Kart kontrolü) dışındaki bir sekmede konumlandırın. Daha ayrıntılı talimatlar için aşağıdaki bağlantıdan **Previewing and editing Custom fields** (Özel alanlara ön izleme yapma ve bu alanları düzenleme) bölümüne bakın.

İşlevi kartlı geçiş cihazı çıkışına ve onay kutusuna atama

Aşağıdaki bağlantıdan **AMC parametreleri ve ayarları** bölümüne bakın.

1. **Cihaz Düzenleyicisi**'nde, cihaz ağacında, çıkış sinyalini kullanmak istediğiniz AMC kartlı geçiş kontrol cihazını seçin.
2. **Çıkışlar** sekmesindeki üst bölmede, kullanmak istediğiniz çıkışı seçin.
3. Orta bölmede **Output data**'yı seçin (Çıkış verileri) **25** yazın ve **Card control**'u (Kart kontrolü) seçin
4. Çıkışı alt bölmeye eklemek için **>** düğmesine tıklayın.
5. Alt bölmedeki **Param11 sütununda** önceki **Onay kutularını yapılandırma** prosedüründe seçtiğiniz Bina kontrol işlevi etiketini seçin.
6. Cihaz ağacını seçin.

Bkz.
- *AMC parametreleri ve ayarları, sayfa 53*
- *Özel alanlara ön izleme yapma ve bunları düzenleme, sayfa 128*

25.1.2 Fazladan bilgi: Kullanıcı tanımlı bilgileri kaydetme

Extra info (Fazladan bilgi) sekmesini, diğer sekmelerde verilmeyen ek alanları tanımlamak için kullanın. Hiçbir ek alan tanımlanmadıysa sekme boş kalır.

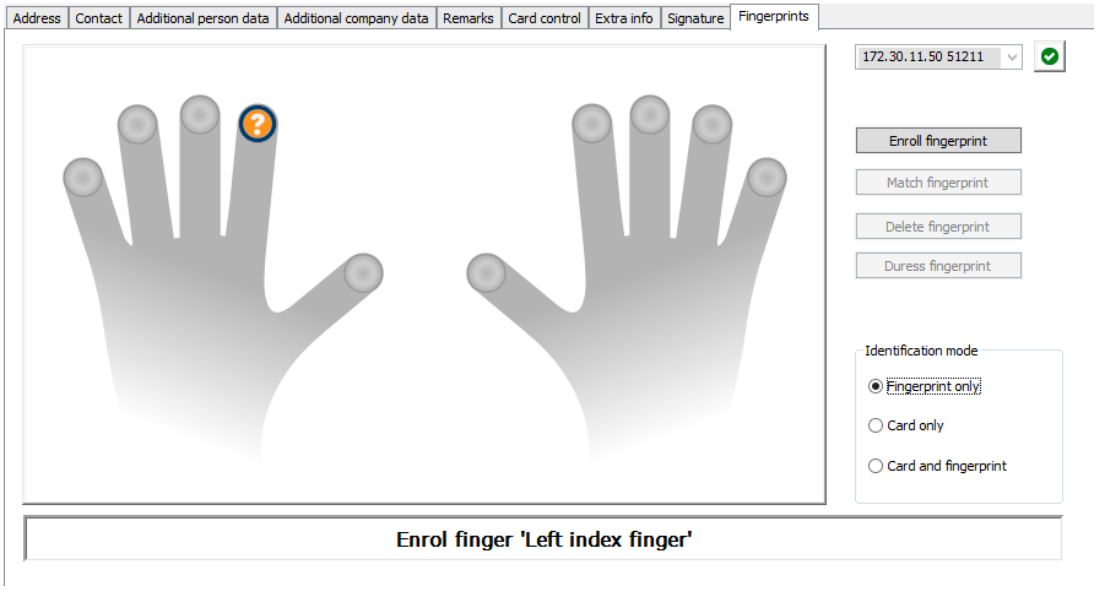
25.1.3 İmzaları kaydetme

İmzaları almak için sistemde Signotec şirketi ürünü bir imza alma pedi bağlı ve yapılandırılmış olmalıdır. Emin olamazsanız sistem yöneticinize danışın.

1. **Signature** (İmza) sekmesine tıklayın
2. Yeni bir imza kaydetmek için **Capture Signature** (İmza Al) düğmesine tıklayın.
3. Özel kalemini kullanarak doğrudan imza alma pedinin üzerinde imzalayın.
4. Onaylamak için imza alma pedindeki onay işaretine tıklayın.
   Yeni imza artık ekranda görüntülenir (Büyütülmüş görünüm için imzaya tıklayın).

İlgili prosedürler:
- Mevcut bir imzanın üzerine yazmak için de **Capture Signature** (İmza Al) düğmesine tıklayın.
- Mevcut bir imzayı silmek için **Delete Signature** (İmzayı Sil) düğmesine tıklayın.

25.1.4 Parmak izi verilerini kaydetme



Ön gereksinimler

- Biyometrik giriş kontrolü gerçekleştirmek için girişlerde bir veya daha fazla parmak izi okuyucusu yapılandırılmalıdır.
- ÖNEMLİ: Bu okuyucular düzenli olarak kart ve parmak izi verilerini sunuculardan alıp saklar. Tek okuyucudaki ayarlar sonuçta hangi kimlik bilgilerinin kabul edildiğine karar verir. Kişi için burada yapılan tüm ayarları geçersiz kılarlar.
- Parmak izlerini kart tabanlı kimlik doğrulaması için (veya buna alternatif olarak) kullanmak üzere tüm kart sahiplerinin parmak izlerinin taranması gerekir.
- Kaydolan kişi, iş istasyonunuza bağlı ve bunun için yapılandırılmış bir parmak izi okuyucunun önündedir. Bu parmak izi kaydı okuyucusunun bir kartlı geçiş okuyucusu **olmaması** gerekir.
- Operatör olarak doğrudan kaydedilen, yani parmak izleri giriş için biyometrik kimlik bilgileri olarak kaydedilecek kişiyle doğrudan iletişim kurmanız gerekir.
- Parmak izlerinin verimli biçimde alınmasını sağlamak için kullanılan belirli bir okuyucuda parmağınızı nasıl art arda göstereceğinizle ilgili bilgi sahibi olmanız gerekir.

Giriş için parmak izi kaydı prosedürü

1. Parmak izleri iletişim kutusuna gidin: **Personnel data** (Personel verileri) > **Persons** (Kişiler) > sekme: **Fingerprints** (Parmak izleri) ve veritabanında kaydedilen kişiyi oluşturun veya bulun.
2. Kaydedilen kişiye parmak izi okuyucuda düzenli giriş için hangi parmağını kullanmak istediğini sorun.
3. El şemasında ilgili parmağı seçin.
   Sonuç: Parmak ucu soru işaretiyle işaretlenir.
4. **Parmak izini kaydet** düğmesine tıklayın.
5. Kaydedilene okuyucuda parmağını göstermesi için gereken talimatları verin.
   Örnek talimatlar aşağıdaki el şemasındaki iletişim bölmesinde okunabilir, ancak farklı okuyucu türleri farklı prosedürler gerektirebilir.
6. Parmak izi başarıyla kaydedilirse bir onay penceresi görünür.

7. Bir **Tanıma modu** seçin; bu, bir parmak izi okuyucusunun kaydedilen kişiden erişim isteğinde bulunduğunda hangi kimlik bilgilerini talep edeceğini belirler. Burada ayarlanan modun yalnızca **Kişiye bağlı doğrulama** okuyucu parametresi olduğunda etkili olacağını unutmayın.
   Seçenekler şunlardır:
   - **Yalnızca parmak izi**: Yalnızca okuyucudaki parmak izi tarayıcısı kullanılır
   - **Yalnızca kart**: Yalnızca okuyucudaki kart tarayıcısı kullanılır
   - **Kart ve parmak izi**: Okuyucudaki iki tarayıcı da kullanılır. Kaydedilen kişi, giriş yapmak için hem kartı hem de seçilen parmağı okuyucuya göstermek zorundadır.
8. Kaydedilen kişinin parmak izini ve kimlik modunu saklamak için (Save (Kaydet)) simgesine tıklayın.

Uyarı!
Okuyucu ayarları kişi ayarlarını geçersiz kılma
Parmak izi iletişim kutusunda seçilen tanıma modunun yalnızca parmak izi okuyucusunun kendisi cihaz düzenleyicide **Person-dependent verification** (Kişiye bağlı doğrulama) seçeneğiyle yapılandırılmışsa çalışacağını unutmayın. Emin olamazsanız sistem yöneticinize danışın.

Baskıyı işaret etmek için parmak izi kaydı prosedürü
Ön koşullar:
- Parmak izi okuyucuları sadece **Cihaz Düzenleyici**'de **Network & Operation modes** (Ağ ve Çalışma modları) sekmesi > **Templates on server** (Sunucudaki şablonlar) > **Card and fingerprint** (Kart ve parmak izi) ayarıyla yapılandırılırsa baskı sinyalleri gönderebilir.
- Kaydedilen kişinin en az bir parmak izi daha önce başarıyla kaydedilmiş ve saklanmış olmalıdır.
- Parmak izi okuyucu çevrimiçidir. Çevrimdışı modda okuyucu elbette sisteme bir baskı sinyali gönderemez.

1. Kaydedilen kişiden, yetkisiz bir kişi tarafından parmak izi okuyucuyu kullanmaya zorlanması durumunda baskıyı işaret etmek için kullanacağı parmağı seçmesini isteyin.
2. Yukarıda açıklanan parmak izi kayıt prosedürünü bu parmak için tekrarlayın.
3. İkinci parmak izi başarıyla kaydedildiğinde, bu parmağı şemada seçin ve **Duress finger** (Baskı parmağı)düğmesine tıklayın.
   Atanan baskı parmağı el şemasında ünlem işaretiyle işaretlenir.

Kaydedilen kişi daha sonra parmak izi okuyucusundaki parmak baskı parmağını kullanıyorsa ve okuyucu çevrimdışı değilse sistem baskıyı bir açılır pencere kullanarak operatöre bildirir.

Saklanan parmak izlerini test etme prosedürü
1. El şemasında, test etmek istediğiniz parmak izini seçin.
2. Kaydedilen kişiye okuyucuya o parmağını göstermesini söyleyin.
3. **Parmak izini eşleştir** düğmesine tıklayın
   Sonuç: Bir açılır pencere, kayıtlı parmak izinin okuyucuya yerleştirilenle eşleşip eşleşmediğini onaylar. Yanlış alarm olasılığını azaltmak için bu prosedürün tekrarlanması gerekebileceğini unutmayın.

Saklanan parmak izlerini silme prosedürü

1. El şemasında, silmek istediğiniz parmak izini seçin.
2. **Parmak izini sil** düğmesine tıklayın
3. Silme işleminin onaylanmasını bekleyin.

25.2 Şirketler

- Bu iletişim kutusu yeni şirketler oluşturmak ve mevcut şirket verileri değiştirmek veya silmek için kullanılabilir.
- Şirketin adı ve kısa adı girilmelidir. Kısa ad, benzersiz olmalıdır.
- Bir şirketin **Persons** (Kişiler) iletişim kutusuna girilmesi zorunluysa bu şirketin personel kayıtlarını oluşturmaya çalışmadan önce bu iletişim kutusunda şirketi oluşturun.
- Personel kayıtları hala şirkete atanmış durumdaysa şirketler sistemden silinemez.

25.3 Kartlar: Kimlik bilgileri ile izin oluşturma ve atama

Bu iletişim kutusunun amacı **kartlar**, **giriş yetkileri** ya da **giriş profilleri** adı verilen giriş yetkisi paketlerini personel kayıtlarına atamaktır.
Giriş yetkileri ve profilleri kartlara değil kişilere atanır.
Bir kişiye atanan yeni kartlar, o kişiye daha önce atanan giriş yetkilerini alır.

Not: Yetkileri paket haline getirmek için giriş profillerini kullanma
Tutarlılık ve kolaylık için giriş yetkileri tek olarak atanmaz, ancak genellikle **Giriş profilleri** halinde paketlenerek bu şekilde atanır.

- Main menu (Ana menü): **> System data (Sistem verileri)** > **Access profiles** (Giriş profilleri)

Kart listesi
Kartlar iletişim kutusunda seçilen kişinin sahip olduğu bir kart listesi görüntülenir. Listede nitelikler arasında şunlar gösterilir:

- Kart kullanımı tipi.
- Kartın yapılandırılan bir çevrimdışı kilitleme sistemi için kullanılıp kullanılamayacağına ilişkin bir işaret.
- Kartın art arda geçersiz PIN kullanılması nedeniyle engellenip engellenmediği. Bu durum özellikle vurgulanır.
- Kartın oluşturulma tarihi
- Kartın son kullanma tarihi (Toplama tarihi).
  Not: Motorlu bir kart okuyucu kullanılıyorsa fiziksel olarak son kullanma tarihi geçen bir kartı alıkoyabilir. Aksi takdirde kart yalnızca geçersiz kılınır.
- Kartın yazdırıldığı tarih ve yazdırılan kart sayısı.
- Kod verilerinin ayrıntıları.

Administered globally (Genel olarak yönetilir) seçeneği
Administered globally (Genel olarak yönetilir) (fotoğraf çerçevesinin yanındaki onay kutusu) ayarına sahip kişilerin verileri, yalnızca ek **Global Administrator** (Genel Yönetici) hakkına sahip operatörler tarafından düzenlenebilir.
Aşağıdaki veriler, bu hakka sahip olmayan operatörler için salt okunurdur:

- **Remarks, Extra info** (Açıklamalar, Fazladan bilgi) sekmeleri ve özel alanlar haricinde **Persons** (Kişiler) iletişim kutusundaki tüm veriler.

– **Cards** (Kartlar) iletişim kutusundaki tüm veriler.
– **PIN Code** (PIN Kodu) iletişim kutusundaki tüm veriler.

Bu **Global Administrator** (Genel Yönetici) hakkı aşağıdaki onay kutusuna atanabilir:
– Main menu (Ana menü): **Configuration** (Yapılandırma) > **Operators and workstations** (Operatörler ve iş istasyonları) > **User rights (Kullanıcı hakları)** > onay kutusu: **Global Administrator** (Genel Yönetici).

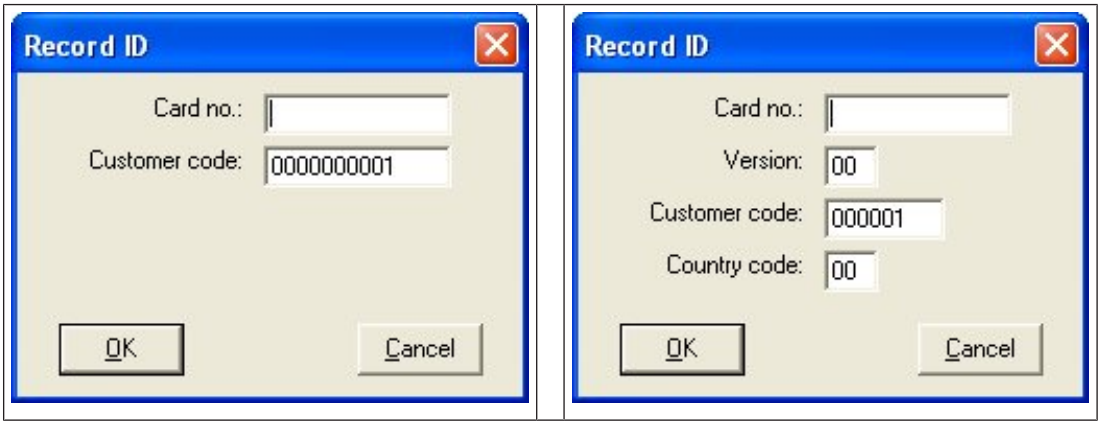
25.3.1 Kişilere kart atama

Giriş
Kartlı geçiş kullanan tüm kişilerin, sahibine **Cards** (Kartlar) iletişim kutusunda atanmış bir kartı veya başka elektronik kimlik bilgileri olması gerekir.
Kart numaraları, manuel olarak veya bir kayıt okuyucusu aracılığıyla atanabilir.

İletişim yolu
Main menu (Ana menü) > **Personnel data** (Personel verileri) > **Cards** (Kartlar)

Ön koşullar
– Kartı almak için gereken personel kaydını **Cards** (Kartlar) iletişim kutusunun başlığına yüklediniz.

Kart verilerini manuel olarak girme
Bir kişiye bir kimlik kartı atamak için **Record card** (Kartı kaydet) düğmesine tıklayın. **Record ID** (Kayıt Kimliği) iletişim kutusu maskesi görünür. Kart türü ile kullanılan kontrol cihazları ve okuyucuların türüne bağlı olarak giriş iletişim kutularından biri görünür.



Kimlik kartının üzerinde yazılı numarayı manuel olarak girin. Kart numaraları otomatik olarak sıfırlarla doldurulur, böylece her zaman 12 basamak olarak kaydedilir. Bazı sistemlerde, bir kimlik kartı kaybolduğunda yeni bir kimlik kartı numarası atanmaz. Bunun yerine, aynı kimlik kartı numarası, daha yüksek bir sürüm numarası ile verilir. Ülke kodu ve müşteri kodu üretici tarafından verilir ve bunların sistemin kayıt dosyasına girilmesi gerekir.
Zaten sistem tarafından kullanılmamışsa kart numarası kişiye atanır. Başarılı atama açılır pencereyle onaylanır.

Kayıt okuyucusu kullanma
Ön koşul
– İş istasyonunuzda bir kayıt okuyucusu yapılandırılır.
Kayıt prosedürü

1. Yapılandırılmış bir kayıt okuyucusunu seçmek için **Record card** (Kartı kaydet) düğmesinin sağ tarafındaki düğmesine tıklayın.

– Kayıt okuyucu seçimini değiştirmek için ACE iletişim kutusunda Yönetici olarak oturum açmanız gerektiğini unutmayın.

2. **Record card** (Kartı kaydet) düğmesine basın ve ekrandaki talimatları izleyin.
3. Okuyucu türüne bağlı olarak artık kart ayrıntılarını bir iletişim kutusuna girebilir veya okuyucuya göstererek verileri karttan okuyabilirsiniz.

Kart değiştirme prosedürü

1. Listeden bir kart seçin.
2. **Change card** (Kartı kaydet) düğmesine tıklayın
3. Açılır pencerede

– Orijinali kalıcı olarak kaybolursa veya hasar görmüşse **Replace card**'ı (Kartı değiştir) seçin.
– Orijinali giriş sırasında yanlış yerleştirilirse veya evde kalmışsa ya da yalnızca geçici bir değişiklik yapılması gerekiyorsa **Temporary card**'ı (Geçici kart) seçin.
  – Geçici kart için geçerlilik süresi girin.
  – Diğer tüm kartları hemen devre dışı bırakmak istiyorsanız bu seçeneği seçin.
  – Geçici kartın süresi dolduğunda orijinal kartların otomatik olarak yeniden etkinleştirilmesi gerekiyorsa bunu seçin.

4. Kaydetmek için **OK**'e (Tamam) tıklayın.

Kartları silme

1. Listeden bir kart seçin.
2. Bir kişinin bir karta olan atamasını kaldırmak için **Delete card** (Kartı sil) düğmesine tıklayın.

Not: Kart sahibinin son kartını silerseniz kişinin durumu **unregistered** (kayıtlı değil) (durum çubuğundaki **Registered**'ın (Kayıtlı) yanındaki kırmızı etiket) olarak değişir. Bu kişi daha sonra giriş kontrolüne daha uzun tabi kalır.

25.3.2 Kimlik kartı yazdırma

Ön koşullar

– Yeni kart sahibinin personel kaydı sistemde önceden bulunmalıdır.
– Genellikle USB ile aşağıdaki donanıma sahip bir iş istasyonu bağlanır:
  – Bir kimlik kartı yazıcısı
  – Kimlik fotoğraflarını çekmek için bir kamera.

Prosedür

İletişim yolu

AMS istemcisi: **Personel verileri** > **Kimlik kartları**

1. Kartı yazdırılacak personel kaydını yükleyin.
2. **Layout** (Yerleşim) açılır menüsünde, kayıtlı yerleşimlerden istediğiniz kart yerleşimini seçin.
3. Aşağıdaki yöntemlerden birini uygulayarak kimlik fotoğrafı elde edin:
   – **Capture** (Yakala) düğmesine tıklayın ve bağlı kameralar listesinden istediğiniz kamerayı seçin.
   – **Görüntüyü içe aktar** düğmesine tıklayın ve fotoğrafın kartın üzerine yazdırılacak kısmını seçmek için kırpma çerçevesini kullanın.

4. Doğru verilerin kimlik kartının üzerinde doğru yerleşimde görünmesini sağlamak için **Preview**'ye (Önizleme) tıklayın.
5. Kimlik kartını yazdırmak için **Print**'e (Yazdır) tıklayın.

Desteklenen Kameralar
İşletim sisteminin kamera olarak tanıdığı tüm USB cihazları.

25.3.3 Authorizations (Yetkiler) sekmesi

Giriş profilleri olarak paketlenen yetkileri atama
Kart sahiplerine yetki atamak için en uygun ve esnek yol, bunları önce Giriş profillerine dağıtmak ve ardından profili atamaktır.
– Giriş profilleri oluşturmak için *Giriş profilleri oluşturma, sayfa 187* bölümüne bakın
– Bu kart sahibine bir Giriş profili atamak için, **Access profile:** (Giriş profili) listesinden tanımlı bir profil seçin

Giriş yetkilerini doğrudan atama
Authorizations (Yetkiler) sekmesinde:
Kişiye daha önce atanmış olan tüm giriş yetkileri soldaki listede görünür.
Atama için kullanılabilen tüm giriş yetkileri sağdaki listede görünür.
Öğeleri seçin ve öğeleri bir listeden diğerine taşımak için listeler arasındaki düğmelere tıklayın.

 seçilen öğeyi atar.

 seçilen öğenin atamasını kaldırır.

 tüm kullanılabilir öğeleri atar.

 tüm atanan öğelerin atamasını kaldırır.

