



BOSCH

Access Management System

AMS configuration and operation

tr

Yazılım Kullanım Kılavuzu

İçindekiler

1	Yardım'ı Kullanma	6
2	Bu belge hakkında	8
3	AMS Sistemine genel bakış	9
4	Sistemi lisanslama	10
5	Takvimi yapılandırma	11
5.1	Özel günleri tanımlama	11
5.2	Gün modellerini tanımlama	13
5.3	Zaman modellerini tanımlama	14
6	Bölmeleri Yapılandırma	17
6.1	Bölmeleri cihazlara atama	17
6.2	Bölmeleri operatörlere atama	18
7	IP adreslerini yapılandırma	19
8	Cihaz düzenleyiciyi kullanma	20
9	Kartlı geçiş alanlarını yapılandırma	22
9.1	Araçlara ait alanları yapılandırma	23
10	Operatörleri ve iş istasyonlarını yapılandırma	26
10.1	İş istasyonlarını oluşturma	26
10.2	İş istasyonu profilleri oluşturma	27
10.3	İş istasyonu profillerini atama	28
10.4	Kullanıcı (operatör) profilleri oluşturma	28
10.5	Kullanıcı (operatör) profillerini atama	29
10.6	Operatörler için şifre belirleme	30
11	Kart kodlarını yapılandırma	32
12	Kontrol cihazlarını yapılandırma	35
12.1	MAC'leri ve RMAC'leri Yapılandırma	35
12.1.1	DMS sunucusundaki bir MAC'i yapılandırma	35
12.1.2	MAC sunucu bilgisayarlarını MAC'leri ve RMAC'leri çalıştırmak için hazırlama	36
12.1.3	Bir MAC'i kendi MAC sunucusunda yapılandırma	37
12.1.4	MAC'lere RMAC ekleme	38
12.1.5	Daha fazla MAC/RMAC çifti ekleme	40
12.1.6	MAC kurucu aracını kullanma	41
12.2	LAC'leri Yapılandırma	42
12.2.1	AMC parametreleri ve ayarları	44
13	Girişleri Yapılandırma	61
13.1	Girişler - giriş	61
13.2	Giriş oluşturma	62
13.3	Ek G/Ç kontrolleri	65
13.4	AMC terminallerini yapılandırma	66
13.5	Kapı modelleri için önceden tanımlanan sinyaller	71
13.6	Özel girişler	76
13.6.1	Asansörler (DM07)	76
13.6.2	Hırsız alarmlı kapı modelleri (DM14)	79
13.6.3	DIP'ler ve DOP'lar (DM15)	82
13.6.4	Tuzak kapı modelleri	83
13.7	Kapılar	85
13.8	Readers (Okuyucular)	88
13.8.1	Rastgele taramayı yapılandırma	98
13.9	Yalnızca PIN'le giriş	98






13.10	AMC genişletme kartları	100
14	Personel verileri için Özel Alanlar	104
14.1	Özel alanlara ön izleme yapma ve bunları düzenleme	104
14.2	Veri alanlarına ilişkin kurallar	106
15	Milestone XProtect'i AMS'yi kullanacak şekilde yapılandırma	108
16	Tehdit Seviyesi Yönetimini Yapılandırma	110
16.1	Tehdit Seviyesi Yönetimine İlişkin Kavramlar	110
16.2	Yapılandırma işlemine genel bakış	110
16.3	Cihaz düzenleyicideki yapılandırma adımları	111
16.3.1	Tehdit seviyesi oluşturma	111
16.3.2	Kapı güvenlik profili oluşturma	111
16.3.3	Okuyucu güvenlik profili oluşturma	112
16.3.4	Kapı ve okuyucu güvenlik profillerini girişlere atama	113
16.3.5	Bir donanım sinyaline tehdit seviyesi atama	114
16.4	Sistem verileri iletişim kutularındaki yapılandırma adımları	115
16.4.1	Kişi güvenlik profili oluşturma	115
16.4.2	Kişi türüne kişi güvenlik profili atama	116
16.5	Personel verileri iletişim kutularındaki yapılandırma adımları	116
17	Personel verilerini oluşturma ve yönetme	117
17.1	Kişiler	117
17.1.1	Kart kontrolü/bina kontrolü seçenekleri	119
17.1.2	Fazladan bilgi: Kullanıcı tanımlı bilgileri kaydetme	119
17.1.3	İmzaları kaydetme	119
17.1.4	Parmak izi verilerini kaydetme	120
17.2	Şirketler	122
17.3	Kartlar: Kimlik bilgileri ile izin oluşturma ve atama	122
17.3.1	Kişilere kart atama	123
17.3.2	Authorizations (Yetkiler) sekmesi	124
17.3.3	Diğer veri sekmesi: Muafiyetler ve özel izinler	125
17.3.4	Kişilere Ofis modunu ayarlama yetkisi verme	125
17.3.5	Smartintego sekmesi	126
17.3.6	Uyarı kartı oluşturma	128
17.4	Geçici kartlar	128
17.5	Personel için PIN kodları	130
17.6	Personel için girişi engelleme	131
17.7	Kartları kara listeye alma	133
17.8	Aynı anda birden fazla kişiyi düzenleme	134
18	Giriş yetkilerini ve profillerini tanımlama	137
18.1	Giriş yetkileri oluşturma	137
18.2	Giriş profilleri oluşturma	138
19	Ziyaretçileri yönetme	139
19.1	Ziyaretçi verileri	139
19.2	Ziyaretçi çok gecikti	144
20	Otoparkları yönetme	146
20.1	Bazı park bölgelerine ilişkin yetkiler	146
20.2	Araç Park Etmeye genel bakış	147
20.3	Genişletilmiş Otopark yönetimi	147
21	Genel bakışlar ve devriyeleri yönetme	149
21.1	Genel bakışları tanımlama	149

21.2	Devriyeleri yönetme	150
21.3	Bakış izleme (eskiden yol kontrolüydü)	151
22	Personelin rastgele taranması	153
23	Olay Görüntüleyici'yi Kullanma	155
23.1	Filtre kriterlerini şu ana göre ayarlama	155
23.2	Bir zaman aralığı için filtre kriterlerini belirleme	155
23.3	Filtre kriterlerini zamandan bağımsız olarak belirleme	156
24	Raporları kullanma	158
24.1	Raporlar: Ana veriler	158
24.1.1	Taşıtlarla ilgili raporlama	160
24.2	Raporlar: Sistem verileri	161
24.3	Raporlar: Yetkiler	162
25	Tehdit Seviyesi Yönetimini Yürütme	164
25.1	Bir tehdit uyarısını kullanıcı arayüzü komutu aracılığıyla tetikleme ve iptal etme	164
25.2	Bir tehdit uyarısını donanım sinyali aracılığıyla tetikleme	165
25.3	Bir tehdit uyarısını uyarı kartı aracılığıyla tetikleme	165
26	Yedekleme ve Geri Yükleme	166
26.1	Yedekleme prosedürü	166
26.2	Geri yükleme prosedürü	167
	Sözlük	169




1 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. Listedenden 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 deęişiklikleri (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)

2 Bu belge hakkında

Bu, Access Management System'in 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.

3 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.

4 Sistemi lisanslama

Ön gereksinimler

- 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.

İletişim yolu: **Configuration** (Yapılandırma) > **Licenses** (Lisanslar)

1. Kartlı Geçiş Yönetim Sistemi AMS'de oturum açın.
Not: AMS, Windows Program Files klasörlerinde yüklüyse Windows Yönetici haklarıyla oturum açın.
2. **Configuration** (Yapılandırma) > **Licenses** (Lisanslar) bölümüne gidin.
3. **Start license manager**'a (Lisans yöneticisini başlat) tıklayın
4. **License Manager** (Lisans Yöneticisi) penceresinde, satın aldığınız temel paketin onay kutusunu işaretleyin.
5. **License Activation** (Lisans Etkinleştirme) açılır penceresinde,
 - Kartlı Geçiş Yöneticisi sunucu bilgisayarının **Computer Signature**'ını (Bilgisayar İmzası) yapıştırın,
 - Temel paket için aldığınız **License Activation Key**'i (Lisans Etkinleştirme Anahtarı) yapıştırın,
 - **Etkinleştir...**'e tıklayın
6. **License Manager** (Lisans Yöneticisi) penceresinde, yeni lisansladığınız temel paketin artık **Activation valid** (Etkinleştirme geçerli) durumunda olduğundan emin olun.
7. **License Manager** (Lisans Yöneticisi) penceresinde,
 - Satın alıp dosya olarak aldığınız lisans paketlerine göz atmak ve bunları etkinleştirmek için **Import Bundle Info**'ya (Paket Bilgilerini İçer Aktar) tıklayın.
 - Satın alıp dosya olarak aldığınız tek lisanslara göz atmak ve bunları etkinleştirmek için **Import License**'a (Lisansı İçer Aktar) tıklayın.
8. **License Manager**'ı (Lisans Yöneticisi) kapatmak için **Close**'a (Kapat) tıklayın.
9. Ana **Licenses** (Lisanslar) iletişim kutusunda, satın aldığınız özelliklerin doğru sayıda birimle gösterildiğinden emin olun.

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.

5 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.

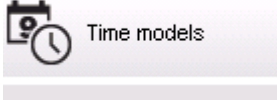
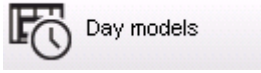
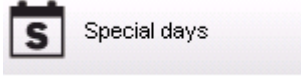
Zaman modelleri, kartlı geçiş sisteminin temel aldığı **takvime** uygulandıklarında etkinlikleri kontrol eder.

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. Bulduğunuz 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.



5.1 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 yıla 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.

📄
📁
⏪
❓
🗑️

Division: Common

« System data

S Special days

🕒 Day models

🕒 Time models

List of available special days

Date (cur. year)	Description	Day model	Division
Mi 01/01/2014	New Year	DMAC-Holiday	Common
Mo 01/20/2014	Martin Luther King Jr. Day	DMAC-Holiday	Common
Mo 02/17/2014	Presidents' Day	DMAC-Holiday	Common
Mo 05/26/2014	Memorial Day	DMAC-Holiday	Common
Fr 07/04/2014	Independence Day	DMAC-Holiday	Common
Mo 09/01/2014	Labor Day	DMAC-Holiday	Common
Mo 10/13/2014	Columbus Day	DMAC-Holiday	Common
Di 11/11/2014	Veterans' Day	DMAC-Holiday	Common
Do 11/27/2014	Thanksgiving Day	DMAC-Holiday	Common
Do 12/25/2014	Christmas Day	DMAC-Holiday	Common

Create, modify, or delete a special day

Description:

Day model: DMAC-Holiday : Holiday : Common

Date: 10/01/**** every year

Days to add: 7

Week day: Montag : after the date

Date in this year: Mo 10/13/2014

Priority: 60 Valid from: until:

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 dönemsellikte 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.

5.2

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.

📄
🔍
⏪
⏩
🗑️

Division: Common

« System data

📅 Special days

🕒 Day models

🕒 Time models

List of available day models of the access control

Day model	Description	Start time	End time	Start time	End time	Start time	End time	Division
DMAC-Holiday	Holiday	01:00:00 AM	07:00:00 AM					Common
DMAC-none	none							Common

Create, modify, or delete day models of the access control

Name:

Description:

Time intervals: Start time:

End time:

1st interval:

2nd interval:

3rd interval:

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.

5.3 Zaman modellerini tanımlama

No.	Day model	6:00AM	12:00PM	6:00PM	Description	Date (1st period)	Division
7274568	DMAC-Holi...				Holiday	Di 07/21/2015	Comm
7274568	DMAC-Holi...				Holiday	Mi 07/22/2015	Comm
7274569	DMAC-Holi...				Holiday	Do 07/23/2015	Comm
7274570	DMAC-Holi...				Holiday	Fr 07/24/2015	Comm
7274571	DMAC-Holi...				Holiday	Sa 07/25/2015	Comm
7274572	DMAC-none				none	So 07/26/2015	Comm

Mevcut zaman modelleri arama listesinden seçilebilir ve ayrıntıları iletişim kutusu alanlarında görüntülenir. Her türlü işleme yeni zaman modelleri oluşturmak için prosedüre uygun olarak gerçekleştirilir.

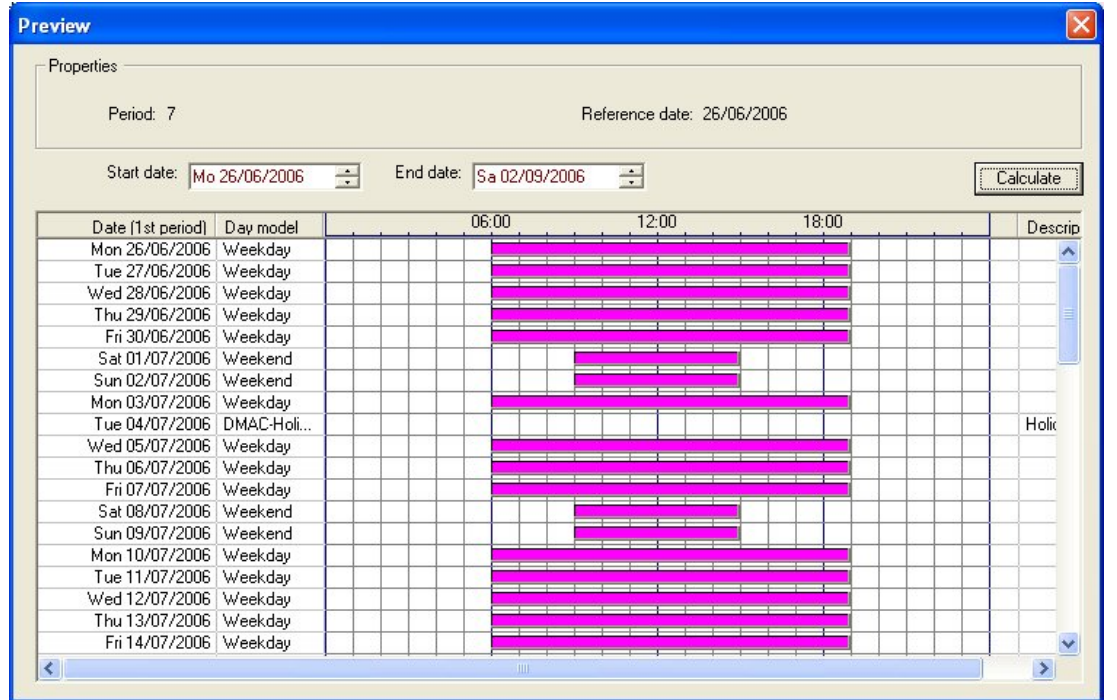
Maske boşsa zaman modelleri en baştan oluşturulur. Bunu yapmak için, bir **ad** ve **dönemdeki** gün sayısını girerek bir başlangıç veya **referans tarihi** girmeniz gerekir. Bu veriler onaylandığında (**Enter**), bunun altındaki **Gün modellerinin atanması** iletişim kutusunda bir liste görünür. Bu 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 tıkladığında, 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 izleme** düğmesine tıklanarak ayrı bir iletişim kutusu açılır ve tatiller dahil en fazla 90 günlük bir süre belirtilebilir. **Calculate** (Hesapla) düğmesine tıkladığında, 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

Name:

Description:

Period:

Reference date:

Ignore special days

No.

Day model

6:00AM

12:00PM

6:00PM

Description

Date (1st period)

Division

7274568	DMAC-Holi...	█	█	█	Holiday	Di 07/21/2015	Commc
7274568	DMAC-Holi...	█	█	█	Holiday	Mi 07/22/2015	Commc
7274569	DMAC-Holi...	█	█	█	Holiday	Do 07/23/2015	Commc
7274570	DMAC-Holi...	█	█	█	Holiday	Fr 07/24/2015	Commc
7274571	DMAC-Holi...	█	█	█	Holiday	Sa 07/25/2015	Commc
7274572	DMAC-none				none	So 07/26/2015	Commc

Holiday

Day model

6:00AM

12:00PM

6:00PM

Description

Date (1st period)

Division

--	--	--	--	--	--	--	--

2019-08 | 2.0 |

Yazılım Kullanım Kılavuzu

Bosch Security Systems

6 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 nesnelere **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

Access Management System: Divisions [Administrator] (Demo mode expires: 07/04/2019 11:21:08 PM)

File Edit Data Help

Division: Common

Divisions:

Division	Colour	Description
Common		(Common division)
ACME Corp		1st floor tenant
BCME Corp		2nd floor tenant

« Main menu

- Device data
- Operators and Workstations
- Options
- Tools
- Licenses
- Divisions**

6.1 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.

6.2**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

7 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) tıklayın** **AccessIPConfig** 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 address** (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.

8 Cihaz düzenleyiciyi kullanma

Giriş

Cihaz Düzenleyici **DevEdit** az sayıda giriş ve cihazın eklenmesi veya silinmesi ya da parametrelerin tek tek eklenmesi, değiştirilmesi veya silinmesi için tasarlanmıştır. Büyük, mevcut yapılandırmaların içe aktarılması için **Main menu** (Ana menü) > **Configuration** (Yapılandırma) > **Tools**'un (Araçlar) altındaki **Configuration Import/Export** (Yapılandırma İçe/Dışa Aktarma) işlevini kullanın.

Cihaz Düzenleyici, aşağıdaki düzenlenebilir hiyerarşilere karşılık gelen görünüm 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 gereksinimler










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





İletişim yolu

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


DevEdit araç çubuğunu kullanma

DevEdit araç çubuğu düğmeleri, örneğin **Devices** (Cihazlar), **Workstations** (İş İstasyonları) veya **Areas** (Alanlar) olmak üzere hangi görünümün etkin olduğundan bağımsız olarak aşağıdaki işlemlere sahiptir.

Düğme	Kısayol	Açıklama
	Ctrl + N	Seçilen düğümün altında yeni bir öge oluşturur. Alternatif olarak, bağlam menüsünü çağırmak için düğüme sağ tıklayın.
	Del	Seçilen ögeyi ve altındaki tüm öğeleri siler.
	Ctrl-Page up	Ağaçtaki ilk öge
	Ctrl -	Önceki öge
	Ctrl +	Sonraki öge
	Ctrl-Page down	Ağaçtaki son öge
	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 DevEdit görünümünde, ağacın kökünden başlayın ve araç çubuğu düğmeleri, menü veya her öğenin bağlam menüsünü kullanarak öğeleri ekleyin (çağırma için sağ tıklayın). Ağaca alt öğeler eklemek için önce alt öğelerin altında görünmesi gereken öğeyi seçin.

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

DevEdit'i kapatmak için **File** (Dosya) > **Exit**'e (Çıkış) tıklayın.

9 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 ayrılanaya kadar başka girişler reddedilebilir.
- Giriş sırası kontrolü ve anti-passback uygulama

Sistem iki tip giriş kontrollü alan arasında ayırım 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 öge 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**'in (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.

9.1

Araçlara ait alanları yapılandırma

Araçlar için alan (otopark, park bölgesi) oluşturma

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

Name starts

Name	Count
Central parking_01	20
Central parking_02	15
Central parking_03	50
Central parking_04	100

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 bölümünde, **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 ıkış okuyucusu şeklinde atadığını unutmayın.

10

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

10.1

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 işaretlemeyen bırakın. Ayrıntılar için bölümüne bakın.
- **Automatic logout after** (Şu süreden sonra oturumu otomatik olarak kapat): Bir oturum kayıt okuyucusuyla oturum otomatik olarak sonlandırıldıktan sonraki saniye sayısı. Sınırsız süre için 0 olarak bırakın.

10.2 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 kullanılabilir?
- 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 kullanılacak 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) bölümünde.

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.

10.3

İş istasyonu profillerini atama

İş istasyonu 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.

10.4

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

10.5

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. İsteddiğiniz 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) bölümünde:

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 Operatör, API tarafından sistem işlevlerini gerçekleştirmek için kullanılamaz. yok)

Read only (Salt Operatör, API tarafından sistem verilerini okumak için kullanılabilir ancak okunur) 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

10.6

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 gereksinimler

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.


Diğer operatörlerin şifrelerini değiştirmeye ilişkin prosedür.

Ön gereksinimler

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 bölümünde, 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/>

Yeni kullanıcı oluşturmak için XREF

11 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

Kart kodlamada hataları önlemek için, tüm sayılar ondalık veya on altılık biçimlerde girilebilir.

Kart üreticisinin talimatlarına göre **Hexadecimal** (On altılık) veya **Decimal** (Ondalık) radyo düğmesini seçin. Girilen tüm değerler otomatik şekilde dahili olarak dönüştürülür.

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 alanları kullanın.

Kart bir operatör iş istasyonunda manuel olarak kayıtlıysa her kart için özelleştirilebilecek varsayılan değerleri gösteren bir iletişim kutusu görüntülenir.

