Access Management System V5.0

Configuração e operação

pt-BR Software manual

Sumário

1	**Utilização da Ajuda**	**7**
2	**Sobre esta documentação**	**9**
3	**Visão geral do sistema AMS**	**10**
3.1	Alcançando a conformidade com a norma UL 1610	**10**
4	**Licenciamento do sistema**	**11**
5	**Configuração do calendário**	**12**
5.1	Definição de dias especiais	**12**
5.2	Definição de modelos de dia	**14**
5.3	Definição de modelos de tempo	**16**
6	**Configuração de divisões**	**19**
6.1	Atribuição de divisões a dispositivos	**20**
6.2	Atribuição de divisões a operadores	**20**
7	**Configuração dos endereços IP**	**21**
8	**Usando o Editor de dispositivos**	**22**
8.1	Modos de configuração e substituições	**23**
9	**Configuração de áreas de controle de acesso**	**24**
9.1	Configuração de áreas para veículos	**25**
10	**Configuração de painéis e áreas de intrusão**	**28**
10.1	Instalação da API do RPS de intrusão no computador do RPS	**29**
10.2	Conexão do sistema de controle de acesso aos painéis de intrusão	**30**
10.2.1	Etapa 1: definição da conexão com a API do RPS	**30**
10.2.2	Etapa 2: configuração das conexões de painel	**30**
10.3	Criação de perfis de autorizações para painéis	**31**
10.4	Atribuição de perfis de autorização do painel a titulares de cartão	**32**
10.5	Controle de portas pelos módulos B901 em painéis de intrusão	**33**
11	**Configuração de operadores e estações de trabalho**	**34**
11.1	Criação das estações de trabalho	**34**
11.2	Criação de perfis de estação de trabalho	**35**
11.3	Atribuição de perfis de estação de trabalho	**36**
11.4	Criação de perfis de usuário (operador)	**37**
11.5	Atribuição de perfis de usuário (operador)	**37**
11.6	Definição de senhas para os operadores	**38**
12	**Configurando cartões**	**40**
12.1	Definição do cartão	**40**
12.1.1	Ativar tipos de cartão	**40**
12.1.2	Criando e modificando	**40**
12.1.3	Ativando/desativando definições de cartão	**42**
12.1.4	Criando dados do cartão no gerenciador de caixas de diálogo	**42**
12.2	Configurando códigos de cartão	**43**
13	**Configuração dos controladores**	**46**
13.1	Configuração de MACs e RMACs	**46**
13.1.1	Configuração de um MAC no servidor DMS	**46**
13.1.2	Preparação de computadores do servidor MAC para executar MACs e RMACs	**47**
13.1.3	Configuração de um MAC em seu próprio servidor MAC	**48**
13.1.4	Adição de RMACs aos MACs	**49**
13.1.5	Adição de pares MAC/RMAC adicionais	**51**
13.1.6	Uso da ferramenta MACInstaller	**52**
13.2	Configuração dos LACs	**53**

13.2.1	Parâmetros e configurações do AMC	**55**
14	**Configuração de DTLS para comunicação segura**	**71**
14.1	Implantação de DTLS de cima para baixo	**73**
15	**Configuração de entradas**	**75**
15.1	Entradas – Introdução	**75**
15.2	Criação de entradas	**76**
15.3	Verificações de E/S adicionais	**79**
15.4	Configuração de terminais do AMC	**80**
15.5	Sinais predefinidos para modelos de porta	**86**
15.6	Entradas especiais	**93**
15.6.1	Elevadores (DM07)	**93**
15.6.2	Modelos de porta com alarmes de intrusão (DM14)	**96**
15.6.3	DIPs e DOPs (DM15)	**102**
15.6.4	Modelos de porta de eclusa	**103**
15.7	Portas	**105**
15.7.1	Espera REX	**109**
15.7.2	Configuração das portas para emitir alarmes locais	**110**
15.8	Leitores	**111**
15.8.1	Configuração da triagem aleatória	**124**
15.9	Acesso apenas com código PIN	**124**
15.10	Placas de extensão do AMC	**126**
16	**Configurações de leitor personalizadas**	**130**
16.1	Introdução	**130**
16.2	A propriedade do leitor: Parâmetros de leitor estendidos	**130**
16.3	Importação de um conjunto de parâmetros do leitor	**130**
16.4	Aplicação de um conjunto de parâmetros aos leitores	**131**
16.5	Gerenciamento de conjuntos de parâmetros do leitor	**132**
16.6	Exclusão de conjuntos de parâmetros do leitor	**133**
17	**Campos personalizados para dados de funcionários**	**134**
17.1	Pré-visualização e edição de campos personalizados	**134**
17.2	Regras para campos de dados	**137**
18	**Configuração do gerenciamento de nível de ameaça**	**138**
18.1	Conceitos do gerenciamento de nível de ameaça	**138**
18.2	Visão geral do processo de configuração	**138**
18.3	Etapas de configuração no Editor de dispositivos	**139**
18.3.1	Criação de um nível de ameaça	**139**
18.3.2	Criação de um perfil de segurança da porta	**140**
18.3.3	Criação de um perfil de segurança do leitor	**141**
18.3.4	Atribuição de perfis de segurança da porta e do leitor a entradas	**141**
18.3.5	Atribuição de um nível de ameaça a um sinal de hardware	**143**
18.4	Etapas de configuração em caixas de diálogo de dados do sistema	**144**
18.4.1	Criação de um perfil de segurança de pessoas	**144**
18.4.2	Atribuição de um perfil de segurança de pessoas a um tipo de pessoa	**145**
18.5	Etapas de configuração em caixas de diálogo de dados pessoais	**145**
19	**Configuração do Milestone XProtect para usar AMS**	**146**
20	**Integração do Otis Compass**	**149**
20.1	Configuração de um sistema Compass no Editor de dispositivos	**150**
20.1.1	Nível 1: configuração do sistema Compass	**150**
20.1.2	Nível 2: grupos de elevadores, dispositivos DES e DER	**151**