Seçenek: **Keep authorizations assigned** (Atanan yetkileri koru)
Bir giriş profilini bir kişiye atamanın etkisi **Keep authorizations assigned** (Atanan yetkileri koru) onay kutusuna bağlıdır:
– Onay kutusu temizlenirse bundan önce yapılan her türlü seçim ve zaten atanmış olan her türlü giriş yetkisi profil atandığında **değiştirilir**.
– Onay kutusu işaretlenirse profilin yetkileri atanan yetkilere **eklenir**.

Yetkilerin zaman aralığını sınırlama
Yetki ve profillerin başlangıç ve bitiş zamanlarını sınırlamak için **Valid from:** (Geçerlilik başlangıcı) ve **until:** (Geçerlilik bitişi) tarih alanlarını kullanın. Hiçbir değer belirlenmemişse yetki hemen ve sınırsız süre için geçerli olur.

Yetki sürelerini tek tek ayarlamak üzere bir iletişim kutusu açmak için  simgesine tıklayın.

Bir yetkinin girişlerini görüntüleme
Herhangi bir listede ait olan girişlerin bir listesini görüntülemek için bir yetkiye sağ tıklayın.

25.3.4 Diğer veri sekmesi: Muafiyetler ve özel izinler

Zaman modeli atama:
Kart sahibinin günlük giriş saatlerini, yani kart sahibinin kimlik bilgilerinin giriş izni vereceği süreleri belirtmek için **Time model** (Zaman modeli) liste kutusunu kullanın.

Kişileri rastgele taramadan çıkarma
Kişileri girişlerde ve çıkışlarda incelemeler için rastgele seçilmekten muaf tutmak için **Rastgele taramadan çıkarıldı** onay kutusunu seçin.

Kişileri için PIN kodu kontrolünden çıkar
Kişileri normal çalışma saatleri dışında PIN kodu okuyucularda PIN kodlarını girmekten muaf tutmak için **PIN kodu kontrolünü devre dışı bırak** onay kutusunu seçin.

Uyarı!
PIN kodu kontrollerinden çıkarma işlemi tüm sistemi etkiler.
Örneğin, bu kişilerin PIN kodları kontrol edilmediğinden kapı modeli 10'da girişlerde alarmları devreye alamayacak veya devreden çıkaramayacaklardır.

Kapı açılma süresini uzatma
Engelli kişilere **Door open too long** (Kapı çok uzun süredir açık) durumu oluşmadan önce bir girişten geçmeleri için üç kat süre vermek üzere **Extended door opening time** (Uzatılmış kapı açılma süresi) onay kutusunu seçin.
Not: Varsayılan uzatma faktörü Cihaz Düzenleyici'deki MAC'in özelliklerinden sıfırlanabilir.
Global Access Settings (Genel Kartlı Geçiş Ayarları) >
Time factor for handicapped persons'ı (Engelliler için zaman faktörü) seçin

Bakış izleme
Bir **Tour** (Bakış) veya **Route** (Güzergah) İstemci menüsü: **Tour monitoring** (Bakış izleme) > **Define routes** (Güzergahları tanımla) iletişim kutusunda tanımlanan katı bir okuyucu sırasıdır.
Bir kart sahibine bir bakış atamak için **Tour monitoring** (Bakış izleme) onay kutusunu ve açılır listeden tanımlı bir tur seçin. Hiçbir bakış tanımlanmadıysa onay kutusu devre dışı olur. Bir **Bakış** bir kart sahibine atandığında, kart sahibi kartını sıradaki ilk okuyucuda taratır taratmaz etkin hale gelir. Bunun ardından sıradaki tüm okuyucular bakış tamamlanana kadar sırayla kullanılmalıdır. Tipik kullanım alanları endüstriyel temiz ortamlar, hijyenik kontrollü veya yüksek güvenlikli alanlarda katı giriş sıraları uygulamaktır.

Kapıların kilidini açma izni
Kart sahibinin kapıların kilidini uzun bir süre boyunca açmasına izin vermek üzere bu onay kutusunu seçin, bkz. **Office mode** (Ofis modu).

Bkz.
– *Kişilere Ofis modunu ayarlama yetkisi verme, sayfa 199*

25.3.5 Kişilere Ofis modunu ayarlama yetkisi verme

Giriş

Ofis modu terimi ofis veya çalışma saatleri sırasında bir girişteki giriş kontrolünün askıya alınmasını tanımlar. Engelsiz genel girişe izin vermek için giriş bu saatlerde açık kalır. Bu saatler dışında Normal mod geçerlidir, yani giriş izni yalnızca okuyucuda geçerli kimlik bilgileri sunan kişilere verilir.

Ofis modu, perakende, eğitim ve tıp tesisleri için tipik bir gereksinimdir.

Ön gereksinimler

Ofis modunun çalışması için, aşağıdaki gereksinimlerin karşılanması gerekir:

Yapılandırmada (cihaz ağacı)

- Bir veya daha fazla giriş, genişletilmiş açık sürelere izin verecek şekilde yapılandırılmalıdır.
- Girişte en az bir tuş takımlı okuyucu kullanılmalıdır.

İstemcide (Persons (Kişiler) iletişim kutuları)

- Bir veya daha fazla kart sahibine girişi ofise modunu geçirip bu moddan çıkarma yetkisi verilmelidir.
- Bu kişilerin kartlarının geçerli olması ve ofis modu saatleri dışında girişe izin vermesi gerekir.

Kişilere ofis modunu ayarlamaları için yetki verme prosedürleri

Bireysel kart sahiplerine yönelik prosedür

1. Şuraya gidin: **Personel verileri** > **Kartlar** > sekme: **Diğer veriler** ve veritabanında belirlenen kart sahibini oluşturun veya bulun.
2. **Kapıların kilidini açma izni** onay kutusunu seçin.
3. Kart sahibinin verilerini kaydetmek için disket simgesine  tıklayın.

Kart sahibi gruplarına yönelik prosedür

1. Şuraya gidin: **Personel verileri** > **Kişi grupları** ve liste penceresinde kart sahiplerinin bir listesini oluşturmak için filtre kriterlerini kullanın.
2. **Değiştirilecek alan** açılır listesinden, **Kapıların kilidini aç**'ı seçin
3. **Kapıların kilidini aç** onay kutusunu seçin.
4. Kart sahiplerinin verilerini kaydetmek için **Değişiklikleri uygula** düğmesine tıklayın.

Kart sahibine ofis modunu başlatma ve durdurma talimatı verme

Bir girişte ofis modunu başlatmak veya durdurmak için, kart sahibi tuş takımında 3 rakamına basar ve ardından özel yetki verilmiş kartını okuyucuya gösterir.

Yetkili bir kart sahibi 3 rakamına basıp kartı yeniden gösterene kadar girişin kilidi açık kalır.

Güvenlik görevlisi kartına sahip güvenlik görevlilerinin özel izin olmaksızın ofis modunu aynı şekilde durdurabileceğini unutmayın.

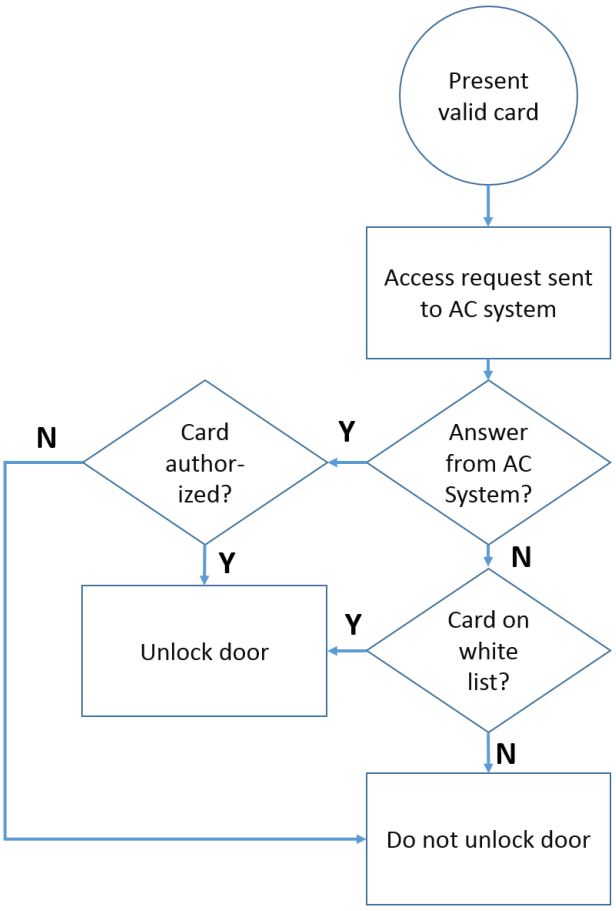
Uyarı!
Kapı için Office (Ofis) modu ve cihaz parametreleri
Office modu Cihaz Düzenleyici'deki bir kapının **Options** (Seçenekler) sekmesinde bulunan **Unlock door** (Kapının kilidini aç) parametresini geçersiz kılarak **0 Normal mode** (0 Normal mod) ve **1 Unlocked** (1 Kilit açıldı) parametrelerine izin verir.

25.3.6 Smartintego sekmesi

SmartIntego kilitleme sistemleri

Giriş

SmartIntego kart okuyucusu, önce ana erişim kontrolü (AC) sistemi aracılığıyla giriş için yetki vermeye çalışır. Bağlantı kurulamazsa kart numarası için saklanan beyaz listeyi arar.



SmartIntego kilitleme sistemine ait giriş yetkileri, çoğunlukla diğer giriş yetkileriyle aynı şekilde atanır.

Ön gereksinimler

- Giriş kontrol sisteminizde bir yapılandırılmış bir SimonsVoss SmartIntego kilitleme sistemi. Talimatlar için yapılandırma kılavuzuna bakın.
- MIFARE Classic veya MIFARE Desfire kartları kullanan kart sahipleri. SmartIntego'da, Kart Seri Numarası (CSN) kullanılır.

Atama prosedürü

Aşağıdaki prosedürde, zaten erişim kontrol sistemi aracılığıyla atanmış olan her türlü yetkilendirmeye ek olarak bir SmartIntego beyaz listesine bir kart numarasının nasıl ekleneceğini açıklanmaktadır.

Beyaz listeler SmartIntego kapılarında yerel olarak saklanır, böylece bir okuyucu MAC bağlantısı kesildiğinde bile beyaz listeye alınan kart numaralarına erişim izni verebilir.

Beyaz listeye ekleme ve listeden silme işlemleri, kart sahibi verileri kaydedilir kaydedilmez ve bir bağlantı olduğunda SmartIntego okuyucularına iletilir.

1. AMS ana istemci menüsünde **Personnel data** (Personel verileri) > **Cards**'ı (Kartlar) seçin.
2. SmartIntego yetkilerini alacak kişiyi seçin
3. **SmartIntego** sekmesini **seçin.**
4. Atamaları yapın:
   - Kişiye daha önce atanmış olan tüm giriş yetkileri soldaki listede görünür.
   - Atama için kullanılabilen tüm giriş yetkileri sağdaki listede görünür.

Öğeleri seçin ve öğeleri bir listeden diğerine taşımak için listeler arasındaki düğmelere tıklayın.

 seçilen öğeyi atar.

 seçilen öğenin atamasını kaldırır.

 tüm kullanılabilir öğeleri atar.

 tüm atanan öğelerin atamasını kaldırır.

25.3.7 Uyarı kartı oluşturma

Bu bölümde, bir tehdit seviyesi tetiklemek için kullanılabilen bir uyarı kartının nasıl oluşturulacağı açıklanmaktadır.

Giriş

Uyarı kartı, bir okuyucuya gösterildiğinde belirli bir tehdit seviyesini tetikleyen bir karttır. Bir tehdit seviyesi yalnızca kartlı geçiş yazılımı aracılığıyla bir uyarı kartı ile iptal edilemez.

Ön koşullar

- Sisteminizde bir kayıt okuyucusu yapılandırılır.
- Sistemde en az bir tehdit seviyesi tanımlanmış olmalıdır.

İletişim yolu

Main menu (Ana menü) > **Personnel data** (Personel verileri) > **Cards** (Kartlar) > **Alert card** (Uyarı kartı)

Prosedür

1. Uyarı kartının atanacağı kişinin kişi kaydını yükleyin
2. Uyarı kartı sekmesinde, Record card'a (Kartı kaydet) tıklayın.
   - Şu açılır pencere görünür: **Select threat level** (Tehdit seviyesi seç)
3. Açılır pencerede istediğiniz tehdit seviyesini seçin ve **OK**'e (Tamam) tıklayın.
   - Şu açılır pencere görünür: **Recording badge ID** (Kimlik kartı kimliği kaydetme)
4. Saha kurulumunuza karşılık gelen normal kart verilerini girin ve **OK**'e (Tamam) tıklayın
   - Kaydettiğiniz uyarı kartı **Alert card** (Uyarı kartı) sekmesindeki listede görünür.

25.4 Geçici kartlar

Geçici bir kart, normal bir kart sahibi tarafından yanlış yerleştirilmiş bir kartın geçici bir yedeğidir. Çevrimdışı kapı hakları da dahil olmak üzere, orijinalin tüm yetki ve sınırlamalarını içeren bir kopyadır.
Kötüye kullanımı önlemek için sistem, kart sahibinin diğer kartlarının bir kısmını veya tamamını sınırlı bir süre için veya engeli manuel olarak kaldırılıncaya kadar engelleyebilir.
Bu nedenle geçici kartlar ziyaretçi kartları olarak kullanmak için **uygun değildir**.

Ön gereksinimler

– Operatör, iş istasyonunda yapılandırılan bir kayıt okuyucusuna erişebilir.
– Sistemde geçici bir kart olarak kayıt etmek için uygun bir fiziksel kart mevcuttur.

Main menu (Ana menü) > **Personnel data** (Personel verileri) > **Cards** (Kartlar)

Prosedür: Geçici kartlar atama

1. Gerekli personel kaydını **Cards** (Kartlar) iletişim kutusuna yükleyin
2. Kart listesinde geçici olarak değiştirilmesi gereken kartı veya kartları seçin.
3. **Change card**'a (Kartı değiştir) tıklayın
4. **Change card** (Kartı değiştir) açılır penceresinde, **Temporary card**'ı (Geçici kart) seçin.
5. **Period** (Süre) listesinden seçeneklerden birini seçin:
   – **Today** (Bugün)
   – **Today and tomorrow** (Bugün ve yarın)
   – **Enter number of days** (Gün sayısını gir)
6. Son seçeneği kullanırsanız kutuda gün için bir tam sayı girin.
   Üç durumda da **Period** (Süre) her zaman ilgili günde gece yarısı sona erer.
7. Gerekirse **Deactivate all cards now** (Tüm kartları şimdi devre dışı bırak) onay kutusunu işaretleyin.
   – Seçilirse bu kart sahibine ait tüm kartlar engellenir.
   – Temizlenirse yalnızca yukarıda seçilen kart engellenir.
8. Gerekirse **Activate card(s) automatically after period** (Kartları şu süreden sonra otomatik olarak etkinleştir:) onay kutusunu işaretleyin.
   – Engellenen kartlar yukarıda tanımlanan **Period** (Süre) sona erdiğinde otomatik olarak engellenir.
9. Geçici kartı kayıt okuyucusuna yerleştirin
10. **OK**
    'e tıklayın Kimlik kartı kimliği kayıt okuyucusu tarafından kaydedilir.
    – Geçici kart geçerlilik süresi ve kod verileri ile birlikte kart listesinde ✓ etkin olarak görünür.
    – Yukarıda yapılan ayarlara bağlı olarak diğer kart veya kartlar engellenmiş × olarak görünür: **Deactivate all cards now** (Tüm kartları şimdi devre dışı bırak).
11. (İsteğe bağlı) Kart listesinde, geçici karta ait **Collecting date** (Toplama tarihi) sütununa tıklayın ve kartı kart sahibinden almak için bir tarih belirleyin.
    Varsayılan değer **Never**'dır (Asla).

Prosedür: Geçici kartları silme

Yanlış yerleştirilen orijinal kart bulunduğunda, geçici kartı aşağıdaki gibi silin:

1. Gerekli personel kaydını **Cards** (Kartlar) iletişim kutusuna yükleyin.
2. Kart listesinden geçici kartı seçin.
3. **Delete card**
   'a (Kartı sil) tıklayın Geçici kart listeden silinir ve yerine geçtiği kart veya kartlar derhal engellenir

Prosedür: Kartlardaki geçici blokları kaldırma

Artık orijinal kartın engellenmesi gerekmiyorsa engellemeyi şu şekilde silin:

1. **Blocking** (Engelleme) iletişim kutusu: **Personnel data** (Personel verileri) > **Blocking** (Engelleme) bölümüne gidin.
2. Kart listesinde, **Lock(s)** (Kilitler) sütununda engellendi olarak işaretlenen kişisel kartı seçin.
3. **Release temporary lock**
   'a (Geçici kilidi kaldır) tıklayın. Engellemeyi kaldırmanın geçici kartları kaldırmadığını unutmayın. Geçici kartların süreleri doğal olarak geçerlilik sürelerinin ardından dolar. Gerekirse bunları manuel olarak silin.

Geçici kartlarla ilgili notlar

- Sistem geçici kartların geçici kartlarla değiştirilmesine izin vermez.
- Sistem, bir kişisel kartın birden fazla geçici karta sahip olmasına izin vermez.
- Bir kart sahibinin elindeki tüm kartların hızlı bir özetini görmek için, farenizi ana iletişim kutusu penceresindeki durum çubuğunda yer alan en soldaki **Registered** (Kayıtlı) etiketli küçük bölmenin üzerine getirin.

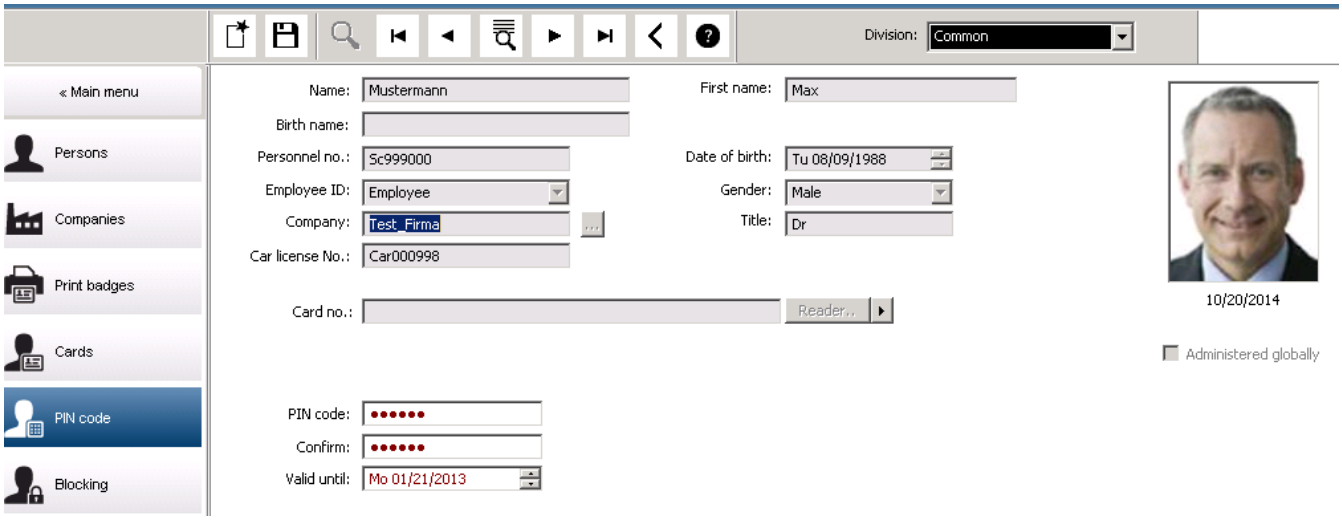
25.5 Personel için PIN kodları

İletişim Kutusu: PIN Kodu

Yüksek güvenlik gereksinimleri olan bölgelere giriş için, giriş yetkisi yeterli olmayabilir. Buralarda bir PIN kodu da girilmelidir. Her kişi veya kimlik kartı tüm alanlar için geçerli bir PIN koduna sahip olabilir. Sistem çok basit kodların (ör. 123456 veya 127721 gibi çift taraflı aynı okunan rakam grupları) kullanılmasını engeller. İletişim kutusundaki her bir kişi için geçerlilik kısıtlanabilir ve belirtilir.

Bir PIN kodu engellendiyse veya süresi dolduysa kimlik kartı tüm diğer alanlar için hala geçerli olsa bile kod istenen alana giriş reddedilir.

Yanlış bir kod üç kez art arda girilirse (varsayılan ayardır; bu 1 ila 99 arasında yapılandırılabilir), bu kart engellenir, örneğin tüm alanlara giriş reddedilir. Bu şekilde engellenen bir kartın engeli Blocking (Engelleme) iletişim kutusuyla kaldırılabilir.



PIN-Code (PIN Kodu) giriş alanına yeni bir PIN kodu girin ve yeniden yazarak onaylayın. PIN kodunun uzunluğu (4-9 arasında, varsayılan değer 6'dır) sistem yöneticisi tarafından yapılandırılır.

Uyarı!
Kart sahiplerinin kart okuyucularda kimlik PIN'lerini girme şekli sisteminizde yapılandırılan okuyucunun türüne bağlıdır. Örneğin:
RS485 kart okuyucularda kart sahibi şunları girer: **4 #** `<the PIN>`
Wiegand ve diğer kart okuyucularda kart sahibi şunları girer: `<the PIN>` **#**
Kart sahiplerini mutlaka PIN'lerini nasıl gireceklerine ilişkin olarak bilgilendirin. Emin olamazsanız sistem yöneticinize danışın.