<p>Kod no. tam (varsayılan)</p>	<p>Yalnızca tesis kodu girilir (on altılık veya ondalık).</p> <div data-bbox="494 1042 1396 1266"> <p>Card default code data</p> <p><input type="radio"/> Hexadecimal</p> <p><input checked="" type="radio"/> Decimal</p> <p>Version: <input type="text"/></p> <p>Country code: <input type="text"/></p> <p>Facility code: <input type="text" value="1"/></p> </div> <p>Kodlama verilerini girme: Tesis kodu üretici tarafından bir ondalık değer olarak girilir: 56720 Decimal (Ondalık) radyo düğmesini seçin ve tesis kodunu girin. Verileri kaydetmek için Uygula düğmesine tıklayın.</p>
<p>Kod no. bölünmüş</p>	<p>Version (Sürüm), Country Code (Ülke Kodu) ve Facility Code'un (Tesis Kodu) tamamı ondalık değerler olarak girilmelidir.</p> <div data-bbox="494 1510 1396 1734"> <p>Card default code data</p> <p><input type="radio"/> Hexadecimal</p> <p><input checked="" type="radio"/> Decimal</p> <p>Version: <input type="text" value="0"/></p> <p>Country code: <input type="text" value="0"/></p> <p>Facility code: <input type="text" value="1"/></p> </div> <p>Kod verilerini girme: Veriler üretici tarafından aşağıdaki ondalık değerler olarak girilir: Version (Sürüm): 2 Country code (Ülke kodu): 99 Facility code (Tesis kodu): 56720 Verileri ilgili metin kutularına girin.</p>

Verileri saklamak için Uygula düğmesine 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 aktarırsa 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) aktarırsa 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.



Check membership only values

Hexadecimal

Decimal

1. value: 150

2. value: 0

3. value: 0

4. value: 0

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.

12 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

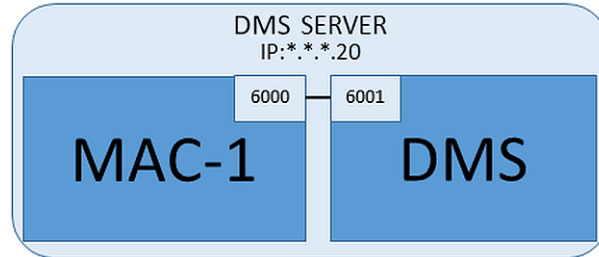
DevEdit'in temel kullanımı aşağıdaki bağlantıda yer alan **Cihaz düzenleyiciyi kullanma** bölümünde açıklanmıştır.

Bkz.

- *Cihaz düzenleyiciyi kullanma, sayfa 20*

12.1 MAC'leri ve RMAC'leri Yapılandırma

12.1.1 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 yükleyin) (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.

12.1.2

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

Bu bölümde bilgisayarların MAC sunucuları olacak şekilde nasıl hazırlanacağı anlatılmaktadır. Varsayılan olarak bir Access Engine 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.

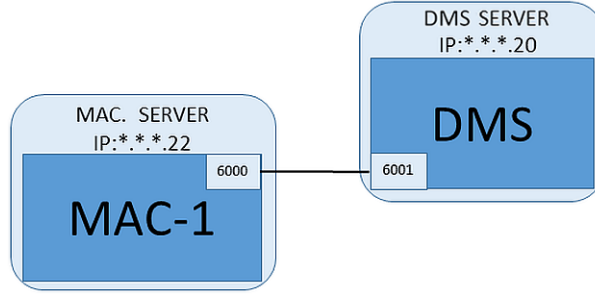
MAC'ler veya RMAC'lerin bulunduğu ayrı bilgisayarlar, bir MAC veya bir RMAC barındırıp barındırmadıklarından bağımsız olarak MAC sunucuları olarak bilinir.

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 sunucular, en son Windows güncellemelerini içeren DMS sunucusuyla aynı işletim sistemine sahiptir.
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 7'de bu bir kurulumdur. Windows 10 ve Windows Server işletim sistemlerinde ise bir özellik olarak etkinleştirilmiştir
6. Bilgisayarı yeniden başlatın

12.1.3 Bir MAC'i kendi MAC sunucusunda yapılandırma



- MAC sunucu bilgisayar bölümünde açıklandığı gibi hazırlanmıştır.
1. DMS sunucusunda, cihaz düzenleyicide bu MAC için **Activate** (Etkinleştir) ve **Load devices** (Cihazları yükle) onay kutularını temizleyerek MAC'i devre dışı bırakın.
 2. MAC sunucusunda, `services.msc` Windows programını kullanarak MAC işlemini durdurun.
 3. `MACInstaller.exe`'yi başlatın
 - ACE için bu, `\AddOns\ACE\MultiMAC\MACInstaller` BIS kurulum ortamında bulunur (aşağıdaki `MACInstaller` aracını kullanma bölümüne bakın).
 -
 4. Aşağıdaki parametreler için değerleri girerek aracın ekranlarında gezinin.

Ekran No.	Parametre	Açıklama
1	Destination Folder (Hedef Klasör)	MAC'in yükleneceği yerel dizin. Mümkün olan her yerde varsayılanı alın.
2	Server (Sunucu)	DMS'in çalıştığı sunucunun adı veya IP adresi.
2	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.
2	Number (MAC System Number) (Numara (MAC Sistem Numarası))	Bu ve tüm MAC'ler için 1 olarak ayarlayın (RMAC'lerin tersine).
2	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.
2	Configure Only (Yalnızca Yapılandır) (radyo düğmesi)	Ana DMS oturum açma sunucusunda bir MAC yapılandırmadığınızdan bunu seçmeyin.
2	Update Software (Yazılımı Güncelle) (radyo düğmesi)	Bir MAC'i ana DMS oturum açma sunucusunda değil kendi bilgisayarında (MAC sunucusu) yapılandırdığınızdan bu seçeneği seçin.

5. Aracı tamamladıktan sonra, MAC sunucusunu yeniden başlatın veya alternatif olarak `services.msc` Windows programını kullanarak MAC sunucusunda MAC işlemini başlatın.
6. DMS sunucusunda, Cihaz Düzenleyici'deki MAC'i seçin.
7. **MAC** sekmesinde, aşağıdaki parametrelerin değerlerini girin:

Parametre	Açıklama
Name (Ad)	Cihaz ağacında görünecek isim, örneğin MAC-1.
Açıklama	ACE 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 ACE Bölümü.

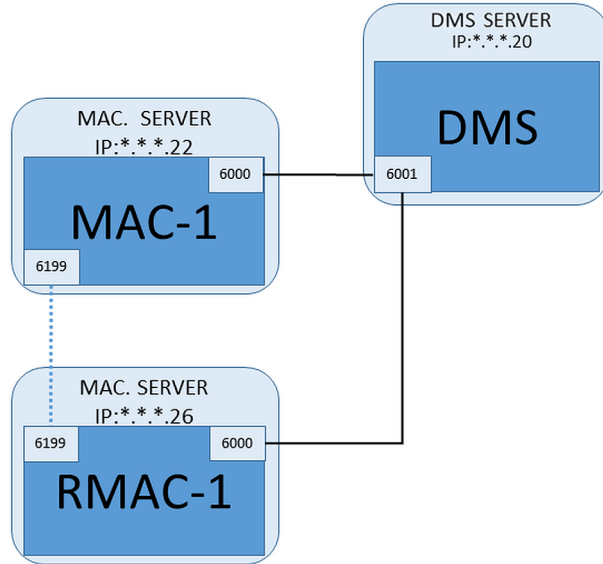
12.1.4

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 dönecekmiş gibi açık tutun.

MAC için MAC sunucusunda

MAC'i bir RMAC ile ortak olarak yeniden yapılandırmak için, aşağıdaki gibi ilerleyin.

- Daha önce hazırlanan 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
 - **Number** (Numara): 1 (tüm MAC'lerin Numarası 1'dir)
 - **Twin** (İkiz): RMAC'in çalışacağı bilgisayarın IP adresi.
 - **Update software** (Yazılımı güncelle): DMS sunucusunu değil bir MAC sunucusunu yapılandırırken bu seçeneği seçin.

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.
 - **Update software** (Yazılımı güncelle): DMS sunucusunu değil bir MAC sunucusunu yapılandırırken bu seçeneği seçin.

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.

Parametre	Açıklama
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.

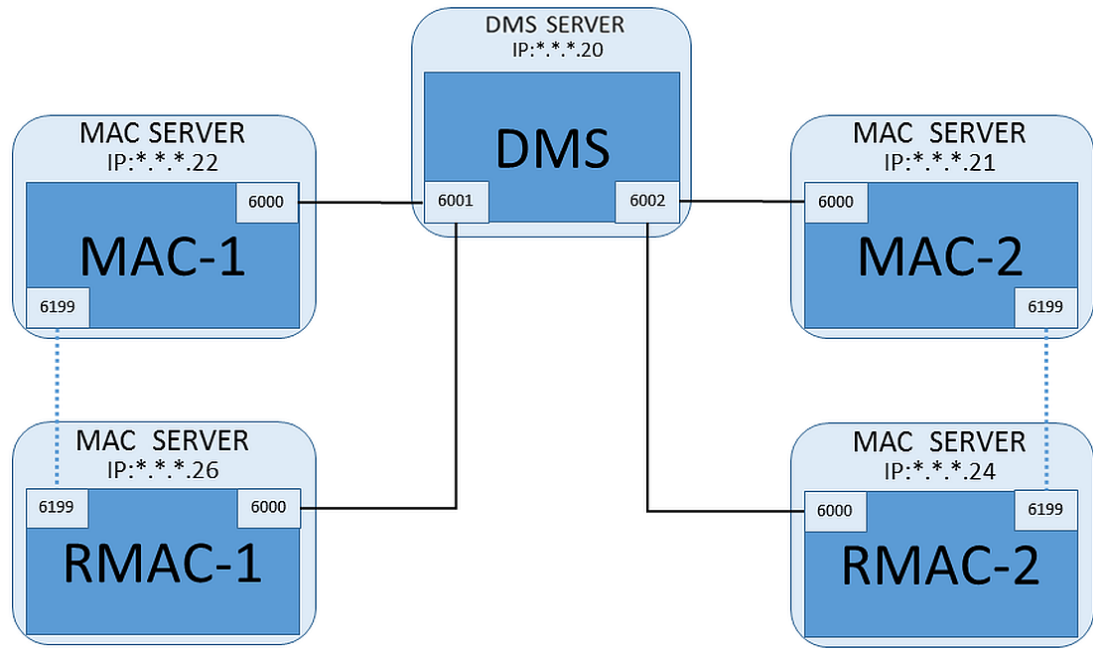
3. **RMAC** sekmesinde, aşağıdaki parametrelerin değerlerini girin:

Parametre	Açıklama
Name (Ad)	Cihaz ağacında görünecek ad. Örneğin, ilgili MAC'in adı MAC-01 ise bu RMAC, RMAC-01 olarak adlandırılabilir.
Açıklama	ACE 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.

12.1.5

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 RMAC'leri varsayılan olarak devre dışı bırakılır. Cihaz düzenleyici'deki ilgili onay kutularını seçerek bunları yapılandırma tarayıcısında yeniden etkinleştirmeyi unutmayın.

12.1.6

MAC kurucu aracını kullanma

`MACInstaller.exe` MAC'ler ile RMAC'leri kendi bilgisayarlarında (MAC sunucuları) yapılandırmak ve yeniden yapılandırmak 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 yaptığandan, yeniden yapılandırmadan önce çalışan her türlü MAC işleminin durdurulması gerekir.

MACInstaller aracı, BIS kurulum ortamında aşağıdaki yolda bulunabilir:

`\BIS_<version>\AddOns\ACE\MultiMAC\MACInstaller.exe`

Bir dizi ekran aracılığıyla, aşağıdaki parametreler için değerleri toplar.

Ekran No.	Parametre	Açıklama
1	Destination Folder (Hedef Klasör)	MAC'in yükleneceği yerel dizin.
2	Server (Sunucu)	DMS'in çalıştığı sunucunun adı veya IP adresi.
2	Port (Port to DMS) (Port (DMS Port))	MAC ve DMS arasında iletişim için kullanılacak DMS sunucusundaki port numarası. Ayrıntılar için aşağıya bakın.
2	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.
2	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.

Ekran No.	Parametre	Açıklama
2	Configure Only (Yalnızca Yapılandır) (radyo düğmesi)	Ana DMS giriş sunucusunda bir MAC'i yeniden yapılandırılıyorsa bu seçeneği seçin. Ayrıntılar için aşağıya bakın
2	Update Software (Yazılımı Güncelle) (radyo düğmesi)	Bir MAC'i ana DMS oturum açma sunucusunda değil kendi bilgisayarında (MAC sunucusu) kuruyor veya yeniden yapılandırılıyorsa bu seçeneği seçin. Ayrıntılar için aşağıya bakın

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.



Uyarı!

Hiyerarşik sistemlerdeki DMS alıcısı portu DMS alıcısı portlarının numaralandırma düzeninin hiyerarşik sistemlerde farklı olduğunu unutmayın. Ayrıntılı bilgi için bkz.

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.

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.

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.

12.2

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 Access Modular Controller .	En fazla dört Wiegand okuyucu, en fazla dört girişi bağlayacak şekilde yapılandırılabilir. Kontrol cihazı sekiz giriş ve sekiz çıkış sinyalinin destekler. Gerekirse genişletme kartları 48 adede kadar ek giriş ve çıkış sinyali sağlayabilir.
AMC2 4R4	Dört RS485 okuyucu arayüzüne sahip Access Modular Controller	En fazla sekiz RS485 okuyucu en fazla sekiz girişe bağlanacak şekilde yapılandırılabilir. Kontrol cihazı sekiz giriş ve sekiz çıkış sinyalinin 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 gereken şekilde iletir.
- Karışık kontrol cihazı çalışması, yalnızca iki kod numarası da aynı şekilde oluşturulmuşsa işe yarar.

12.2.1


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 isimleri garanti eder, ancak bunların tek tek üzerine yazılabilir. Üzerine yazılması durumunda, kimliklerin benzersiz olduğundan emin olmak kullanıcının sorumluluğundadır. Bu nedenle, DHCP sunucularına yapılan Ağ bağlantılarında ağ adının kullanmasını öneririz.

Controller description (Kontrol cihazı açıklaması)	alfa sayısal: 0 - 255 basamak	Bu metin OPC dalında görüntülenir.
Communication to host enabled (Ana bilgisayar iletişimi etkin)	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	Varsayılan değer = etkin Onay kutusu geçerli ayarı gösterir ve aynı zamanda değiştirmek için de kullanılabilir. Ana bilgisayar bağlantısının durumu, Gezin'deki şu simgelerle gösterilir: Kontrol cihazı çeşidi: etkin etkin değil AMC2 4W   AMC2 4R4   Devre dışı bırakma, daha sonraki bir tarihte kartlı geçiş sistemine dahil edilecek cihazların oluşturulması ve parametrelendirilmesi için bir araç sağlar. Cihazlar etkinleştirilmemeli ve böylece devreye alınana kadar ana bilgisayarın veritabanına eklenmelidir. Bu ayrıca, cihazların ana bilgisayar tarafından gereksiz yere sorgulanmasını da azaltır.  Bir yazılım güncellemesinden sonra güvenlik nedeniyle tüm kontrol cihazları çevrimdışı olarak ayarlanır (onay kutusu işaretli değildir). Bu, kurulumun eski yazılımla çalışmaya devam edebilmesini ve yeni yazılımla adım adım hızlandırılabilmesini sağlar. Kurulumdaki yeni kontrol cihazlarını ilgili kutularını işaretleyerek yavaş yavaş ekleyin.
Kontrol Cihazı Arayüzü		
Interface Type (Arayüz Tipi)	COM UDP	COM'da bağlantı MAC COM portlarının biri aracılığıyla AMC'ye yapılır.

		<p>UDP'de (= kullanıcı veri iletisi protokolü) ise bağlantı ağ ile yapılır. Bu bağlantı tipi seçildiğinde, "ana bilgisayar adı" ve "uzaktan kontrol edilen port" parametreleri ayarlanabilir hale gelir.</p>  <p>"UDP" arayüz tipi ile DIP anahtarı "5" AMC'de ayarlanmalıdır. Ayrıca anahtar "1"i ON (AÇIK) konumuna getirmeniz önerilir.</p>
PC COM port (PC COM portu)	<p>sayısal: Şu COM portları ile: 1 - 256 Şu UDP portları ile: 1 - 65535</p>	<p>Bu AMC'nin MAC'ye bağlı olduğu COM bağlantı noktalarının sayısı. Dönüştürücüler aracılığıyla ethernet bağlantıları için, sanal COM portları üretilir ve burada gösterilir. "UDP" tipi ile MAC'in AMC'den bilgi alacağı portu girin. Bu bağlantı noktası bilinmiyorsa alan boş bırakılabilir ve otomatik olarak bir serbest bağlantı noktası seçilir.</p>
Bus number (Veri yolu numarası)	<p>sayısal: 1 - 8</p>	<p>AMC-MUX arayüz adaptörünü kullanarak 8 adede kadar kontrol cihazı bir COM portunda yapılandırılabilir. Bu gibi durumlarda, her AMC'nin DIP anahtarıyla verilen benzersiz adresini girin.</p> <p>Not: Anahtar 5 burada göz ardı edilebilir çünkü adresleme için sadece ilk 4 anahtar kullanılır. UDP bağlantılarında varsayılan ayarı (= 0) kullanın</p>
IP Address/ Hostname (IP Adresi/ Ana Bilgisayar Adı)	<p>AMC'nin ağ adı veya IP adresi</p>	<p>Bu giriş kutusu sadece UDP port tipi olarak seçilirse 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 olmayan ağlarda IP adresi verilmelidir.</p>
UDP Port (UDP Portu)	<p>sayısal: 1 - 10001 - varsayılan yapılandırmayla</p>	<p>Bu giriş kutusu sadece UDP port tipi olarak seçilirse etkinleştirilir. Bu, MAC mesajlarını alacak olan AMC portudur.</p>

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 "Ortak"	Bu salt okunur bir bilgilendirme alanıdır. "Bölümler", BIS Yöneticisi'nde oluşturulan ve sürdürülen birden çok özerk taraf arasında bir kartlı geçiş kurulumunu bölmek için kullanılan araçlardır.

AMC girişlerini yapılandırma

AMC 4-W
Inputs
Outputs
Terminals

Name	Serial resistor	Parallel resistor	Time model	Messages
01, AMC 4-W-8	2K2	1K2	<No time model>	03, Open, close, Line cut, short circuit
02, AMC 4-W-8	1K5	1K	<No time model>	00,
03, AMC 4-W-8	none	none	<No time model>	00,
04, AMC 4-W-8	none	none	<No time model>	00,
05, AMC 4-W-8	none	none	<No time model>	00,
06, AMC 4-W-8	none	none	<No time model>	00,
07, AMC 4-W-8	none	none	<No time model>	00,
08, AMC 4-W-8	none	none	<No time model>	00,

Input type

Digital mode, single Analog mode, 4 state

Events

Time model: <No time model> ▼

Open, close

Line cut, short circuit

Resistors

serial

none

1K

1K2

1K5

1K8

2K2

2K7

3K3

3K9

4K7

5K6

6K8

8K2

parallel

none

1K

1K2

1K5

1K8

2K2

2K7

3K3

3K9

4K7

5K6

6K8

8K2

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 etkinleştirilmiştir
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), **Closed** (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

AMC 4-W Inputs Outputs Terminals

Output	Action type	Max. duration	Delay	Period	Pulsing	Duration	Count	Time model	Message
01, AMC 4-W-8	used	by an	entrance !					000, <No time model>	(
02, AMC 4-W-8	used	by an	entrance !					000, <No time model>	(
03, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	(
04, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	(
05, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	(
06, AMC 4-W-8	used	by an	entrance !					000, <No time model>	(
07, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	(
08, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	(

Output data

State

- Input activated
- Input normal
- Input short circuit tamper
- Input open tamper
- Input enabled
- Input disabled
- Output set
- Output reset
- Door open
- Door closed
- Door opened unauthorised
- Door left open
- Reader shows access gran
- Reader shows access deni
- Time model active

Events

Create events: Time model: 000, <No time model>

Behaviour

Action type: 1 - Follow state

Max. duration: 0 sec.

Delay: 0 sec.

Period: 0 sec.

Pulsing

Enable:

Pulse width: 0 1/10 sec.

of pulses: 0

Output	Op1	Description	Param11	Param12	Op2	Description	Parameter21
03		Door open	10b, DM 10b	NORMDOOR, Door-6			
03	OR	Door opened unauthorised	10b, DM 10b	NORMDOOR, Door-6			
05		Door open	01a, DM 01a-6	NORMDOOR, Door-7			
05	OR	Door opened unauthorised	01a, DM 01a-6	NORMDOOR, Door-7			

Tablodaki AMC çıkışlarını seçme

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

Output	Action type	Max. duration	Delay	Period	Pulsing	Duration	Count	Time model	Messages
01, AMC 4-W-8	used	by an	entrance !					000, <No time model>	00
02, AMC 4-W-8	used	by an	entrance !					000, <No time model>	00
03, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	00
04, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	00
05, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	00
06, AMC 4-W-8	used	by an	entrance !					000, <No time model>	00
07, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	00
08, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	00

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

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.

Çıktılar: 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. Listedenden seçilen tüm girişler için parametre ayarlarındaki değişiklikler benimsenir.

The screenshot shows the 'Events' configuration window. At the top, there is a 'Create events' checkbox which is checked, and a 'Time model' dropdown menu set to '001, normal week'. Below this, there are two main sections: 'Behaviour' and 'Pulsing'. In the 'Behaviour' section, the 'Action type' dropdown is set to '2 - Trigger'. There are three input fields: 'Max. duration' (0 sec), 'Delay' (1 sec), and 'Period' (10 sec). In the 'Pulsing' section, there is an 'Enable' checkbox which is unchecked. Below it are two more input fields: 'Pulse width' (0 1/10 sec) and '# of pulses' (0).

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 (Gecik me)	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 bunları tetiklemek için yapılandırılmış durumları içeren bir tablo.