20.1.3	Nível 3: dispositivos DET	**153**
20.2	Configuração de campos personalizados para propriedades de titular de cartão específicas da Otis	**155**
20.3	Criação e configuração de autorizações para elevadores Otis	**157**
21	**Configuração do IDEMIA Universal BioBridge**	**158**
21.1	Configuração do BioBridge no sistema de controle de acesso da Bosch	**158**
21.2	Configuração do BioBridge no MorphoManager	**159**
21.2.1	Perfis de Wiegand	**160**
21.2.2	Configuração do dispositivo biométrico	**161**
21.2.3	Dispositivo biométrico	**164**
21.2.4	Configuração do usuário	**166**
21.2.5	Grupos de distribuição de usuários	**166**
21.2.6	Configuração do ODBC para BioBridge	**167**
21.2.7	Configuração do sistema BioBridge	**170**
21.3	Configuração do cliente de inscrição do BioBridge	**172**
21.3.1	Adição de um operador de inscrição ao MorphoManager	**172**
21.3.2	Configuração de computadores cliente do MorphoManager para tarefas de inscrição	**173**
21.3.3	Teste do cliente de inscrição	**175**
21.4	Suporte para diferentes formatos e tecnologias de cartão	**175**
21.5	Modos de identificação em dispositivos biométricos	**179**
21.5.1	Cartão OU biometria	**179**
21.5.2	Cartão E biometria	**181**
21.5.3	Somente biometria	**182**
21.6	Observações técnicas e limites	**182**
22	**Conformidade com a norma EN 60839**	**185**
23	**Definição de autorizações e perfis de acesso**	**186**
23.1	Criação de autorizações de acesso	**186**
23.2	Criação de perfis de acesso	**187**
24	**Criação e gerenciamento de dados de funcionários**	**189**
24.1	Pessoas	**190**
24.1.1	Opções de controle do cartão ou do edifício	**191**
24.1.2	Informações adicionais: gravação de informações definidas pelo usuário	**192**
24.1.3	Gravação de assinaturas	**192**
24.1.4	Cadastramento de dados de impressão digital	**193**
24.1.5	Registro dos dados de veias da palma da mão	**195**
24.2	Companies (Empresas)	**199**
24.3	Cartões: criação e atribuição de credenciais e permissões	**199**
24.3.1	Atribuição de cartões a pessoas	**200**
24.3.2	Impressão de crachás	**201**
24.3.3	Guia de autorizações	**202**
24.3.4	Guia de outros dados: isenções e permissões especiais	**203**
24.3.5	Autorizar pessoas a ativarem o modo Escritório	**204**
24.3.6	Guia SmartIntego	**205**
24.3.7	Criação de um cartão de alerta	**206**
24.4	Cartões temporários	**207**
24.5	Códigos PIN para funcionários	**208**
24.6	Bloqueio do acesso para funcionários	**210**
24.7	Cartões da lista negra	**211**
24.8	Edição de várias pessoas simultaneamente	**213**

24.8.1	Autorizações de grupo	**214**
24.9	Alteração da divisão para pessoas	**215**
24.10	Definição da área para pessoas ou veículos	**216**
24.10.1	Procedimento para redefinir a localização de todos os titulares de cartões e veículos	**217**
24.11	Personalizando e imprimindo formulários para dados de pessoal	**217**
25	**Gerenciamento de visitantes**	**219**
25.1	Dados do visitante	**219**
25.2	Visitante atrasado	**224**
26	**Gerenciamento de estacionamentos**	**227**
26.1	Estacionamento prolongado	**227**
26.2	Bilhetes de estacionamento	**228**
26.3	Exportação dos números de utilização do estacionamento	**234**
26.4	Exportação do controle de validade de automóveis	**234**
26.5	Autorizações para várias zonas de estacionamento	**235**
26.6	Relatório do estacionamento	**236**
26.7	Gerenciamento do estacionamento ampliado	**237**
27	**Gerenciamento de rondas de segurança e patrulhas**	**239**
27.1	Definição de rondas de segurança	**239**
27.2	Gerenciamento de patrulhas	**240**
27.3	Monitoramento de rondas (anteriormente controle de caminhos)	**241**
28	**Triagem aleatória de funcionários**	**243**
29	**Usando o visualizador de eventos**	**245**
29.1	Definição de critérios de filtragem para tempo relativo ao presente	**245**
29.2	Definição de critérios de filtragem para um intervalo de tempo	**246**
29.3	Definição de critérios de filtragem independentes do tempo	**246**
30	**Uso de relatórios**	**248**
30.1	Relatórios: Dados mestre	**248**
30.1.1	Relatório sobre veículos	**250**
30.2	Relatórios: Dados do sistema	**251**
30.3	Relatórios: Autorizações	**252**
31	**Operação do gerenciamento do nível de ameaça**	**254**
31.1	Acionamento e cancelamento de um alerta de ameaça por meio de um comando da interface do usuário	**254**
31.2	Acionamento de um alerta de ameaça por sinal de hardware	**255**
31.3	Acionamento de um alerta de ameaça por cartão de alerta	**255**
32	**Operação do Swipe ticker**	**256**
32.1	Casos especiais	**258**
33	**Backup e restauração**	**259**
33.1	Backup do sistema	**259**
33.2	Restauração de um backup	**260**
33.2.1	Restauração de RMACs em uma nova instalação	**262**
	Glossário	**263**

1 Utilização da Ajuda

Como usar este arquivo de ajuda.

Botões da barra de ferramentas

Botão	Função	Descrição
	Hide (Ocultar)	Clique neste botão para ocultar o painel de navegação (guias de índice, índice remissivo e pesquisa), deixando apenas o painel de ajuda visível.
	Show (Mostrar)	Quando o botão Hide (Ocultar) é clicado, ele é substituído pelo botão Show (Mostrar). Clique neste botão para abrir novamente o painel Navigation (Navegação).
	Back (Voltar)	Clique neste botão para percorrer a cadeia de tópicos vistos mais recentemente.
	Forward (Avançar)	Clique neste botão para avançar novamente pela mesma cadeia de tópicos
	Print (Imprimir)	Clique neste botão para imprimir. Selecione entre "Print the selected topic" (Imprimir o tópico selecionado) e "Print the selected heading and all subtopics" (Imprimir o cabeçalho selecionado e todos os sub-tópicos).

Guias

Contents (Índice) Esta guia exibe um índice hierárquico. Clique no ícone de livro  para abri-lo  , e em seguida clique no ícone do tópico  para exibir o tópico.

Index (Índice remissivo) Esta guia exibe um índice remissivo dos termos em ordem alfabética. Selecione um tópico na lista ou digite uma palavra para encontrar o(s) tópico(s) que a contém.

Search (Pesquisa) Utilize esta guia para localizar qualquer texto. Digite o texto no campo e em seguida clique no botão: **List Topics (Listar tópicos)** para localizar os tópicos que contêm todas as palavras digitadas.

Redimensionamento da janela de ajuda

Arraste o canto ou a borda da janela até o tamanho desejado.

Outras convenções utilizadas nesta documentação

– Texto literal (rótulos) na interface do usuário é exibido em **negrito**.

Por exemplo, **Tools (Ferramentas), File (Arquivo), Save As... (Salvar como...)**

- Sequências de cliques são concatenadas usando o caractere **>** (sinal de maior que).
  Por exemplo, **File > New > Folder (Arquivo > Novo > Pasta)**
- Mudanças no tipo de controle (por exemplo, menu, botão, caixa de seleção, tabulação) dentro de uma sequência são indicadas logo antes do rótulo do controle.
  Por exemplo, clicar no menu: **Extra > Options (Extra > Opções) >** guia: **View (Exibir)**
- Combinações de teclas são indicadas de duas maneiras:
  - Ctrl+Z significa manter pressionada a primeira tecla enquanto pressiona a segunda
  - Alt, C significa pressionar e soltar a primeira tecla, e em seguida pressionar a segunda
- As funções dos botões de ícone são descritas entre colchetes após o próprio ícone.
  Por exemplo, [Save] ([Salvar])

2 Sobre esta documentação

Este é o principal manual de software para o Access Management System.
Ele abrange o uso do principal programa do gerenciador de caixas de diálogo, denominados a partir de agora como AMS

– A configuração de um sistema de controle de acesso no AMS.
– A operação do sistema configurado por operadores do sistema.