Hırsız alarm sistemlerini (IDS) devreye almak için PIN Kodu.
4-8 basamaklı bir PIN girin (varsayılan = 6; doğrulama PIN'iyle aynı uzunluktadır). Bu PIN bir IDS'yi kurmak için kullanılacaktır.
Bu alanların görüntülenmesi parametrelendirilebilir. Kontrol sadece **ayrı IDS PIN**'i kontrol etkinse kullanılabilir.

– Main menu (Ana menü) > **Configuration** (Yapılandırma) > **Options** (Seçenekler) > **PIN codes** (PIN kodları)

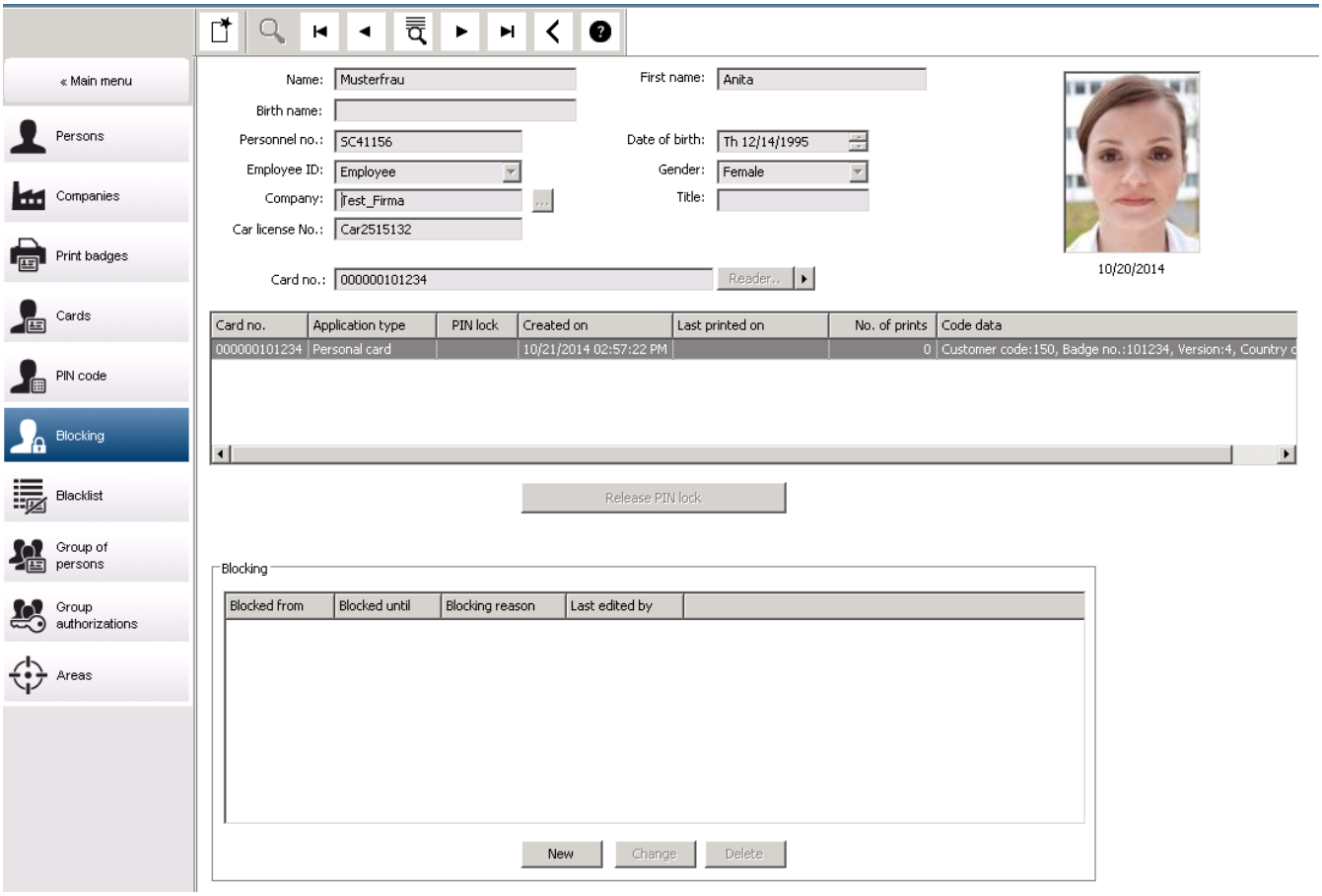
Gerekirse bir bitiş tarihi seçin.
IDS PIN'ini girmek için giriş alanları kullanılamıyorsa IDS'yi kurmak ve devre dışı bırakmak için doğrulama PIN'i de kullanılabilir. Ancak, giriş alanları bu iletişim kutusunda gösterilirse kurma PIN'i yalnızca IDS için kullanılabilir.
Varsayılan ayar: PIN Koduyla Kurma giriş alanları görünmezdir.

Alarm (Baskı) PIN'leri
Baskı altındaki kişiler özel bir PIN kodu aracılığıyla sessiz bir alarm tetikleyebilir. Sessiz alarmın saldırgan tarafından fark edilmemesi gerektiğinden, giriş izni verilir, ancak sistem operatörleri baskı için uyarılır.
Aynı anda etkinleştirilen iki çeşit mevcuttur ve tehdit edilen kişi bunlar arasından seçim yapabilir:

– PIN kodunu ters sırada girme (123123 yerine 321321)
– PIN'i 1 artırma (örneğin: 123123 yerine 123124). Son basamak 9 olursa PIN'in yine de artırıldığını, böylece 123129 PIN'inin 123130'un baskı PIN'i olduğunu unutmayın.

25.6 Personel için girişi engelleme

İletişim Kutusu: Engelleme
Bazı durumlarda bir Kişinin girişini geçici olarak reddetmek veya MAC tarafından uygulanan bir engellemeyi kaldırmak gerekir (ör. yanlış bir PIN kodlarının üç kez girilmesi veya rastgele tarama nedeniyle).
Engelleme, kullanılan kimlik bilgilerinden bağımsız olarak, bu kişi için tüm giriş reddedildiği anlamına gelir.



1. Kişiyi her zamanki gibi seçin.
2. Blocking (Engelleme) bölmesinde **New**'a tıklayarak seçili kişi için bir engelleme oluşturun.
3. Açılır iletişim kutusuna ek bilgiler girin:
   - **Blocked from/until** (Engellenme başlangıcı/bitişi): (Bitiş zamanı belirtilmediyse kişi engel manuel olarak kaldırılana kadar engellenir.)
   - **Block type:** (Engelleme türü)
   - **Blocking reason:** (Engelleme nedeni) (Kişinin kaydı için engelleme tipi `Manual` ise)
4. Engellemeyi kaydetmek için açılır penceredeki **Save**'e (Kaydet) tıklayın.

- Gerekirse listeden bir engelleme seçin ve bunu değiştirmek veya silmek için **Change**'e (Değiştir) veya **Delete**'e (Sil) tıklayın.

Engelleme tipi olarak **Manuel lock** (Manuel kilit) seçilmişse kişinin kaydı için bir **Blocking reason** (Engelleme nedeni) girin.

Uyarı!
Engelleme, belirli bir kimlik bilgisine değil kişiye uygulanır. Bu nedenle, yeni bir kimlik kartı tahsis ederek engellemeyi iptal etmek veya önlemek mümkün değildir.

25.7 Kartları kara listeye alma

İletişim Kutusu: Kara Liste

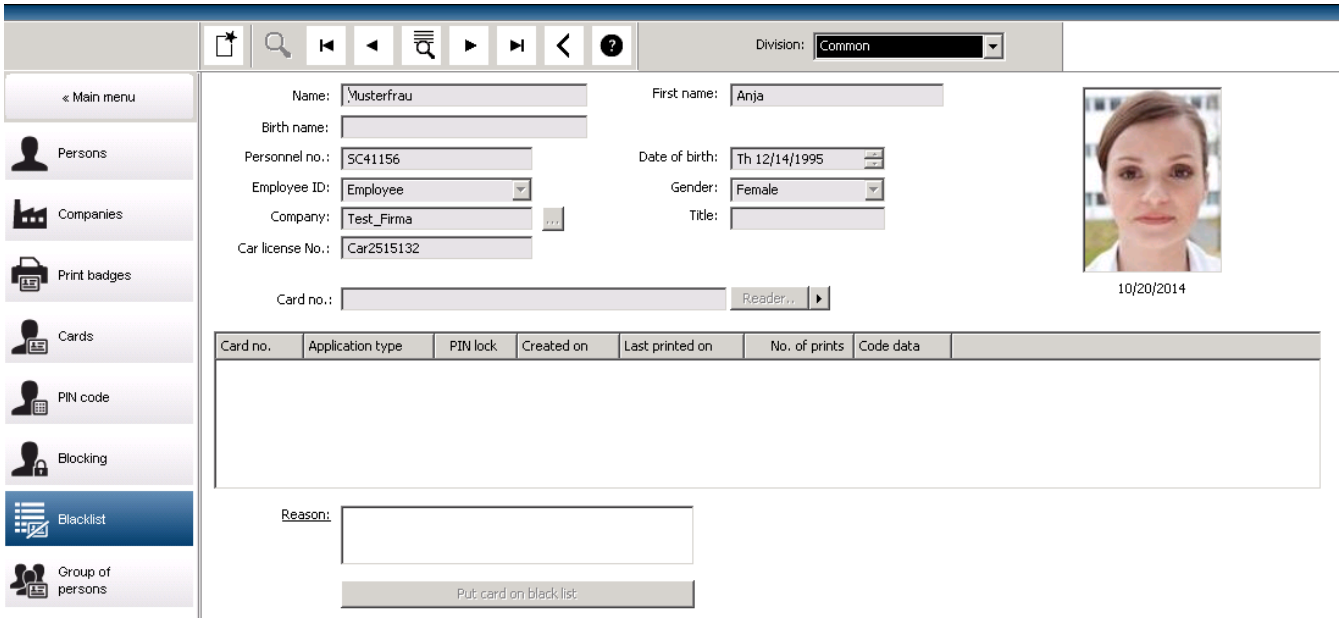
Örneğin çalınan veya kaybolan kartlar gibi bir daha asla kullanılmaması gereken kartlar kara liste tablosuna girilir.

Kişinin değil kimlik bilgisinin kara listeye alındığını unutmayın.

Uyarı!

İşlem geri alınamaz. Kara listedeki kartların engelleri asla kaldırılamaz, ancak bunun yerine değiştirilmelidir.

Kara listeye alınan kartlar giriş izni vermez. Bunun yerine kullanım girişimi bir günlük dosyasına kaydedilir ve bir alarm oluşturulur.



Main menu (Ana menü) > **Personnel data** (Personel verileri) > **Blacklist** (Kara listeye al)

1. Kimlik kartı kara listeye alınacak kişiyi seçin.
2. Bu kart sahibine birden fazla kart atandıysa **Kimlik Kartı No.** listesinden kartı seçin.
3. **Reason** (Neden) giriş alanına bu kartı kara listeye alma nedenini girin.
4. **Blacklist this card** (Bu kartı kara listeye al) düğmesine tıklayın.
5. Açılır pencerede kara listeye alma işlemini onaylayın.

Kart derhal uygulanacak şekilde kara listeye alınır.

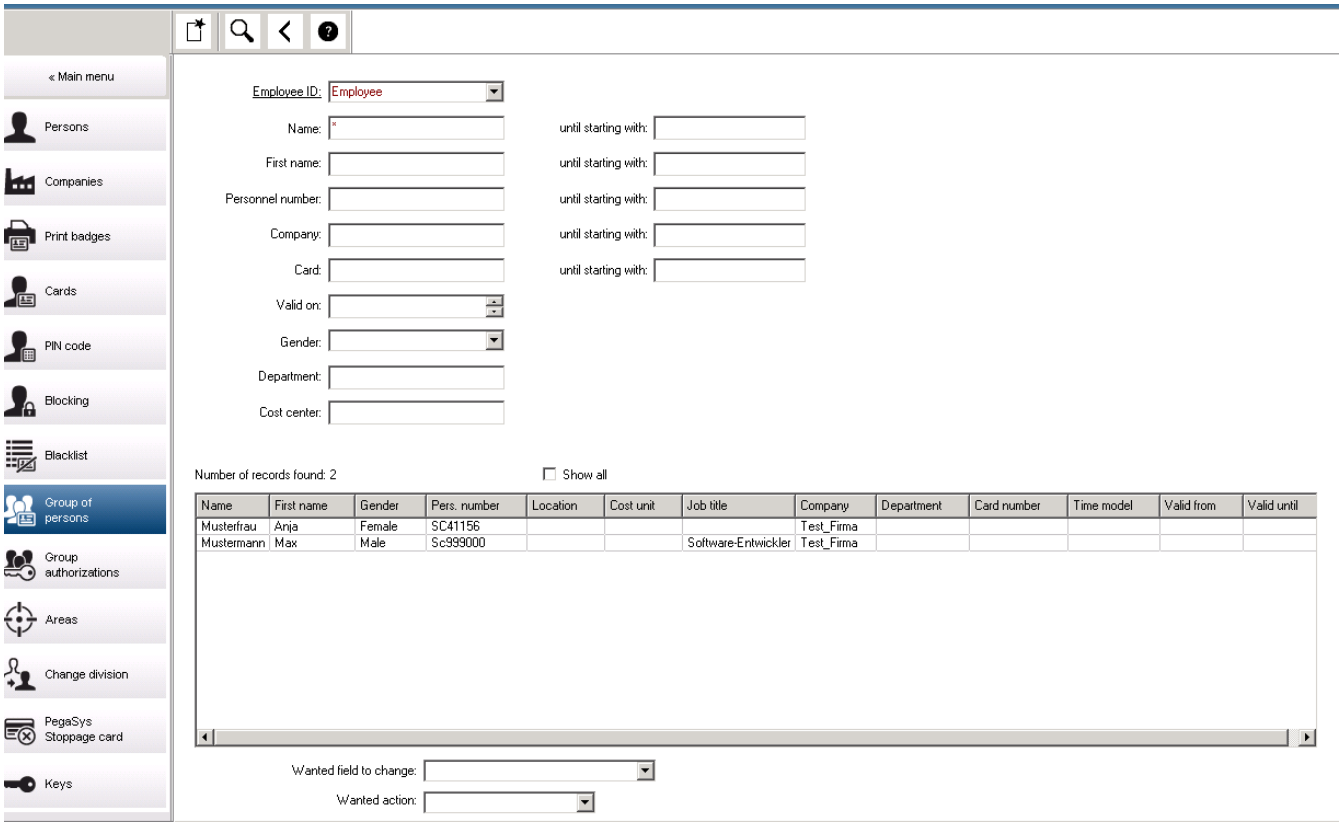
Uyarı!

Kara listeye alma kart sahiplerini **değil** kartları etkiler.

Aynı kart sahibine ait olan kara listeye alınmamış kartlar engellenmez.

25.8 Aynı anda birden fazla kişiyi düzenleme

Kişi Grubu



Başka bir iletişim kutusu grup değişikliklerinin tanımlanabileceği bir kişi grubu seçer. Seçilen kişi grubu üzerinde kontrolü korumak için, ilk on kişi adlarla birlikte gösterilir ve gerçek veriler veritabanını oluşturur (gerçek veriler: Departman olarak “ST-AC” seçildiyse örneğin “ST-ACS” ve “ST-ACX” görüntülenir). Ayrıca, seçilen grubun kişi sayısı görüntülenir.
Kişi grubu seçildikten sonra aşağıdaki girişler seçilebilir:

- Çalışan Kimliği
- Name (Ad)
- First name (Ad)
- Personel numarası
- Company (Şirket)
- Kart
- Geçerlilik tarihi
- Gender (Cinsiyet)
- Departman
- Maliyet birimi
- Tanımlandıysa ayrılan alanlar

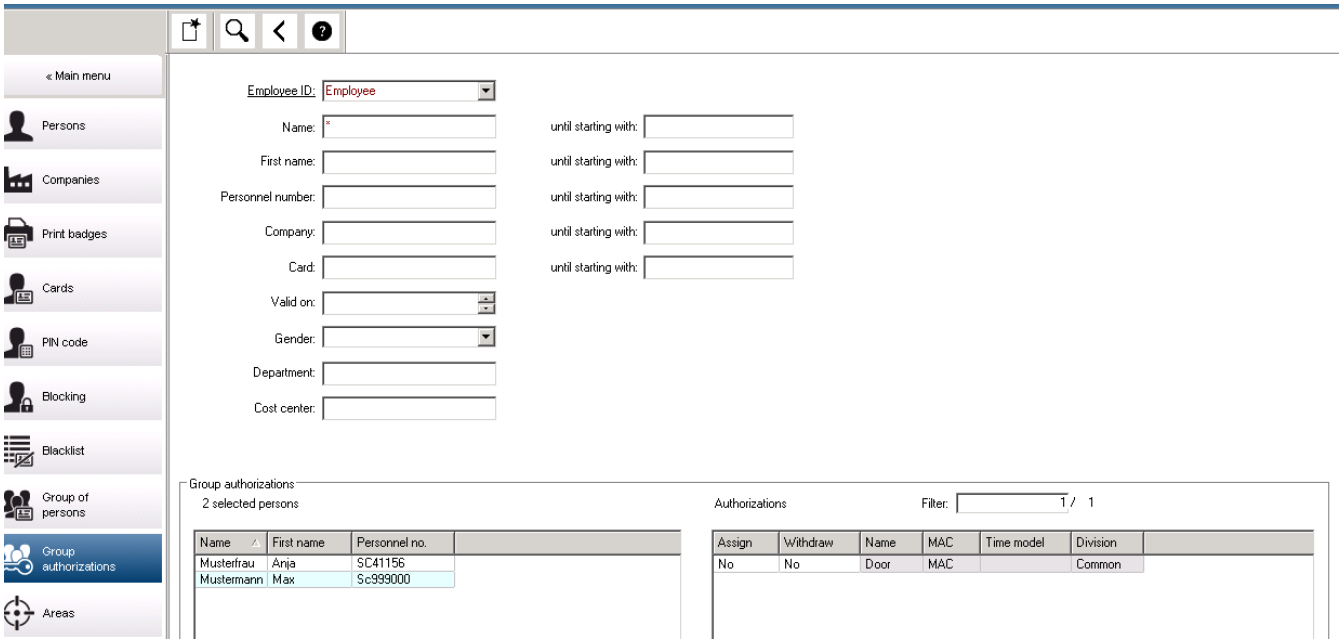
Ardından değiştirme seçeneği seçilebilir:

- Değiştirilecek alan
- İstenen işlem
- Eski değer
- Yeni değer.

Böylece tasarlanan değerler sırasıyla **Eski değer** veya **Yeni değer** alanına girilir. **Değişiklikleri uygula** düğmesini seçip **Tüm seçilen kişiler için değişiklikler uygulansın mı?** güvenlik isteği onaylanarak işlem tamamlanır. İşlem devam ederken örneğin iletişim kutusu kullanılamaz. Alan *1 ila *4 tarafından tetiklenen işlemler muhtemelen diğer alanlardan (yıldızsız) daha fazla zaman alır ve tüm değişikliklere izin verilmez. Dolayısıyla **Desired action** (İstenen işlem) **New value** (Yeni değer) ile karşılaştırılamaz, çünkü bu girişler standart ürün tarafından karşılanmaz. **Old value** (Eski değer) ve **New value** (Yeni değer) alanları da sırayla değişiklik gösterebilir.

25.8.1 Grup yetkileri

Grup Yetkisi



[Grup Yetkisi] menü öğesinde aşağıdaki arama kriterleri desteklenir:

- Çalışan Kimliği
- Name (Ad)
- First name (Ad)
- Personel numarası
- Company (Şirket)
- Kart
- Geçerlilik tarihi
- Gender (Cinsiyet)
- Departman
- Maliyet birimi
- Tanımlandıysa ayrılan alanlar

Bundan sonra, bir liste iletişim kutusunun tüm seçilen kişileri (ad, soyadı ve personel no. ile) görüntüleyen alt kısmını gösterir. Tüm yetkiler sağ alttaki açıklamaları, zaman modeli ve **[Assign]** (Ata) ve **[Withdraw]** (Geri al) sütunlarıyla birlikte gösterilir. Yetki listesi açıldığında geçerli yetkiler gösterilmez ve **[Assign]** (Ata) ve **[Withdraw]** (Geri Al) sütunları önceden “No” (Hayır) olarak ayarlanır. Bu noktada, “Hayır”ı “Evet”e veya tersine dönüştüren sütunlardan birindeki alana çift tıklayarak yetkiler tek tek atanabilir. Değişiklikleri yürüt'e

tıklamak "Evet" atanmış tüm yetkilerin sırasıyla tüm seçili kişilere eklenmesini veya geri alınmasını sağlar. Genellikle seçilen kişiler tamamen aynı yetkilere sahip olmadığından, kişilere ait tüm diğer yetkiler değişmeden kalır.

25.9 Kişiler için bölümü değiştirme

Giriş

Change division (Bölümü değiştir), sistemde bulunan bir personel kaydı kümesinin bölümünü değiştirmeye yönelik güçlü bir iletişim kutusudur.

Uyarı!

Bu özelliği son derece dikkatli bir şekilde kullanın!

Bölümdeki bir değişikliğin, değiştirdiğiniz personel kayıtlarına ilişkin önemli sonuçları olabilir.

Ön koşullar

Personel kayıtlarının bölümünü değiştiren operatör, bu kişiler ile ve iki bölümü birden düzenlemeye yönelik yetkilere sahip olmalıdır.