Output	Op1	Description	Param11	Param12	Op2	Description	Parameter21	Parameter22
07		Door open	10b, DM 10b	NORMDO...				
07	OR	Door closed	10b, DM 10b	NORMDO...				
07	OR	Door opened ...	10b, DM 10b	NORMDO...				
07	OR	Door left open	10b, DM 10b	NORMDO...	AND	Door left open	10b, DM 10b	NORMDOOR, ...

Çıkışları tetiklemek için durumları yapılandırma


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

- Üst liste kutusundan bir veya birkaç çıkış seçin.
- **State** (Durum) listesinden bir Durum seçin.
- Bu durumu iletebilen seçilmiş bir duruma yönelik birkaç cihaz veya kurulum varsa » düğmesi » düğmesinin yanında etkinleştirilir.
» simgesine tıklayarak (veya duruma çift tıklayarak) her cihaz için ilk cihaz (örneğin AMC, ilk giriş) ve kurulum (örneğin ilk sinyal, ilk kapı) ile durumundan 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 bir VEYA kısayolu 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:

- Bir duruma rastgele bir sütunda seçilerek başka bir koşulun eklendiği bir durum atanmalıdır.
- 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 kısayolu atanabilir.
Atanan her koşul için, **bir** VE kısayolu oluşturulabilir.

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  simgesine tıklanarak oluşturulur.

Çıkışların parametrelerini değiştirme

Liste girişleri değiştirilebilir.

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 tıkladığında, bir düğme parametre için geçerli girişlerden oluşan bir açılır listeyi açar.

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	01, AMC 4-W-2
04	OR	Door open	06a, Timemgm	

01, AMC 4-W-2

02, AMC 4-W-2

03, AMC 4-W-2

04, AMC 4-W-2

05, AMC 4-W-2

06, AMC 4-W-2

07, AMC 4-W-2

08, AMC 4-W-2

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_ID, AMC_ID16_002_1	In, 01, AMC_ID16_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 dışı müdahalesi	3	Dirençli yerel giriş yapılandırıldı
Giriş açık dış müdahalesi	4	Dirençli yerel giriş yapılandırıldı
Giriş etkin	5	Yerel giriş zaman modeliyle etkinleştirildi
Giriş devre dışı	6	Yerel giriş zaman modeliyle devre dışı bırakıldı
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	---
Okuyucu Mesajları	23	(Ayrıntılar mevcut yazılım sürümüne bağlıdır)
LAC Mesajları	24	(Ayrıntılar mevcut yazılım sürümüne bağlıdır)

Çıkışları yapılandırma

Kapı modelleri ya da tek atama ile birlikte sinyal atanmanın 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 UGM'ye 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	REVDOR, 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	REVDOR, Revolving Door

Aynı koşullar, örneğin optik bir sinyale ek olarak bir akustik sinyale de ihtiyacınız olursa ve aynı zamanda UGM'ye 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	---	---

Terminaler sekmesindeki sinyalleri tanımlama

Terminals (Terminaler) 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** (Terminaler) sekmesinde değişiklik yapamazsınız. Düzenlemeler yalnızca giriş sayfasının terminaler sekmesinde yapılabilir. Bu nedenle terminal ayarları gri bir arka plan üzerinde görüntülenir. Kırmızı renkte görüntülenen girişler, ilgili çıkışların sinyal yapılandırmalarını gösterir.

AMC 4-R4 | Inputs | Outputs | Terminals

Signal allocation of 'AMC 4-R4' with 12 signal pairing

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				

13

13.1

Girişleri Yapılandırma

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 paylaşılabilir.
- 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.

13.2

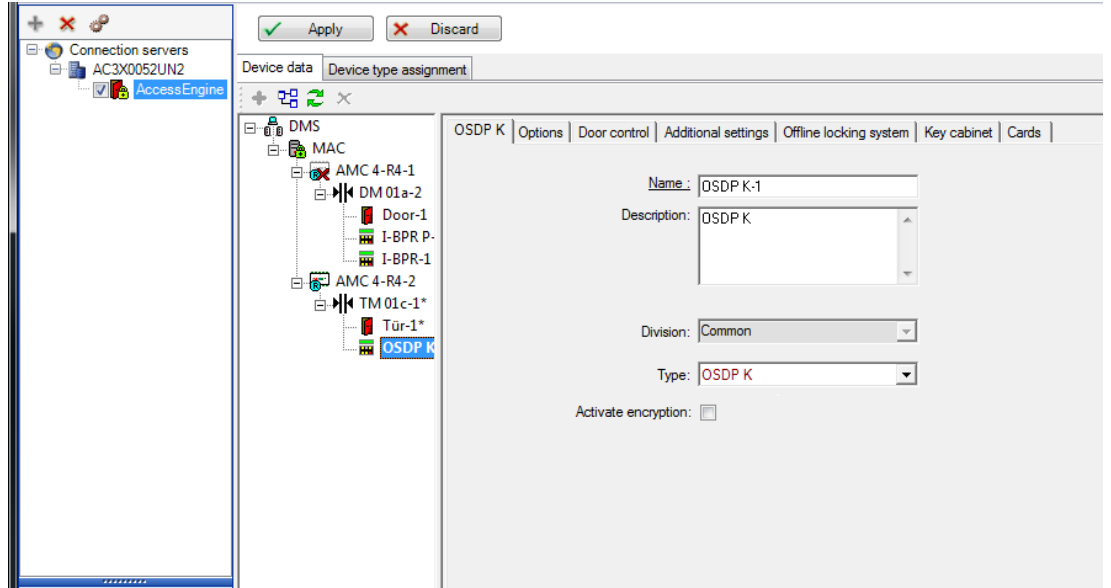
Giriş oluşturma

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	HID 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		
TB30 LE		X		
TB15 HI1		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
R40				X
R30				X
R15				X

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



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.



DM 01a | Terminals

Entrance name: DM 01a

Entrance description: DM 01a

Location: Outside

Destination: Outside

Division: Common

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	Kartlı geçiş sisteminin, kendi kararını vermeden önce kartlı geçiş sisteminden bir karar beklediği süre.
Division (Bölüm)	Salt okunur bir alan	Okuyucunun ait olduğu tanımlanmış bölüm. Varsayılan bölüm Common 'dir (Ortak).

Latency alarm device (Gecikme alarmı cihazı) (sadece giriş modelleri 10 ve 14 için)	100 - 9999	Kapı açıcının bir alarm verilmeden etkinleştirilebileceği zaman aralığı. Bu, ayarlanan ve daha sonra okuyuculara gönderilen bir okuyucu parametresidir. Bu parametrenin birimi saniyenin onda biridir (1/10).
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.

13.3

Ek G/Ç kontrolleri

Ek G/Ç kontrolleri, örneğin bir ziyaretçiyi Otomatik Numara Plaka Tanıma'ya (ANPR) göre tanımlamaya yardımcı olabilir.

AMC, AMC G/Ç kontağı aracılığıyla 1 giriş alır:

- Ziyaretçi Ek G/Ç kontrolüne izin verdi

AMC, "yetkili olmayan" bir sinyal durumunda girişi engeller.

The screenshot displays the 'Device data' tab in the software interface. On the left, a tree view shows the hierarchy of devices under 'DMS', including 'AMC-RCWM', 'DM 01a-1', 'DM 10a-1', and 'AMC 086482'. The 'AMC 086482' device is expanded to show its configuration, including 'Parking-lot 05-1' and 'Barrier-1'. On the right, the 'Signal allocation' table for 'AMC 086482' with 42 signal pairing is visible. The table lists various input signals and their corresponding output signals.

T..	entrance	Input signal	entrance	Output signal
6482	01	Parking-lot 05-1 Door contact	Parking-lot 05-1	Release door
6482	02	Parking-lot 05-1 "Request to exit" button	Parking-lot 05-1	Door is unlocked
6482	03	Parking-lot 05-1 Passage locked	Parking-lot 05-1	Stoplight green
6482	04	Parking-lot 05-1 Passage completed	Parking-lot 05-1	Alarm masking
6482	05	Parking-lot 05-2 Door contact	Parking-lot 05-2	Release door
6482	06	Parking-lot 05-2 "Request to exit" button	Parking-lot 05-2	Door is unlocked
6482	07	Parking-lot 05-2 Passage locked	Parking-lot 05-2	Stoplight green
6482	08	Parking-lot 05-2 Passage completed	Parking-lot 05-2	Alarm masking
116_002_1	01	Parking-lot 05-1 External access decision accep...	Parking-lot 05-1	External access ...
116_002_1	02	Parking-lot 05-1 External access decision denied		
116_002_1	03	Parking-lot 05-2 External access decision accepted	Parking-lot 05-2	External access decli...
116_002_1	04	Parking-lot 05-2 External access decision denied		
116_002_1	05			
116_002_1	06			
116_002_1	07			

Kart Durumu	Sinyal = 1:ANPR yetkili	Sinyal = 0: ANPR yetkilendirilmedi
Karta yetki verildi	Giriş	Geçersiz araç numarası olayı
Kart kara listede	Yetki verilmedi - kara liste	Yetki verilmedi - kara liste
Kartın süresi doldu	Yetki verilmedi - süresi doldu	Yetki verilmedi - süresi doldu
Bu okuyucu için karta yetki verilmedi	Yetki verilmedi	Yetki verilmedi

Ziyaretçi tanınmasa bile bariyeri manuel olarak açmak mümkündür.

Bu işlev için AMC G/Ç kontaklarına bir anahtar bağlanmıştır.

AMC, giriş sinyali analiz edilmeden önce bir **Additional check active** (Ek kontrol etkin) çıkış sinyali ayarlar.

Yeni bir ziyaretçi kaydedilirse araç plakası bilgisi operatör tarafından BIS'e (raporlar için) ve ANPR sistemine (tarama için) girilmelidir.

ANPR, kayıtlı bir aracı kendi veritabanından tanır.

13.4 AMC terminallerini yapılandırma

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

B..	T..	entrance	Input signal	entrance	Output signal
0	01	DM 01a	Door contact	DM 01a	Release door
0	02	DM 01b	Door contact	DM 01b	Release door
0	03	DM 01b	"Request to exit"...		
0	04				
0	05				
0	06				
0	07				
0	08				

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

B..	T..	entrance	Input signal	entrance	Output signal
0	01	DM 01a	Door contact	DM 01a	Release door
0	02	DM 01b	Door contact	DM 01b	Release door
0	03	DM 01b	"Request to exit" ▾		
0	04		< not assigned >		
0	05		"Request to exit" button		
0	06		Bolt sensor		
0	07		Passage locked		
0	08		Sabotage		

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

B..	T..	entrance	Input signal	entrance	Output signal
0	01	DM 01a	Door contact	DM 01a	Release door
0	02	DM 01b	Door contact	DM 01b	Release door
0	03	DM 01b	"Request to exit"...		
0	04	DM 01b	Bolt sensor ▾		
0	05				
0	06				
0	07				
0	08				

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

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				

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 giriş çift tıkladığında, 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
Kapı sensörü	
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 kalıcı olarak kilitlemek için de kullanılabilir.
Sabotaj	Harici bir denetleyicinin sabotaj 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.
Yerel açma etkin	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
Harici giriş kararı reddedildi	Harici bir sistem girişi kabul ediyorsa sinyal ayarlanır

Çıkış sinyalleri tablosu

Çıkış Sinyalleri	Açıklama
Kapı açıcı	
Geçit: Ters yönü kilitle	Tuzağın diğer tarafını kilitletler. Bu sinyal, kapı açıldığında gönderilir.
Alarm bastırma	...IDS'ye. IDS'nin bir hırsız alarmı mesajı oluşturmasını önlemek için kapı açık olduğu sürece ayarlanır.
Gösterge yeşil	Gösterge lambası: Kapı açık olduğu sürece kontrol edilir.

Kapı çok uzun süredir açık	Üç saniyelik darbe. Kapı çok uzun süre açıksa.
Kamera etkinleştirme	Kamera, bir geçişin başında etkinleştirilir.
Açık turnike gelişi	
Açık turnike gidişi	
Kapı kalıcı olarak açık	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	- Kapı sensörü - "Çıkış talebi" düğmesi - Cıvata sensörü - Giriş kilitleme - Sabotaj - Yerel açma etkin - Harici giriş kararı kabul edildi - Harici giriş kararı reddedildi	- Kapı açıcı - Geçit: ters yönü kilitle - Alarm bastırma - Gösterge yeşil - Kamera etkinleştirme - Kapı çok uzun süredir açık - 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 kilitleme - Sabotaj - Harici giriş kararı kabul edildi - Harici giriş kararı reddedildi	- Geçit: ters yönü kilitle - Açık turnike gelişi - Açık turnike gidişi - Alarm bastırma - Kamera etkinleştirme - Kapı çok uzun süredir açık - Harici giriş kararı etkin
05	Otopark girişi veya çıkışı - maksimum 24 park bölgesi Zaman ve devam okuyucuları Harici giriş kararı mevcut	- Kapı sensörü - "Çıkış talebi" düğmesi - Giriş kilitleme - Geçiş tamamlandı - Harici giriş kararı kabul edildi - Harici giriş kararı reddedildi	- Kapı açıcı - Alarm bastırma - Gösterge yeşil - Kapı çok uzun süredir açık - Kapı kalıcı olarak açık - 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	- Kapı sensörü - "Çıkış talebi" düğmesi - Giriş kilitlendi - Geçiş tamamlandı - Harici giriş kararı kabul edildi - Harici giriş kararı reddedildi	- Kapı açıcı - Alarm bastırma - Gösterge yeşil - Kapı çok uzun süredir açık - Kapı kalıcı olarak açık - Harici giriş kararı etkin
10	Giriş ve çıkış okuyucusu ile IDS kurma/devre dışı bırakma özelliğine sahip basit kapı Zaman ve devam okuyucuları Harici giriş kararı mevcut	- Kapı sensörü - "Çıkış talebi" düğmesi - IDS: Kurulmaya hazır - IDS: Kuruldu - Sabotaj - IDS: Kurma isteği - Harici giriş kararı kabul edildi - Harici giriş kararı reddedildi	- Kapı açıcı - Kamera etkinleştirme - IDS: Kurma - IDS: Devre dışı bırakma - Kapı çok uzun süredir açık - Harici giriş kararı etkin
14	Giriş ve çıkış okuyucusu ile IDS kurma/devre dışı bırakma özelliğine sahip basit kapı Zaman ve devam okuyucuları	- Kapı sensörü - "Çıkış talebi" düğmesi - IDS: Kurulmaya hazır - IDS: Kuruldu - Sabotaj - IDS: Kurma isteği	- Kapı açıcı - Kamera etkinleştirme - IDS: Kurma - Kapı çok uzun süredir açık
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 kısılır.

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, işlemlere atanamaz ve parametreleri kontrol cihazları ve kartları 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 parametrelili işlemler 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.



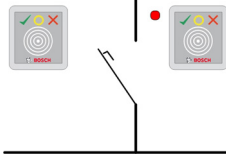
Uyarı!

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

13.5

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
Kapı sensörü	Kapı açıcı
"Çıkış talebi" düğmesi	Geçit: Ters yönü kilitle
Sabotaj	Gösterge yeşil
Yerel açma etkin	Kamera etkinleştirme
	Kapı çok uzun süredir açık



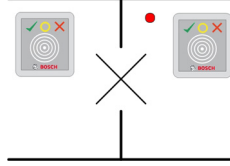
Uyarı!

Özellikle karşı taraftaki kilit olmak üzere tekleme işlevi 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	Açık turnike gelişi
"Çıkış talebi" düğmesi	Açık turnike gidişi
Sabotaj	Giriş kilitlendi
	Kamera etkinleştirme
	Kapı çok uzun süredir açık
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
Kapı sensörü	Kapı açıcı
"Çıkış talebi" düğmesi	Kapı kalıcı olarak açık
Giriş kilitlendi	Gösterge yeşil
Geçiş tamamlandı	Alarm bastırma
	Kapı çok uzun süredir açık

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 girişi kontrol etmez, ancak zaman ve devam amacıyla özel olarak kullanılır. Bunlar kapıları kontrol etmez, sadece kart verilerini zaman ve devam sistemine iletir.

Sonuç olarak, hiçbir sinyal tanımlanmaz. Bu okuyucular genellikle zaten kontrol edilen bir alana kurulur.



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. Okuyuculardan birini gelen okuyucusu, birini ise giden okuyucusu olarak tanımladığınızdan emin olun.

Her girişte olduğu gibi, yetkiler oluşturmak ve atamak gereklidir. Access Engine'de, **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 C:\MgtS\AccessEngine\AC\TAEExchange dizininde TAccExc_EXP.txt 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 kişi tarafından sıralanmaz, ancak yönetim modülünün aldığı kronolojik sırayla tüm ayırma işlemlerini içerir. Dosyadaki alan ayracı noktalı virgüldür.

Giriş Modeli 07 çeşitleri



Model çeşitleri:

07a	Maks. 56 katlı asansör
07b	Maks. 56 katlı asansör

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 çağdırdıktan 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

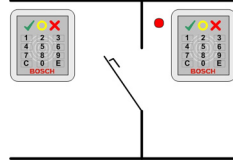


Olası sinyaller:

Giriş sinyalleri	Çıkış sinyalleri
Kapı sensörü	Kapı açıcı
"Çıkış talebi" düğmesi	Kapı uzun süredir açık
Giriş kilitlendi	Trafik ışığı yeşil
Geçiş tamamlandı	Alarm bastırma
	Kapı çok uzun süredir açık

Bariyer kontrolü için altta yatan bir kontrol (SPS) varsayılır. **Kapı modeli 5c**'nin aksine, bu giriş yapılandırılabilir 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
------------------	------------------

Kapı sensörü	Kapı açıcı
IDS: Kuruldu	IDS: Kurma
IDS: Kurulmaya hazır	IDS: Devre dışı bırakma [sadece DM 10e]
"Çıkış talebi" düğmesi	Kamera etkinleştirme
Cıvata sensörü	Kapı çok uzun süredir açık
Sabotaj	
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.

I-BPR okuyucuları: (örneğin DELTA 1010, INTUS 1600)

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.

BPR okuyucusu: (Wiegand 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.]

13.6

Özel girişler

13.6.1

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

Access Engine Sisteminin giriş yetkilendirme iletişim kutularında, bir kişinin yetkisine belirli katları atayabilirsiniz.

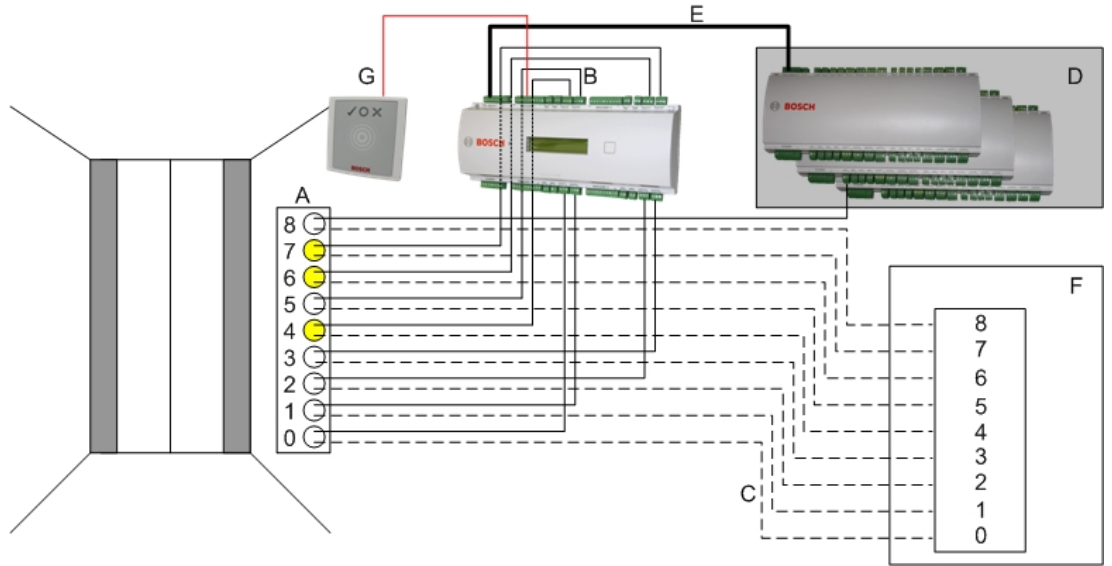
Asansör **07a** giriş modeli kullanılarak oluşturulduysa bir kart sahibi kimlik kartını gösterir ve izin aldığı katlar kullanılabilir hale gelir.