Documentação relacionada

Os tópicos a seguir são documentados separadamente:

– A instalação AMS e seus programas auxiliares.
– A operação do AMS - Map View.

3 Visão geral do sistema AMS

O Access Management System é um poderoso sistema de controle de acesso puro, executado sozinho ou em sincronia com o BVMS, o principal sistema de gerenciamento de vídeo da Bosch.

Seu poder se origina do equilíbrio único entre tecnologias de ponta e comprovadas:

- Projetado para usabilidade: interface de usuário prática com Map View no estilo arrastar e soltar, e diálogos de cadastro biométrico otimizados.
- Projetado para segurança de dados: com suporte para os padrões mais recentes (UE-GDPR 2018), sistemas operacionais, bancos de dados e interfaces de sistema criptografadas.
- Projetado para resiliência: controladores de acesso principal em camada média oferecem failover e reposição automáticos de controladores de acesso locais em caso de falha na rede.
- Projetado para o futuro: atualizações periódicas e um canal cheio de melhorias inovadoras.
- Projetado para escalabilidade: oferecendo níveis de entrada baixo a alto
- Projetado para interoperabilidade: APIs RESTful, com interfaces para gerenciamento de vídeos da Bosch, manuseio de eventos e soluções de parceiros especializados.
- Projetado para proteger o investimento: permite aproveitar seu hardware de controle ao acesso instalado, porém, oferecendo maior eficiência

3.1 Alcançando a conformidade com a norma UL 1610

Os critérios para tornar seu sistema AMS compatível com a norma **UL 1610 grau 3** são descritos na nota técnica **Conformidade com a norma UL 1610 para sistemas AMS** (apenas em inglês), que está disponível para download na mesma página no catálogo online do produto AMS.

4 Licenciamento do sistema

Pré-requisitos

– O sistema foi instalado com êxito.
– Você fez login no computador do servidor AMS, preferencialmente como Administrador.

Procedimento para licenças adquiridas

Pré-requisitos: você adquiriu licenças com base na assinatura deste computador. Entre em contato com o representante de vendas para obter instruções.

Ativação da licença

Caminho

– Gerenciador de caixas de diálogo do AMS > **Menu principal** > **Configuração** > **Licenças**

1. Clique em **Gerenciador de licenças**
   O assistente do **Gerenciador de licenças** é aberto.
2. Clique em **Salvar** para salvar as informações do sistema em um arquivo.
3. Clique em **Continuar**.
4. Faça login no Remote Portal remote.boschsecurity.com com as credenciais da sua empresa.
5. Selecione o produto que deseja licenciar e siga as instruções no portal para gerar e baixar seu arquivo de licença.
6. Retorne ao **Gerenciador de licenças**.
7. Clique em **Continuar**.
8. Clique em **Importar** para localizar o arquivo de licença que você baixou e adicioná-lo ao seu sistema.
9. Clique em **Concluir**.

Aviso!
Se você encontrar alguma mensagem de erro durante o processo, entre em contato com o suporte da Bosch.

Aviso!
Efeitos de alterações de hardware e software
Alterações no hardware do servidor podem invalidar sua licença e fazer com que o software para de funcionar. Consulte o suporte técnico antes de fazer alterações no servidor.

Procedimento para o modo de demonstração

O Modo de demonstração licencia todos os recursos do sistema durante um período limitado. Use o Modo de demonstração somente em ambientes não relacionados à produção para testar os recursos antes de adquiri-los.

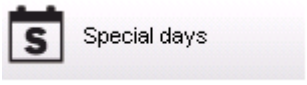
1. Faça login no Gerenciador de acesso
2. Navegue até **Configuration (Configuração)** > **Licenses (Licenças)**
3. Clique no botão **Activate Demo Mode (Ativar modo de demonstração)**
4. Verifique se os recursos estão listados na janela da caixa de diálogo **Licenses (Licenças)**.

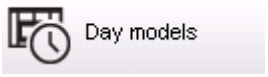
O modo de demonstração é ativado para 5 horas. Observe que o tempo de expiração é exibido próximo ao topo da caixa de diálogo **Licenses (Licenças)** e na barra de títulos da maioria das janelas de caixa de diálogo.

5 Configuração do calendário

O agendamento de atividades de controle de acesso é governado por **modelos de tempo**.
Um **modelo de tempo** é uma sequência abstrata de um ou mais dias, cada um deles descrito por um **modelo de dia**.
Os modelos de tempo controlam atividades quando são aplicados ao **calendário** subjacente do sistema de controle de acesso.
O calendário do sistema de controle de acesso se baseia no calendário do sistema operacional do computador host, mas o amplifica com **dias especiais** definidos livremente pelo administrador do sistema de controle de acesso.
Os dias especiais podem ser fixados em uma data específica no calendário ou definidos em relação a um evento cultural, como a Páscoa. Podem ser recorrentes ou não.
A configuração de um calendário eficaz para o sistema de controle de acesso é composta pelas seguintes etapas.