İletişim yolu

Main menu (Ana menü) > **Personnel data** (Personel verileri) > **Change division** (Bölümü değiştir)

Prosedür

1. **Filter persons** (Kişileri filtrele) bölmesinde, aşağıdaki alanlardan birine veya daha fazlasına filtre kriterleri girin:

Filter (Filtre)	**Remarks / Description** (Açıklamalar/Tanım)
Last name (Soyadı)	Tüm kişileri eşleştirmek için tek bir yıldız işareti ya da yıldız işareti **olmayan**harfler kullanın
Personnel no. from/ to (Personel no. başlangıç/bitiş)	Bir değer aralığı tanımlamak için iki alanı da kullanın
Employee ID (Employee type) (Çalışan kimliği (Çalışan tipi))	Listeden seçin
Division (Bölüm)	Filtreyi uygula düğmesi yalnızca bu bölümdeki kişileri gösterir
Company (Şirket)	Mevcut şirketlerden seç
Department (Departman)	
Card no. (from/to) (Kart no. başlangıç/ bitiş)	Bir değer aralığı tanımlamak için iki alanı da kullanın

2. **Apply filter**
   'a (Filtre uygula) tıklayın Filtreyle eşleşen tüm kişiler **Selected persons** (Seçilen kişiler) listesinde gösterilir**.**

3. Seçilen kişiler kümesini daha da daraltmak için **Selected persons** (Seçilen kişiler) listesinde bir veya daha fazla satıra tıklayın ve ardından **Remove** (Kaldır) düğmesine tıklayın. Bir seferde birden fazla kayıt seçmek için Ctrl ve Shift tuşlarını kullanın.
   – **ÖNEMLİ:** Devam etmeden önce, **Selected persons** (Seçilen kişiler) listesinin yalnızca bölümünü değiştirmek istediğiniz kişileri içerdiğinden emin olun.
4. **New division** (Yeni bölüm) listesinden, seçilen kişilerin hedef bölümünü seçin.
5. **Change division of persons**'a (Kişilerin bölümünü değiştir) tıklayın
   Selected persons (Seçilen kişiler) listesindeki TÜM kişiler **New division**'a (Yeni bölüm) taşınır.

Bir bölümden başka bölüme geçişin etkileri
Persons (Kişiler)
– Giriş yetkileri ve yol kontrolü
– Önceki bölümün bağlantıları silinir.
– Ortak kategorisine ait verilerin bağlantıları korunur.
Companies (Şirketler)
– Önceki bölüme ait şirketlerin bağlantıları silinir.

Ortak bölümden başka bölüme geçişin etkileri
– Giriş yetkileri ve yol kontrolü
– Ortak ve yeni bölümün bağlantıları korunur.
– Diğer bölümün bağlantıları silinir.

Bir bölümden Ortak bölüme geçişin etkileri
Tüm bağlantılar korunur.

25.10 Kişiler veya araçlara yönelik alanı ayarlama

Giriş
Bu bölümde bir kart sahibinin kayıt yerinin veya aracının tanımlanan bir alandan diğerine nasıl geçirileceği açıklanmaktadır. Bu, kart sahibi bir alandan kartını taratmadan başka bir alana geçtiyse gerekli olabilir. Böyle koşullarda, sıkı antipassback sistemleri, gerçek ve kayıtlı konumlar aynı olana kadar kart sahibinin girmesine izin vermez.

Ön koşullar
– Sisteminizde giriş alanları tanımlandı ve kullanılıyor. Belgeler için aşağıdaki bağlantıya bakın.
– Operatör olarak kart sahibinin verilerini değiştirme yetkiniz vardır.

Tek kart sahiplerinin ve araçlarının konumunu sıfırlama prosedürü
İletişim yolu
Main menu (Ana menü) > **Personnel data** (Personel verileri) > **Areas** (Alanlar)

1. Kart sahibini her zamanki gibi veritabanından seçin
2. **Location** (Konum) listesinden yeni bir konum seçin veya
3. **Location of the vehicle** (Aracın konumu) listesinden kart sahibinin aracı için yeni bir konum seçin
4. Kaydetmek için  simgesine tıklayın

Bkz.

– *Kartlı geçiş alanlarını yapılandırma, sayfa 24*

25.10.1 Tüm kart sahiplerinin ve araçlarının konumunu sıfırlama prosedürü

Bu prosedür örneğin bir tahliye eğitiminden sonra gerekli hale gelebilir. Tüm konumlar **UNKNOWN** (BİLİNMİYOR) olarak ayarlanır, böylece giriş sırası izleme ve antipassback devam edebilir.

Prosedür

İletişim yolu

Main menu (Ana menü) > **System data** (Sistem verileri) > **Reset areas unknown** (Bilinmeyen alanları sıfırla)

– **Set the areas of all persons present to UNKNOWN**'a (Mevcut tüm kişilere ait alanları BİLİNMİYOR olarak ayarla) tıklayın

veya

– **Set the areas of all parking vehicles to UNKNOWN**'a (Park eden tüm araçlara ait alanları BİLİNMİYOR olarak ayarla) tıklayın

25.11 Personel verileri formlarını özelleştirme ve yazdırma

Genel bilgiler

Kart sahibi verilerini veritabanından yazdırmak için formları özelleştirmek amacıyla **Forms**'u (Formlar) kullanın. Bu işlev yerel veri gizliliği yasalarınız açısından zorunlu olabilir.
Şablon formları sağlanır. Bu şablonlar HTML dosyaları olarak dışa aktarılabilir, gereksinimlerinize göre özelleştirilebilir ve iletişim kutusu yöneticisinde kullanmak için yeniden içe aktarılabilir.
Formları **Personnel data** (Personel verileri) > **Print badges** (Kimlik kartlarını yazdır) iletişim kutusundan görüntüleyip yazdırabilirsiniz.

İletişim yolu

– AMS Ana menüsü > **Configuration** (Yapılandırma) > **Options** (Seçenekler) > **Forms** (Formlar)

Formu özelleştirme

1. **Forms** (Formlar) iletişim kutusundaki **Available forms** (Mevcut formlar) listesinde, özelleştirmek istediğiniz şablonu seçin. Bu, genellikle veritabanındaki tüm kişisel veri alanlarını içeren `AllPersonalData_EN`, şablonudur.
2. Formu sisteminizdeki yeni bir HTML dosyasına kaydetmek için **Export**'a (Dışa aktar) tıklayın
3. HTML dosyasını gereksinimlerinize göre özelleştirmek için bir HTML düzenleyicisi kullanın
4. Özelleştirilmiş HTML dosyasını iletişim kutusu yöneticisine aktarmak için **Forms** (Formlar) iletişim kutusunda **Insert**'e (Ekle) tıklayın.
   – (İsteğe bağlı) Form yalnızca belirli bir Bölüm için geçerliyse **Division** (Bölüm) sütunundan yeni bir bölüm seçin.
   – (İsteğe bağlı) Görüntülenmemiş formu bir HTML görüntüleyicisinde görüntülemek için **Preview**'a (Ön izleme) tıklayın.
   – (İsteğe bağlı) Bir formu listeden silmek için **Delete**'e (Sil) tıklayın.

Form görüntüleme ve yazdırma

1. İletişim kutusu yöneticisinde, şuraya gidin:

– AMS ana menüsü > **Personnel data** (Personel verileri) > **Print badges** (Kimlik kartlarını yazdır)

2. İstediğiniz personel kaydını forma yükleyin
3. **Form** listesinden bir form seçin.
4. **Print form**'a (Formu yazdır) tıklayın
   – Form seçilen personel kaydının verileriyle görüntülenir ve seçtiğiniz yazıcıya gönderilir.

26 Ziyaretçileri yönetme

Ziyaretçiler giriş kontrolünde özel bir duruma sahiptir ve diğer personel verilerinden ayrı tutulur. Bu nedenle, ziyaretçi verileri ayrı iletişim kutularında oluşturulur ve tutulur.

26.1 Ziyaretçi verileri

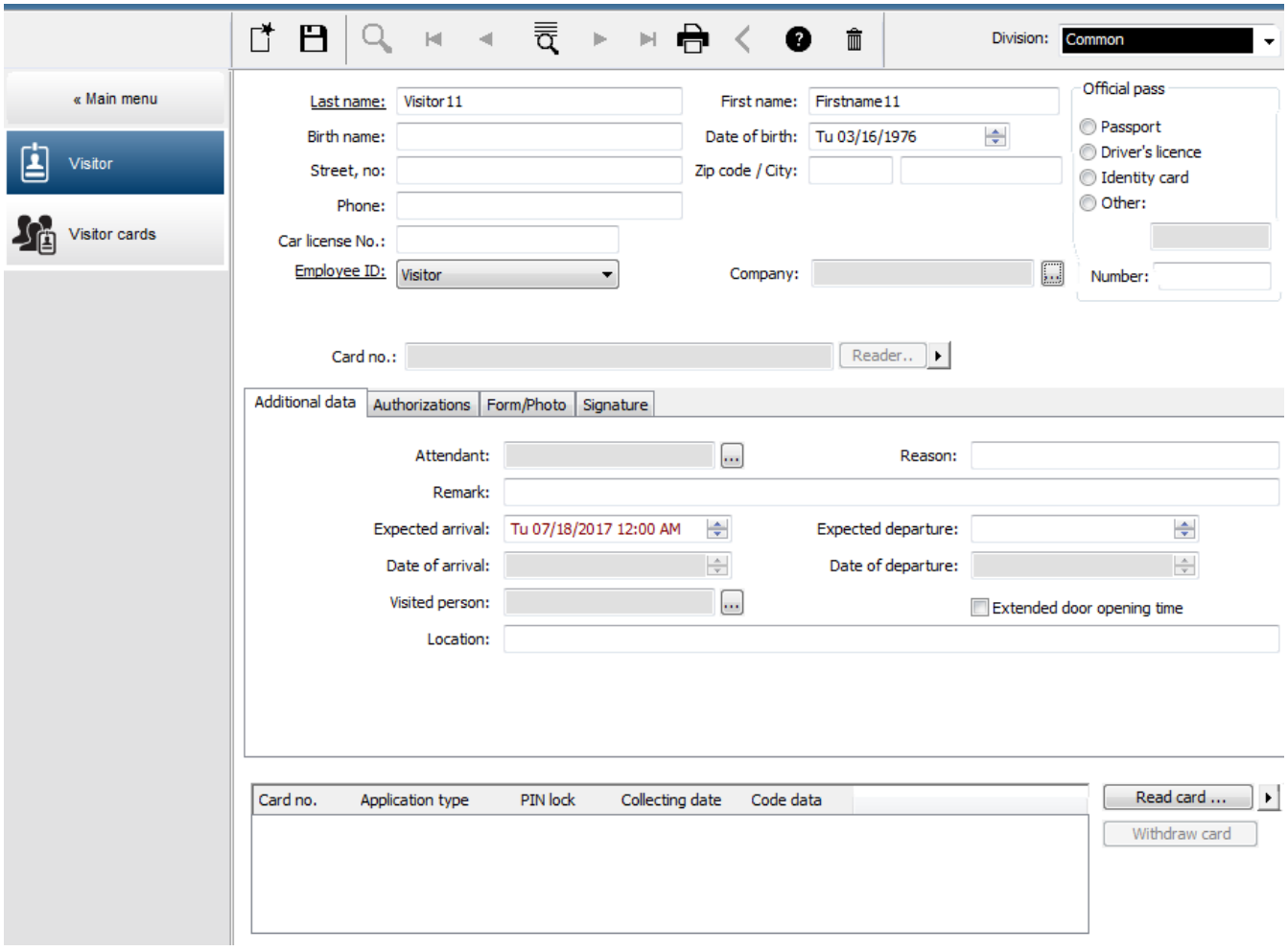
Giriş

Sistem, ziyaretçi verilerinin hızlı ve kolay yönetilmesini destekler. Dolayısıyla zaten bilinen ziyaretçilerin verileri girilebilir ve ziyaretçi gelmeden önce giriş yetkileri atanabilir. Ziyaretçi geldiğinde, yalnızca kartın atanması gerekir. Ziyaretin sonunda kart iade edildiğinde, kimlik kartı ile kişi arasındaki bağlantı yeniden silinir ve yetkiler otomatik olarak geri alınır.
Ziyaretçinin verileri kullanıcı tarafından silinmezse kimlik kartı son kez iade edildikten sonra yapılandırılan miktarda sürenin sonunda (varsayılan değer 6 ay) bu sistem tarafından yapılır.
Harici ziyaretçilerin yönetimi için iki iletişim kutusu vardır.

- **Ziyaretçiler** iletişim kutusu ziyaretçi verilerini ve ziyaretçi giriş yetkilerini girmek için kullanılır.
- **Ziyaretçi kartları** iletişim kutusu ise ziyaretçi kartlarının kaydını ve silinmesini düzenler.

İletişim Kutusu: Ziyaretçiler

Ziyaretçiler diğer kişilerden net bir şekilde ayrılmış bir duruma sahiptir ve bu nedenle ziyaretçilere ayrı bir iletişim kutusunda işlem yapılır. **Ziyaretçi** kimliğine sahip kişiler, **Kişiler** iletişim kutusunda oluşturulamaz veya bu kişiler için bu amaçla iletişim kutusunda kayıtlı kimlik kartları yoktur.
Diğer şeyler arasında, **Ziyaretçiler** iletişim kutusunda **Çalışan Kimliği** giriş alanı yoktur.
Ziyaretçiler için ayrı bir veritabanı tablosu olduğundan, burada açıklanan iletişim kutusunda oluşturulan kişiler otomatik olarak ziyaretçiler olarak tanımlanır. Bu nedenle bu, burada ziyaretçiler dışında hiç kimsenin oluşturulamayacağı anlamına gelir. Buna uygun olarak, seçimler yalnızca bu iletişim kutusunda ilgili veritabanı tablosunda yapılır. Bunun tersine, sistemde kayıtlı tüm kişiler diğer personel verileri iletişim kutularında seçilebilir, ancak her zaman ziyaretçiler için kullanılamayabilirler (**Kartlar** iletişim kutusu).
Ziyaretçi verileri bilindiğinde, sisteme ziyaretçi gelmeden önce tamamen veya kısmen girilebilir. Bu, verileri zaten kayıtlı olan ziyaretçiler için bekleme sürelerini en aza indirir.

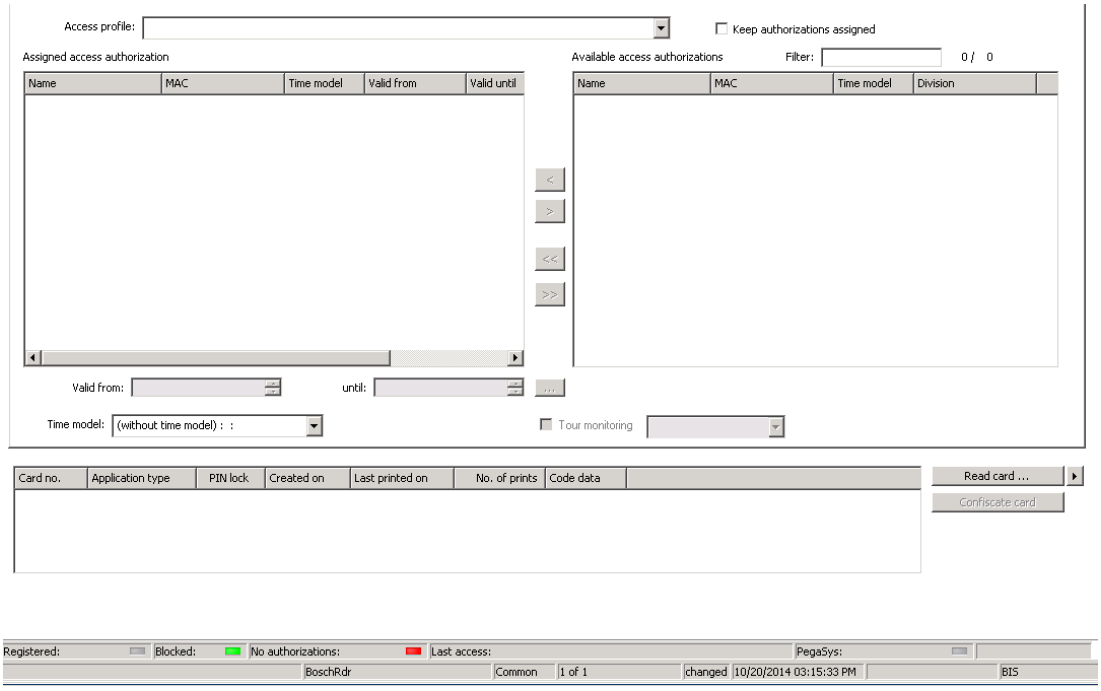


Aşağıdaki giriş alanlarına ziyaretin **Nedeni**, ziyaretçinin ziyaret ettiği **Konum** ve bir **Açıklama** girilebilir.

Beklenen varış ve **beklenen ayrılış** alanlarına veri girmeyi tercih ederseniz bu tarihler **geçerlilik başlangıcı** ve **geçerlilik bitişi** alanlarında da görünür.

Ziyaretçi verileri sırasıyla bir ziyaretçi kimlik kartına atandığında ve bir ziyaretçi kimlik kartından ayrıldığında ilgili tarihler sistem tarafından **Varış tarihi** ve **Ayrılış tarihi** alanlarına girilir.

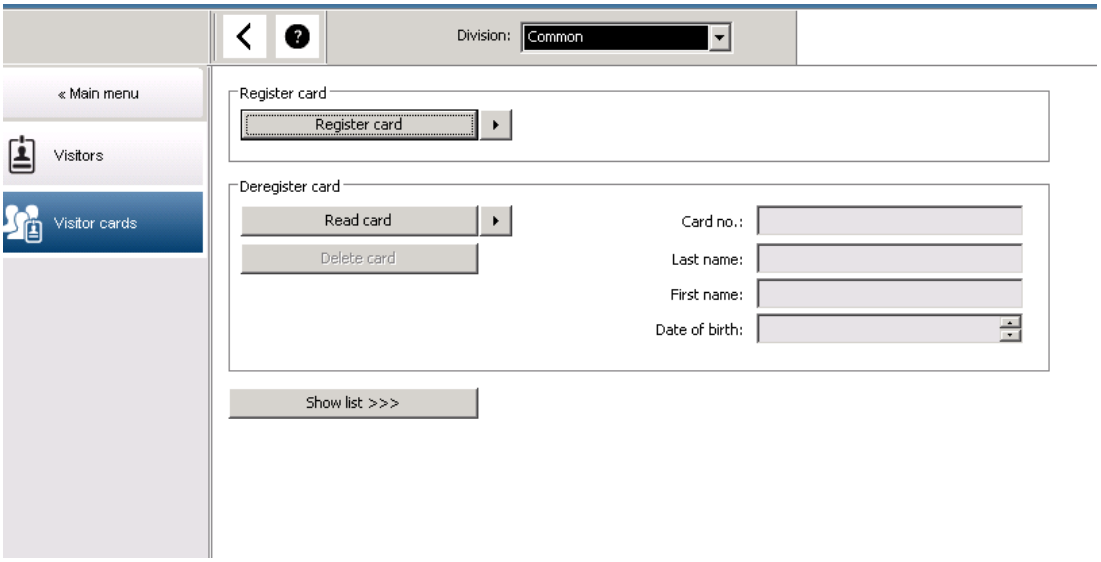
Kartlar iletişim kutusunda olduğu gibi, örneğin engelli kişiler için daha kolay giriş sağlamak için ziyaretçilere daha uzun kapı açılış süreleri atamak da mümkündür.



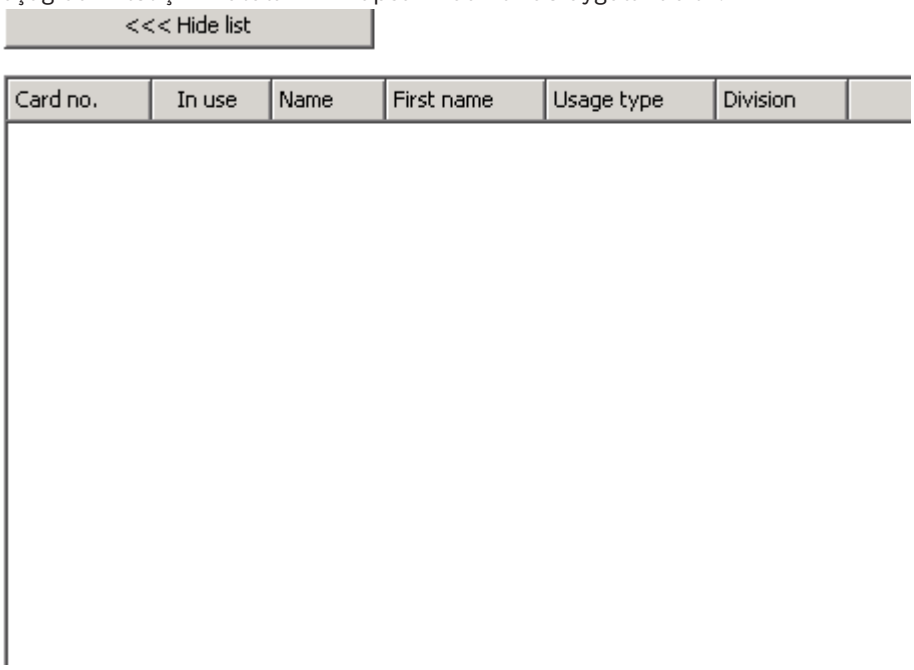
Yetki ata iletişim kutusu alanında eş sesli seçim listesinde mevcut bir ziyaretçi profili seçilebilir veya yetkiler işaretlenip sağdaki listeden aktarılarak soldaki **Atanan giriş yetkisi** listesinden **Mevcut giriş yetkisi** listesinden tek giriş yetkileri seçilebilir.
Bu iletişim kutusunda yalnızca Ziyaretçi profilleri olarak işaretlenen Giriş profilleri seçilebilir. Böylece genel yetkilerin atanması yoluyla ziyaretçilerin özel alanlara giriş yapması engellenir. Giriş yetkilerinin doğrulanması da her yetki için kendisi tarafından ayarlanabilir.
Kart okuma sırasında hata oluşursa kimlik kartı numarası da manuel olarak verilebilir. Geçerli tarih eş zamanlı olarak varış tarihi olarak saklanır.
Ziyaretten sonra, ziyaretçi kimlik kartını iade eder. Bu kimlik kartı bir kart okuyucuda okunurken veya kimlik kartı numarası manuel olarak girilirken ilişkili kişi seçilir ve bu kişinin verileri ekranda görüntülenir.
Operatör, kartın iade edildiğini onaylar. Kimlik kartı ve ziyaretçi arasındaki ilişki **Confiscate card** (Karta el koy) düğmesi kullanılarak kaldırılır. Bu eylemin tarih ve saati ayrılış tarihi olarak saklanır.