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:

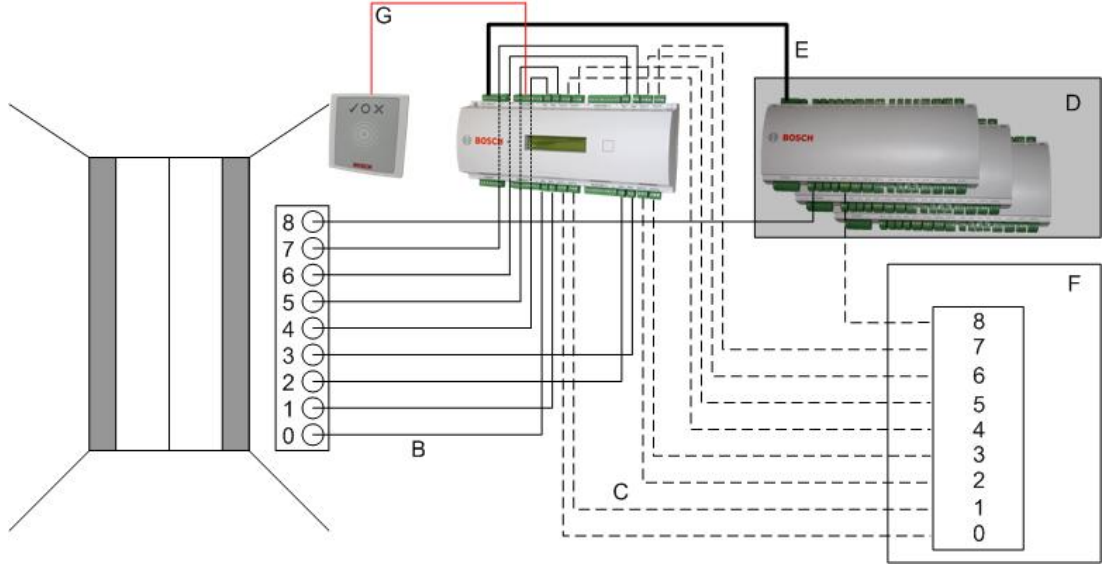
Aşağıdaki görüntüde, 07a kapı modeli kullanılan bir asansörün bağlantı şeması gösterilmektedir.



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.

GripID	Name	Description	target location	Division
65	Floor		Outside	Common
66	Floor-1		Outside	Common
67	Floor-2		Outside	Common
68	Floor-3		Outside	Common

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.

GrpID	Name	Description	target location	Division
65	Floor		Outside	Common
66	Floor-1			
67	Floor-2			
68	Floor-3			

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 sürelerle erişimi kısıtlar.

GrpID	Name	Description	target location	public access	Time model	Div
65	Floor-4		Building B - staff restaurant	<input checked="" type="checkbox"/>	TM-elevator	Co
66	Floor-5		Building B - kitchen	<input type="checkbox"/>	<no time modell>	Co
67	Floor-6		Building B - server room	<input type="checkbox"/>	<no time modell>	Co
68	Floor-7		Building B - fitness center	<input checked="" type="checkbox"/>	<no time modell>	Co

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

Name	Description	State	Division
Elevator 07a	Elevator 07a	<input checked="" type="checkbox"/>	Common
Elevator 07c	Elevator 07c	<input type="checkbox"/>	Common

Name	Description	From	To	State
Floor		Building C - extension	Building C - extension - 1. floor	<input checked="" type="checkbox"/>
Floor-1		Building C - extension	Building C - extension - 2. floor	<input checked="" type="checkbox"/>
Floor-2		Building C - extension	Building C - managing board	<input type="checkbox"/>
Floor-3		Building C - extension	Building C - secretary	<input checked="" type="checkbox"/>

13.6.2 Hırsız alarmlı kapı modelleri (DM14)

Hırsız algılama sistemlerini kurma ve devre dışı bırakma - DM 14

Giriş modeli 10'un aksine, DM 14 kurulabilir/devre dışı bırakılabilir.

New entrance
✕

Settings

Entrance model: DM 14a: Common door with entry and exit reader and IDS rearming (arming authorizati

Max. number outputs/authorizations: 8 / 4

Readers

1st inbound reader: WIE1 Reader: Wiegand Reader

1st outbound reader: WIE1 Reader: Wiegand Reader

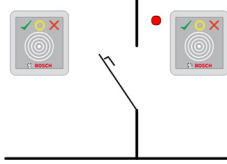
2nd inbound reader (optional): <No reader defined>

2nd outbound reader (optional): : <No reader defined>

OK
Cancel

Bir kurma alanı, girişin ilk sayfasındaki büyük harfle belirlenir. Bir kurma alanına bir giriş atayarak, bir okuyucudaki kurma işlemi, o alanın tüm girişlerine uygulanır.

Giriş Modeli 14



Model çeşitleri:

14a	Giriş ve çıkış okuyucusu ile IDS kurma/devre dışı bırakma özelliğine sahip normal kapı
14b	Giriş, basmalı düğme ve IDS kurma/devre dışı bırakma özelliğine sahip normal kapı

Olası sinyaller:

Giriş sinyalleri	Çıkış sinyalleri
Kapı sensörü	Kapı açıcı
IDS: Kuruldu	IDS: Kurma
IDS: Kurulmaya hazır	Kamera etkinleştirme
"Çıkış talebi" düğmesi	Kapı çok uzun süredir açık
Cıvata sensörü	
Sabotaj	
IDS: Kurma talebi düğmesi	

Kapı modeli 14 ile, IDS'nin (hırsız algılama sistemi) alandaki herhangi bir okuyucudan kurulabileceği güvenli alanlar oluşturmak mümkündür. Böyle bir durumda **IDS armed** (IDS kurulu) ve **IDS ready to arm** (IDS kurmaya hazır) sinyallerinin her girişte çoğaltılması gerekir. Kapı modeli 10'un aksine, kapı modeli 14'te tuş takımı olan veya olmayan okuyucular kullanabilir. Diğer bir fark, kurma/devre dışı bırakma yetkilerinin atanmasıdır. Yalnızca uygun yetkilere sahip kart sahipleri, kurma/devre dışı bırakma işlemi yapabilir.

Klavye okuyucuları bulunması durumunda, kurma ve devre dışı bırakma işlemleri kapı modeli 10 ile gerçekleştirilir.

Klavye bulunmayan okuyucularda, kurma işlemi PIN kodunu girilerek gerçekleştirilmez, ancak okuyucunun yanındaki tuş takımı okuyucularının 7 tuşuyla aynı işleve sahip bir anahtar kullanılarak gerçekleştirilir. Bu anahtarı kullandıktan sonra, alarm cihazının durumu okuyucunun renkli LED'leriyle gösterilir:

- Devre dışı bırakıldı = dönüşümlü yeşil ve kırmızı ışık
- Kurulu = sürekli kırmızı ışık

Uygun şekilde yetkilendirilmiş bir kart göstererek kurun.

Anahtarı kullanarak ve uygun şekilde yetkilendirilmiş bir kart göstererek devre dışı bırakın.

Kapı açma devre dışı bırakmadan sonra otomatik değildir, ancak kartın tekrar gösterilmesini gerektirir.

Giriş Modeli 14 ile kurmaya ilişkin yetkiler

Giriş 14 iletişim kutusunun ilk sekmesi, "Kurma alanları" oluşturmak için ek bir parametre içerir. Birkaç model 14 Girişi aynı kurma alanına başvurabilir, böylece bu alandaki herhangi bir okuyucu IDS'yi (hırsız algılama sistemi) kurabilir veya devreden çıkarabilir.

Bu durumda **IDS armed** (IDS kurulu) ve **IDS ready to arm** (IDS kurulmaya hazır) sinyallerinin diğer girişlere ait girişlerde çoğaltılmaları gerekir. Aynı kurma alanı için ikinci bir giriş modeli oluşturulduğunda, cihaz düzenleyici çoğaltma işlemini sizin için yapar. İkinci kapının sinyalinin açıklaması, birinci giriş modelinin ilgili sinyalinin sinyal numarasıyla genişletilir: Ör. 1:04 [= 1. karttaki dördüncü sinyal]

Board	T...	entrance	Input signal	entrance	Output signal
AMC 4-R4	01	DM 14b	Door contact	DM 14b	Release do
AMC 4-R4	02	DM 14b	1:04:IDS armed	DM 14b	Arming IDS
AMC 4-R4	03	DM 14b	1:05:IDS ready t...		
AMC 4-R4	04	DM 14b	Arm IDS		
AMC 4-R4	05	DM 14b	"Request to exit"...		
AMC 4-R4	06	DM 14b-1	Door contact	DM 14b-1	Release do

Giriş modeli 14'ün bir örneğini oluşturduktan sonra **Arming authorizations** (Kurma yetkileri) ek sekmesi bunu oluşturarak üretilen yetkileri gösterir. Kullanıcı kurma/devre dışı bırakma yetkileri için adları serbestçe seçebilir.

DM 14a Arming authorizations Terminals

Name of disarming authorization:

Description:

Name of the arming authorization:

Description:

Yetkileri sıralarken, giriş modeli 14'ün oluşturulan tüm örnekleri **Access authorizations** (Giriş yetkileri) ve **Area/Time Authorizations** (Alan/Zaman Yetkileri) iletişim kutularının **Arming** (Kurma) sekmesinde belirtilir. Kurma ve devre dışı bırakma yetkileri ayrı olarak atanabilir.

Division: New division 2

Authorization name:

Description:

Entrance Time management Elevator Parking lot Arming

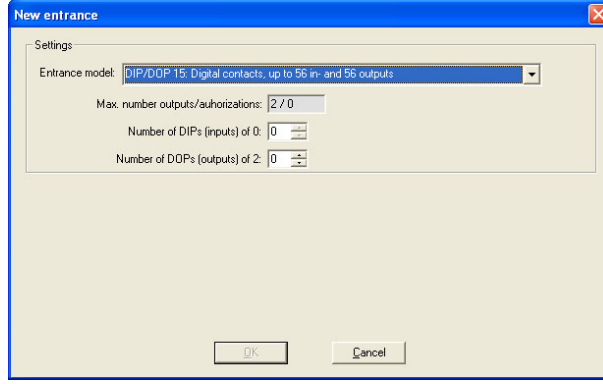
Name	Description	From	To	Armed	Disarmed	Division
Management	DM 14a	Building C - extension	Building C - management	✓	✓	Common
Server room	DM 14a	Building C - extension	Building C - secretary	✓	✓	Common
DM 14a	DM 14a	Outside of the system	Building C	✓	✓	Common
Building A	DM 14a	Outside of the system	Building A - floor 1 - right	✓	✓	Common

13.6.3

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 BIS'in grafiksel kullanıcı arabiriminde 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.

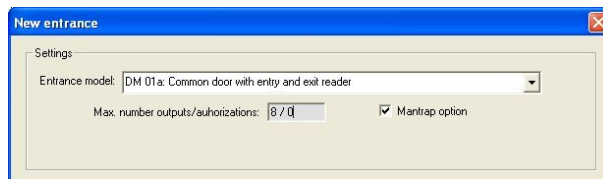
Bir yeniden başlatma işleminin her zaman DOP'nin buna manuel olarak atanan son duruma sıfırlanmasını sağlamak için, cihaz ağacında DOP'yi seçin ve ana penceredeki **Keep state** (Durumu koru) onay kutusunu seçin.

13.6.4

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.



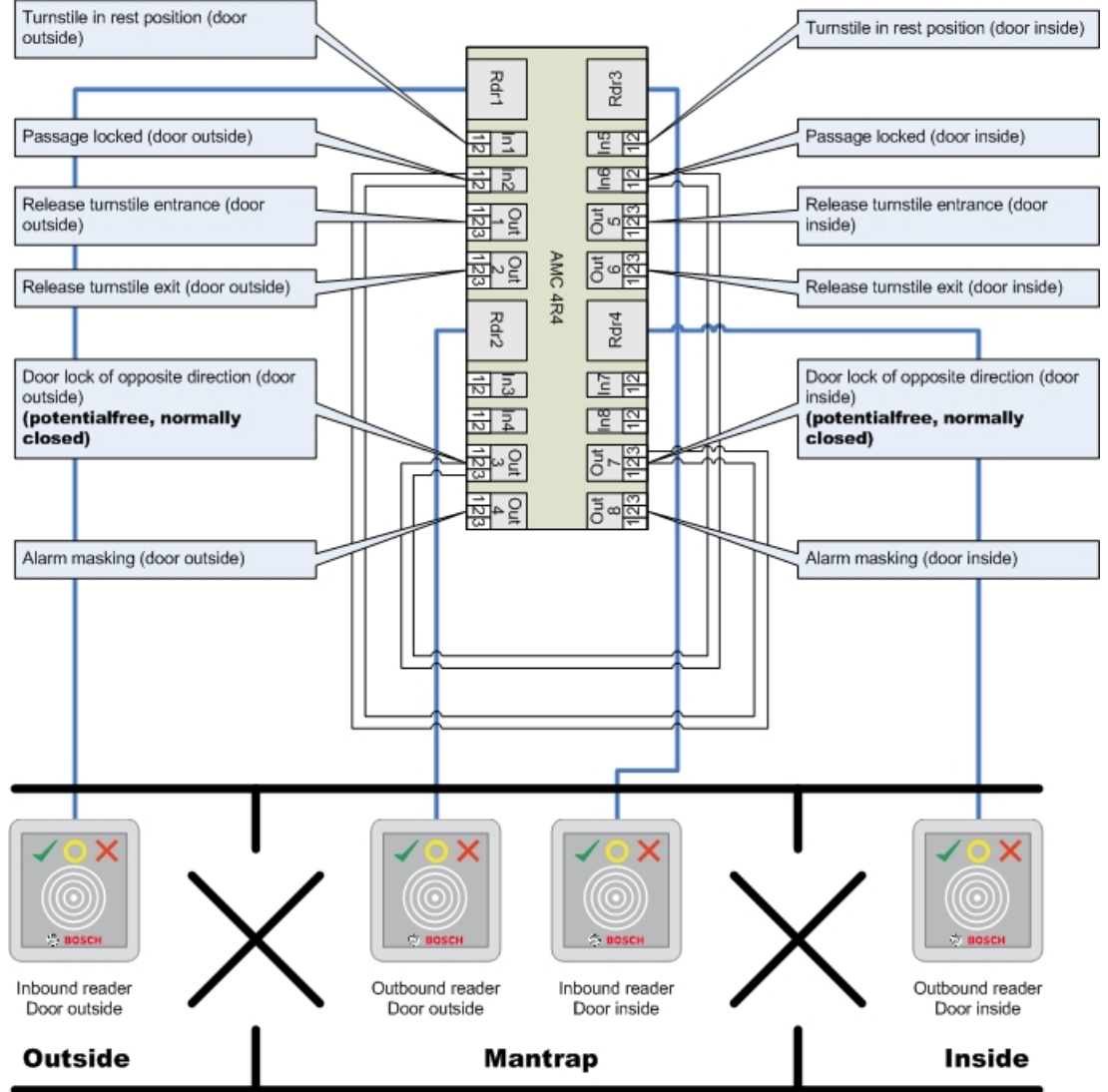
01 ve 03 numaralı tüm model tiplerini birleştirebilirsiniz, ancak bu seçeneği tuzaka ait iki girişte de ayarlayabilirsiniz.

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 erişimin 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.

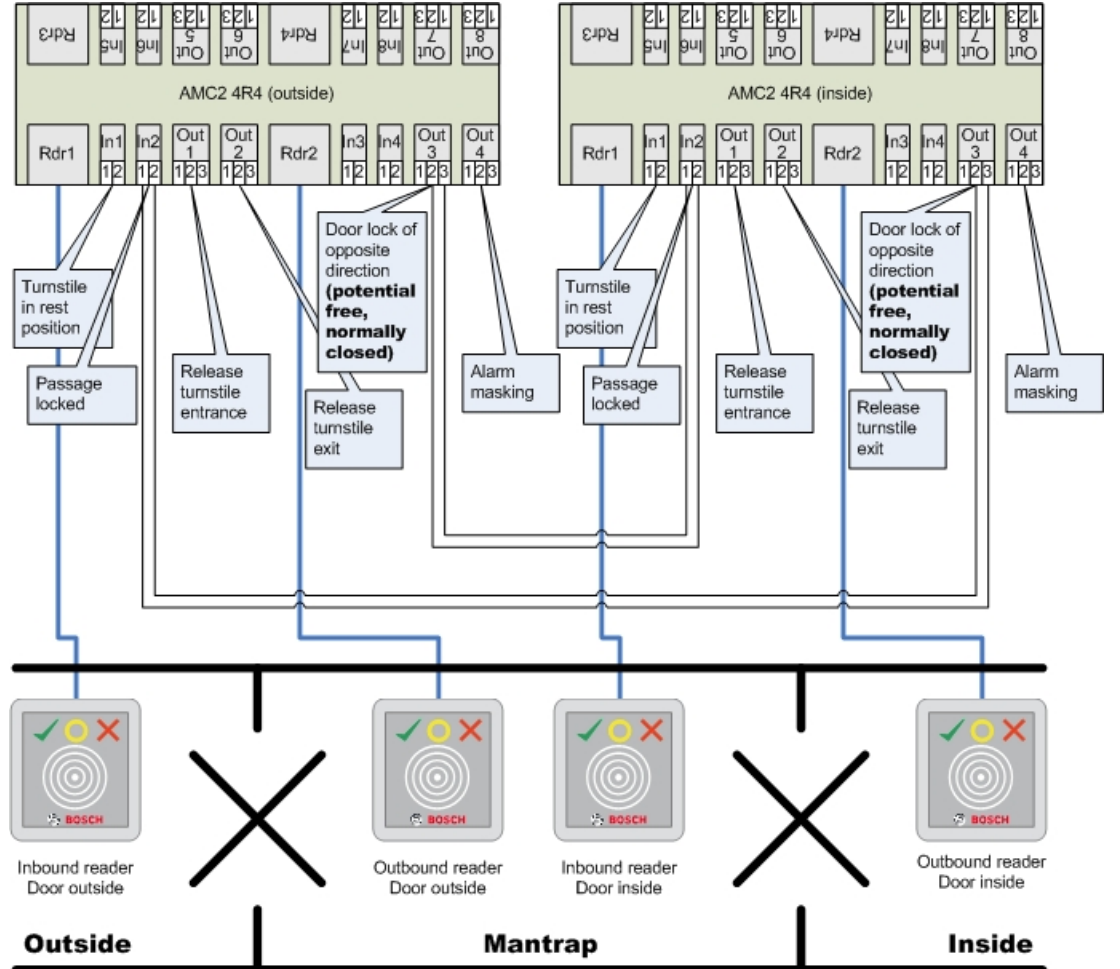


Uyarı!

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.

13.7

Kapılar

Kapı Yapılandırma: Genel Parametreler

Şekil 13.1:

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).	Bu salt okunur bir alandır. Cihaz hiyerarşisindeki her kapı için cihaz düzenleyici DevEdit'te bölümlere atamalar yapılır
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.

Kapı Yapılandırma: Seçenekler

The screenshot shows a configuration window for a door. It includes several settings with checkboxes and dropdown menus:

- Out of order:
- Unlock door: 0 = Door is in normal mode (dropdown)
- Time model: (no time model) (dropdown)
- Max. lock activation time: 50 / 1/10 sec.
- Min. lock activation time: 10 / 1/10 sec.
- Door inertia: 0 / 1/10 sec.
- Alarm open time: 300 / 1/10 sec.
- Door strike mode: 1 = Disable "request to exit" button immediately (dropdown)
- Door contact:
- Bolt contact:
- Extended door open time (handicapped persons):

Parametre	Olası değerler	Açıklamalar
Manuel çalıştırma	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.
Unlock door (Kapının kilidini aç)	0 = Kapı normal modda 1 = Kapının kilidi açıldı 2 = Kapının kilidi zaman modeline göre açıldı	0 = normal mod (varsayılan) - kapı kimlik bilgilerinin giriş haklarına bağlı olarak kilitletir 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.

	<p>3 = Kapı ilk geçişten sonra zaman modeline göre açık</p> <p>5 = Kapı uzun süreli olarak engellendi</p> <p>6 = Kapı zaman modeline göre engellendi</p>	<p>3 = ilk kişinin erişimi olana kadar zaman modeli etkin olduğu sürece kilitlidir - ardından zaman modeli etkin olduğu sürece açıktır.</p> <p>5 = manuel olarak engeli kaldırılana kadar engellenir.</p> <p>6 = zaman modeli etkin olduğu sürece kilitlidir - kapı kontrolü yoktur, kapı zaman modeli etkinken kullanılamaz.</p>
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.
Max. lock activation time (Maks. kilit etkinleştirme süresi)	0 - 9999	1/10 saniye olarak kapı açıcının etkinleştirilmesi için gereken zaman aralığı - varsayılan: Kapılar için 50, döner kapılar için 10 (03) ve bariyerler için 200 (05c veya 09c).
Min. lock activation time (Min. kilit etkinleştirme süresi)	0 - 9999	Kapı açıcının etkinleştirilmesi için saniyenin 1/10'u olarak minimum zaman aralığı. Elektromanyetik kilitlerde manyetikliği gidermek için biraz zamana ihtiyaç vardır - varsayılan: 10.
Door inertia (Kapı eylemsizliği)	0 - 9999	Etkinleştirme süresi geçtikten sonra, kapı bu zaman aralığında alarm verilmeden saniyenin 1/10'unda açılabilir. Hidrolik kapıların basınç oluşturmak için biraz zamana ihtiyacı vardır - varsayılan: 0.
Alarm open time (Alarm açık kalma süresi)	0 - 9999	Kapı bu zaman aralığından sonra açık kalırsa saniyenin 1/10'unda bir mesaj gönderilir (kapı çok uzun süre açık kaldı) - varsayılan: 300. 0 = zaman aşımı yok, mesaj yok
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)
Door contact (Kapı kontağı)	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)
Bolt contact (Cıvata kontağı)	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	0 = kapının cıvata kontağı yok (= varsayılan) 1 = kapının cıvata kontağı var. Kapı açıldığında veya kapatıldığında bir mesaj gönderilir.