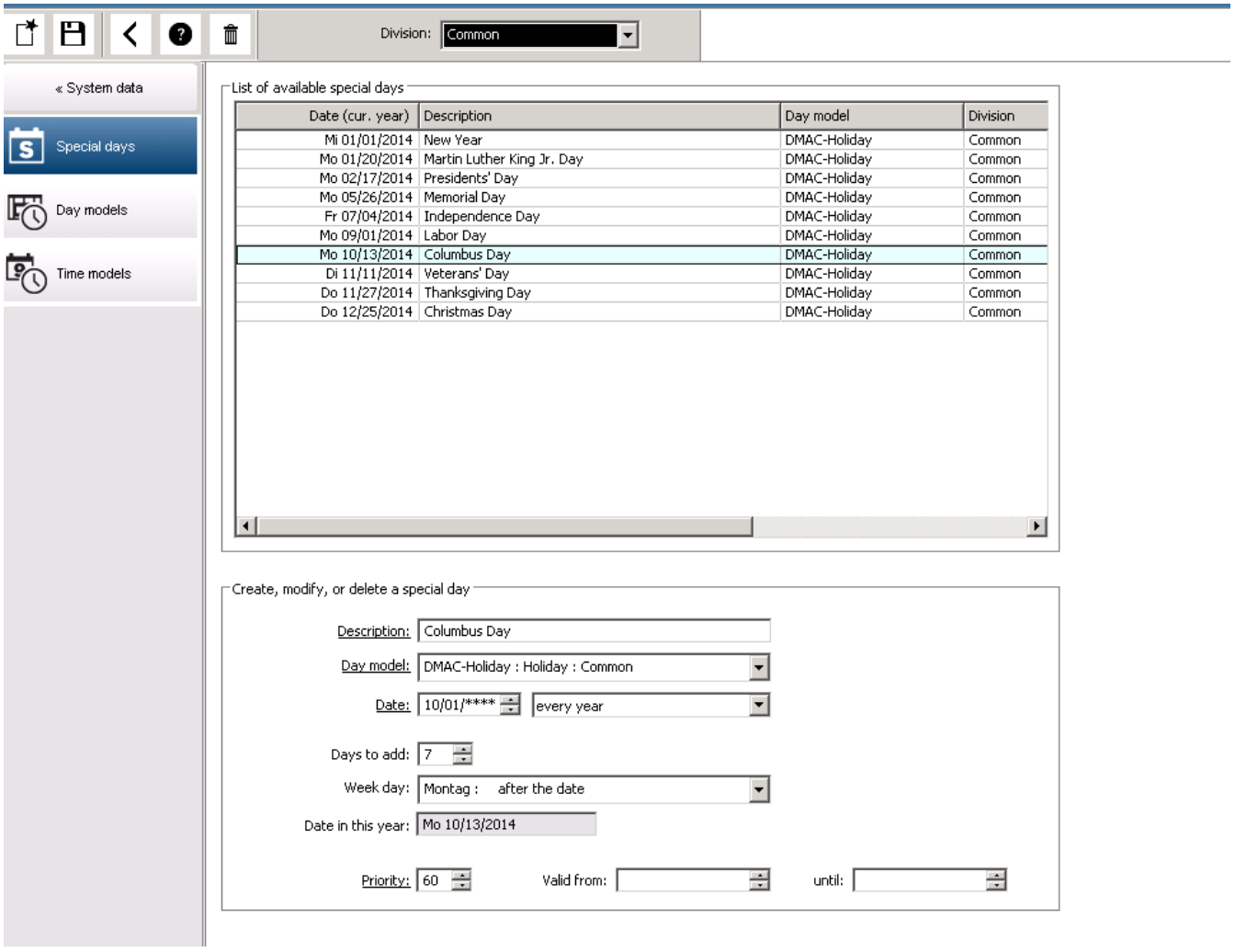
1. Defina os **dias especiais** do calendário que se aplicam à sua localização.
2. Defina **modelos de dia** que descrevem os períodos ativos e inativos de cada tipo de dia. Por exemplo, o modelo de dia para um feriado será diferente do modelo para um dia útil normal. O trabalho em turnos também afetará o tipo e o número de modelos de dia necessários.
3. Defina **modelos de tempo** formados por um ou mais modelos de dia.
4. Atribua modelos de tempo para titulares de cartões, autorizações e entradas.





5.1 Definição de dias especiais

Quando aberta, no campo de listagem superior da caixa de diálogo é exibida uma lista que contém todos os feriados especificados. Observe que todas as datas de feriados mostradas referem-se apenas ao ano em curso. No entanto, o calendário é atualizado de ano para ano de acordo com os dados inseridos.
Abaixo da lista há diferentes campos da caixa de diálogo para a criação de novos dias especiais, e para a alteração ou exclusão dos dias especiais existentes. Para adicionar um novo dia especial, pelo menos três destes campos devem conter dados. Primeiro, digite **uma descrição e** uma **data** nos respectivos campos. Em terceiro lugar, a **categoria** à qual pertence este dia especial deve ser selecionada na lista de seleção apropriada.



A data é especificada em várias etapas. Antes de tudo, uma data base é inserida no campo **Date (Data)**. Neste momento, a data descreve um evento no ano em curso. Se agora o usuário especifica a frequência de um retorno periódico na lista de seleção ao lado do campo de data, as partes da data definidas pela periodicidade serão substituídas por "caracteres curinga" (*).

uma vez	__.__.____
uma vez por ano	__.__.****
uma vez por mês durante um ano	__.**.____
uma vez por mês a cada ano	__.**.****
dependendo da Páscoa	**.**.****

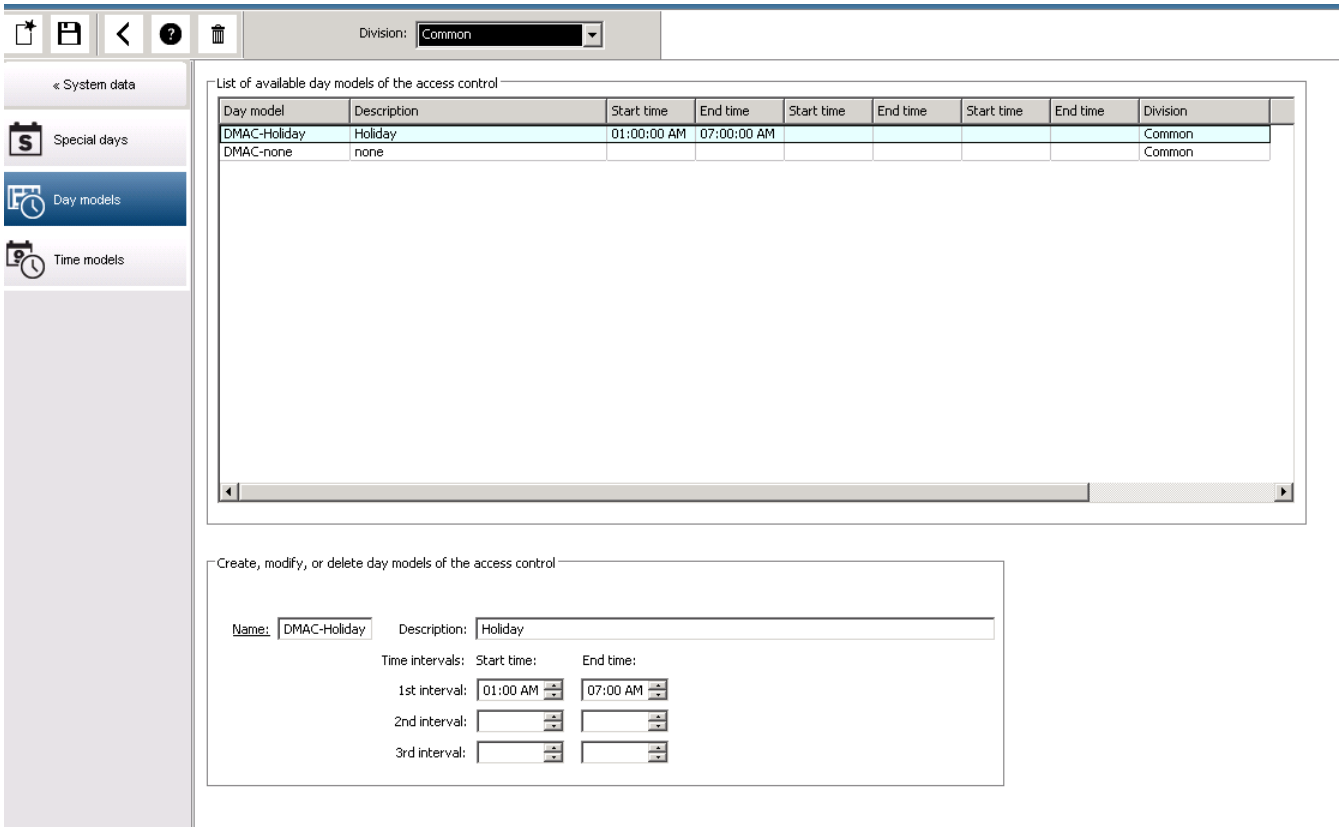
Os feriados que dependem da Páscoa não são especificados com sua data, mas com a diferença de dias desde o domingo de Páscoa. A data do domingo de Páscoa no ano em curso é indicada no campo **Date within this year (Data dentro deste ano),** e a variação desta data é digitada ou selecionada no campo **Days to add (Dias a adicionar)**. O número máximo de dias é 188, então pela adição ou subtração você pode definir todos os dias do ano.
Os outros dados, por exemplo, o **dia da semana** do feriado, são opcionais. Observe que a lista de dias da semana é determinada pelas configurações regionais do sistema operacional (SO). Isso inevitavelmente resulta na exibição de diversos idiomas, onde os idiomas do sistema de controle de acesso e do SO diferem.