İletişim Kutusu: Ziyaretçi Kartları
Sistemdeki bazı kartlar ziyaretçi kartları olarak ayrılmıştır. Normalde bir ziyaretçi kartı gelen bir ziyaretçiye atanır ve ziyaretçi ayrılırken iade edilir. Böylece kart yeniden kullanılabilir. Bu tür kartların ziyaretçilere atanabilmesi için bu iletişim kutusunda ziyaretçi kartları olarak kaydedilmesi gerekir:

Uyarı!
Genel olarak, ziyaretçi kimlik kartları yeniden kullanılabilmelerini sağlamak için ad veya fotoğraf olmadan oluşturulur.



Kayıt için **Kimlik kartını kaydet** düğmesine tıklayın.
Ardından, daha önce açıklanan giriş prosedürü (**Personel verileri** bölümündeki **Kişiler** ve **Kimlik kartları** kısımları) kimlik kartını tespit etmek için kimlik kartı numarasıyla birlikte kullanılır. Bu sistemin kimlik kartını ziyaretçi kimlik kartı olarak tanımasını sağlar ve ardından aşağıdaki iletişim kutularının kapsamı dahilinde uygulanabilir.



Ziyaretçi kimlik kartlarının daha hızlı atanmasını sağlamak için, mevcut tüm kimlik kartlarının taranması önerilir, böylece bu kartlar sonraki iletişim kutusunda ilgili ziyaretçilere atanabilir. Ziyaretin sonunda, ziyaretçi kimlik kartını iade eder. Bu kimlik kartını bir iletişim kutusu okuyucusunda taratarak veya kimlik kartı numarasını girerek kartın atandığı kişi seçilir ve bu kişinin verileri ekranda görüntülenir. [Kimlik kartı numarasını manuel olarak girmek ve okuyucuların kullanımına geçmek için lütfen **İletişim Kutusu: Kartlar** ve **İletişim Kutusu: Ziyaretçiler**'deki açıklamalara bakın.] Kullanıcı, kimlik kartının iade edildiğini onaylar. Ziyaretçinin kimlik kartı ve personel verileri arasındaki bağlantı düğme kullanılarak kaldırılır. Geçerli tarih ayrılış tarihi olarak saklanır.

Bir Ziyaretçi formunu yazdırma

Ziyaretçiler iletişim kutusunun araç çubuğu ziyaretçi sertifikası yazdırmak için ek bir düğme  içerir. Diğer şeyler arasında ziyaretçiyi kabul eden kişi bu ziyaretçi sertifikasını ziyaretçinin gelip gelmediğini ve ne zaman gelip ayrıldığını doğrulamak için kullanabilir.

Visitor pass

Entry	Exit

First- and lastname
Steven Visitor

Company

☐ Proof of authority for plant area

Registration plate

Passed card

Contact person Phone Department

Reason of visit

Visit appointment
☐ Yes ☐ No

Type of official
Passport

Number of offical document

I accept the terms and conditions overleaf

Location, date Sign of visitor

Identy card with photo seen ?
☐ Yes ☐ No

Sign of plant protective force

To complete from visited person

Arrival at _____
Departure at _____

To sign on visited person

27 Otoparkları yönetme

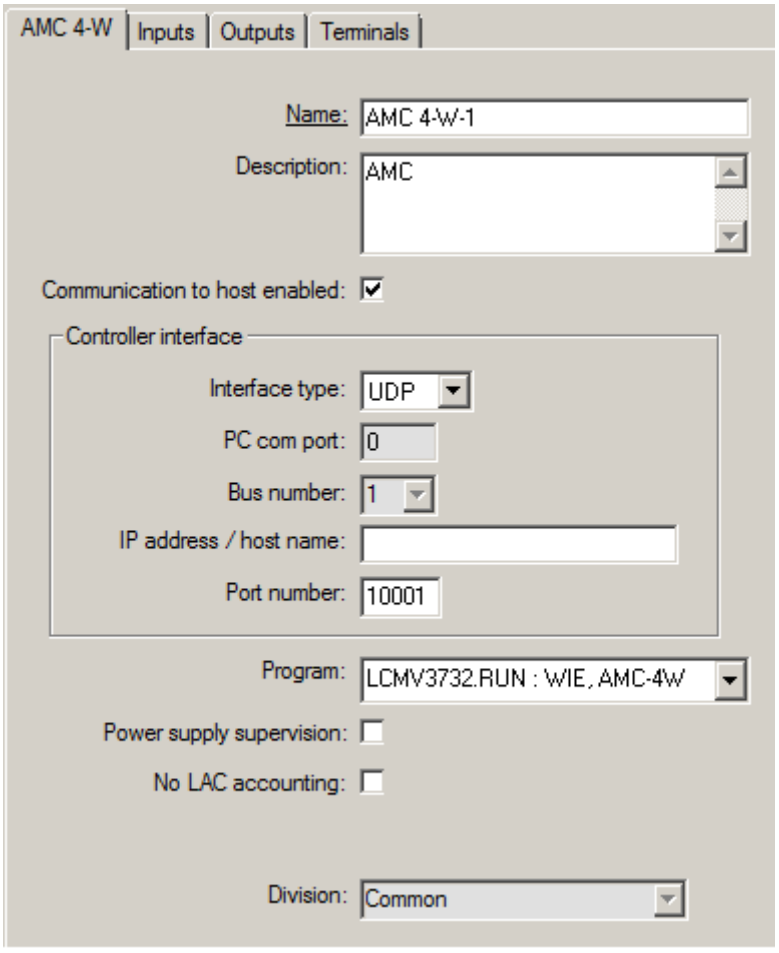
27.1 Bazı park bölgelerine ilişkin yetkiler

Bazı otoparklarda engelli ve engelli olmayan sürücüler için bölgeler vardır. Bu durumda aşağıdaki kurallar geçerlidir:

– Yalnızca engelli olmayan kişiler için hala park yerleri bulunduğu sürece sezon bileti sahiplerinin giriş yapmasına izin verilir.
– Engelli veya engelli olmayan kişiler için hala park yerleri bulunduğu sürece engelli kişilerin giriş yapmasına izin verilir.

Uyarı!
Bu, önceden bilet sahiplerinin kurallara uyduğunu varsayar. Bu özellikle şu anlama gelir:
Engelli olmayan kişiler engellilere yönelik bir park yerine park etmez
Engelli kişiler uygun olduğu sürece engellilere yönelik park yerlerini kullanır

Birkaç yetkiye sahip bir kişi engelli olsun ya da olmasın ikisine de erişebilir. AMC, park bölgelerinin yapılandırılan sıralı düzenine göre kişiye yer ayırmaya çalışır. Bir bölgenin dolu olması durumunda, sonraki yetkili ve serbest bölge için arama devam eder.
MAC ve AMC'de sayaç hesaplaması:
1) Bir AMC bir otoparkın tüm girişlerini ve çıkışlarını kontrol eder:
=> AMC kendi başına sayar ve çevrimiçi olurken MAC tarafından düzeltilebilir.
2) Bir otoparkın girişleri ve çıkışları farklı AMC'lere bölünür:
=> MAC, çevrimiçi çalışma durumunda AMC için sayar. Çevrimdışı çalışırken, AMC'ler girişe izin verir (buna göre yapılandırıldıysa) ancak saymaz.
Bir otoparkı birkaç AMC kontrol ediyorsa AMC yapılandırmasında **No LAC accounting** (LAC hesaplaması yok) onay kutusunu işaretleyin.



27.2 Otopark raporu

Parking lot list Date 08.11.2013 , 14:51:23 Page 1

Parking area	Zone	Vehicle count	State
Main Park		51	
	Zone A	30	full
	Zone B	9	--
	Zone C	12	--
Building A		39	
	Zone A	30	full
	Zone B	9	--
Building B		39	
	Zone A	30	full
	Zone B	9	--

27.3 Genişletilmiş Otopark yönetimi

Giriş

Operatör standart dışı boyutlarda araçları telafi etmek için otopark alanındaki park yeri sayısını ayarlayabilir, örneğin:

– Kamyonlar

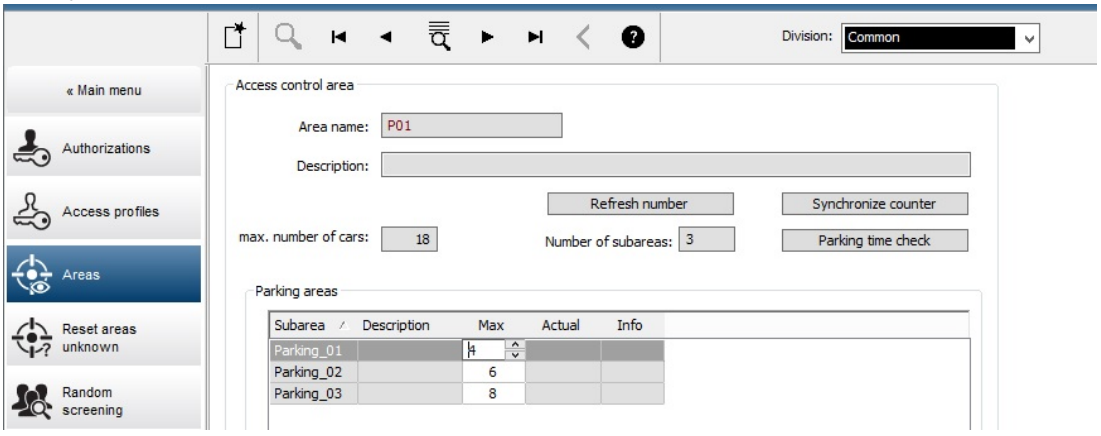
– Engelli girişi
– Motosikletler

İletişim yolu

Ana menü > **Personel verileri** > **Alanlar**

Prosedür

1. Otopark alanını seçin
2. **Parking areas** (Otopark alanları) bölmesinde **Max** (Maks.) sütunundaki değeri o alan için yeni park yeri sayısı olarak ayarlayın.



Notlar:

– **Max** sütununda yapılan ayarlar, **Areas** yapılandırmasında yapılan ayarları geçersiz kılar. Aşağıdaki bağlantıdan **Araçlar için alanları yapılandırma** bölümüne bakın.
– **Max** (Maks.) sütunundaki bir `0` sütun Unlimited (Sınırsız) anlamına gelir; tüm araç sayımı kapatılır.

Bkz.

– *Araçlara ait alanları yapılandırma, sayfa 25*

28 Genel bakışlar ve devriyeleri yönetme

Genel bakışlara giriş

Genel bakış tesis etrafında kart okuyucularla işaretlenen bir güzergahtır. Bu güzergahta, **Güvenlik görevlisi** çalışan türündeki kişiler okuyucuyu fiziksel olarak ziyaret ettiklerini kanıtlamak için özel bir güvenlik görevlisi kartı göstermelidir.

Güvenlik görevlisi kartları girişleri açmaz, ancak yalnızca izleme için kullanılabilir. Girişleri açmak için güvenlik görevlisinin ek olarak bir giriş kartına ihtiyacı vardır.

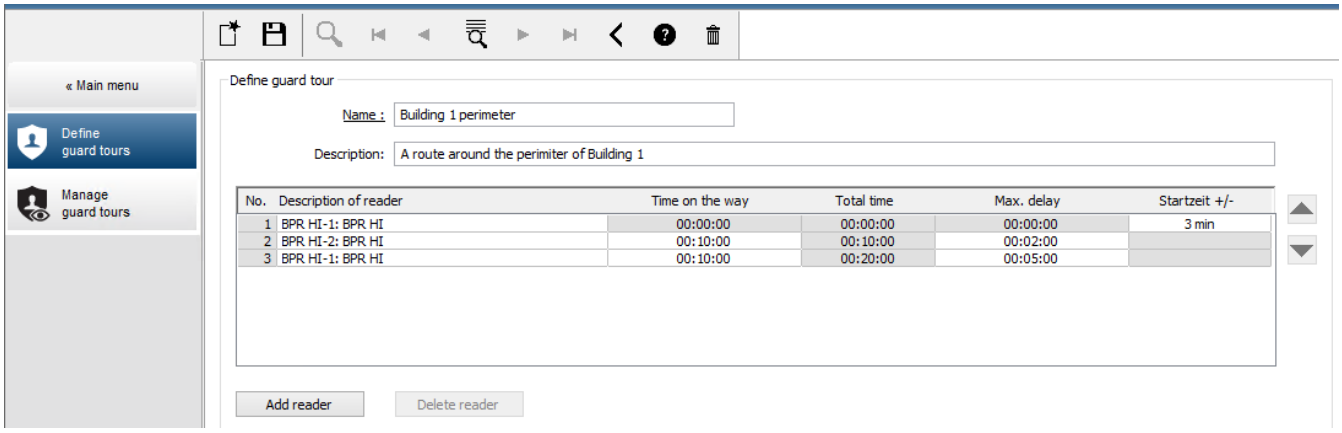
Genel bakış, aralardaki yaklaşık yürüyüş süreleriyle birlikte bir dizi okuyucudan oluşur. Okuyucular arasındaki maksimum kabul edilebilir gecikme ve başlangıç süresinden kabul edilebilir sapma (+/-) Genel bakışın da nitelikleridir. Bu tanımlanan hata paylarının dışındaki sapmalar potansiyel olarak alarmları tetikleyebilir ve **Devriyeler**'de kaydedilir.

Devriyelere Giriş

Devriye belirli bir tarih ve saatte Genel bakışın tersidir. Her devriye adil nedenlerle sistemde benzersiz bir varlık olarak oluşturulur ve kaydedilir.

28.1 Genel bakışları tanımlama

Guard tours (Genel bakışlar) > **Define guard tours**'u (Genel bakışları tanımla) seçin



- **Name** (Ad) metin alanında, Genel bakış için bir ad girin
- **Description** (Açıklama) metin alanına güzergaha ilişkin daha ayrıntılı bir açıklama girin (isteğe bağlı).

Genel bakışa okuyucu ekleme:

1. **Add reader** (Okuyucu ekle) düğmesine tıklayın.
   Tabloda bir satır oluşturulur.
2. **Okuyucu açıklaması** sütununda, açılır listeden bir okuyucu seçin.
3. Kabul edilebilir sapmalar için değerleri girin:
   - Bu, sıradaki ilk okuyucuysa **Başlangıç saati +/-**'nin altına bu genel bakışta bir devriye için başlangıç zamanı olarak hala kabul edilebilir olacak önceki ve sonraki dakikaları girin.
   - Bu, sıradaki ilk okuyucu **değilse Yolda geçen zaman**'ın altına güvenlik görevlisinin önceki okuyucudan bu okuyucuya gitmesi için gereken saati (sa:dd:ss) girin. Gecikmeler hariç toplam süre **Toplam süre** sütununda artar.
4. **Maks. gecikme**'nin altına bir devriyenin **Gecikti** olarak işaretlenmesine neden olmadan kabul edilebilir olmaya devam edecek maksimum **Yolda geçen zaman** miktarını girin.

5. Gerektiği kadar fazla okuyucu ekleyin. Genel bakış birden fazla kez geçerse veya geri dönerse aynı okuyucunun birden fazla kez işlem görebileceğini unutmayın.

– Bir okuyucuyu sıradan silmek için, satırı seçin ve **Okuyucuyu sil** düğmesine tıklayın.
– Bir okuyucunun sıradaki yerini değiştirmek için, satırı seçin ve yukarı/aşağı  düğmelerine tıklayın.

28.2 Devriyeleri yönetme

Guard tours (Genel bakışlar) > **Manage guard tours**'u (Genel bakışları yönet) seçin

Yeni bir devriye planlama

Belirli bir genel bakışla birlikte bir devriye planlamak için aşağıdaki işlemleri yapın:

1. Devriye için istediğiniz güvenlik görevlisi kartına sahip olduğunuzdan emin olun ve yapılandırılmış bir giriş kartı okuyucusuna veya doğrudan bağlı kayıt okuyucusuna giriş yapın.
2. **Genel bakışlar** sütununda, tanımlanan genel bakışlardan birini seçin.
3. **Yeni devriye...** düğmesine tıklayın.
   Bir açılır pencere görünür.
4. Açılır pencerede, isterseniz açılır listedeki genel bakışı değiştirin.
5. Devriyenin önceden tanımlanmış bir başlangıç zamanı olması gerekiyorsa **Başlangıç saati ayarla:** onay kutusunu seçin.
   – Başlangıç tarihini ve saatini girin.
   – İsterseniz geç veya erken başlangıçlar için hata payını ayarlamak üzere **Başlangıç saati +/-** döndürme kutusuna tıklayın.
6. Sağ oka tıklayın ve güvenlik görevlisi kartını kaydetmek için kullanmak istediğiniz okuyucuyu seçin. Okuyucunun seçim için burada görünmeden önce sistemde zaten yapılandırılmış olması gerektiğini unutmayın.
7. Güvenlik görevlisi kartını okumaya başlamak için yeşil artı düğmesine tıklayın, kartı okuyucuya gösterin ve açılır penceredeki talimatları izleyin.
   Güvenlik görevlisi kartı devriyede kullanım için kaydedilir.
8. Bu devriye için alternatif güvenlik görevlisi kartlarını kaydetmek üzere önceki adımı tekrarlayın. Her durumda devriye sırasında gösterilen ilk kartın söz konusu devriye boyunca tüm okuyucularda kullanılması gerektiğini unutmayın.
9. **Tamam**'a tıklayın. Seçilen genel bakış listede **planned** (planlandı) olarak işaretlenir.

Devriye izleme

Tüm planlı ve etkin devriyeler listenin üst kısmına taşınır. Planlı veya etkin birden fazla devriye varsa seçilen devriye kırmızı renkle çerçeve içine alınır. Diğer bilgileri almak için çerçeveye tıklayın.

Güvenlik görevlisi genel bakıştaki ilk okuyucuda kartını gösterdiğinde bir devriye başlatılır. Devriye için alternatif kartlar tanımlanmış olsa bile devriyenin geri kalanı boyunca bu kart kullanılmalıdır.

Devriyenin **Durum**'u **Etkin** olarak değişir.

Planda ulaşılan her okuyucu yeşil bir onay işareti ✔ alır. O anda seçili olan devriyede yer alan okuyucular arasındaki planlı ve gerçek zamanlar iletişim penceresinin alt yarısında görüntülenir.

Planlı süreyle **Maks. gecikme**'nin toplamından sonra ulaşılan her okuyucu kırmızı bir ⊘ işareti alır. Devriye **Delayed** (Gecikti) olarak işaretlenir.

Bu durumda, güvenlik görevlisi sorun olmadığını onaylamak için operatörü arar. Ardından operatör **Resume patrol** (Devriyeyi devam ettir) düğmesine tıklar. Okuyucu ek bir "c" bulunan yeşil bir onay işareti alır. Güvenlik görevlisi artık sonraki okuyucuda devriyeye devam edebilir.
Etkin devriyede öngörülmeyen ancak zararsız bir gecikme varsa güvenlik görevlisi planı düzeltmek için operatörü arayabilir. **Delay (min)** (Gecikme (dk.)) döndürme kutusuna gecikme dakikalarını girin ve **Apply** (Uygula) düğmesine tıklayın.
Bir devriye planlandığı gibi tamamlanamazsa operatör **Interrupt** (Kes) düğmesine tıklayarak devriyeyi durdurabilir. Devriyenin **State**'i (Durum) **Aborted** (Durduruldu) olarak değiştir ve listede planlı ve etkin genel bakışların altına düşer.

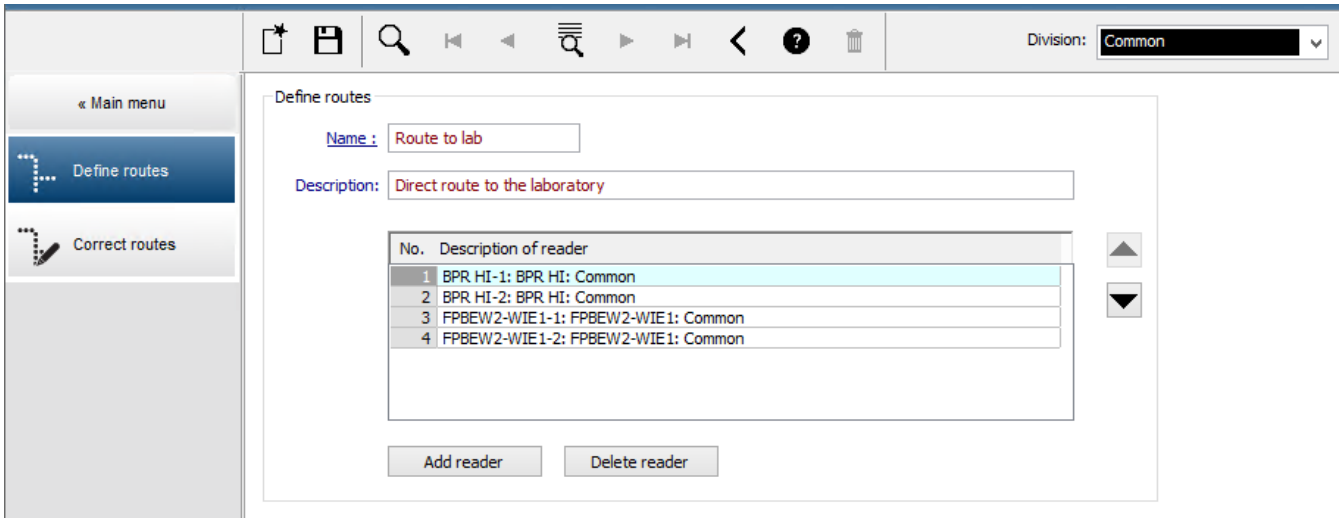
28.3 Bakış izleme (eskiden yol kontrolüydü)

Giriş

Bir Güzergah (veya Tur), kişinin yetkilerinden bağımsız olarak tesisteki hareketlerine yön vermek için kartlı geçiş sisteminde tanımlı kişilere uygulanabilecek önceden tanımlanan bir okuyucu sırasıdır.
Tipik kullanım alanları endüstriyel temiz ortamlar, hijyenik kontrollü veya yüksek güvenlikli alanlarda katı giriş sıraları uygulamaktır.