Uzatılmış kapı açılma süresi (engelli kişiler)	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	0 = kilit etkinleştirme süresi normal. 1 = kilit etkinleştirme süresi, sistem genelinde EXTIMFAC parametresinde ayarlanan faktör ile genişletilir. Bunun amacı, engelli kişilere kapıdan geçmek için daha fazla zaman vermektir. (=varsayılan)
--	---	---

Kapı Yapılandırma: Olaylar

The following events will be available for use under "Associations":

Intrusion:

Door state open/close:

Parametre	Olası değerler	Açıklamalar
Intrusion (Hırsız alarmı)	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	0 = hırsız alarmı mesajı yok. Bu, bir kapı içeriden serbestçe açılabilirse faydalıdır. 1 = Yetkisiz açılmanın ardından bir mesaj tetiklenir. Bir sonraki mesaj sonraki kapanışı gösterir. (varsayılan)
Door state open/closed (Kapı durumu açık/kapalı)	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	0 = "kapı açık" mesajı gönderilmez (varsayılan) 1 = açılış veya kapanıştan sonra bir mesaj gönderilir.

13.8

Readers (Okuyucular)

Okuyucu Yapılandırma: Genel Parametreler

I-BPR K Options Door control Additional settings Cards

Name: I-BPR K

Description: I-BPR K

Division: Common

Type: I-BPR K

Activate encryption: Supported only by OSDP v2 readers.

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

I-BPR K | Options | Door control | Additional settings | Offline locking system | Key cabinet | Cards

PIN code required:

Time model for PIN codes:

Access also by PIN code alone:

Reader terminal / bus address:

Attendant required:

Membership check:

Membership time model:

Group access:

Deactivate reader beep if access granted:


Deactivate reader beep if access denied:

VDS - Mode:

Max. time for arming: 1/10 Sec.

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	Bu alan sadece okuyucu bir giriş cihazına sahipse etkindir. Karttaki yetkiler ve giriş sırası (etkinse) gibi kontrollerin PIN'in doğruluğuna göre öncelikli olduğunu unutmayın.

	sadece zaman modelinin dışındaysa gerekli	
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'in (Üyelik kontrolü) sadece sistemde önceden tanımlanmış kart tanımlarıyla (gri arka planlı) çalıştığını, özelleştirilmiş tanımlarla çalışmadığını unutmayın. 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.
 <p>"Deactivate Reader Beep" (Okuyucu Bip Sesini Devre Dışı Bırak) işlevleri ilgili okuyucu üretici yazılımına bağlıdır. Bazı okuyucuların üretici yazılımı bu işlevi desteklemeyebilir.</p>		
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
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

I-BPR K
Options
Door control
Additional settings
Cards

Reader blocking:

Time model to block reader:

Office mode:

Manual operation:

Check time model upon access:

Additional verification:

Host request timeout: 1/10 sec.

Open door if no answer from host:

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 - <i>Time model to block reader</i> (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 Office mode'da (Ofis modu) kullanılmasını sağlar,
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 BVMS veya BIS 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 (<i>Area Change</i> (Alan Değişikliği) veya <i>Person Countings</i> (Kişi Sayıları) ile çalışmaz). Bu kontrol sadece Ana bilgisayar doğrulaması

		<p>devre dışıysa (0) ve <i>Open door if no answer from host</i> (Ana bilgisayardan yanıt alınamazsa kapıyı aç) etkinse (1) devrededir.</p> <p>1 - 9999 = okuyucuyu kullanmak için bir BIS sorgusu gereklidir. Sorgunun, belirtilen süre içinde yanıtlanması gerekir. Süre dolduğunda, AMC Open door if no answer from host (Ana bilgisayardan yanıt alınamazsa kapıyı aç) parametresini kontrol eder ve kendisi için karar verir. Değerler saniyenin 1/10'udur. (Varsayılan = 30)</p>
Open door if no answer from host (Ana bilgisayardan yanıt alınamazsa kapıyı aç)	<p>0 = devre dışı bırakıldı (onay kutusu işaretli değil)</p> <p>1 = etkin (onay kutusu işaretli)</p>	<p>Bu kontrol, sadece Host verification (Ana makine doğrulaması) ayarlandıysa etkindir.</p> <p>0 = bir ana bilgisayar kararına ihtiyaç varsa ancak alınamıyorsa kapıyı açmaz (çevrimdışı işlem).</p> <p>1 = AMC'den serbest bırakılabiliyorsa zaman aşımından sonra kapıyı açar. (=varsayılan)</p>
Check parking ticket credits (Otopark bilet kredilerini kontrol et)	<p>0 = devre dışı bırakıldı (onay kutusu işaretli değil)</p> <p>1 = etkin (onay kutusu işaretli)</p>	Etkinse (1) park bileti kredileri kontrol edilir.
Check overstayed parking (Uzun süreli parkı kontrol et)	<p>0 = devre dışı bırakıldı (onay kutusu işaretli değil)</p> <p>1 = etkin (onay kutusu işaretli)</p>	Etkinse (1) park süresinin çok uzun olup olmadığı kontrol edilir.

Okuyucu Yapılandırma: Ek Ayarlar

I-BPR K Options Door control Additional settings Cards

Access sequence check: 0 - Deactivated

Time management:

Double access control

Enable:

Door group ID: ..

Anti-Pass-Back timeout: 5 minutes

Random screening

Random screening:

Screening rate: ..

Timeout random screening: .. Minutes

REX button active when IDS armed:

Read permanently:

Parametre	Olası değerler	Açıklamalar
Access sequence check (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 (BİLİNMIYOR) 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.



BIS platformunda, genel olarak tüm giriş sıralamasını kontrol etmek veya devre dışı bırakmak için bir MAC komutu vardır.

<p>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.</p> <p>Not: Bu komut, sadece Enable access sequence (Giriş sırasını etkinleştir) parametresinin ayarlandığı okuyucular için erişim sırasını değiştirebilir. <i>Tüm okuyucular için giriş sırası kontrolünü devre dışı bırakmaz/etkinleştirmez.</i></p>		
Time Management (Zaman Yönetimi)	0 = devre dışı bırakıldı (onay kutusu işaretli değil) 1 = etkin (onay kutusu işaretli)	Etkinse (1) Ace işlemi, zaman ve devam sistemi 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	Geniştirilmiş 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. Bu parametrenin, bir basmalı düğmenin yerine bir okuyucu kullanıldığında da ayarlanması gerekir.
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

WIE1K Reader | Options | Door control | Additional settings | Offline locking system | Biometrics | Key cabinet | Cards

Card validation

Motorized card reader:

Withdraw card:

Triggering criteria:

- Blocked card
- Visitor card
- Card is blacklisted
- Invalid time model
- Invalid area/time model
- No authorization
- Always collect
- Collect visitor cards on collecting date
- Collect visitor cards on last day of validity
- Collect other cards (no visitor cards) on collecting date
- Collect other cards (no visitor cards) on last day of validity
- Time model defined and invalid, independent of access and reader parameters
- Area/Time model defined and invalid, independent of access and reader parameters

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.

13.8.1

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.

13.9

Yalnızca PIN'le giriş

Arka plan


Tuş takımlı okuyucular yalnızca PIN'le girişe izin verecek şekilde yapılandırılabilir. Okuyucular bu şekilde yapılandırıldığında, BIS 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) bölümünde, **Assign virtual cards (PIN)** (Sanal kart (PIN) ata) onay kutusunu seçin.
5. Yaptığınız değişiklikleri kaydetmek için  simgesine veya **Apply**'a (Uygula) tıklayın

Tüm 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) bölümünde, 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** bölümünden okuyucuyu seçin.
Workstations (İş istasyonları) bölümünün sağında özel bir okuyucu yapılandırma bölümü görünür.
5. **Card usage default** (Kart kullanım varsayılana) 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

13.10 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.

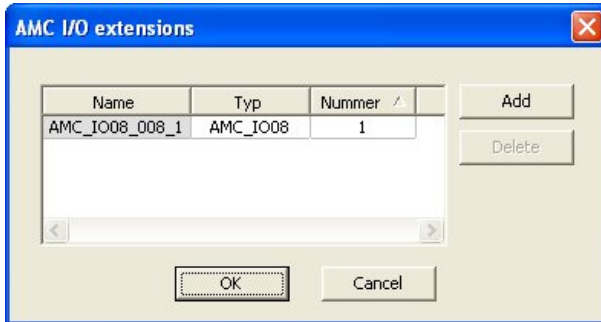


Uyarı!



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

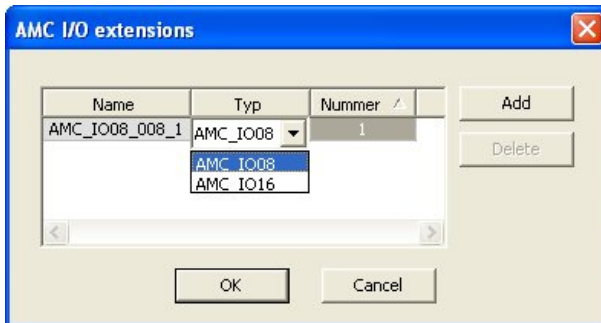
Genişletmelerin oluşturulması için bir seçim iletişim kutusu görüntülenir.



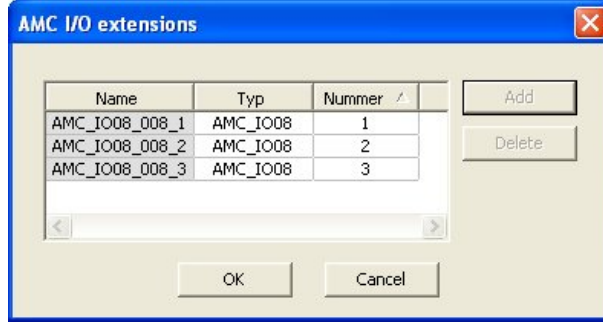
AMC-EXT'nin iki çeşidi vardır:

- 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. Genişletme 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 bulunduğu için, 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.

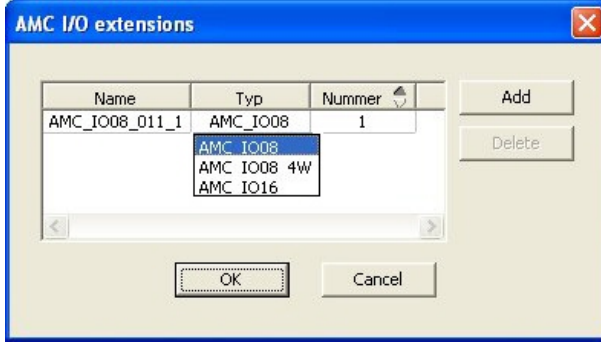
Sistemde bir AMC2 4W-EXT oluşturmak için Gezgini'de istediğiniz ana AMC2 4W'ye sağ tıklayın ve bağlam menüsünden **New object** (Yeni nesne) > **New extension board**'u (Yeni genişletme kartı) seçin.



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 "Ortak"	Bu salt okunur alan sadece Divisions (Bölümler) özelliğinin lisanslandığı ve kullanıldığı durumlarda geçerlidir.

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

Geniřletme kartlarını silme

Bir genişletme kartı yalnızca arayüzlerinden hiçbirisi 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

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

14 Personel verileri için Özel Alanlar

Giriş

Personel için veri alanları birçok şekilde özelleştirilebilir:

- **Visible** (Görünür) olup olmadıkları, yani ACE istemcisinde görüntülenip görüntülenmedikleri
- **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.)
- ACE istemcisinde 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.

14.1 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

Overview Bu sekme ve alt sekmeleri (**Address (Adres)**, **Contact (İletişim)**, **Additional (Genel Bakış) 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 ACE İstemcisindeki hangi sekmelerde görüneceğine ilişkin kabaca bir WYSIWYG genel bakışı içerir.

Details Bu sekmede, her önceden tanımlanmış veya kullanıcı tanımlı veri alanı için bir (Ayrıntılar) 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 yansıtabilecek şekilde serbestçe yazılabilir.

Etiket metni	Açıklama
Field type (Alan tipi)	<p>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.</p> <ul style="list-style-type: none"> - Text field (Metin alanı) <ul style="list-style-type: none"> - 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) <ul style="list-style-type: none"> - Sunulan metin alanındaki birleşik kutunuz için geçerli değerleri girin. Bunları virgül veya satır başı karakterleriyle ayırın. - Numerical input (Sayısal giriş) <ul style="list-style-type: none"> - Sunulan döndürme kutularındaki sayısal giriş için minimum ve maksimum değerlerinizi girin. - Building control 1 (Bina kontrolü 1) ve Building control 2 (Bina kontrolü 2) <ul style="list-style-type: none"> - 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)	Benzersiz olmayan reddedilen veri alanı içerikleri oluşturmak için bu onay kutusunu seçin. Örneğin, personel numaraları tüm çalışanlar için benzersiz olmalıdır.
	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 bölümü vardır.

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

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

14.2

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.

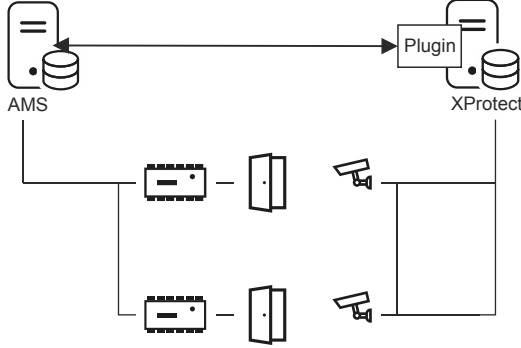
15

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.

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 İçerme Sihirbazı görünür.
4. **Local Machine**'i (Yerel Makine) **Store Location** (Saklama Konumu) olarak seçin ve **Next**'e (İleri) tıklayın
5. **Place all certificates...**'i (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) tıklayın **Associate 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.

16

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.

16.1

Tehdit Seviyesi Yönetimine İlişkin Kavramlar

- **Threat** (Tehdit), bir kartlı geçiş sistemindeki girişlerin bazılarında 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. Yönlendirmeli kapılar (ör. turnikeler ve insan tuzakları) yalnızca çıkış yapılmasına izin verir.
- 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**'inin (Güvenlik profilleri) bir özneliğidir. Her tehdit seviyesi Ana Giriş Kontrol Cihazı'nın (MAC) okuyucularını atanmış 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 öznelik 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.

16.2

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.

16.3

Cihaz düzenleyicideki yapılandırma adımları

Bu bölümde cihaz düzenleyicide gerekli olan yapılandırma adımları açıklanmaktadır.

16.3.1


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.

16.3.2

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 bölme 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) bölümündeki **Threat level** (Tehdit seviyesi) bölümü **State** (Durum) sütunundaki **undefined** (tanımlanmadı) değeriyle birlikte daha önce oluşturulan tehdit seviyeleriyle doldurulur.
- 3. **Door security profile** (Kapı güvenliği profili) bölümünde, bu profilin atanacağı kapı türü için bir ad girin.
 - Yeni profil adı **Selection** (Seçim) bölümünde görünür. İstenirse bu, söz konusu bölümde **Delete**'e tıklanarak yapılandırmadan silinebilir.
- 4. (İsteğe Bağlı) Operatörlerin profili doğru olarak atamasına yardımcı olmak için profile ait bir açıklama girin.
- 5. Bu profil yönlendirmeli kapılara (örneğin, turnike veya insan tuzağı) 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

16.3.3

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 bölme 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) bölümü **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) bölümünde, bu profilin atanacağı okuyucu türü için bir ad girin.
 - Yeni profil adı **Selection** (Seçim) bölümünde görünür. İstenirse bu, söz konusu bölümde **Delete**'e tıklanarak yapılandırmadan silinebilir.
- 4. (İsteğe Bağlı) Operatörlerin profili doğru olarak atmasına 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.

16.3.4

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 bölümünde 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** bölümünde, 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 görüldüğünü 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.

16.3.5

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.

16.4

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.

16.4.1

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)

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?
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)

16.4.2


Kişi türüne kişi güvenlik profili atama

İletişim yolu

- **Main menu** (Ana menü) > **System data** > **Person Type** (Kişi Türü)
- **ACE client** (ACE istemcisi) > **System data** (Sistem verileri) > **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

16.5

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 116*
- *Personel verilerini oluşturma ve yönetme, sayfa 117*

17

Personel verilerini oluřturma 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?

17.1

Kişiler

Genel olarak yönetilir onay kutusu seçili olan kişilerin verileri, yalnızca ek **Genel Yönetici** hakkına sahip operatörler tarafından düzenlenebilir. Bu hak, BIS Yapılandırma Tarayıcısı'nın operatör iletişim kutusunda ayarlanır.

Korumalı veriler şunlardır:

- **Açıklamalar** sekmesi ile **Fazladan bilgi** sekmesindeki özel olarak tanımlanan ek bilgi alanlar hariç **Kişiler** iletişim kutusundaki tüm veriler.
- **Kartlar** iletişim kutusundaki tüm veriler.

- **PIN Kodu** iletiřim kutusundaki tm veriler.
Bu kiřilerin tm diđer verileri herhangi bir operatr tarafından dzenlenebilir.

Ařađıdaki tabloda kaydedilebilecek ana veri trleri gsterilmektedir. Neredeyse tm alanlar isteđe bađlıdır. Zorunlu alanlar kullanıcı arayznde altı çizili etiketlerle aıka iřaretlenir.

Sekme	Alan adı
İletiřim kutusu bařlıđı	Name (Ad)
	First name (Ad)
	Birth name (Kızlık soyadı) (bazı kltrlerde dođum adı olarak anılır)
	Personnel no. (Personel no.)
	Date of birth (Dođum tarihi)
	Employee ID (alıřan kimliđi) (Kiři tr olarak da bilinir)
	Gender (Cinsiyet)
	Company (řirket)
	Title (Bařlık)
	ID card no. (Kimlik kartı no.)
	Car license no. (Araba ruhsatı no.)
Address (Adres)	Zip code (Posta kodu) (bazı kltrlerde zip kodu olarak anılır)
	Cadde, no.
	lke, eyalet
	Milliyet
İletiřim	Diđer telefon
	řirket telefonu
	řirket faksı
	Cep telefonu
	Telefon
	E-Posta
	Web sayfası adresi
Ek Kiři Verileri	Lakap (bazı kltrlerde diđer ad olarak kullanılır)
	Dođum yeri
	Medeni durum
	Resmi kimlik kartı
	Kimlik kartı no.
	Geerlilik bitiři

	Yükseklik
Ek Őirket Verileri	Departman
	Konum
	Maliyet merkezi
	İř unvanı
	Eřlik eden (Eskort)
	Ziyaret nedeni
	Açıklamalar
Açıklamalar	(Kiři 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.

17.1.1

Kart kontrolü/bina kontrolü seçenekleri

17.1.2

Fazladan bilgi: Kullanıcı tanımlı bilgileri kaydetme

Extra info (Fazladan bilgi) sekmesini, diđer sekmelerde verilmeyen [ek alanları](#) tanımlamak için kullanın. Hiçbir ek alan tanımlanmadıysa sekme boş kalır.

17.1.3

İmzaları kaydetme

İmzaları almak için sistemde Signotec Őirketi ürünü bir imza alma pedi bađlı ve yapılandırılmıř olmalıdır. Emin olamazsanız sistem yöneticinize danıřın.

1. **Signature** (İmza) sekmesine tıklayın
2. Yeni bir imza kaydetmek için **Capture Signature** (İmza Al) düđmesine tıklayın.
3. Özel kalemimi kullanarak doğrudan imza alma pedinin üzerinde imzalayın.
4. Onaylamak için imza alma pedindeki onay işaretine tıklayın.
Yeni imza artık ekranda görüntülenir (Büyütölmüş görünüm için imzaya tıklayın).

İlgili prosedürler:

- Mevcut bir imzanın üzerine yazmak için de **Capture Signature** (İmza Al) düđmesine tıklayın.
- Mevcut bir imzayı silmek için **Delete Signature** (İmzayı Sil) düđmesine tıklayın.

17.1.4


Parmak izi verilerini kaydetme

Ön gereksinimler

- Biyometrik giriş kontrolü gerçekleřtirmek 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. Kiři 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 kiři, iř istasyonunuza baėlı ve bunun için yapılandırılmıř bir parmak izi okuyucunun önündedir.
- Operatör olarak doğrudan kaydedilen, yani parmak izleri giriş için biyometrik kimlik bilgileri olarak kaydedilecek kiřiyle doğrudan iletiřim kurmanız gerekir.
- Parmak izlerinin verimli biçimde alınmasını saėlamak için kullanılan belirli bir okuyucuda parmaėınızı nasıl art arda göstereceėinizle ilgili bilgi sahibi olmanız gerekir.

Giriř için parmak izi kaydı prosedürü

1. Parmak izleri iletiřim kutusuna gidin: **Personnel data** (Personel verileri) > **Persons** (Kiřiler) > sekme: **Fingerprints** (Parmak izleri) ve veritabanında kaydedilen kiřiyi oluřturun veya bulun.
2. Kaydedilen kiřiye parmak izi okuyucuda düzenli giriş için hangi parmaėını kullanmak istediėini sorun.
3. El řemasında ilgili parmaėı seçin.
Sonuç: Parmak ucu soru iřaretiyle iřaretlenir.
4. **Parmak izini kaydet** düėmesine tıklayın.
5. Kaydedilene okuyucuda parmaėını göstermesi için gereken talimatları verin.
Örnek talimatlar ařaėıdaki el řemasındaki iletiřim bölmesinde okunabilir, ancak farklı okuyucu türleri farklı prosedürler gerektirebilir.
6. Parmak izi bařarıyla kaydedilirse bir onay penceresi görünür.