A atribuição de um **período de validade** também é opcional. Se nenhuma duração for especificada, as configurações padrão tornam a validade ilimitada a partir da data de digitação.
Uma **prioridade** também pode ser definida. A prioridade, que vai de 1 a 100, define se o feriado deve ser usado. Se dois feriados caírem na mesma data, o feriado com a maior prioridade vem em primeiro lugar. No caso de prioridades iguais, o feriado que será usado permanece indefinido.
Feriados com prioridade "0" são desativados e não serão utilizados.
A caixa de diálogo **Time Models (Modelos de tempo)** mostra apenas os feriados ativos, isto é, com prioridade maior que 0.

Aviso!
Um modelo de tempo da divisão "Comum" só pode usar feriados atribuídos à divisão "Comum".
Um modelo de tempo de uma divisão específica "A" só pode usar feriados atribuídos à divisão "A".
Não é possível misturar feriados entre divisões, ou seja, cada divisão só pode usar os feriados especificamente atribuídos a ela em seu modelo de tempo específico.

5.2 Definição de modelos de dia

Os modelos de dia definem um padrão para qualquer dia. Eles podem ter até três intervalos de tempo.
Quando a caixa de diálogo é aberta, todos os modelos de dia existentes são exibidos.



Use a caixa de diálogo para definir ou modificar o nome, as descrições e os intervalos do modelo. O ícone  inicia um novo modelo.
As horas Inicial e Final do intervalo são inseridas em horas e minutos. Quando esta hora é atingida, o intervalo é ativado ou desativado, respectivamente. Para marcar mais claramente estes horários como delimitadores, o painel da lista os exibe com segundos (sempre 00). Por exemplo, uma autorização em um modelo de tempo que contenha o intervalo 08:00–15:30 permite o acesso das 08:00 às 15:30, mas vai impedir o acesso às 15:30:01.
As horas inicial e final são submetidas a verificações lógicas ao serem inseridas, por exemplo, uma hora inicial deve ser anterior à sua hora final correspondente.
Uma consequência disso é que nenhum intervalo pode ultrapassar a meia-noite, e deve ser dividido neste ponto:

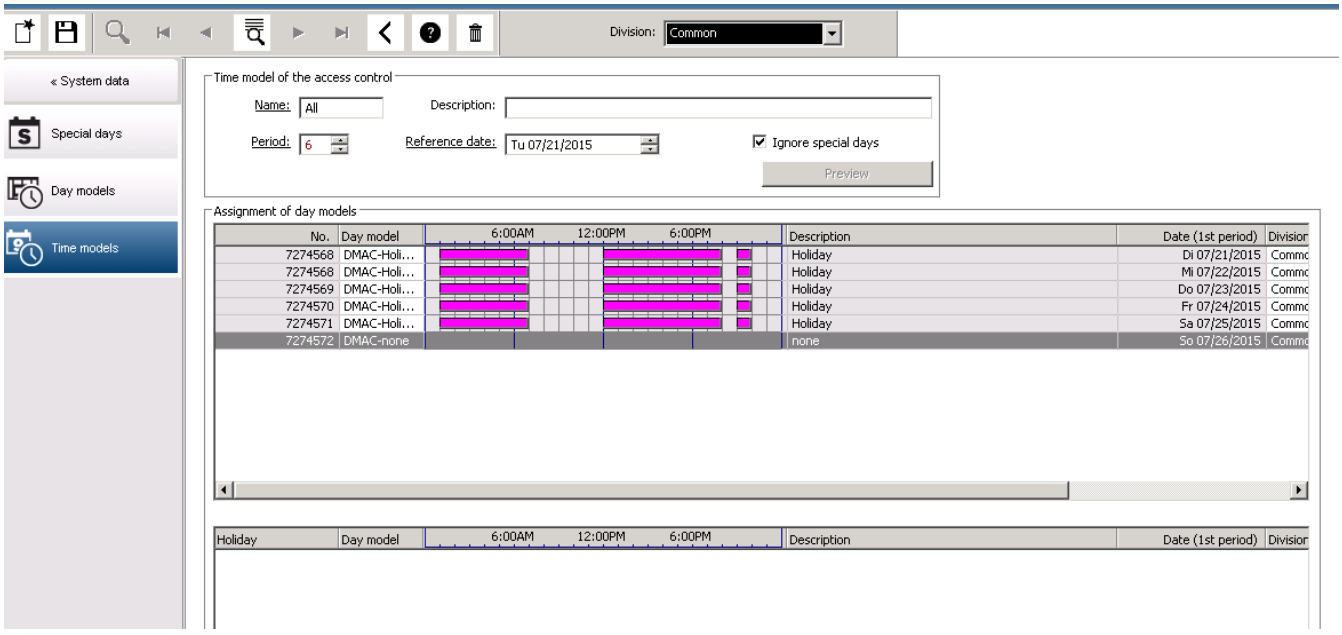
1º Intervalo	de:	...	até:	00:00
Intervalo seguinte	de:	00:00	até:	...

Com a exceção da meia-noite (00:00) nenhuma sobreposição é permitida entre os delimitadores de intervalo de um modelo de dia individual. Observe que isto impede a digitação da mesma hora para o final de um intervalo e o início do seguinte.
Exceção: no entanto, o intervalo de 24 horas tem ambas as horas inicial e final definidas como 00:00.

Aviso!
Dica: Você pode verificar os intervalos visualizando-os na caixa de diálogo Modelos de tempo: primeiro crie um modelo de dia contendo estes intervalos (System data > Calendar > Day models (Dados do sistema > Calendário > Modelos de dia)). Em seguida, atribua esse modelo de dia a um modelo de tempo fictício com o período de um dia (System data > Calendar > Time models (Dados do sistema> Calendário > Modelos de tempo)). Em seguida, os intervalos são ilustrados no gráfico de barras.
Saia da caixa de diálogo Time models (Modelos de tempo) sem salvar as alterações.

O modelo de dia só pode ser excluído se não tiver sido atribuído a um dia especial, e se não estiver sendo usado em um modelo de tempo.