Güzergahları tanımlama

1. Ana menüde **Tour monitoring** (Bakış izleme) > **Define routes**'u (Güzergahları tanımla) seçin
2. Güzergah için bir ad girin (en fazla 16 karakter)
3. Daha ayrıntılı bir açıklama girin (isteğe bağlı)
4. Genel bakışlarda olduğu gibi bir okuyucu sırası oluşturmak için **Okuyucu ekle** düğmesine tıklayın. Bir okuyucunun sıradaki yerini değiştirmek için ok düğmelerini, kaldırmak için ise **Okuyucuyu sil** düğmesini kullanın.



Bir kişiye güzergah atama

Bir kişiye güzergah atamak için aşağıdaki işlemleri yapın:

1. Ana menüde **Personnel data** (Personel verileri) > **Cards**'a (Kartlar) tıklayın
2. Atanacak kişinin personel kaydını yükleyin.

3. **Other data** (Diğer veriler) sekmesinde, **Tour monitoring** (Bakış izleme) onay kutusunu seçin
4. Bunun yanındaki açılır listeden tanımlı bir güzergah seçin (bir güzergah tanımlamak için önceki bölüme bakın).
5. Personel kaydını kaydedin.

Güzergah, atanan kişi kartını güzergahtaki ilk okuyucuya gösterdiğinde etkinleştirilir. Güzergahtaki diğer okuyucular artık sırada kullanılmalıdır, yani yalnızca sıradaki sonraki okuyucu giriş izni verir. Güzergah tamamen ters çevrildikten sonra kişi, yetkileri dahilinde herhangi bir okuyucuda ayırma işlemi yapabilir.

Güzergahları düzeltme ve izleme

1. Ana menüde **Tour monitoring** (Bakış izleme) > **Correct routes**'u (Güzergahları düzelt) seçin
2. Güzergaha atanan kişinin personel kaydını yükleyin.
3. Güzergahta ilgili kişiyi bulmak için, **Determine location** (Konumu belirle) düğmesine tıklayın.
4. Zaten başarıyla geçilmiş olan okuyucular listede yeşil bir onay işareti ✔ alır.
5. Güzergahta bir kişinin konumunu sıfırlamak veya düzeltmek için, **Set location** (Konumu ayarla) düğmesine tıklayın.

29 Personelin rastgele taranması

Rastgele tarama işlemi

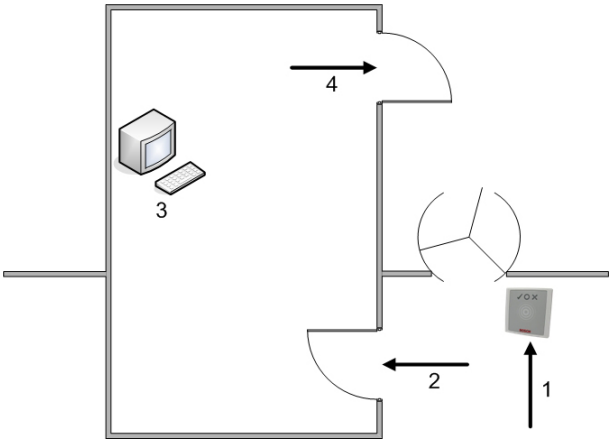
1. Bir kart sahibi kartını rastgele tarama için yapılandırılmış bir okuyucuya gösterir.
   Not
   Yalnızca tanımlanan yöndeki girişten geçme yetkisi olan kişiler rastgele seçilebilir. Yetkiler rastgele tarama gerçekleşmeden önce kontrol edildiği için herhangi bir yetkisiz kişi engellenir ve seçin işlemine dahil edilmez.
2. Karıştırıcı bu kişiyi tarama için seçerse bu kişinin kartı tüm sistem genelinde engellenir.
   - Olay, sistem olay günlüğüne kaydedilir.
   - **Engelleme** iletişim kutusuna **Rastgele tarama** şeklinde işaretli bir sınır süre girişi eklenir. [Aşağıdaki şekil - sayı 1]
   - Personel veri iletişim kutularının durum çubuğu Engellenen "LED"leri Rastgele yanıp sönerken (yanıp sönen mor) görüntüler.

Uyarı!
Rastgele taramadan çıkarıldı parametresi ayarlanan (**Kartlar** iletişim kutusu, **Diğer veriler** sekmesinde) kişiler tarama işlemine dahil edilmez.

3. Rastgele seçilen kişi ayrı bir güvenlik kulübesinde yapılacak diğer kontroller için davet edilir.
4. Bu kontroller yapıldıktan sonra güvenlik görevlisi engellemeyi **Engelleme** iletişim kutusunda aşağıdaki gibi sıfırlar:
   - Liste kontrolü **Engelleme** listesinden ilgili engellemeyi seçin.
   - **Sil** düğmesine tıklayın.
   - **Evet**'e tıklayarak silme işlemini onaylayın.

Rastgele taranan kişi artık kartını yetkili olduğu tüm okuyucularda yeniden kullanabilir.

Rastgele tarama için örnek oda yerleşimi



1 = Kartı gösterme - tarama - sistem genelinde engelleme
2 = Kart sahibi güvenlik kulübesine girer
3 = Kart sahibi aranır ve ardından iletişim kutusu aracılığıyla engelleme kartından kaldırılır.
4 = Kart sahibi, kartı tekrar okuyucuya göstermeden güvenlik kabinini terk eder.

Uyarı!
Tarama yüzdesi zaman içinde kümülatif olarak elde edilir. Örneğin, %10 rasgele taramada, hala art arda iki kişinin seçilebilme olasılığı vardır (100'de 1, yani 1/10 x 1/10).

30 Olay Görüntüleyici'yi Kullanma

Giriş

Olay Görüntüleyici, uygun şekilde yetkilendirilmiş operatörlerin sistem tarafından kaydedilen olayları incelemelerini ve ekranda, yazdırılmış veya `.CSV` dosyaları şeklinde raporlar üretmelerini sağlar.

İstediğiniz kayıtları Olay Günlüğü veritabanından almak ve görüntülemek için filtre kriterleri ayarlayın ve **Refresh**'e (Yenile)  tıklayın. Bu işlem istenen veri miktarına bağlı olarak birkaç dakika sürebilir.

Filtre kriterleri farklı şekillerde ayarlanabilir:

Bağıl	Mevcut zamana göre olayları seçmek için.
Aralık	Olayları serbestçe tanımlanabilen bir zaman aralığı içinde seçmek için
Toplam	Olayları oluş zamanlarından bağımsız olarak seçmek için

Ön koşullar

İletişim kutusu yöneticisine giriş yaptınız.

İletişim yolu

İletişim yöneticisi ana menüsü > **Reports** (Raporlar) > **Event viewer** (Olay görüntüleyicisi)

30.1 Filtre kriterlerini şu ana göre ayarlama

1. **Time period**'ın (Zaman dilimi) altındaki **Relative** (Bağıl) radyo düğmesini seçin
2. **Search within the last** (Sonuncuda ara) kutusunda, aranacak olan sayı zaman birimlerini ayarlayın ve örneğin hafta, gün, saat, dakika, saniye olmak üzere kullanılacak birimi seçin.
3. **Event types** (Olay türleri) menüsünde, aranacak etkinlik kategorisini ve ardından ilginizi çeken olay türlerini seçin.
4. **Maximum number** (Maksimum sayı) menüsünde, olay görüntüleyicisinin almaya kalkıştığı olayların sayısını sınırlayın. Performans nedenleriyle değeri **(unlimited)** (sınırsız) olarak bırakmak **önerilmez**.
5. İlginizi çeken diğer filtre kriterlerini belirtin:
   - Soyadı
   - First name (Ad)
   - Personel numarası
   - Kart numarası
   - Kullanıcı (yani, sistem operatörü)
   - Cihaz adı
   - Alan adı.

- Olayları toplamaya başlamak için **Refresh**'e  , durdurmak için ise **Cancel**'a (İptal) tıklayın.
- Sonuçları kaydetmek için  veya yazdırmak için  simgesine tıklayın.
- Başka bir aramanın sonuçlarını silmek için  simgesine tıklayın.

30.2 Bir zaman aralığı için filtre kriterlerini belirleme

1. **Time period**'ın (Zaman dilimi) altındaki **Interval** (Aralık) radyo düğmesini seçin
2. **Time from, Time until** (Başlangıç zamanı, Bitiş zamanı) tarih seçicilerinde olayların aranacağı dönemin başlangıcını ve sonunu tanımlayın.
3. **Event types** (Olay türleri) menüsünde, aranacak etkinlik kategorisini ve ardından ilginizi çeken olay türlerini seçin.
4. **Maximum number** (Maksimum sayı) menüsünde, olay görüntüleyicisinin almaya kalkıştığı olayların sayısını sınırlayın. Performans nedenleriyle değeri **(unlimited)** (sınırsız) olarak bırakmak **önerilmez**.
5. İlginizi çeken diğer filtre kriterlerini belirtin:
   - Soyadı
   - First name (Ad)
   - Personel numarası
   - Kart numarası
   - Kullanıcı (yani, sistem operatörü)
   - Cihaz adı
   - Alan adı.

- Olayları toplamaya başlamak için **Refresh**'e  , durdurmak için ise **Cancel**'a (İptal) tıklayın.
- Sonuçları kaydetmek için  veya yazdırmak için  simgesine tıklayın.
- Başka bir aramanın sonuçlarını silmek için  simgesine tıklayın.

30.3 Filtre kriterlerini zamandan bağımsız olarak belirleme

1. **Time period**'ın (Zaman dilimi) altındaki **Total** (Toplam) radyo düğmesini seçin
2. **Event types** (Olay türleri) menüsünde, aranacak etkinlik kategorisini ve ardından ilginizi çeken olay türlerini seçin.
3. **Maximum number** (Maksimum sayı) menüsünde, olay görüntüleyicisinin almaya kalkıştığı olayların sayısını sınırlayın. Performans nedenleriyle değeri **(unlimited)** (sınırsız) olarak bırakmak **önerilmez**.
4. İlginizi çeken diğer filtre kriterlerini belirtin:
   - Soyadı
   - First name (Ad)
   - Personel numarası
   - Kart numarası
   - Kullanıcı (yani, sistem operatörü)
   - Cihaz adı
   - Alan adı.

- Olayları toplamaya başlamak için **Refresh**'e  , durdurmak için ise **Cancel**'a (İptal) tıklayın.
- Sonuçları kaydetmek için  veya yazdırmak için  simgesine tıklayın.

– Başka bir aramanın sonuçlarını silmek için  simgesine tıklayın.

31 Raporları kullanma

Bu bölüm, sistem ve olay günlüğü verilerini filtrelemek ve net biçimlerde sunmak için kullanılabilecek bir rapor işlevleri koleksiyonunu açıklar.

İletişim yolu

Main menu (Ana menü) > **Reports** (Raporlar).

Rapor araç çubuğunu kullanma

Yazdırmadan önce bir ön izleme görüntülemek için  simgesine tıklayın.

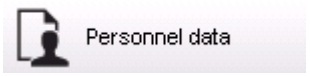
Ön izlemenin kendi araç çubuğu vardır:

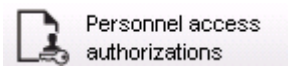
- Yazdırmadan ön izlemeden çıkmak için ✕ simgesine tıklayın.
- İleri ve geri göz atmak veya sayfa sayısına göre sayfaları tek tek seçmek için ön izleme araç çubuğundaki ok tuşlarını |◀ ◀ 2 of 17 ▶ ▶| kullanın.
- Varsayılan yazıcınızı kullanarak hemen yazdırmak için  simgesine tıklayın.
- Diğer yazdırma seçeneklerine izin veren bir Print Setup (Yazdırma Ayarları) iletişim kutusu aracılığıyla yazdırmak için simgesine tıklayın.
- Raporu PDF, RTF ve Excel gibi çeşitli dosya biçimlerine aktarmak için simgesine tıklayın.
- Araç çubuğunun sağındaki numaralar şunları gösterir:
  - Filtre kriterlerine karşılık gelen mevcut veritabanı girişlerinin toplam sayısı.
  - Ön izlemede görüntülenen veritabanı girişlerinin yüzdesi.

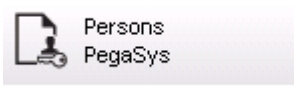
31.1 Raporlar: Ana veriler

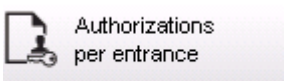
Raporlara genel bakış - Ana Veriler

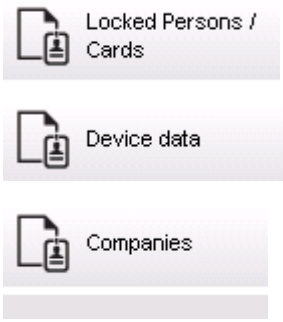
Ana Verilere ilişkin raporlar kişiler, ziyaretçiler ve bunların giriş yetkileriyle ilgili tüm raporları içerir. Ayrıca, cihaz verileri ve şirket verileri de görüntülenebilir.











Rapor: Personel Verileri
Raporlar oluşturulurken iki filtre uygulanabilir.
Kişi filtresi: Burada, her zamanki personel veri alanlarına dayalı operatör filtresi.
Giriş kartı filtresi: Burada, operatör kart numaraları, numara aralıkları, durum ve engelleme durumuna göre filtreleme yapabilir.

Rapor: Ziyaretçiler
Personel verilerine benzer şekilde ziyaretçi raporları burada oluşturulabilir. Bunu yaparken örneğin henüz gelen ancak önceden kayıtlı olan ziyaretçiler seçilebilse bile oluşturulan tüm ziyaretçi verilerine erişilebilir.

Rapor: Personel Giriş Yetkileri
Bu rapor, sistemde kayıtlı giriş yetkilerine ilişkin bir genel bakış sunar ve aynı zamanda bu yetkilerin atandığı kişileri de gösterir.
Filtreler açısından, kişisel veriler ve belirli yetkilerin seçimi kullanılabilir:
- Personel verileri: Soyadı, ad, personel no.
- Tüm yetkilerin doğrulanması.
- Giriş eklendiği yetkinin adı.
- Varsa zaman modelinin adı.
- Girişin yönü.
- Özel yetkinin doğrulanması.

Rapor: Kara Liste
Bu iletişim kutusunda, çeşitli nedenlerle kara listeye alınan tüm veya istenen kimlik kartları seçiminin ayrıntılarını sunan bir liste yazdırılabilir.

Rapor: Engellenen Kişiler/Kartlar
Bu iletişim kutusu tüm engellenen kişilerle ilgili veriler içeren raporlar oluşturmak için kullanılabilir.
Belirtilen zaman aralıklarındaki engellemeleri bulmak için tarihleri kullanın.

Rapor: Cihaz Verileri
İletişim kutusu, cihaz verilerine, örneğin cihaz adına veya cihaz tipine göre raporlar oluşturmak için kullanılabilir.

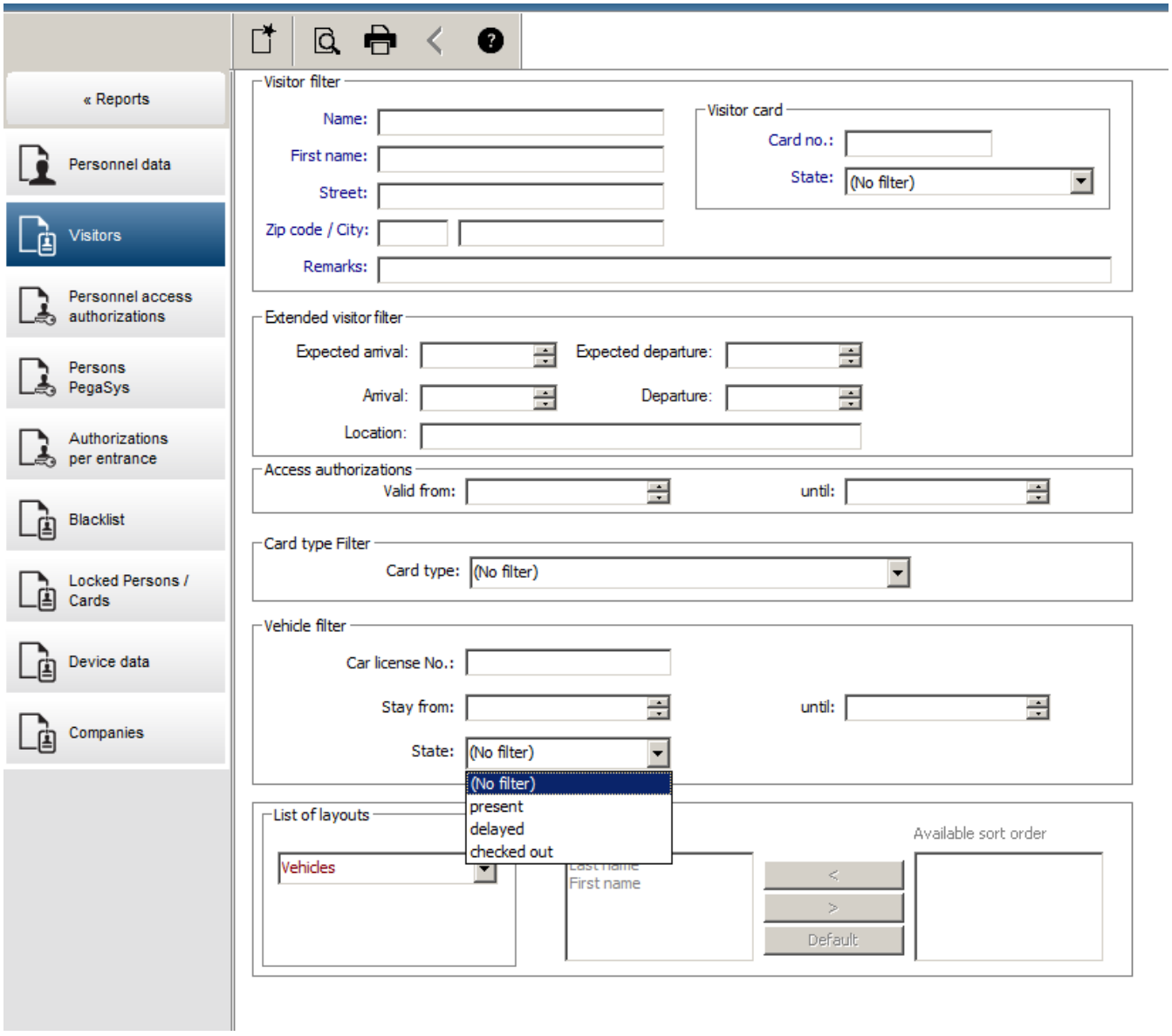
Rapor: Şirketler
Şirketler rapor iletişim kutusu bir listedeki şirket verilerini sıralamak için kullanılır.
Örneğin, belirli bir harfle başlayan şirketleri bulmak için yıldız işareti kullanın.

31.1.1 Taşıtlarla ilgili raporlama

Raporlar > Ziyaretçiler iletişim kutusunda, yerleşim listesinden **Araçlar** seçilebilir. **Araçlar** seçildikten sonra **Araç filtresi** iletişim kutusu alanı etkinleştirilir ve araçlar ile durumlarını filtrelemek için operatör tarafından kullanılabilir.

Durum aşağıdaki gibi görüntülenir:

- Mevcut: Ziyaret henüz bitmemiştir ve zaman henüz dolmamıştır.
- Gecikti: Ziyaret henüz bitmemiştir, ancak zaman dolmuştur,
- Çıkış yapıldı: Ziyaretçi tüm giriş kartlarını iade etmiştir.

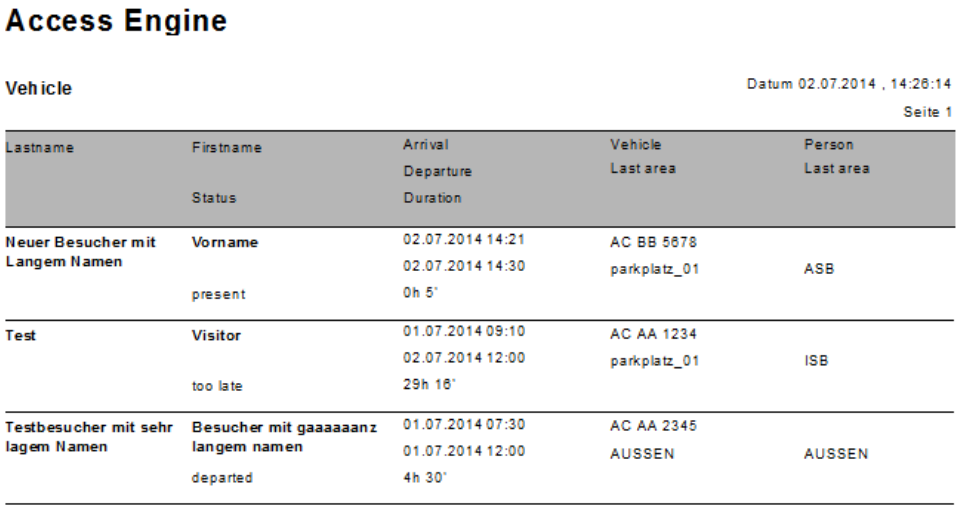


Araç raporu'nu yalnızca ziyaretçiler kullanabilir çünkü beklenen varış tarihi, beklenen ayrılış tarihi, varış tarihi ve ayrılış tarihi yalnızca **Ziyaretçiler** veritabanı tablosundaki ziyaretçiler tarafından kullanılabilir.