7. Bir **Tanım modu** seçin; bu, bir parmak izi okuyucusunun kaydedilen kişiden erişim isteğinde bulunduğunda hangi kimlik bilgilerini talep edeceğini belirler. Burada ayarlanan modun yalnızca **Kişiyeye bağılı 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** (Kişiyeye bağılı doğrulama) seçeneğiyle yapılandırılmışsa çalışacağını unutmayın. Emin olamazsanız sistem yöneticinize danışın.

Baskıyı işaret etmek için parmak izi kaydı prosedürü

Ön gereksinimler:

- 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 kişiyeye 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.

17.2

Őirketler

- Bu iletiŐim kutusu yeni Őirketler oluŐturmak ve mevcut Őirket verileri deęiŐtirmek veya silmek iin kullanılabilir.
- Őirketin adı ve kısa adı girilmelidir. Kısa ad, benzersiz olmalıdır.
- Bir Őirketin **Persons** (KiŐiler) iletiŐim kutusuna girilmesi zorunluysa bu Őirketin personel kayıtlarını oluŐturmaya alıŐmadan nce bu iletiŐim kutusunda Őirketi oluŐturun.
- Personel kayıtları hala Őirkete atanıŐ durumdaysa Őirketler sistemden silinemez.

17.3

Kartlar: Kimlik bilgileri ile izin oluŐturma ve atama

Bu iletiŐim kutusunun amacı **kartlar**, **giriŐ yetkileri** ya da **giriŐ profilleri** adı verilen giriŐ yetkisi paketlerini personel kayıtlarına atamaktır.

GiriŐ yetkileri ve profilleri kartlara deęil kiŐilere atanır.

Bir kiŐiye atanan yeni kartlar, o kiŐiye daha nce atanan giriŐ yetkilerini alır.

Not: Yetkileri paket haline getirmek iin giriŐ profillerini kullanma

Tutarlılık ve kolaylık iin giriŐ yetkileri tek olarak atanmaz, ancak genellikle **GiriŐ profilleri** halinde paketlenerek bu Őekilde atanır.

- Main menu (Ana men): > **System data (Sistem verileri)** > **Access profiles** (GiriŐ profilleri)

Kart listesi

Kartlar iletiŐim kutusunda seilen kiŐinin sahip olduęu bir kart listesi grntlenir. Listede nitelikler arasında Őunlar gsterilir:

- Kart kullanımını tipi.
- Kartın yapılandırılan bir evrimdıŐı kilitleme sistemi iin kullanılıp kullanılmayacaęına iliŐkin bir iŐaret.
- Kartın art arda geersiz PIN kullanılması nedeniyle engellenip engellenmedięi. Bu durum zellikle vurgulanır.
- Kartın oluŐturulma tarihi
- Kartın son kullanma tarihi (Toplama tarihi).

Not: Motorlu bir kart okuyucu kullanılıyorsa fiziksel olarak son kullanma tarihi geen bir kartı alıkoyabilir. Aksi takdirde kart yalnızca geersiz kılınır.

- Kartın yazdırıldıęı tarih ve yazdırılan kart sayısı.
- Kod verilerinin ayrıntıları.

Administered globally (Genel olarak ynetilir) seeneęi

Administered globally (Genel olarak ynetilir) (fotoęraf erevesinin yanındaki onay kutusu) ayarına sahip kiŐilerin verileri, yalnızca ek **Global Administrator** (Genel Ynetici) hakkına sahip operatrler tarafından dzenlenebilir.

AŐaęıdaki veriler, bu hakka sahip olmayan operatrler iin salt okunurdur:

- **Remarks, Extra info** (Aıklamalar, Fazladan bilgi) sekmeleri ve zel alanlar haricinde **Persons** (KiŐiler) iletiŐim kutusundaki tm veriler.
- **Cards** (Kartlar) iletiŐim kutusundaki tm veriler.
- **PIN Code** (PIN Kodu) iletiŐim kutusundaki tm veriler.

Bu **Global Administrator** (Genel Ynetici) hakkı aŐaęıdaki 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).

17.3.1

Kişilere kart atama

Giriş

Giriş kontrolü altındaki bir kişinin, sahibine Cards (Kartlar) iletişim kutusunda atanmış bir kartı veya başka elektronik kimlik bilgileri olması gerekir.

Kart numaraları, bir kayıt okuyucusu aracılığıyla manuel veya otomatik olarak atanabilir.

İletişim yolu

Main menu (Ana menü) > **Personnel data** (Personel verileri) > **Cards** (Kartlar)

Ön koşul

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 okuyucu kullanma

Ön koşul

Çalışmakta olduğunuz iş istasyonuna bir kayıt okuyucusu bağlandı.

Kayıt prosedürü

1. Yapılandırılmış bir kayıt okuyucusunu seçmek için **Record card** (Kartı kaydet) düğmesinin sağ tarafındaki  düğmesine tıklayın.
2. **Record card** (Kartı kaydet) düğmesine basın ve ekrandaki talimatları izleyin.

- Okuyucu türüne baėlı olarak artık kart ayrıntılarını bir iletiřim kutusuna girebilir veya okuyucuya göstererek verileri karttan okuyabilirsiniz.

Kart deėiřtirme prosedürü

- Listeden bir kart seçin.
- Change card** (Kartı kaydet) düğmesine tıklayın
- Açılır pencerede kart verilerini düzenleyin ve kaydetmek için OK'e (Tamam) tıklayın.

Kartları silme

- Listeden bir kart seçin.
- Bir kişinin bir karta olan atamasını kaldırmak için **Delete card** (Kartı sil) düğmesine tıklayın.

Not: Kart sahibinin son kartını silerseniz kişinin durumu **unregistered** (kayıtlı deėil) (durum çubuğundaki **Registered**'ın (Kayıtlı) yanındaki kırmızı etiket) olarak deėiřir. Bu kişi daha sonra giriř kontrolüne daha uzun tabi kalır.

17.3.2

Authorizations (Yetkiler) sekmesi

Giriř profilleri olarak paketlenen yetkileri atama

Kart sahiplerine yetki atamak için en uygun ve esnek yol, bunları önce Giriř profillerine daėıtmak ve ardından profili atamaktır.

- Giriř profilleri oluřturmak için *Giriř profilleri oluřturma, sayfa 138* bölümüne bakın
- Bu kart sahibine bir Giriř profili atamak için, **Access profile:** (Giriř profili) listesinden tanımlı bir profil seçin

Giriř yetkilerini doğrudan atama

Authorizations (Yetkiler) sekmesinde:

Kiřiye daha önce atanmış olan tüm giriř yetkileri soldaki listede görünür.

Atama için kullanılabilen tüm giriř yetkileri saėdaki listede görünür.

Öğeleri seçin ve öğeleri bir listeden diėerine taşımak için listeler arasındaki düğmelere tıklayın.



seçilen öğeyi atar.



seçilen öğenin atamasını kaldırır.



tüm kullanılabilir öğeleri atar.



tüm atanmış öğelerin atamasını kaldırır.

Seçenek: **Keep authorizations assigned** (Atanan yetkileri koru)

Bir giriř profilini bir kişiye atamanın etkisi **Keep authorizations assigned** (Atanan yetkileri koru) onay kutusuna baėlıdır:

- Onay kutusu temizlenirse bundan önce yapılan her türlü seçim ve zaten atanmış olan her türlü giriř yetkisi profil atandığında **deėiřtirilir**.
- Onay kutusu iřaretlenirse profilin yetkileri atanmış yetkilere **eklenir**.

Yetkilerin zaman aralıėını sınırlama

Yetki ve profillerin bařlangıç ve bitiş zamanlarını sınırlamak için **Valid from:** (Geçerlilik bařlangıcı) ve **until:** (Geçerlilik bitiři) tarih alanlarını kullanın. Hiçbir deėer 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.

17.3.3

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 **Kapı çok uzun süredir açık** durumu oluşmadan önce bir girişten geçmeleri için üç kat süre vermek üzere **Uzatılmış kapı açılma süresi** onay kutusunu 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 sırasındır. 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 güvenliqli 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).

17.3.4

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 çalıřması için, ařağıdaki gereksinimlerin karřılanması gerekir:

Yapılandırmada (cihaz ağacı)


- Bir veya daha fazla giriř, geniřletilmiş açık sürelerle izin verecek řekilde yapılandırılmalıdır.
- Giriřte en az bir tuř takımlı okuyucu kullanılmalıdır.

İstemcide (Persons (Kiřiler) iletiřim kutuları)

- Bir veya daha fazla kart sahibine giriři ofise modunu geçirip bu moddan çıkarma yetkisi verilmelidir.
- Bu kiřilerin kartlarının geçerli olması ve ofis modu saatleri dıřında giriře izin vermesi gerekir.

Kiřilere ofis modunu ayarlamaları için yetki verme prosedürleri**Bireysel kart sahiplerine yönelik prosedür**

1. řuraya gidin: **Personel verileri** > **Kartlar** > sekme: **Diđer veriler** ve veritabanında belirlenen kart sahibini oluřturun 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. řuraya gidin: **Personel verileri** > **Kiři grupları** ve liste penceresinde kart sahiplerinin bir listesini oluřturmak için filtre kriterlerini kullanın.
2. **Deđiřtirilecek alan** açılır listesinden, **Kapıların kilidini aç**'ı seçin
3. **Kapıların kilidini aç** onay kutusunu seçin.
4. Kart sahiplerinin verilerini kaydetmek için **Deđiřiklikleri uygula** düđmesine tıklayın.

Kart sahibine ofis modunu bařlatma ve durdurma talimatı verme

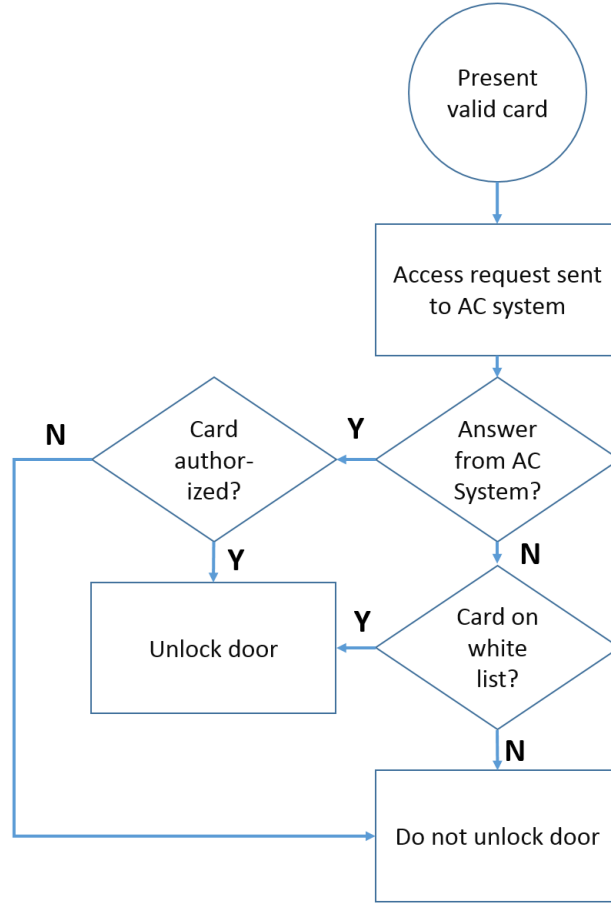
Bir giriřte ofis modunu bařlatmak veya durdurmak için, kart sahibi tuř takımında 3 rakamına basar ve ardından özel yetki verilmiř kartını okuyucuya gösterir.

Yetkili bir kart sahibi 3 rakamına basıp kartı yeniden gösterene kadar giriřin kilidi açık kalır.

Güvenlik görevlisi kartına sahip güvenlik görevlilerinin özel izin olmaksızın ofis modunu aynı řekilde durdurabileceđini unutmayın.

17.3.5**SmartIntego sekmesi****SmartIntego kilitleme sistemleri****Giriř**

SmartIntego kart okuyucusu, önce ana eriřim kontrolü (AC) sistemi aracılıđıyla giriř için yetki vermeye çalıřır. Bađlantı kurulamazsa kart numarası için saklanan beyaz listeyi arar.



SmartIntego kilitleme sistemine ait giriş yetkileri, çoğunlukla diđer 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


Ařağıdaki 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:
 - Kişiyeye 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 diđerine taşımak için listeler arasındaki düğmelere tıklayın.

 seçilen öğeyi atar.

 seçilen öğenin atamasını kaldırır.

 tüm kullanılabilir öğeleri atar.

 tüm atanmış öğelerin atamasını kaldırır.

17.3.6

Uyarı kartı oluřturma

Bu bölümde, bir tehdit seviyesi tetiklemek için kullanılabilen bir uyarı kartının nasıl oluřturulacağı açıklanmaktadır.

Giriř

Uyarı kartı, bir okuyucuya gösterildiğinde belirli bir tehdit seviyesini tetikleyen bir karttır. Bir tehdit seviyesi yalnızca kartlı geçiř yazılımı aracılığıyla bir uyarı kartı ile iptal edilemez.

Ön kořullar

- Sisteminizde verileri karta yazmak için bir iletiřim kutusu okuyucusu takılı olmalıdır.
- Sistemde en az bir tehdit seviyesi tanımlanmış olmalıdır.

İletiřim yolu

Main menu (Ana menü) > **Personnel data** (Personel verileri) > **Cards** (Kartlar) > **Alert card** (Uyarı kartı)

Prosedür

1. Uyarı kartının atanacağı kiřinin kiři kaydını yükleyin
2. Uyarı kartı sekmesinde, Record card'a (Kartı kaydet) tıklayın.
 - řu açılır pencere görünür: **Select threat level** (Tehdit seviyesi seç)
3. Açılır pencerede istediğiniz tehdit seviyesini seçin ve **OK**'e (Tamam) tıklayın.
 - řu açılır pencere görünür: **Recording badge ID** (Kimlik kartı kimlięi kaydetme)
4. Saha kurulumunuza karřılık gelen normal kart verilerini girin ve **OK**'e (Tamam) tıklayın.
 - Kaydettiğiniz uyarı kartı **Alert card** (Uyarı kartı) sekmesindeki listede görünür.

17.4

Geçici kartlar

Geçici bir kart, normal bir kart sahibi tarafından yanlış yerleřtirilmiş bir kartın geçici bir yedeęidir. Çevrimdışı kapı hakları da dahil olmak üzere, orijinalin tüm yetki ve sınırlamalarını içeren bir kopyadır.

Kötüye kullanımı önlemek için sistem, kart sahibinin dięer kartlarının bir kısmını veya tamamını sınırlı bir süre için veya engeli manuel olarak kaldırılincaya kadar engelleyebilir.

Bu nedenle geçici kartlar ziyaretçi kartları olarak kullanmak için **uygun deęildir**.

Ön gereksinimler

- Operatör, iř istasyonunda yapılandırılan bir kayıt okuyucusuna erişebilir.
- Sistemde geçici bir kart olarak kayıt etmek için uygun bir fiziksel kart mevcuttur.
- Geçici kartın alıcısı zaten en az bir adet başka karta sahiptir.

Main menu (Ana menü) > **Personnel data** (Personel verileri) > **Cards** (Kartlar)

Prosedür: Geçici kartlar atama

1. Gerekli personel kaydını **Cards** (Kartlar) iletiřim kutusuna yükleyin
2. Kart listesinde geçici olarak deęiřtirilmesi gereken kartı veya kartları seçin.
3. **Change card**'a (Kartı deęiřtir) tıklayın
4. **Change card** (Kartı deęiřtir) 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 seçeneđi 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 řimdi devre dıřı bırak) onay kutusunu iřaretleyin.
 - Seçilirse bu kart sahibine ait tüm kartlar engellenir.
 - Temizlenirse yalnızca yukarıda seçilen kart engellenir.
8. Gerekirse **Activate card(s) automatically after period** (Kartları řu süreden sonra otomatik olarak etkinleřtir:) onay kutusunu iřaretleyin.
 - Engellenen kartlar yukarıda tanımlanan **Period** (Süre) sona erdiğinde otomatik olarak engellenir.
9. Geçici kartı kayıt okuyucusuna yerleřtirin
10. **OK**
'e tıklayın Kimlik kartı kimliđi kayıt okuyucusu tarafından kaydedilir.
 - Geçici kart geçerlilik süresi ve kod verileri ile birlikte kart listesinde ✓ etkin olarak görünür.
 - Yukarıda yapılan ayarlara bađlı olarak diđer kart veya kartlar engellenmiř ✗ olarak görünür: **Deactivate all cards now** (Tüm kartları řimdi devre dıřı bırak).
11. (İsteđe bađlı) Kart listesinde, geçici karta ait **Collecting date** (Toplama tarihi) sütununa tıklayın ve kartı kart sahibinden almak için bir tarih belirleyin.
Varsayılan deđer **Never**'dir (Asla).

Prosedür: Geçici kartları silme

Yanlıř yerleřtirilen orijinal kart bulunduđunda, geçici kartı ařađıdaki gibi silin:

1. Gerekli personel kaydını **Cards** (Kartlar) iletiřim kutusuna yükleyin.
2. Kart listesinden geçici kartı seçin.
3. **Delete card**
'a (Kartı sil) tıklayın Geçici kart listeden silinir ve yerine geçtiđi kart veya kartlar derhal engellenir

Prosedür: Kartlardaki geçici blokları kaldırma

Artık orijinal kartın engellenmesi gerekmiyorsa engellemeyi řu řekilde silin:

1. **Blocking** (Engelleme) iletiřim kutusu: **Personnel data** (Personel verileri) > **Blocking** (Engelleme) bölümüne gidin.
2. Kart listesinde, **Lock(s)** (Kilitler) sütununda engellendi olarak iřaretlenen kiřisel kartı seçin.
3. **Release temporary lock**
'a (Geçici kilidi aç) tıklayın **Blocking** (Engelleme) listesinde kalan kayda dikkat edin. Liste, yalnızca geçmiş ve řimdiki mevcut kayıt için tüm engellemelerin geçmişini içerir.

Geçici kartlarla ilgili notlar

- Sistem geçici kartların geçici kartlarla deđiřtirilmesine izin vermez.
- Sistem, bir kiřisel kartın birden fazla geçici karta sahip olmasına izin vermez.
- Bir kart sahibinin elindeki tüm kartların hızlı bir özetini görmek için, farenizi ana iletiřim kutusu penceresindeki durum çubuđunda yer alan en soldaki **Registered** (Kayıtlı) etiketli küçük bölmenin üzerine getirin.

17.5

Personel iin PIN kodları

İletişim Kutusu: PIN Kodu

Yksek gvenlik gereksinimleri olan blgelere giriř iin, giriř yetkisi yeterli olmayabilir. Buralarda bir PIN kodu da girilmelidir. Her kiři veya kimlik kartı tm alanlar iin geerli bir PIN koduna sahip olabilir. Sistem ok basit kodların (r. 123456 veya 127721 gibi ift taraflı aynı okunan rakam grupları) kullanılmasını engeller. İletişim kutusundaki her bir kiři iin geerlilik kısıtlanabilir ve belirtilir.

Bir PIN kodu engellendiyse veya sresi dolduysa kimlik kartı tm diđer alanlar iin hala geerli olsa bile kod istenen alana giriř reddedilir.

Yanlıř bir kod  kez art arda girilirse (varsayılan ayardır; bu 1 ila 99 arasında yapılandırılabilir), bu kart engellenir, rneđin tm alanlara giriř reddedilir. Bu Őekilde engellenen bir kartın engeli Blocking (Engelleme) iletiřim kutusuyla kaldırılabilir.

The screenshot shows the 'PIN code' configuration page for a user named 'Mustermann, Max'. The interface includes a sidebar with navigation options: Main menu, Persons, Companies, Print badges, Cards, PIN code (selected), and Blocking. The main area contains the following fields:

- Name: Mustermann
- First name: Max
- Birth name: (empty)
- Personnel no.: Sc999000
- Date of birth: Tu 08/09/1988
- Employee ID: Employee
- Gender: Male
- Company: Test_Firma
- Title: Dr
- Car license No.: Car000998
- Card no.: (empty) Reader..
- PIN code: (masked with red dots)
- Confirm: (masked with red dots)
- Valid until: Mo 01/21/2013

A photo of the user is shown on the right, with the date 10/20/2014 and the status 'Administered globally'.

PIN-Code (PIN Kodu) giriř alanına yeni bir PIN kodu girin ve yeniden yazarak onaylayın. PIN kodunun uzunluđu (4-9 arasında, varsayılan deđer 6'dır) sistem yneticisi tarafından yapılandırılır.

Uyarı!



Kart sahiplerinin kart okuyucularda kimlik PIN'lerini girme Őekli sisteminizde yapılandırılan okuyucunun trne bađlıdır. rneđin:

RS485 kart okuyucularda kart sahibi Őunları girer: 4 # <the PIN>

Wiegand ve diđer kart okuyucularda kart sahibi Őunları girer: <the PIN> #

Kart sahiplerini mutlaka PIN'lerini nasıl gireceklerine iliřkin olarak bilgilendirin. Emin olamazsanız sistem yneticinize danıřın.

Hırsız alarm sistemlerini (IDS) devreye almak iin PIN Kodu.

4-8 basamaklı bir PIN girin (varsayılan = 6; dođrulama PIN'iyile aynı uzunluktadır). Bu PIN bir IDS'yi kurmak iin kullanılacaktır.

Bu alanların grntlenmesi 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 kullanılmıyorsa 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.

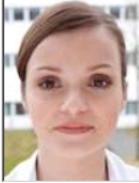
17.6

Personel için giriři 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.