5.3 Definição de modelos de tempo



Os modelos de tempo existentes podem ser selecionados na lista de pesquisa, e seus detalhes são exibidos nos campos da caixa de diálogo. Todo o processamento é realizado em conformidade com o procedimento para a criação de novos modelos de tempo.

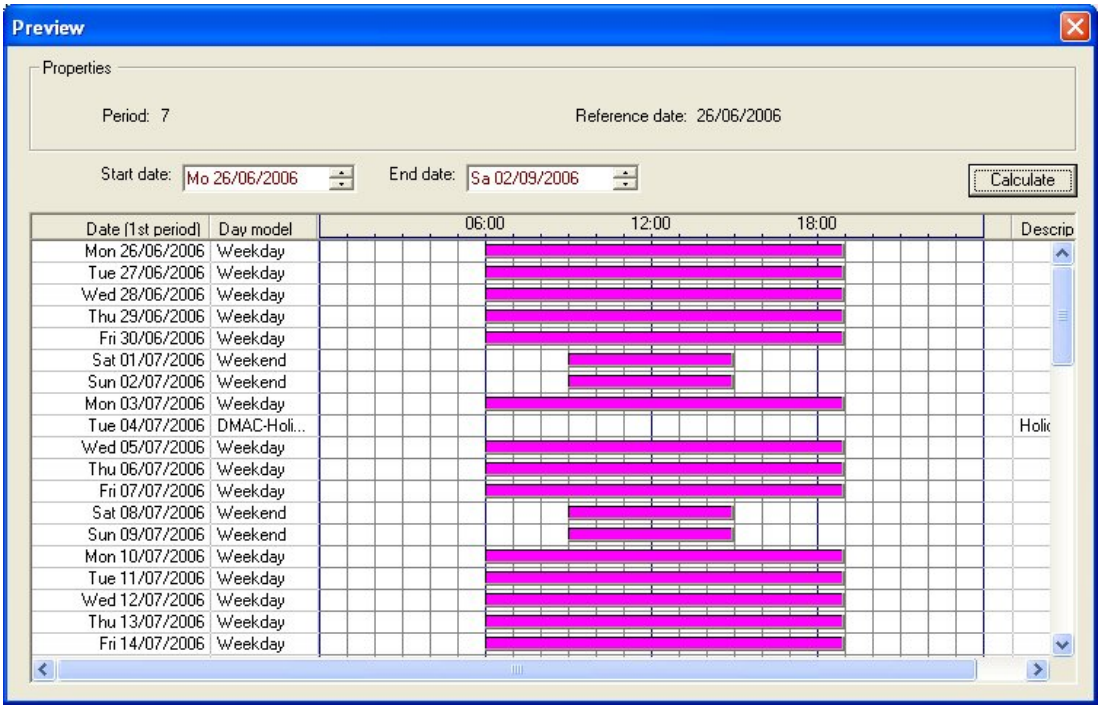
Se a máscara estiver vazia, o modelo de tempo pode ser criado do zero. Para tanto, você deve inserir um **nome** e o número de dias em **período** e selecionar uma data inicial ou **data de referência**. Quando esses dados são confirmados (**Enter**), uma lista é exibida no campo **Assignment of day models (Atribuição de modelos de dia)** da caixa de diálogo abaixo. O número de linhas dessa lista corresponde ao número de dias estabelecidos acima, e as colunas já contêm um número progressivo e as datas do período, começando com a data inicial selecionada.

Somente os itens da coluna **"Name" (Nome)** podem ser alterados ou inseridos pelo usuário na lista – como já mencionado, os itens das colunas **"No" (Número)** e **"Date" (Data)** são originados das declarações do cabeçalho da caixa de diálogo; a coluna **"Description" (Descrição)** é preenchida pelo sistema com a seleção de um modelo de dia, e as explicações digitadas nesta caixa de diálogo.

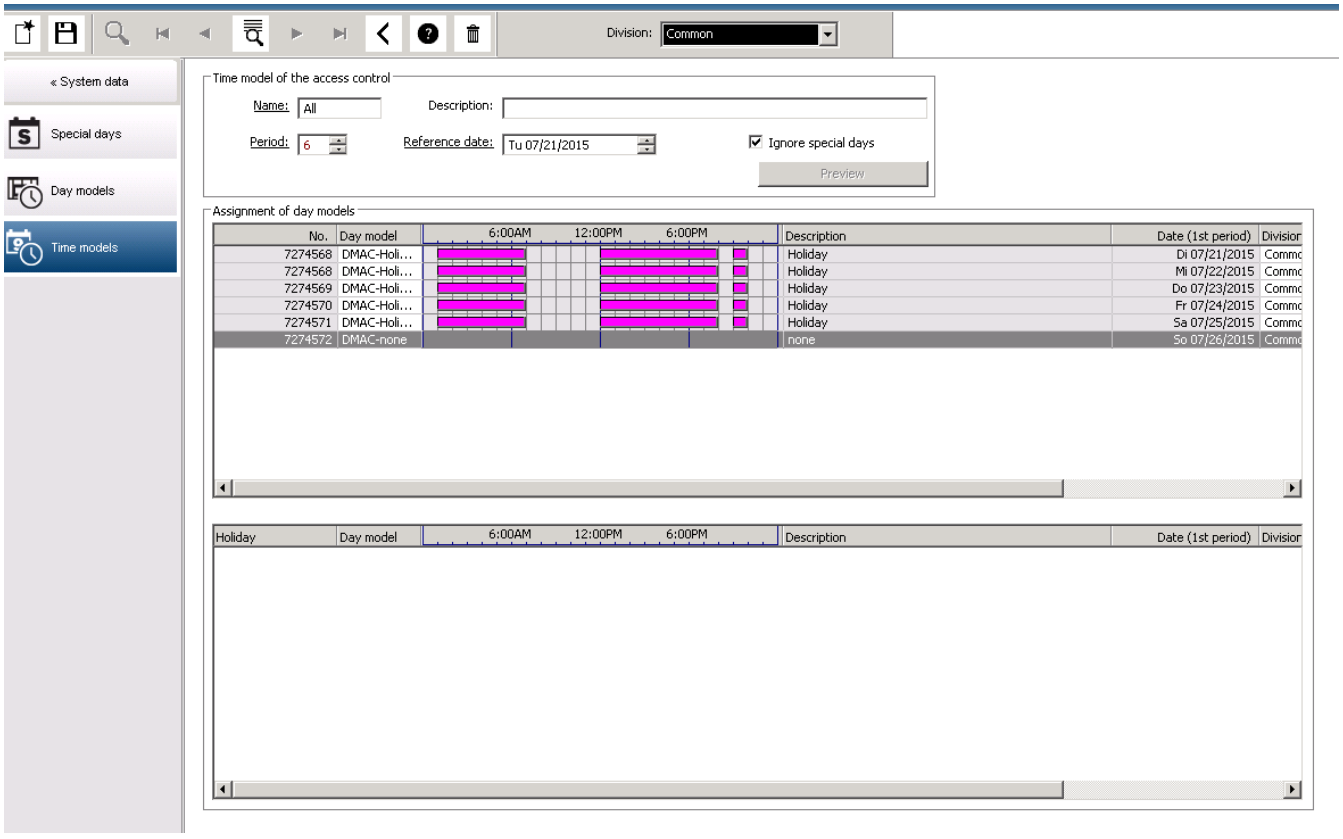
Ao clicar duas vezes na linha relevante da coluna **Day model (Modelo de dia)**, um campo de listagem é ativado para seleção. Um dos modelos de dia existentes pode ser selecionado nesta lista. Desse modo, um modelo de dia específico pode ser atribuído a cada dia do período. Quando o usuário passa para outra linha, uma descrição existente do modelo de dia selecionado é indicada pelo sistema na coluna **Description (Descrição)**.