Rapor yalnızca **Kişiler** veritabanı tablosunda kayıtlı araç numaralarını gösterir. Böylece bir araç numarası değiştirildikten sonra, rapor diğer sonuçları sağlar.

Süre aşağıdaki gibi hesaplanır:

- Ziyaretçi zaten çıkış yaptıysa dakika olarak varış ve ayrılış arasındaki fark görüntülenir.
- Ziyaretçi henüz çıkış yapmadıysa dakika olarak varıştan şu anda kadar geçen süre görüntülenir



Access Engine

Vehicle

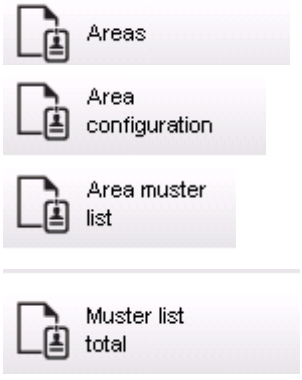
Datum 02.07.2014 , 14:26:14
Seite 1

Lastname	Firstname Status	Arrival Departure Duration	Vehicle Last area	Person Last area
Neuer Besucher mit Langem Namen	**Vorname** present	02.07.2014 14:21 02.07.2014 14:30 0h 5'	AC BB 5678 parkplatz_01	ASB
Test	**Visitor** too late	01.07.2014 09:10 02.07.2014 12:00 29h 16'	AC AA 1234 parkplatz_01	ISB
Testbesucher mit sehr lagem Namen	**Besucher mit gaaaaaanz langem namen** departed	01.07.2014 07:30 01.07.2014 12:00 4h 30'	AC AA 2345 AUSSEN	AUSSEN

31.2 Raporlar: Sistem verileri

Raporlar - Sistem Verileri

Ana verilerin tersine, sistem verileri sisteme atanan bilgilerdir ve kişi, kimlik kartı veya şirketle ilgili değildir. Bu raporlar aşağıda daha ayrıntılı olarak açıklanmaktadır.



Rapor: Alanlar

Bu iletişim kutusu bir rapordaki konumları sıralamak için kullanılabilir. İletişim kutusu yalnızca seçim için farklı binaları ve başka bölgeleri sunan tek bir alan filtresi içerir. İlgili alan sol fare tıklamasıyla seçilir. Kullanıcı **Yazdır** ile yazdırma işlemini başlatmadan önce **Ön İzleme** düğmesini kullanarak raporu ekranda görüntüleyebilir.
Mevcut iki yerleşim vardır.

	Standart	Konumda bulunan kişiler, otopark yok
	Otopark yeri işgali	Konumda bulunan kişiler, yalnızca otoparklar

Görüntülenen veri kümelerinin güncel olduğundan emin olmak için, alanlara ait son kart taramaları da belirtilir.
Bu nedenle çeşitli olaylar için kişilerin konumları hakkında güvenilir bilgiler verilebilir.

Rapor: Alan Yapılandırması

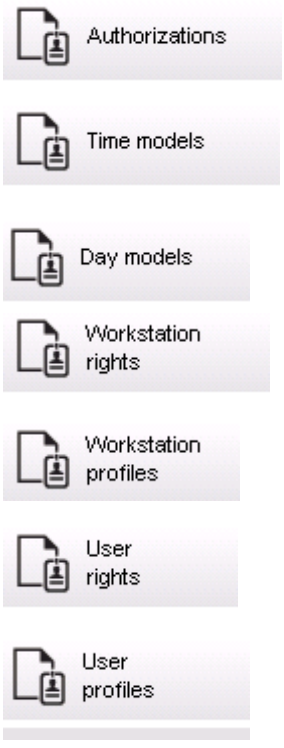
Tanımlanan alanlar ve işaret bulunan alt alanları otoparkları ve maksimum kişi veya araba sayısını gösterir.

Rapor: Alan Toplanma Listesi
Yalnızca sayısal verilere göre belirtilmenin yanı sıra bir alandaki kişiler ada göre de belirtilebilir.
Tek alanlara ilişkin tarama süreleri sayesinde bu raporlar aynı zamanda her tek kişi için de süreleri içerir.

Rapor: Toplanma Listesi Toplamı
İlke olarak, toplanma listeleri **Areas** (Alanlar) rapor iletişim kutusuna karşılık gelir; ancak giriş kontrolüne göre o anda söz konusu alanda bulunan kişi sayısı hakkında bilgi sağlayan belirli bölgelere ait listeler sunar.

31.3 Raporlar: Yetkiler

Genel Bakış
Bu menü öğesinde, ilgili iletişim kutularında belirtilen çeşitli yetkilerden oluşan bir özet sunulur:



Rapor: Yetkiler
Bu iletişim kutusu sistemde tanımlanan giriş yetkilerini görüntülemek için kullanılabilir. Tek giriş yetkilerine ait olan girişler gösterilir. Seçilen zaman modelinin adı görüntülenir. Ayrıca, bu rapor yetkinin atandığı kişi sayısını gösterir.

Rapor: Zaman Modelleri
Bu rapor sistemde seçildiği gibi tanımlanan zaman modellerini görüntülemek için kullanılabilir. Bu rapor modeller ilişkili tüm verilerin yanı sıra modelin uygulandığı kişilerin sayısını görüntüler.

Rapor: Gün Modelleri
Bu rapor tüm gün modellerini adları, açıklamaları ve içerikleri aralıklarla birlikte görüntüler.

Rapor: İş İstasyonu Hakları
Bu iletişim kutusu sistemde tanımlanan iş istasyonlarına atanan iş istasyonu haklarını görüntülemek için kullanılabilir.

Rapor: İş İstasyonu Profilleri
Bu iletişim kutusu sistemde tanımlanan iş istasyonu profillerini görüntülemek için kullanılabilir; bu, tek iş istasyonlarında yapılabilen sistem işlemlerinin net bir biçimde gösterilmesine olanak tanır.

Rapor: Kullanıcı Hakları
Bu iletişim kutusu sistemde tanımlanan kullanıcılar için atanan kullanıcı profillerini görüntülemek için kullanılabilir.

Rapor: Kullanıcı Profilleri
Bu iletişim kutusu sistemde tanımlanan kullanıcı profilleri için atanan iletişim kutularını ve iletişim kutusu haklarını görüntülemek için kullanılabilir.

32 Tehdit Seviyesi Yönetimini Yürütme

Bu bölümde, bir tehdit seviyesini tetikleme ve iptal etmenin çeşitli yolları açıklanmaktadır. Arka plan bilgileri için bkz. *Tehdit Seviyesi Yönetimini Yapılandırma, sayfa 132* bölümü

Giriş

Bir tehdit seviyesi bir tehdit uyarısıyla etkinleştirilir. Tehdit uyarısı aşağıdaki yollardan biriyle tetiklenebilir:

- Yazılım kullanıcı arayüzündeki bir komut ile
- Bir yerel giriş kontrol cihazında, örneğin bir basma düğmesi için tanımlanan giriş sinyaliyle.
- Bir okuyucudan uyarı kartını geçirerek

Tehdit uyarılarının kullanıcı arayüzü komutu veya donanım sinyaliyle iptal edilebileceğini, ancak uyarı kartıyla iptal edilemeyeceğini unutmayın.

Bkz.

- *Tehdit Seviyesi Yönetimini Yapılandırma, sayfa 132*

32.1 Bir tehdit uyarısını kullanıcı arayüzü komutu aracılığıyla tetikleme ve iptal etme

Bu bölümde, bir tehdit uyarısının bir AMS Map View'da (AMS Harita Görünümü) nasıl tetikleneceği açıklanmaktadır.

İletişim yolu

- AMS Map View (AMS Harita Görünümü) >  (Cihaz ağacı)

Ön koşullar

- En az bir tehdit seviyesi tanımlanmış olmalıdır
- Cihaz düzenleyicisinde en az bir tehdit seviyesi Etkin olarak işaretlenmiş olmalıdır.
- Harita Görünümü ve AMS operatörü olarak şu gerekli izinleriniz olmalıdır:
  - Tehdit seviyelerini devreye alma
  - Tehdit uyarısının tetiklenmesi gerektiği durumlarda Bölümdeki MAC veya MAC'leri görüntüleme.

Bir tehdit uyarısı tetikleme prosedürü

1. AMS Map View'daki (AMS Harita Görünümü) cihaz ağacında tehdit uyarısının tetiklendiği MAC cihazına sağ tıklayın.
   - Bu MAC'te yürütmeye yetkiniz bulunan komutları içeren bir bağlam menüsü görünür
   - Henüz hiçbir tehdit seviyesi devrede değilse menü, **Activate Threat level** "`<name>`" (Tehdit seviyesini etkinleştir) etiketli bir veya daha fazla öğeyi içerir. Burada, tehdit seviyesinin adı cihaz düzenleyicide tanımlanır.
2. Tetiklemek istediğiniz tehdit seviyesini seçin.
   - Tehdit seviyesi devreye girer.

Bir tehdit uyarısını iptal etme prosedürü

Ön koşul: Zaten bir tehdit seviyesi devrede olmalıdır.

1. AMS Map View'daki (AMS Harita Görünümü) cihaz ağacında tehdit uyarısının iptal edildiği MAC cihazına sağ tıklayın.
   - Bu MAC'te yürütmeye yetkiniz bulunan komutları içeren bir bağlam menüsü görünür

2. Bağlam menüsünden **Deactivate Threat level**'ı (Tehdit seviyesini devre dışı bırak) seçin.
   – O anda geçerli tehdit seviyesi devre dışı bırakılır.

32.2 Bir tehdit uyarısını donanım sinyali aracılığıyla tetikleme

Bu bölümde, bir tehdit uyarısı tetiklemek için donanım giriş sinyalinin nasıl gönderileceği açıklanmaktadır.

Ön koşullar
– En az bir tehdit seviyesi tanımlanmış olmalıdır
– Cihaz ağacında en az bir giriş yapılandırılmış olmalıdır.
– Bir AMC'de donanım sinyalleri tanımlanmış ve bir cihaz ona sinyal gönderecek olan AMC'deki doğru terminale bağlanmış olmalıdır. Gerekirse giriş sinyalini yapılandırmayla ilgili talimatlar için bu bölümün sonundaki bağlantıya tıklayın veya sistem yöneticinizle iletişime geçin.

Prosedür
Cihazı devreye alın, bu cihaz genellik AMC'ye bağlı olan basmalı düğmesi veya donanım anahtarıdır.
Tehdit uyarısını iptal etmek için, **Threat level: Deactivate** (Tehdit seviyesi: Devre dışı bırak) olarak tanımlanan giriş sinyalini gönderen cihazı devreye alın.

Bkz.
– *Bir donanım sinyaline tehdit seviyesi atama, sayfa 136*

32.3 Bir tehdit uyarısını uyarı kartı aracılığıyla tetikleme

Bu bölümde, bir tehdit uyarısının bir uyarı kartı aracılığıyla nasıl tetikleneceği açıklanmaktadır.

Ön koşullar
– En az bir tehdit seviyesi tanımlanmış olmalıdır
– Cihaz ağacında en az bir giriş yapılandırılmış olmalıdır.
– Belirli bir kart sahibi için bir uyarı kartı oluşturulmuş olmalıdır. Gerekirse uyarı kartı oluşturmayla ilgili talimatlar için bu bölümün sonundaki bağlantıya tıklayın veya sistem yöneticinizle iletişime geçin.

Prosedür
1. Kart sahibi, kendi özel uyarı kartını binadaki herhangi bir **parmak izi dışı** okuyucuya gösterir.
   – Söz konusu kart için tanımlanan tehdit seviyesi etkinleştirilir.
2. Tehdit geçtiğinde, tehdit seviyesini kullanıcı arayüzü komutu veya donanım anahtarı aracılığıyla iptal edin. Tasarımsal olarak, bir tehdit seviyesini bir uyarı kartı aracılığıyla iptal etmek mümkün değildir.

Bkz.
– *Uyarı kartı oluşturma, sayfa 201*

33 Kart geçirme ekranını çalıştırma

Giriş

Kart geçirme ekranı, Harita görünümü operatörlerinin, tesise girenleri veya tesisten ayrılanları gerçek zamanlı olarak izlemelerine yardımcı olan bir araçtır.

Genel bilgiler

Kart geçirme ekranı AMS Map View'ın içinde giriş olaylarının son 10 dakikasını dinamik bir kaydırma listesinde görüntüleyen bir uygulamadır. En fazla 50 giriş olayı görüntülenir ve 10 dakikadan eski olan olaylar otomatik olarak listeden çıkarılır. Operatör, sistemdeki tüm okuyucuları izleyebilir veya bir alt küme seçebilir.

Listedeki her kayıt, olay ayrıntılarını ve kullanılan kimlik bilgisini içerir, örneğin:

- Gözle kimlik onayı için kart sahibinin adı ve saklanan fotoğrafı.
- Bir zaman damgası.
- Saklanmışsa şirket ve/veya departman adı.
- Kimlik bilgisinin kullanıldığı giriş ve okuyucu
- Renkli etikete sahip bir olay kategorisi:
  - Yeşil: Geçerli bir kimlik bilgisiyle tamamlanmış bir giriş
  - Sarı: Örneğin kart sahibinin kilidi çevirip kapıyı açamaması gibi geçerli bir kimlik bilgisiyle yapılmış tamamlanmamış bir giriş
  - Kırmızı: Geçersiz bir kimlik bilgisiyle bir gerçekleştirilemeyen bir giriş denemesi. Örneğin kimlik bilgisinin kara listeye alınması, bilinmemesi veya süresinin dolması gibi geçerlilik türü gösterilir

Kart geçirme ekranı kendi arşivlerini tutmaz, sistem veritabanındaki giriş olaylarını ayıklar ve görüntüler. Dinamik kaydırma daha yakın çalışma için duraklatılabilir veya diğer Harita görünümü uygulamalarıyla paralel kullanım için ayrı bir pencerede açılabilir.

Uyarı!

Düzenlemelerden sonraki gecikme

AMS'deki kimlik fotoğraflarında ve kart sahibinin diğer verilerinde yapılan değişikliklerin kart geçirme ekranına yansıması için birkaç dakika gerekir. Senkronizasyon gerçekleşene kadar, Kart geçirme ekranı eski verilerle gerçek zamanlı olarak tepki vermeye devam eder.

Ön koşullar

Operatörün kullanıcı profili için kart geçirme ekranını çalıştırmak üzere özel bir yetki gerektirir.

1. Ana AMS uygulamasında şu menüye gidin: **Configuration** (Yapılandırma) > **User profiles** (Kullanıcı profilleri)
2. İstediğiniz operatörün profil adını yükleyin
3. Tablodan **Access Manager Maps** (Kartlı Geçiş Yöneticisi Haritaları) > **Special functions** (Özel işlevler) > Swipe ticker**'ı (Kart geçirme ekranı) seçin**

Kart geçirme ekranını başlatma

- Harita görünümü'nde aracı başlatmak için  simgesine tıklayın.

İzlenecek okuyucuları seçme

Okuyucular daha önce seçilmemişse veya seçimi değiştirmek istiyorsanız şu adımları izleyin:

1. Kart geçirme ekranı penceresinde  (ayarlar) simgesine tıklayın.
   Filter devices (Cihazları filtrele) penceresi açılır.
2. Cihaz ağacından, izlemek istediğiniz girişlerin veya okuyucuların onay kutularını seçin.
   Onay kutuları şu şekilde davranır:
   Bir giriş seçerseniz tüm alt cihazları varsayılan olarak seçilir.
   Tek alt cihazların onay kutuları gerekli değilse temizlenebilir.
   Bir ana cihazın **tüm** alt öğeleri seçildiyse ana cihazın onay kutusu beyaz renktedir.
   Yalnızca **bazıları** seçilmişse ana cihazın onay kutusu gri olur.
3. Okuyucuları seçmeyi tamamlamak için **OK**'e (Tamam) tıklayın ve **Filter devices** (Cihazları filtrele) penceresini kapatın.

Seçilen okuyucuları haritada görüntüleme

- Kart geçirme ekranındaki bir kayda çift tıklayın.

⇨ Kart geçirme ekranı otomatik olarak duraklatılır.

⇨ Harita görünümü, ana pencerede, kendi harita hiyerarşisinde bulunan ilk ilgili harita sahnesini görüntüler ve çift tıkladığınız okuyucuyu vurgular.

Kart geçirme ekranını duraklatma

- Kart geçirme ekranı penceresinde  simgesine tıklayın veya dinamik ekranı duraklatmak için listedeki bir kayda çift tıklayın

⇨ Dinamik ekran donar. Gelen olay kayıtları ara belleğe alınır ancak görüntülenmez.

⇨ Listenin en üstüne, olay akışının duraklatıldığını belirten bir bildirim eklenir.

Duraklatılmış bir kart geçirme ekranını devam ettirme

- Kart geçirme ekranı penceresinde, dinamik ekranı sürdürmek için  simgesine tıklayın

⇨ Dinamik listede, seçilen okuyucularda son 10 dakika içinde gerçekleşen tüm giriş olayları en fazla 50 adede kadar olmak üzere kronolojik sırada (önce en yeni) görüntülenir.

⇨ 50 en yeni olaydan veya 10 dakikadan daha eski giriş olayları listeden kaldırılır.

⇨ Yeni giriş olayları meydana geldikleri sırada yeniden gerçek zamanlı olarak görüntülenir.

Kart geçirme ekranını ayrı bir pencerede çoğaltma

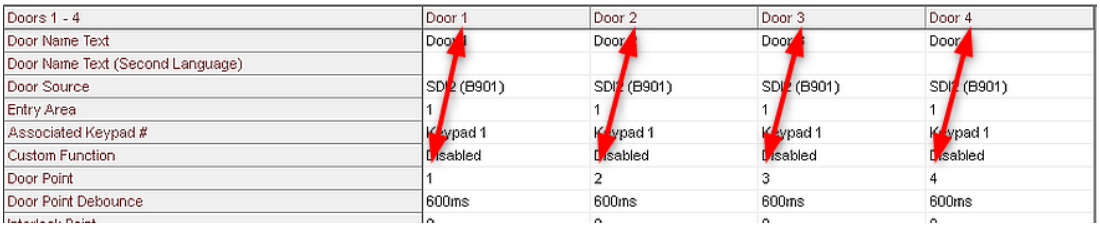
Bir seferde yalnızca bir adet yinelenen ekran penceresi açılabileceğini unutmayın.

1. Kart geçirme ekranı penceresinde  (ek pencere) simgesine tıklayın.
   Ayrı pencere yinelenen bir penceredir ve ana penceredeki ekrandan bağımsız **değildir**.
   Aynı ayarlara uyar.
   Alarm listesi gibi diğer Harita görünümü uygulamaları artık ana pencerede çalıştırılabilir.
2. Ayrı pencerede tamamladığınızda, kapatmak için başlık çubuğunu kullanın.

33.1 Özel durumlar

Map View Kart geçirme ekranı ve B901 kapıları

AMS Map View'da **Kart geçirme akranı** uygulaması için doğru bilgileri sağlamak amacıyla B901 kapılarının kimlik bilgileri kapı noktalarının kimlik bilgileriyle eşleşmelidir. Yani 1 numaralı Kapı 1 numaralı Kapı Noktası'na, 2 numaralı Kapı 2 numaralı Kapı Noktasına atanmalıdır.



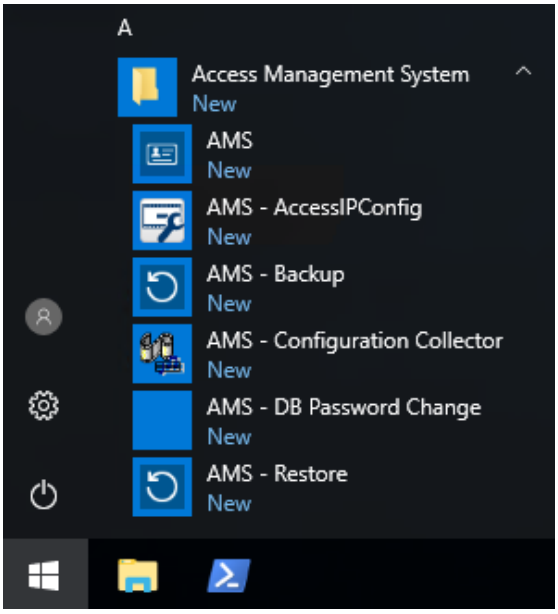
Doors 1 - 4	Door 1	Door 2	Door 3	Door 4
Door Name Text	Door 1	Door 2	Door 3	Door 4
Door Name Text (Second Language)				
Door Source	SDI2 (B901)	SDI2 (B901)	SDI2 (B901)	SDI2 (B901)
Entry Area	1	1	1	1
Associated Keypad #	Keypad 1	Keypad 1	Keypad 1	Keypad 1
Custom Function	Disabled	Disabled	Disabled	Disabled
Door Point	1	2	3	4
Door Point Debounce	600ms	600ms	600ms	600ms

B901 kapı kontrol cihazına bu atamaları, hırsız alarm panellerini ve kontrol cihazlarını yapılandıran RPS aracında yapın.