10/20/2014

Card no.	Application type	PIN lock	Created on	Last printed on	No. of prints	Code data
000000101234	Personal card		10/21/2014 02:57:22 PM		0	Customer code:150, Badge no.:101234, Version:4, Country d

Blocking

Blocked from	Blocked until	Blocking reason	Last edited by

1. Kiřiyi her zamanki gibi sein.
2. Blocking (Engelleme) blmesinde **New**'a tıcklayarak seili kiři iin bir engelleme oluřturun.
3. Aılır iletiřim kutusuna ek bilgiler girin:
 - **Blocked from/until** (Engellenme bařlangıcı/bitiři): (Bitiř zamanı belirtilmediyse kiři engel manuel olarak kaldırılana kadar engellenir.)
 - **Block type**: (Engelleme tr)
 - **Blocking reason**: (Engelleme nedeni) (Kiřinin kaydı iin engelleme tipi `Manual` ise)
4. Engellemeyi kaydetmek iin aılır penceredeki **Save**'e (Kaydet) tıcklayın.
 - Gerekirse listeden bir engelleme sein ve bunu deėiřtirmek veya silmek iin **Change**'e (Deėiřtir) veya **Delete**'e (Sil) tıcklayın.

Engelleme tipi olarak **Manuel lock** (Manuel kilit) seilmiřse kiřinin kaydı iin bir **Blocking reason** (Engelleme nedeni) girin.



Uyarı!

Engelleme, belirli bir kimlik bilgisine deėil kiřiye uygulanır. Bu nedenle, yeni bir kimlik kartı tahsis ederek engellemeyi iptal etmek veya nlemek mmkn deėildir.

17.7 Kartları kara listeye alma

İletişim Kutusu: Kara Liste

rneđin alınan veya kaybolan kartlar gibi bir daha asla kullanılmaması gereken kartlar kara liste tablosuna girilir.

Kiřinin deđil kimlik bilgisinin kara listeye alındıđını unutmayın.



Uyarı!

İřlem geri alınamaz. Kara listedeki kartların engelleri asla kaldırılamaz, ancak bunun yerine deđiřtirilmelidir.

Kara listeye alınan kartlar giriř izni vermez. Bunun yerine kullanım giriřimi bir gnlk dosyasına kaydedilir ve bir alarm oluřturulur.

🏠 🔍 ⏪ ⏩ 🔍 ⏪ ⏩ ⏪ ⏩ ?

Division: Common

« Main menu

Persons

Companies

Print badges

Cards

PIN code

Blocking

Blacklist

Group of persons

Name:

Birth name:

Personnel no.:

Employee ID:

Company:

Car license No.:

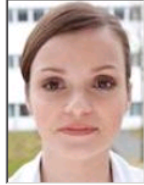
Card no.:

First name:

Date of birth:

Gender:

Title:



10/20/2014

Card no.	Application type	PIN lock	Created on	Last printed on	No. of prints	Code data

Reason:

Main menu (Ana men) > **Personnel data** (Personel verileri) > **Blacklist** (Kara listeye al)

1. Kimlik kartı kara listeye alınacak kiřiyi seđin.
2. Bu kart sahibine birden fazla kart atandıysa **Kimlik Kartı No.** listesinden kartı seđin.
3. **Reason** (Neden) giriř alanına bu kartı kara listeye alma nedenini girin.
4. **Blacklist this card** (Bu kartı kara listeye al) dđmesine tıklayın.
5. Aılır pencerede kara listeye alma iřlemini onaylayın.

Kart derhal uygulanacak řekilde kara listeye alınır.



Uyarı!

Kara listeye alma kart sahiplerini **deđil** kartları etkiler.

Aynı kart sahibine ait olan kara listeye alınmamıř kartlar engellenmez.

17.8 Aynı anda birden fazla kiřiyi dzenleme

Kiři Grubu

- < Main menu
- Persons
- Companies
- Print badges
- Cards
- PIN code
- Blocking
- Blacklist
- Group of persons
- Group authorizations
- Areas
- Change division
- PegaSys Stoppage card
- Keys

Employee ID: Employee

Name: *

First name:

Personnel number:

Company:

Card:

Valid on:

Gender:

Department:

Cost center:

until starting with:

until starting with:

until starting with:

until starting with:

until starting with:

Number of records found: 2 Show all

Name	First name	Gender	Pers. number	Location	Cost unit	Job title	Company	Department	Card number	Time model	Valid from	Valid until
Mustefrau	Anja	Female	SC41156				Test_Firma					
Mustermann	Max	Male	Sc999000			Software-Entwickler	Test_Firma					

Wanted field to change:

Wanted action:

Bařka bir iletiřim kutusu grup deęiřikliklerinin tanımlanabileceęi bir kiři grubu seęer. Seęilen kiři grubu zerinde kontrol korumak iin, ilk on kiři adlarla birlikte gsterilir ve gerek veriler veritabanını oluřturur (gerek veriler: Departman olarak "ST-AC" seęildiyse rneęin "ST-ACS" ve "ST-ACX" grntlenir). Ayrıca, seęilen grubun kiři sayısı grntlenir.

Kiři grubu seęildikten sonra ařaęıdaki giriřler seęilebilir:

- alıřan Kimlięi
- Name (Ad)
- First name (Ad)
- Personel numarası
- Company (řirket)
- Kart
- Geerlilik tarihi
- Gender (Cinsiyet)
- Departman
- Maliyet birimi
- Tanımlandıysa ayrılan alanlar

Ardından deęiřtirme seęeneęi seęilebilir:

- Deęiřtirilecek alan
- İstenen iřlem
- Eski deęer
- Yeni deęer.

Bylece tasarlanan deęerler sırasıyla **Eski deęer** veya **Yeni deęer** alanına girilir. **Deęiřiklikleri uygula** dğmesini seip **Tm seilen kiřiler iin deęiřiklikler uygulansın mı?** gvenlik isteęi onaylanarak iřlem tamamlanır. iřlem devam ederken rneęin iletiřim kutusu kullanılamaz. Alan *1 ila *4 tarafından tetiklenen iřlemler muhtemelen dięer alanlardan (yıldızsız) daha fazla zaman alır ve tm deęiřikliklere izin verilmez. Dolayısıyla **Desired action** (İstenen iřlem) **New value** (Yeni deęer) ile karřılařtırılmaz, nk bu giriřler standart rn tarafından karřılanmaz. **Old value** (Eski deęer) ve **New value** (Yeni deęer) alanları da sırayla deęiřiklik gsterebilir.

Grup Yetkisi

« Main menu
🔍 ⏪ ⏹

- Persons
- Companies
- Print badges
- Cards
- PIN code
- Blocking
- Blacklist
- Group of persons
- Group authorizations
- Areas

Employee ID: Employee

Name: * until starting with:

First name: until starting with:

Personnel number: until starting with:

Company: until starting with:

Card: until starting with:

Valid on:

Gender:

Department:

Cost center:

Group authorizations

2 selected persons

Name	First name	Personnel no.
Musterrfrau	Anja	SC41156
Mustermann	Max	Sc999000

Authorizations

Filter: / 1

Assign	Withdraw	Name	MAC	Time model	Division
No	No	Door	MAC		Common

[Grup Yetkisi] men oęesinde ařaęıdaki arama kriterleri desteklenir:

- alıřan Kimlięi
- Name (Ad)
- First name (Ad)
- Personel numarası
- Company (řirket)
- Kart
- Geerlilik tarihi
- Gender (Cinsiyet)
- Departman
- Maliyet birimi
- Tanımlandıysa ayrılan alanlar

Bundan sonra, bir liste iletiřim kutusunun tm seilen kiřileri (ad, soyadı ve personel no. ile) grntleyen alt kısmını gsterir. Tm yetkiler saę alttaki aıklamaları, zaman modeli ve **[Assign]** (Ata) ve **[Withdraw]** (Geri al) stnlarıyla birlikte gsterilir. Yetki listesi aıldığında geerli yetkiler gsterilmez ve **[Assign]** (Ata) ve **[Withdraw]** (Geri Al) stnları nceden "No" (Hayır) olarak ayarlanır. Bu noktada, "Hayır"ı "Evet"e veya tersine dnřtren stnlardan birindeki alana ift tıklayarak yetkiler tek tek atanabilir. Deęiřiklikleri yrt'e

tıklamak "Evet" atanmıř tm yetkilerin sırasıyla tm seili kiřilere eklenmesini veya geri alınmasını saęlar. Genellikle seilen kiřiler tamamen aynı yetkilere sahip olmadıęından, kiřilere ait tm dięer yetkiler deęiřmeden kalır.

18

18.1


Giriş yetkilerini ve profillerini tanımlama


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) Listedenden bir **Inactivity limit** (Hareketsizlik sınırı) seçin.
Bu, 14-365 gün arasında belirlenen bir süredir. Bu yetkinin atandığı bir kişi, belirlenen süre içinde kullanılmazsa 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**'i (Kurulu) veya **Disarmed**'i (Devre Dışı) seçin.
7. Listedenden 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)



18.2 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.

19 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.

19.1 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.

📄 📁 🔍 ⏪ ⏩ 🖨️ ⏴ ⏵ ❓ 🗑️

Division: Common

Last name: First name:

Birth name: Date of birth:

Street, no: Zip code / City:

Phone:

Car license No.:

Employee ID: Company:

Official pass

Passport

Driver's licence

Identity card

Other:

Number:

Card no.: Reader.. ▶

Additional data

Authorizations
Form/Photo
Signature

Attendant: ... Reason:

Remark:

Expected arrival: Expected departure:

Date of arrival: Date of departure:

Visited person: ... Extended door opening time

Location:

Card no.	Application type	PIN lock	Collecting date	Code data

Read card ... ▶
Withdraw card

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.

< ?
Division: Common

« Main menu

Visitors

Visitor cards

Register card

Register card ▶

Deregister card

Read card ▶

Delete card

Card no.:

Last name:

First name:

Date of birth:

Show list >>>

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.

<<< Hide list

Card no.	In use	Name	First name	Usage type	Division	

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.

Entry		Exit	
First- and lastname Steven Visitor		Company _____	
<input type="checkbox"/> Proof of authority for plant area		Registration plate _____	
Passed card			
Contact person	Phone	Department	
Reason of visit	Visit appointment <input type="checkbox"/> Yes <input type="checkbox"/> No		
Type of official Passport	Number of official document		
I accept the terms and conditions overleaf			
_____		_____	
Location, date		Sign of visitor	
Identy card with photo seen ? <input type="checkbox"/> Yes <input type="checkbox"/> No		To complete from visited person	
_____		Arrival at _____	
Sign of plant protective force		Departure at _____	

		To sign on visited person	

19.2

Ziyaretçi çok gecikti

Ziyaretçi çok gecikti görünümü müşterinin ziyaretçilerin konum dahilinde nerede kaldığını ve beklenen ayrılış saatini aşmış olduklarını kontrol etmesini sağlar.

Yetkili BIS kullanıcılarının bu web sitesini görüntüleyebilmeleri için başlangıç ekranlarında yapılandırılmış bir bağlantıya sahip olması gerekir.

Ayrıca, BIS'te DMS cihazı için bir tetikleyici yapılandırılabilir, böylece Ziyaretçi çok gecikti mesajı alındığında bir alarm etkinleştirilebilir, bu sonrasında web sitesini açar ve yalnızca ilgili kişiyi son bilinen yerleriyle birlikte görüntüler.

[ekrandaki web sitesine bakın]

Ziyaretçi çok gecikti mesajına yol açan olaylar:

Bir kart bir ziyaretçiye atandıysa operatör beklenen ayrılış zamanını girer. Ziyaret sona erdiğinde ziyaretçi kartı resepsiyon masasına iade eder. Burada bir operatör kartı iptal eder. Alternatif olarak motorlu bir kart okuyucu ziyaretçiler için çıkış okuyucusu olarak kullanılabilir ve tesisten ayrıldığında ziyaretçinin kartına el koyacak şekilde yapılandırılabilir.

Ziyaretçi önceden ayarlanan ayrılış zamanından önce kartı iade etmezse ziyaretçinin hala tesiste olup olmadığına bakılmaksızın sistem tarafından bir **Visitor too late** (Ziyaretçi çok gecikti) mesajı oluşturulur.

Bu zamanı geçmiş kart iadeleri kontrolü düzenli aralıklarla yapılır (ör. dakikada bir). Kart iade edilene kadar her kontrol tarafından bir **Visitor too late** (Ziyaretçi çok gecikti) mesajı oluşturulur. Zaman aralığı şu dizinin altındaki sunucunun kayıt defterinde yapılandırılabilir:

`HKLM\Software\Micos\SPS\Default\VLDP\Interval`



Uyarı!

Bu mesajı oluşturulması şu dizinin altında sunucunun kayıt defterinde devre dışı bırakılabilir:

`HKLM\Software\Micos\SPS\Default\VLDP\Active`

Bu özellik müşterinin atanmış yetkiliyle buluşmayan veya resepsiyonda geri geldiğini bildirmeyen ya da verilen zaman dilimi içinde yetkiliyle buluştuktan sonra kapıdan çıkan tüm ziyaretçileri tespit etmesini sağlar.

Şunlar kontrol edilir:

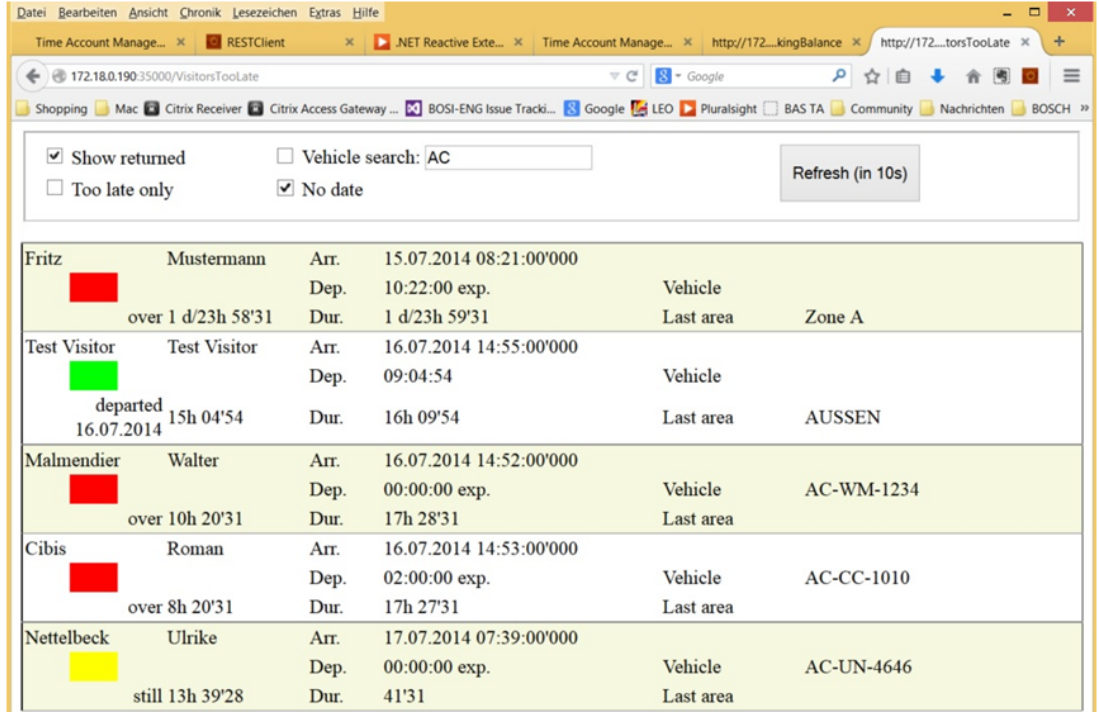
- Ziyaretçinin bina giriş etiketi için son kullanılan alan,
- Ziyaretçinin bina giriş etiketini geri alıp almadığı,
- Ziyaretçinin varsa araç etiketini geri alıp almadığı.

Bir **Ziyaretçi çok gecikti** ve **Araç çok gecikti** raporu oluşturulur.

İade edilmezse etiketin geçerli alanı "ziyaretçi çok gecikti" raporuna yazdırılabilir.

Ziyaretçi durumu web sitesinde renkli çubuklarla görüntülenir:

- **Yeşil:** Ziyaretçi tüm giriş kartlarını iade etmiştir.
- **Sarı:** Ziyaret henüz bitmemiştir ve zaman henüz dolmamıştır.
- **Kırmızı:** Ziyaret henüz bitmemiştir ve zaman henüz dolmamıştır, örneğin **Ziyaretçi çok gecikti**.



Name	Arr.	Dep.	Dur.	Vehicle	Last area	Zone
Fritz Mustermann over 1 d/23h 58'31	15.07.2014 08:21:00'000	10:22:00 exp.	1 d/23h 59'31	Vehicle	Last area	Zone A
Test Visitor departed 15h 04'54 16.07.2014	16.07.2014 14:55:00'000	09:04:54	16h 09'54	Vehicle	Last area	AUSSEN
Malmendier Walter over 10h 20'31	16.07.2014 14:52:00'000	00:00:00 exp.	17h 28'31	Vehicle	Last area	AC-WM-1234
Cibis Roman over 8h 20'31	16.07.2014 14:53:00'000	02:00:00 exp.	17h 27'31	Vehicle	Last area	AC-CC-1010
Nettelbeck Ulrike still 13h 39'28	17.07.2014 07:39:00'000	00:00:00 exp.	41'31	Vehicle	Last area	AC-UN-4646

Sayfa 30 saniyede bir otomatik olarak yenilenir. Yenileme süresi web sayfasının içinde yapılandırılabilir. Ayrıca, operatörün görünümü **Show returned** (İade edilenleri göster), **Too late only** (Yalnızca çok geç) ve **Vehicle search** (Araç arama) filtreleri kullanılarak ayarlanabilir.

20

20.1

Otoparkları yönetme

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.

Birkaç AMC bir otoparkı kontrol ediyorsa AMC yapılandırmasında **AMC hesaplaması yok** onay kutusunu işaretleyin.

AMC 4-W | Inputs | Outputs | Terminals

Name: AMC 4-W-1

Description: AMC

Communication to host enabled:

Controller interface

Interface type: UDP

PC com port: 0

Bus number: 1

IP address / host name:

Port number: 10001

Program: LCMV3732.RUN : WIE, AMC-4W

Power supply supervision:

No LAC accounting:

Division: Common

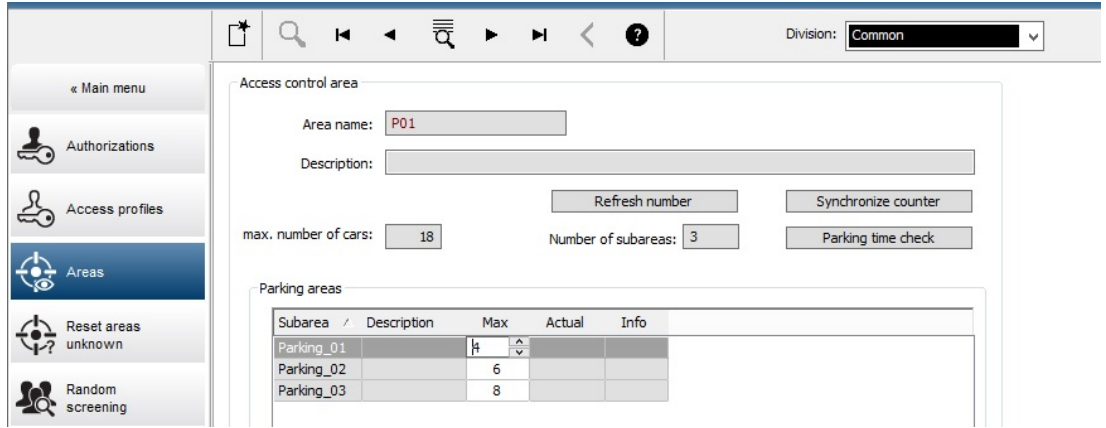
20.2 Araç Park Etmeye genel bakış

Aracın Durumu	Aracın Durumu	Aracın Durumu	Aracın Durumu
...

20.3 Genişletilmiş Otopark yönetimi

Operatör standart dışı boyutlarda araçları telafi etmek için otopark alanındaki park yeri sayısını ayarlayabilir, örneğin:

- Kamyonlar
 - Engelli girişi
 - Motosikletler
1. Otopark alanını seçin
 2. **Otopark alanları** bölümünde **Maks.** sütunundaki değeri o alan için yeni park yeri sayısı olarak ayarlayın.



« Main menu

Authorizations

Access profiles

Areas

Reset areas unknown

Random screening

Access control area

Area name: P01

Description:

max. number of cars: 18

Number of subareas: 3

Refresh number

Synchronize counter

Parking time check

Parking areas

Subarea	Description	Max	Actual	Info
Parking_01		4		
Parking_02		6		
Parking_03		8		

Ana menü > Personel verileri > Alanlar

21

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.

21.1

Genel bakışları tanımlama

Guard tours (Genel bakışlar) > **Define guard tours**'u (Genel bakışları tanımla) seçin

Define guard tour

Name:

Description:

No.	Description of reader	Time on the way	Total time	Max. delay	Startzeit +/-
1	BPR HI-1; BPR HI	00:00:00	00:00:00	00:00:00	3 min
2	BPR HI-2; BPR HI	00:10:00	00:10:00	00:02:00	
3	BPR HI-1; BPR HI	00:10:00	00:20:00	00:05:00	

- **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. Gerekli 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.

21.2

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 öngörülmeven 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 değiştirir ve listede planlı ve etkin genel bakışların altına düşer.