Os **feriados** predefinidos, junto com os modelos de dia relevantes, são mostrados no campo de listagem inferior para fins de verificação e navegação. Para o modelo de tempo selecionado ou recém-criado, a atribuição de modelos de dia a certos feriados pode ser alterada. No entanto, essas alterações só serão aplicadas a este modelo de tempo específico – as modificações gerais que devem se aplicar a todos os modelos existentes e futuros só poderão ser realizadas na caixa de diálogo Feriados. Em linha com estas definições, os modelos de dia são, então, atribuídos aos dias da semana, levando em consideração os feriados.

Em seguida, em conformidade com essas definições, os dias da semana são confrontados com os modelos de dia atribuídos levando em consideração os dias especiais. Para verificar rapidamente se os modelos de dia foram utilizados e atribuídos corretamente – especialmente no caso dos feriados – esta caixa de diálogo contém uma **visualização** que mostra a alocação diária de certos períodos.
Finalmente, uma caixa de diálogo separada é aberta clicando no botão **Preview (Visualizar)** e um período de até 90 dias pode ser especificado, incluindo feriados. Ao clicar no botão **Calculate (Calcular)**, o relatório é composto e exibido como mostrado abaixo – este processo pode levar alguns segundos, dependendo do tamanho do intervalo.



Na configuração padrão, os dias especiais são aplicados aos modelos de tempo de acordo com suas definições. No entanto, se excepcionalmente os dias especiais não exigirem nenhuma consideração, isto pode ser configurado selecionando a opção **Ignore special days (Ignorar dias especiais)**. Simultaneamente, os itens das duas listas inferiores são excluídos, para que fique imediatamente evidente para o usuário que os dias e categorias de dia especiais não são utilizados neste modelo.


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

6 Configuração de divisões

Introdução

O sistema pode ser licenciado opcionalmente para fornecer controle de acesso conjunto para uma propriedade que é compartilhada por qualquer número de partes independentes, chamadas de **divisões**.

Os operadores do sistema podem ter uma ou mais divisões atribuídas a eles. Os operadores então veem apenas as pessoas, dispositivos e entradas dessas divisões.

Quando o recurso **Divisões** não for licenciado, todos os objetos gerenciados pelo sistema pertencerão a uma única divisão chamada **Comum**.

Pré-requisitos

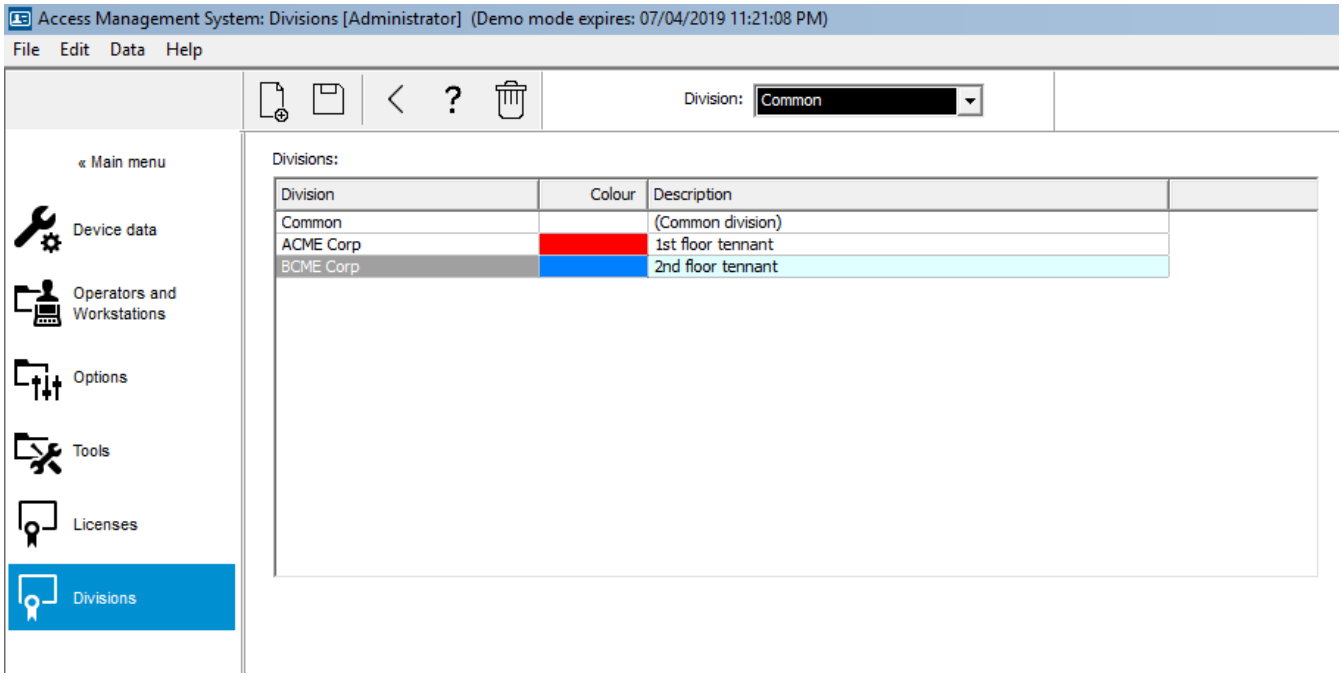
– O recurso Divisões deve estar licenciado para a instalação.

Caminho da caixa de diálogo

– Main menu (Menu principal) > **Configuration (Configuração)** > **Divisions (Divisões)**
– Navegador de configuração do BIS > **Locations (Locais)** > **Divisions (Divisões)**

Procedimento

1. Clique no botão ✚ ou clique com o botão direito do mouse em **Common (Comum)** e selecione **Add new division (Adicionar nova divisão)** no menu de contexto.
2. Clique em  na barra de ferramentas.
   – Uma divisão é criada com um nome padrão.
3. Substitua o nome padrão e (opcional) insira uma descrição para o benefício de outros operadores.
4. Clique na coluna **Color (Cor)** para atribuir uma cor para ajudar a diferenciar os ativos da divisão na interface do usuário.
5. Clique em **Apply (Aplicar)** para salvar
6. Clique em  para salvar



6.1 Atribuição de divisões a dispositivos

Atribuição de divisões a dispositivos no Editor de dispositivos

Caminho da caixa de diálogo

Main menu (Menu principal) > **Configuration (Configuração)** > **Device data (Dados do dispositivo)**

Pré-requisitos

– As divisões devem estar licenciadas e funcionado.
– Pelo menos uma divisão deve ter sido criada.