34 Yedekleme ve Geri Yükleme

Backup & Restore (Yedekleme ve Geri Yükleme) işlevi sisteminizi verileriyle birlikte yeni bir AMS sürümüne veya yeni bir bilgisayara taşımanıza imkan verir.
Backup and Restore (Yedekleme ve Yeniden Yükleme) sadece AMS sunucusunun kurulu olduğu makinede çalıştırılabilir. Windows Başlat menüsünde iki kısayol bulunur:

- Yedek oluşturmak için **AMS - Backup** (AMS-Yedekleme)
- Yedeği geri yüklemek için **AMS - Restore** (AMS-Geri Yükleme):

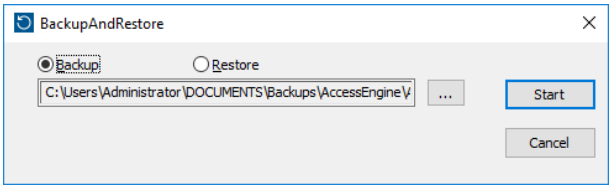


34.1 Sistemi yedekleme

Bu bölümde, AMS uygulamasına ait bir yedeğin nasıl oluşturulacağı ve SQL Server yedekleme dosyalarının nasıl bulunacağı açıklanmaktadır.

AMS uygulamasının yedeğini oluşturma

1. Windows Başlat menüsünde, **AMS-Backup**'a (AMS Yedekleme) sağ tıklayın ve **Run as administrator**'ı (Yönetici olarak çalıştır) seçin.
   - **Backup and Restore** (Yedekleme ve Geri Yükleme) aracı önceden seçilen **Backup** (Yedekleme) seçeneği ile başlatılır.



2. `.GZ` dosyasının kaydedileceği yolu girin.
3. Yedeklemeyi başlatmak için **Start**'a (Başlat) tıklayın.
   - **Backup and Restore** (Yedekleme ve Geri Yükleme) aracı tek bir `.GZ` dosyası oluşturur ve ilerlemesini bir açılır pencerede görüntüler.
4. Bu dosyayı başka bir bilgisayardaki güvenli depolama alanına kopyalayın. Veri güvenliği için DMS sunucusundaki tek kopyayı **bırakmayın**.

SQL Server yedekleme dosyalarını bulma ve kopyalama.

1. AMS sunucu bilgisayarındaki dosya gezginini kullanarak SQL Server'ın `.BAK` dosyalarının tutulduğu konuma gidin.

- Dosya yolu şu şekildedir (burada `<version>` ve `<instance name>` sisteminize bağlı değişkenlerdir):
  `C:\Program files\Microsoft SQL Server\MSSQL<version>.<instance name>\MSSQL\Backup\`
- Dosya adları şu biçimdedir:
  `acedb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak`
  `Bosch.AlarmDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak`
  `Bosch.EventDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak`
  `Bosch.MapDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak`
  `Bosch.MapViewDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak`
  `Bosch.StatesDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak`

2. **Tüm** `.BAK` dosyalarını başka bir bilgisayardaki güvenli depolama alanına kopyalayın. Veri güvenliği için DMS sunucusundaki tek kopyaları **bırakmayın**.

Uyarı!
AMS Olay günlüğünün varsayılan yolu:
`C:\Program Files (x86)\Access Management System\Access Engine\AC\LgfLog\`

34.2 Bir yedeği geri yükleme

Ön koşullar

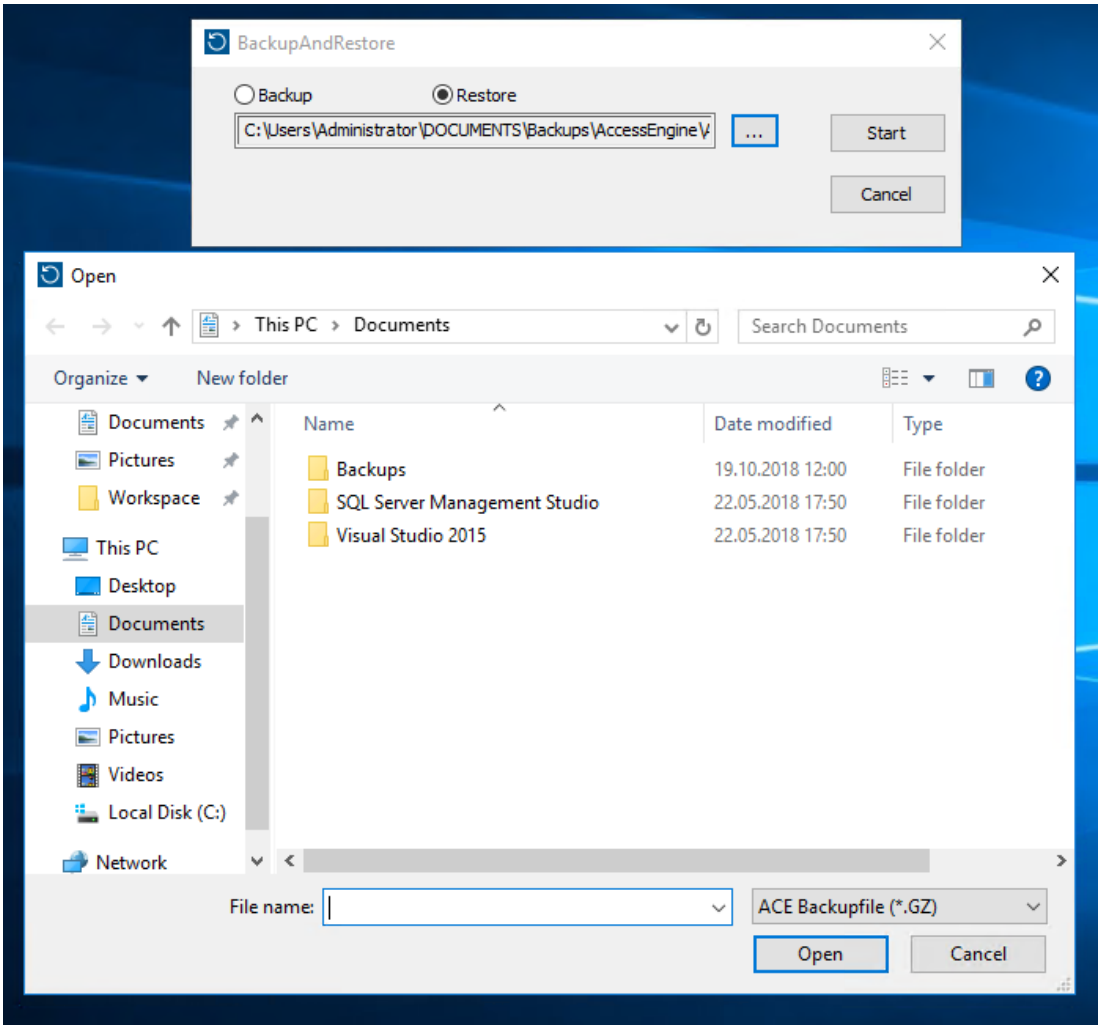
- **Backup and Restore** (Yedekleme ve Geri Yükleme) aracı tarafından oluşturulan `GZ` dosyası
- Yedekleme prosedürü sırasında kullandığınız SQL Server'ın oluşturduğu `.BAK` dosyaları.
- `sa` gibi **sysadmin** haklarına sahip bir SQL hesabı.
- **Lisanslara** ve **sertifikalara**göre hazırlanmış uygun bir hedef bilgisayar:
  - **Licenses** (Lisanslar): Hedef bilgisayar (yedeği geri yüklediğiniz yer) için en azından yedeklemeyi yaptığınız bilgisayardaki eş değer lisanslar gereklidir.
  - **Certificates** (Sertifikalar): Hedef bilgisayarın herhangi bir istemcisi için ilk bilgisayarda kurulumla oluşturulanlar değil, hedef bilgisayarda kurulumla oluşturulan yeni sertifikalar gereklidir.
    İstemci sertifikalarının oluşturulması ve kurulması için **AMS Kurulum Kılavuzu**'na başvurun.

Prosedür

1. AMS programında, AMS uygulamasını durdurmak için **File** (Dosya) > **Exit**'e (Çıkış) tıklayın.
2. Program sonlandırıldığında, Windows **Hizmetleri** uygulamasını çalıştırın ve tüm `Access Engine` ve `Access Management System` hizmetlerinin durdurulduğundan emin olun. Aksi takdirde bu hizmetleri burada durdurun.
3. **Yalnızca eğer**bir RMAC (yedek yük devri MAC'i) ana veya 1. MAC ile kullanıyorsanız sonraki alt bölüme geçin ve bu adıma dönmeden önce orada açıklanan prosedürü gerçekleştirin.
4. Orijinal bilgisayardan kaydettiğiniz MSSQL `.BAK` dosyalarını yeni bilgisayarda tam olarak aynı konuma kopyalayın.

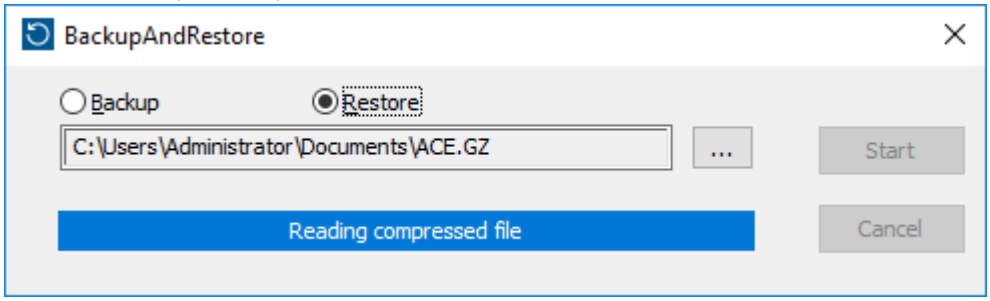
- Dosya yolu şu şekildedir (burada `<version>` ve `<instance name>` sisteminize bağlı değişkenlerdir):
  `C:\Program files\Microsoft SQL Server\MSSQL<version>.<instance name>\MSSQL\Backup\`

5. Windows Başlat menüsünde, **AMS-Restore**'a (AMS Geri Yükleme) sağ tıklayın ve **Run as administrator**'ı (Yönetici olarak çalıştır) seçin.
   - **Backup and Restore** (Yedekleme ve Geri Yükleme) aracı önceden seçilen **Restore** (Geri Yükleme) seçeneği ile başlatılır.
6. **[...]** düğmesine tıklayarak dosya sistemindeki `GZ` yedekleme dosyasını bulun ve bu dosyayı seçmek için **Open**'a (Aç) tıklayın.



7. Geri yükleme işlemini başlatmak için **Start**'a (Başlat) tıklayın.
8. Sunucu kimlik bilgileri istendiğinde, sunucu bilgisayarın oturum açma kimlik bilgilerini değil, `sa` gibi bir MSSQL sysadmin kullanıcısının kimlik bilgilerini girin.

– Geri yükleme işlemi başlar



9. Geri yükleme işlemi tamamlandığında Windows **Hizmetleri** uygulamasını çalıştırın ve tüm `Access Engine` ve `Access Management System` hizmetlerini manuel olarak yeniden başlatın.
10. Yedeklenen verileri geçerli sistem verileriyle yeniden eşitlemek için `AMS Server Setup.exe` sunucu kurulum programını Yönetici olarak yürütün.

Bkz.
– *Sistemi yedekleme, sayfa 241*

34.2.1 RMAC'leri yeni bir kuruluma geri yükleme

Not: Bu prosedür yalnızca MAC'ler ve RMAC'lere sahip bir sistemin yedeğini farklı bir donanıma geri yüklediğiniz durumda geçerlidir.

Giriş

Bir yedeği yeni bilgisayarlara geri yüklerseniz yedekleme dosyasında depolanan MAC ve RMAC'in IP adreslerini yeni donanımın IP adresleri olarak yeniden yapılandırmanız gerekir. Bu yapılandırmayı yeni donanımda MACInstaller aracını çalıştırarak yapın.
MACInstaller aracı kurulum ortamında `\AddOns\MultiMAC\MACInstaller.exe` dizininde bulunur
MACInstaller aracının kullanımı *MAC kurucu aracını kullanma, sayfa 51* bölümünde ayrıntılı olarak açıklanmaktadır.

Prosedür

1. MACInstaller aracını 1.MAC'in çalıştığı bilgisayarda çalıştırın. Bu bilgisayar DMS sunucusu veya 1.MAC'e özel bir sunucu olabilir.
   – Araçta, birincil MAC (bu bilgisayar) ve RMAC'in yeni IP adreslerini belirleyin.
2. MACInstaller aracını RMAC'in çalıştığı bilgisayarda çalıştırın.
   – Araçta, birincil MAC ve RMAC'in (bu bilgisayar) yeni IP adreslerini belirleyin.
3. **Restore procedure** (Geri yükleme prosedürü) prosedüründe kaldığınız adıma dönün.

Bkz.
– *MAC kurucu aracını kullanma, sayfa 51*

Sözlük

1. MAC (birinci MAC)

Bir BIS Access Engine (ACE) veya Access Manager (AMS) sistemindeki birincil MAC (Ana Giriş Kontrol Cihazı). DMS ile aynı bilgisayarda bulunabilir, ancak aynı zamanda bir MAC sunucusu olarak bilinen ayrı bir bilgisayarda bir yardımcı MAC gibi de bulunabilir.

Access Sequence Monitoring (Giriş Sırası İzleme)

Bir kişinin ve aracın bir tanımlı Alandan başka birine kadar kimlik kartının her taraması kaydedilerek ve kartın daha önce tarandığı Alanlardan giriş izni verilerek izlenmesi.

ACS

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

aktarma

özel olarak tanımlanan koşulda bir alarmı askıya almak için.

Alan (Kurma)

Bir kartlı geçiş sisteminde giriş modeli 14'ün giriş gruplandırması. Bu girişlerin birindeki hırsız alarm sistemini aynı anda kurma veya devre dışı bırakma, Arming area (Kurma alanı) parametresinin aynı tek harfli işarete sahip olduğu tüm girişlerde aynı etkiye sahiptir.

AMC donanım anahtarı

AMC'nin belirli donanım parametrelerinden oluşturduğu dahili kimlik doğrulama kodu. Kullanıcıya gösterilmez.

Ana anahtar

Sistemin DCP'den (Cihaz İletişim Şifresi) ürettiği ve karlı geçiş cihazlarını korumak için kullandığı kod. Ana anahtar hiçbir zaman herhangi bir kullanıcıya görünmez.

anti-passback

Bu arada kart söz konusu Alandan çıkmak için taranmadıkça bir kart sahibinin belirli bir süre içinde bir alana girmesinin iki kez engellendiği basit bir Giriş Sırası İzleme biçimi. Anti-passback bir kişinin kimlik bilgilerini izinsiz bir ikinci kişi tarafından kullanılmak üzere bir girişten geri almasını engeller.

asansör grubu

Uyumlu bir şekilde aynı katlara hizmet veren bir asansör grubu. Her asansör grubu bir Hedef Giriş Sunucusu (DES) ile yönetilir.

Beyaz liste (SmartIntego)

Beyaz liste, bir SmartIntego kilitleme sisteminin kart okuyucularında yerel olarak saklanan kart numaralarının listesidir. Okuyucunun MAC'i çevrimdışıysa okuyucu numaraları kendi yerel beyaz listesinde bulunan kartlara giriş izni verir.

CSN

Kart Seçim Numarası.

Çalışma modu

Bir kartlı geçiş cihazının Cihaz Düzenleyicisi'nin dışında verilen komutlara yanıt verirken Cihaz Düzenleyicisi'ndeki durumu. Yapılandırma değişiklikleri yalnızca işlem modu sona erdikten ve yapılandırma modu geri yüklendikten sonra yürürlüğe girer.

DCP

Kartlı geçiş sisteminin, genellikle AMC cihazları olan tüm alt yerel giriş kontrol cihazlarıyla ağ iletişimini şifrelemek için kullanılan bir ana anahtar oluşturduğu şifredir.

Doğrulama PIN'i

Daha yüksek güvenlik uygulamak için fiziksel bir kimlik bilgisiyle birlikte kullanılan bir Kişisel Tanıma Numarası (PIN).

DSN

Veri Kaynağı adı. Veri kaynağının Açık Veritabanı Bağlantısı'ndaki (ODBC) adı.

DTLS

Veri Birimi Taşıma Katmanı Güvenliği gizlice dinleme ve dış müdahaleye karşı koruma sağlayan güvenli bir iletişim protokolüdür.

Giriş

Giriş terimi bütünüyle bir giriş noktasındaki giriş kontrol mekanizmasını belirtir: Okuyucular, bir çeşit kilitlenebilir bariyer ve donanım elemanları arasından geçirilen elektronik sinyal dizileri ile tanımlanan bir giriş prosedürünü kapsar.

Hedef Giriş Sunucusu (DES)

Seyahat sürelerini optimize etmek için bir asansör grubunu yöneten bilgisayardır.

Hedef Giriş Terminali (DET)

Asansör yolcularının bir asansör grubu için hedef istekleri girebilecekleri cihaz.

Hedef Girişi Yeniden Yönlendiricisi (DER)

Bir Otis CompassPlus sistemindeki bir Hedef Giriş Sunucusu (DES) ile aynı seviyede bulunan bir bilgisayar. Tüm asansör gruplarına bağlanır ve işi, DES cihazlarının verimliliğini artırmaktır.

Hedef Gönderme Sistemi (DDS)

Hedef Yönetim Sistemi olarak da bilinir, ancak yalnızca DDS kısaltması kullanılır. Otis CompassPlus, bir tür DDS'dir.

IDS

Hırsız alarm sistemi olarak da bilinen hırsız algılama sistemi.

IPConfig aracı

Kartlı geçiş sistemi içindeki donanım cihazlarının ağ ve ağ güvenlik ayarlarını yapılandırmak için kullanılan ayrı bir yardımcı program.

Kapı modeli

Belirli bir giriş tipinde saklanan bir yazılım şablonu. Kapı modelleri, giriş kontrol sistemlerinde girişlerin tanımını kolaylaştırır.

MAC (Ana Giriş Kontrol Cihazı)

Kartlı geçiş sistemlerinde, genellikle AMC'ler (Access Modular Controllers) olan yerel giriş kontrol cihazlarını koordine eden ve kontrol eden bir sunucu programı.

MAC sunucusu

Donanım: Bir MAC veya RMAC'nin çalıştığı bir Access Engine (ACE) veya Access Management System'daki (AMS) bir bilgisayar (DMS sunucusu dışında).

Montaj noktası

İnsanların bir binayı tahliye ettikten sonra beklemeleri gereken yer.

Nokta

Hırsızlık denetimli bir alanda yapılan hırsızlığı tespit etmek için bir sensör. Bazı bağlamlarda noktalar, bölgeler veya sensörler olarak adlandırılmış olabilir.

Normal mod

Ofis modunun aksine, normal mod yalnızca okuyucuda geçerli kimlik bilgileri sunan kişilere giriş izni verir.

Ofis modu

Ofis veya çalışma saatleri sırasında bir girişteki giriş kontrolünün askıya alınması.

Rastgele LCD anahtarı

AMC'nin her yeniden başlatıldığında yeniden oluşturduğu geçici alfa sayısal kod. Anahtar AMC'nin sıvı kristal ekranında (LCD) görüntülenebilir ve ağ iletişiminin kimliğini doğrulamak için yazılım araçları tarafından istenebilir.

REX

"Çıkış talebi". Kapıdan çıkış yapılmasına izin vermek için bir kapının içeriden kilidinin açılmasını talep eden sinyal. Sinyal tipik olarak girişin iç kısmında bulunan bir basma düğmesi veya çubuk tarafından, bazen de bir hareket dedektörü tarafından tetiklenir.

RMAC

Mevcut bir MAC'nin eş zamanlı bir ikizi olan ve ilk MAC hata verirse veya bağlantısı kesilirse verilerin yönetimini devralan yedek bir ana giriş kontrol cihazı (MAC).

RPS

Uzaktan Programlama Yazılımı. Bir ağdaki yangın veya hırsız alarmı kontrol panellerini yöneten program.

SmartIntego

Simons Voss Technologies'in ürettiği bir dijital kilitleme sistemi. SmartIntego, bazı Bosch giriş kontrol sistemlerine entegre edilir.

şifre entropisi

Rastgeleliği, kullanılabilir simge sayısı ve kullanılan gerçek simge sayısı gibi faktörlerden hesaplanan şifre gücü ölçüsü.

takip

Birisinin kendi kimlik bilgilerini göstermeden bir giriş aracılığıyla yetkili bir kart sahibini yakından izleyerek giriş kontrolünden kurtulma.

Tanıma PIN'i

Giriş için gerekli tek kimlik bilgisi olan bir Kişisel Tanıma Numarası (PIN).

Tehdit uyarısı

Tehdit seviyesini tetikleyen bir alarm. Uygun yetkiye sahip kişiler ani bir eylemle, örneğin operatör kullanıcı arayüzü, donanım sinyali (ör.

basmalı düğme) ile veya herhangi bir okuyucuya özel bir alarm kartı göstererek bir tehdit uyarısı tetikleyebilir.

Veri Yönetim Sistemi (DMS)

Sistemde kartlı geçiş verilerini yönetmek için en üst düzey bir süreç. DMS, verileri ana kartlı geçiş cihazlarına (MAC) gönderir. MAC ise daha sonra bu verileri yedek kartlı geçiş cihazlarına (genellikle AMC) gönderir.

Yapılandırma modu

Cihaz Düzenleyicisi'ndeki kartlı geçiş cihazlarının varsayılan durumu. Değişiklikler yürürlüğe girer ve alt cihazlara hemen yayılmaz.

Yerel Giriş Kontrol Cihazı (LAC)

Okuyucular ve kilitler gibi çevre kartlı geçiş donanımlarına giriş komutları gönderen ve genel kartlı geçiş sistemi için bu donanımdan gelen istekleri işleyen bir donanım cihazı. En yaygın kullanılan LAC, bir Access Modular Controller veya AMC'dir.

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

Building solutions for a better life.

202309211041