21.3 Bakış izleme (eskiden yol kontrolüydü)

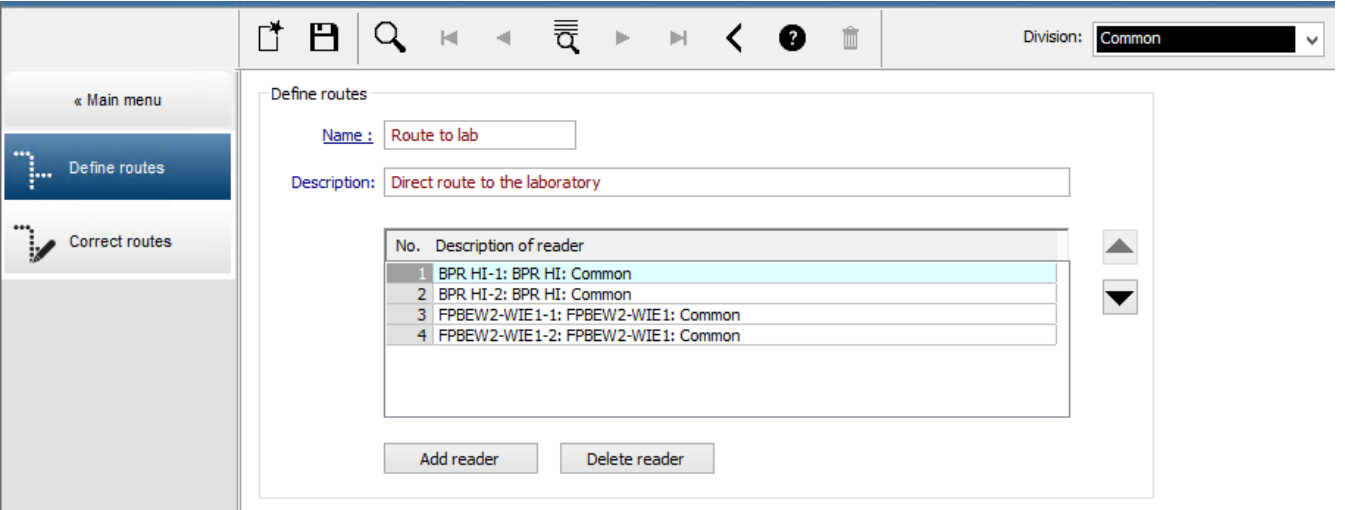
Giriş

Bir Güzergah (veya Tur), kişinin yetkilerinden bağımsız olarak tesisteki hareketlerine yön vermek için kartlı geçiş sisteminde tanımlı kişilere uygulanabilecek önceden tanımlanan bir okuyucu sırasdır.

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.



No.	Description of reader
1	BPR HI-1: BPR HI: Common
2	BPR HI-2: BPR HI: Common
3	FPBEW2-WIE 1-1: FPBEW2-WIE 1: Common
4	FPBEW2-WIE 1-2: FPBEW2-WIE 1: Common

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.

22

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.

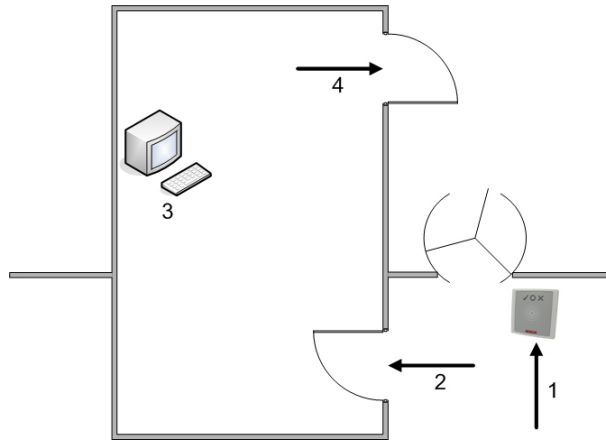
2. Karıştırıcı bu kişiyi tarama için seçerse bu kişinin kartı tüm sistem genelinde engellenir.
 - Olay, sistem olay günlüğüne kaydedilir.
 - **Engelleme** iletişim kutusuna **Rastgele tarama** şeklinde işaretli bir sınır süre girişi eklenir. [Aşağıdaki şekil - sayı 1]
 - Access Engine'deki personel veri 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 işlemi 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 $1/10 \times 1/10$).

23

Olay Görüntüleyici'yi Kullanma

Giriş

Olay Görüntüleyici, uygun şekilde yetkilendirilmiş operatörlerin sistem tarafından kaydedilen olayları incelemelerini ve basılı veya ekran üzerinde raporlar üretmelerini sağlar.

İstediğiniz kayıtları Olay Günlüğü veritabanından almak ve görüntülemek için filtre kriterleri

ayarlayın ve **Refresh**'e  tıklayın.

Filtre kriterleri farklı şekillerde ayarlanabilir:

Bağlı 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 gereksinimler

İletişim kutusu yöneticisine giriş yaptınız.

İletişim yolu



İletişim yöneticisi ana menüsü > **Reports** (Raporlar) > **Event viewer** (Olay görüntüleyicisi)


23.1

Filtre kriterlerini şu ana göre ayarlama

1. **Time period**'in (Zaman dilimi) altındaki **Relative** (Bağlı) 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)
 - Kod verileri
 - 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.




23.2


Bir zaman aralığı için filtre kriterlerini belirleme

1. **Time period**'in (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)
 - Kod verileri
 - 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.

23.3

Filtre kriterlerini zamandan bağımsız olarak belirleme

1. **Time period**'in (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)
 - Kod verileri
 - 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.

24


Raporları kullanma

Bu bölüm, sistem ve olay günlüğü verilerini filtrelemek ve net biçimlerde sunmak için kullanılacak 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:



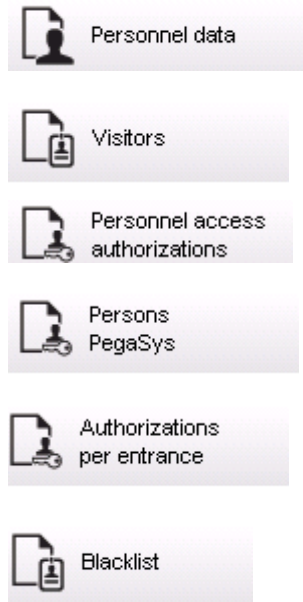
- Yazdırmadan ön izlemeden çıkmak için  simgesine tıklayın.
- İleri ve geri göz atmak veya sayfa sayısına göre sayfaları tek tek seçmek için ön izleme araç çubuğundaki ok tuşlarını   kullanın.
- Varsayılan yazıcınızı kullanarak hemen yazdırmak için  simgesine tıklayın.
- Diğer yazdırma seçeneklerine 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.

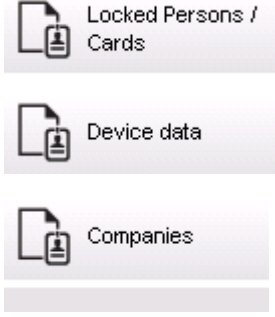
24.1

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 yapılabilir.

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.

24.1.1

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	Arrival Departure	Vehicle Last area	Person Last area
	Status	Duration		
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 langem Namen	Besucher mit gaaaaanz langem namen departed	01.07.2014 07:30 01.07.2014 12:00 4h 30'	AC AA 2345 AUSSEN	AUSSEN

24.2

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.

-  Areas
-  Area configuration
-  Area muster list
-  Muster list total

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 izleme** 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

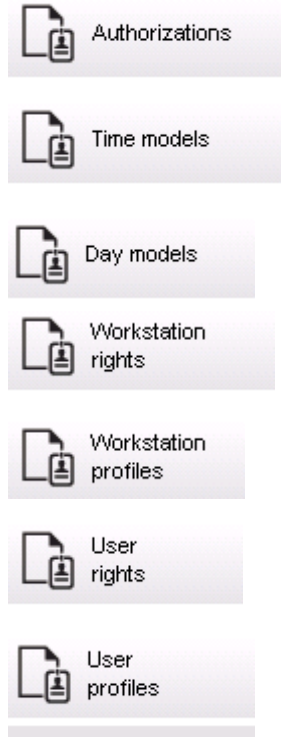
İlke olarak, toplanma listeleri **Areas** (Alanlar) rapor iletişim kutusuna karşılık gelir; ancak giriş kontrolüne göre o anda söz konusu alanda bulunan kişi sayısı hakkında bilgi sağlayan belirli bölgelere ait listeler sunar.

24.3

Raporlar: Yetkiler

Genel Bakış

Bu menü ögesinde, 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.

25 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 110* 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 110*

25.1 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 uyarısını 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'** (Tehdit seviyesini devre dışı bırak) seçin.
 - O anda geçerli tehdit seviyesi devre dışı bırakılır.

25.2 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 yapılandırma ile ilgili talimatlar için bu bölümün sonundaki bağlantıya tıklayın veya sistem yöneticinizle iletişime geçin.

Prosedür

Cihazı devreye alın, bu cihaz genellikle 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 114*

25.3 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 oluşturma ile 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 128*

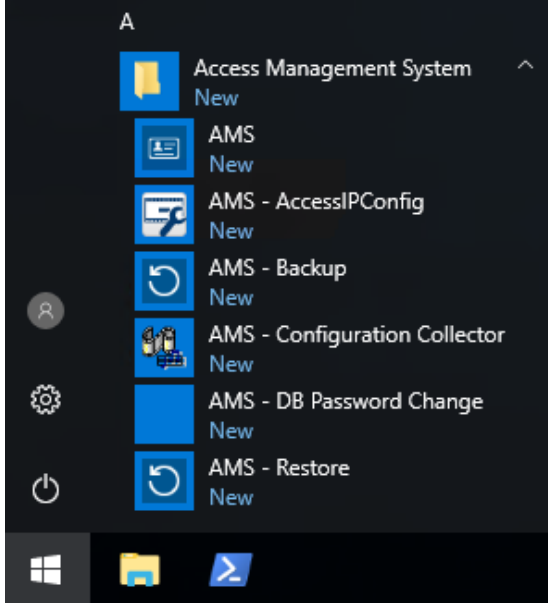
26

Yedekleme ve Geri Yükleme

Backup & Restore (Yedekleme ve Geri Yükleme) işlevi, ilk bilgisayar arızalanırsa kurulumunuzu farklı bir bilgisayarda yeniden oluşturmanızı sağlar.

Backup and Restore (Yedekleme ve Yeniden Yükleme) sadece AMS sunucusunun kurulu olduğu makinede başlatılabilir. Kolaylık için, iki kısayol oluşturulur:

- Yedek oluşturmak için **AMS - Yedekleme**
- Yedeği geri yüklemek için **AMS - Geri Yükleme:**

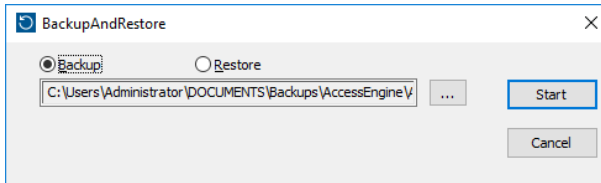


26.1

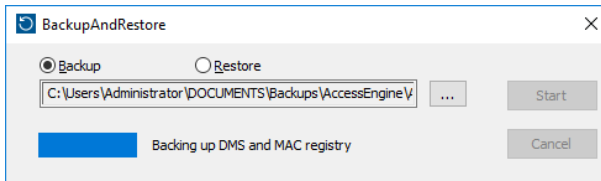
Yedekleme prosedürü

1. **AMS - Backup** (AMS - Yedekleme) kısayoluna tıklayın.

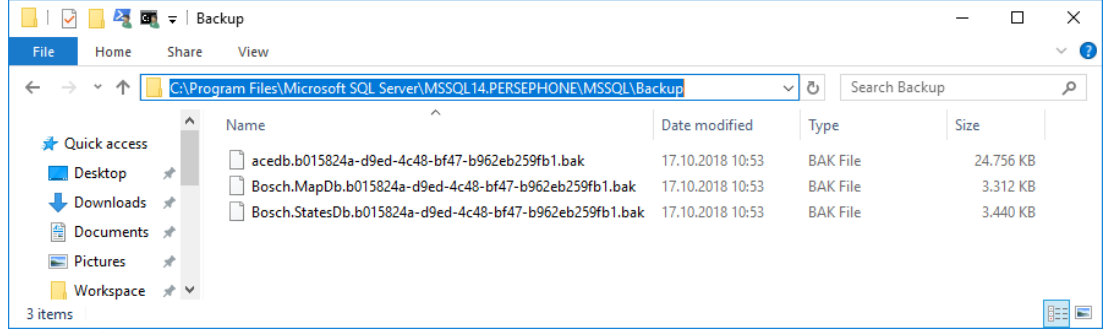
Bu, **Backup and Restore** (Yedekleme ve Geri Yükleme) aracını başlatır:



2. GZIP dosyasının kaydedileceği bir yol girin.
3. Yedeklemeyi başlatmak için **Start**'a (Başlat) tıklayın.
Bir ilerleme çubuğu gösterilir.
Tamamlandığında GZIP dosyası oluşturulur.



Veritabanı yedeğinin konumu, SQL Server sürümüne ve veritabanı örneğinin adına bağlıdır. Örneğin, AMS SQL Server örnek adı "PERSEPHONE" ise yedekleme şu konumda bulunur:



ÖNEMLİ: Bosch, veri güvenliği için bu klasörü ve GZIP dosyasını güvenli ve uzak bir yere kopyalamanızı önerir. Tek yedek kopyayı DMS sunucu bilgisayarında bırakmayın.



Uyarı!

Olay günlüğü şu varsayılan yolun altında kaydedilir (kurucunuz farklı bir yol seçmiş olabilir):
C:\Program Files (x86)\Access Management System\Access Engine\AC\LgfLog\

26.2

Geri yükleme prosedürü

Ön gereksinimler

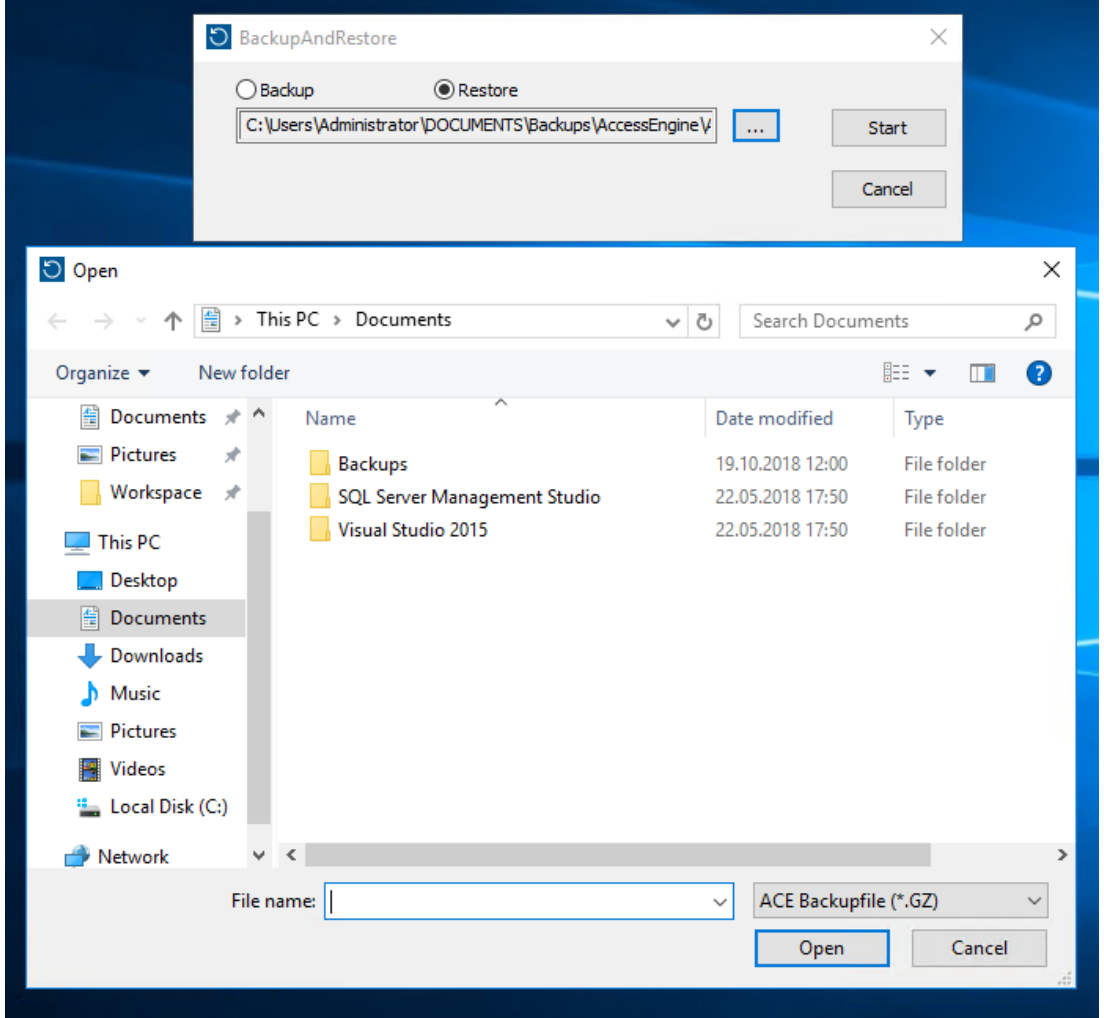
- **Backup and Restore** (Yedekleme ve Geri Yükleme) aracı tarafından oluşturulan GZIP dosyası
- SQL Server tarafından SQL Server yedekleme klasöründe oluşturulan yedekleme verileri.
- sa gibi **sysadmin** haklarına sahip bir SQL hesabı.

Hedef bilgisayarla ilgili notlar

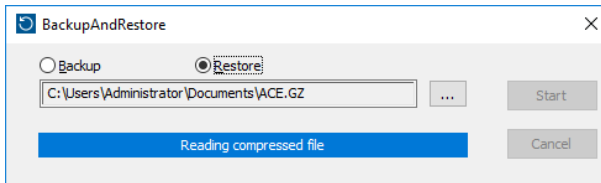
- Geri yüklenen yapılandırmayı çalıştırmak için, hedef bilgisayar (yedeği geri yüklediğiniz) en az yedeklemenin yapıldığı bilgisayardakilere eşdeğer lisanslar bulunmasını gerektirir.
- Hedef bilgisayarın herhangi bir istemcisi için ilk bilgisayarda kurulumla oluşturulanlar değil, hedef bilgisayarda kurulumla oluşturulan sertifikalar gereklidir. İstemci sertifikalarının kurulumu için kurulum kılavuzuna bakın.

Prosedür

1. AMS programında, **File** (Dosya) > **Exit**'e (Çıkış) tıklayarak tüm çalışan hizmetleri durdurun.
2. Program sonlandırıldığında, Windows **Hizmetleri** uygulamasını çalıştırın ve tüm **Access Engine** ve **Access Management System** hizmetlerinin durdurulduğundan emin olun.
3. Windows Başlat > **AMS - Geri Yükleme**'ye tıklayın
4. GZIP yedekleme dosyasını bulmak ve seçmek için **[...]** düğmesine tıklayın.



5. Geri yükleme işlemini başlatmak için **Başlat**'a tıklayın.
6. **SQL sysadmin** giriş kimlik bilgilerini girin.
Geri yükleme işlemi başlar



7. Geri yükleme işlemi tamamlandığında, Windows **Hizmetleri** uygulamasını başlatın ve tüm Access Engine ve Access Management System hizmetlerinin yeniden başlatıldığından emin olun.
Başlatılmadıysa manuel olarak yeniden başlatın.
8. Masaüstünden **AMS Map View**'ı (AMS Harita Görünümü) başlatın.
9. Harita Görünümünde MAC'i bulup sağ tıklayın.
10. Verileri yedeklemeden geçerli sistem verileriyle yeniden senkronize etmek için **Cold start MAC**'i (MAC'i soğuk başlatma) seçin.

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.

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.

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.

Doğrulama PIN'i

Daha yüksek güvenlik uygulamak için fiziksel bir kimlik bilgisiyle birlikte kullanılan bir Kişisel Tanıma Numarası (PIN).

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.

IDS

Hırsız alarm sistemi olarak da bilinen hırsız algılama sistemi.

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 Controller) olan Yerel Giriş Kontrol Cihazlarını koordine eden ve kontrol eden bir sunucu programı.

MAC sunucusu

Donanım: Bir MAC veya bir RMAC'nin çalıştığı DMS sunucusundan ayrı bir Access Engine ağındaki bir bilgisayar.

Montaj noktası

İnsanların bir binayı tahliye ettikten sonra beklemeleri gereken yer.

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.

Otomatik plaka tanıma (ANPR)

Genellikle karayolu taşıtlarının plakalarını okumak ve işlemek için video teknolojisinin kullanılması.

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).

SmartIntego

Simons Voss Technologies'in ürettiği bir dijital kilitleme sistemi. SmartIntego, bazı Bosch giriş kontrol sistemlerine entegre edilir.

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)

Access Engine'de kartlı geçiş verilerini yönetmek için en üst düzey bir süreç. DMS, verileri daha sonra AMC'lere sağlayan MAC'lere sağlar.

Veri Yönetim Sistemi (DMS)

Access Engine'de kartlı geçiş verilerini yönetmek için en üst düzey bir süreç. DMS, verileri daha sonra AMC'lere sağlayan MAC'lere sağlar.

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

© Bosch Security Systems B.V., 2020