Procedimento

1. Selecione o dispositivo para atribuição na árvore de dispositivos.
   – O Editor de dispositivos é exibido no painel de diálogo principal.
2. Na lista Division (Divisão), selecione a nova divisão para o dispositivo
   – A caixa de listagem reflete a nova divisão.
3. Clique em  (Salvar) para salvar

Aviso!
Todos os componentes de uma entrada devem pertencer a uma divisão
O sistema só permitirá que você salve uma entrada quando todos os seus componentes pertencerem à mesma divisão.

6.2 Atribuição de divisões a operadores

Atribua divisões aos operadores na caixa de diálogo **User rights (Direitos de usuário)**

Caminho da caixa de diálogo

Main menu (Menu principal) > **Configuration (Configuração)** > **Operators and workstations (Operadores e estações de trabalho) > User rights (Direitos de usuário)**

Pré-requisitos

– As divisões devem estar licenciadas e funcionado.
– Pelo menos uma divisão deve ter sido criada.
– Pelo menos um operador deve ter sido criado no sistema

Procedimento

1. Na caixa de diálogo **User rights (Direitos de usuário)**, selecione o registro pessoal do operador a ser atribuído.
2. Na guia **Divisions (Divisões)**, use as teclas de seta para mover as divisões da lista de **Available divisions (Divisões disponíveis)** para a lista de **Assigned divisions (Divisões atribuídas)** desse operador.
3. Clique em  (Salvar) para salvar

7 Configuração dos endereços IP

Os controladores de acesso locais na rede exigem um esquema consistente de endereços IP para participarem do sistema de controle de acesso. A ferramenta **AccessIPConfig** localiza os controladores na rede e fornece uma interface conveniente para administrar seus endereços e outras opções de rede de forma centralizada.

Pré-requisitos

– Os controladores de acesso locais estão ligados e conectados à rede.
– Você tem um esquema para os endereços IP dos controladores e suas senhas, se necessário.

Caminho da caixa de diálogo

Main menu (Menu principal) > **Configuration (Configuração)** > **Tools (Ferramentas)**

Procedimento

1. Siga o caminho da caixa de diálogo acima e clique em **Configuration AMC and fingerprint devices (Configuração de AMC e de dispositivos de impressões digitais)**
   A ferramenta **AccessIPConfig** é aberta.
2. Clique em **Scan AMCs (Digitalizar AMCs)**
   Os controladores de acesso locais disponíveis na rede são listados, cada um com os seguintes parâmetros:
   – **MAC address (Endereço MAC)**: o endereço do hardware do controlador. Observe, isso **não** é o endereço do Controlador de acesso principal, que é chamado de MAC apenas por coincidência.
   – **Stored IP address (Endereço IP armazenado)**:
   – **Port number (Número de porta)**: o padrão é `10001`
   – **DHCP**: o valor é **Yes (Sim)** somente se o controlador estiver configurado para receber um endereço IP do DHCP
   – **Current IP addresss (Endereço IP atual)**
   – **Serial number (Número de série)**
   – Observações adicionadas pela equipe de configuração da rede
3. Clique duas vezes em um AMC na lista para alterar seus parâmetros em uma janela pop-up. Como alternativa, selecione a linha do AMC desejado e clique em **Set IP... (Definir IP...)** Observe que poderá ser necessário inserir uma senha, caso tenha sido configurada para o dispositivo.
   Os parâmetros modificados são armazenados assim que você clicar em OK na janela pop-up.
4. Ao terminar de configurar os parâmetros de IP dos controladores, clique em **File (Arquivo)** > **Exit (Sair)** para fechar a ferramenta.
   Você retornará ao aplicativo principal.

Para obter informações mais detalhadas, clique em **Help (Ajuda)** na ferramenta **AccessIPConfig** para exibir seu próprio arquivo de ajuda.

8 Usando o Editor de dispositivos

Introdução

O Editor de dispositivos é uma ferramenta para adicionar, excluir ou modificar entradas e dispositivos.

O Editor de dispositivos oferece visualizações para as seguintes hierarquias editáveis:

- **Configuração do dispositivo**: os dispositivos eletrônicos dentro do sistema de controle de acesso.
- **Estações de trabalho**: os computadores que cooperam no sistema de controle de acesso.
- **Áreas**: as áreas físicas em que o sistema de controle de acesso é dividido.

Pré-requisitos

O sistema está instalado corretamente, licenciado e na rede.

Caminho da caixa de diálogo

- **Main menu (Menu principal)** > **Configuration (Configuração)** > **Device data (Dados do dispositivo)**
- **Navegador de configuração do BIS** > **Connections (Conexões)** > **Device data (Dados do dispositivo)**

Usando a barra de ferramentas do Editor de dispositivos

A barra de ferramentas do Editor de dispositivos oferece as seguintes funções, independentemente da visualização ativa: **Dispositivos**, **Estações de trabalho** ou **Áreas**.

Botão	Atalho	Descrição
	Ctrl + N	Cria um novo item abaixo do nó selecionado. Como alternativa, clique com o botão direito no nó para exibir o menu de contexto.
	Del	Exclui o item selecionado e tudo abaixo dele.
	Ctrl-Page up	Primeiro item na árvore
	Ctrl -	Item anterior
	Ctrl +	Próximo item
	Ctrl-Page down	Último item na árvore
	Ctrl-A	Expande e recolhe a árvore.
	Ctrl-K	Atualiza os dados recarregando-os no banco de dados. **Todas as alterações não salvas são descartadas.**
	Ctrl-S	Salva a configuração atual
	Ctrl-F	Abre uma janela de pesquisa

		Abrir a árvore **Configuração do dispositivo**
		Abrir a árvore **Estações de trabalho**
		Abrir a árvore **Áreas**

Em todas as visualizações do Editor de dispositivos, comece na raiz da árvore e adicione itens usando os botões da barra de ferramentas, o menu ou o menu de contexto de cada item (clique com o botão direito para acessá-lo). Para adicionar subitens a um dispositivo, primeiro selecione o dispositivo pai em que os subitens devem aparecer.

Copiando e colando dispositivos AMC

Para copiar dispositivos AMC de uma parte da árvore para outra:

1. Clique com o botão direito no dispositivo AMC e selecione **Copiar** no menu de contexto.
2. Clique com o botão direito em um dispositivo pai adequado em qualquer lugar da árvore e selecione **Colar** no menu de contexto.
   - O dispositivo é copiado para o novo local com seus subdispositivos e configurações.
   - Parâmetros de dispositivo, como **Endereço IP** e **Nome**, que devem ser exclusivos, **não** são copiados.
3. Insira valores exclusivos para os parâmetros de dispositivo que precisarem deles. Até fazer isso, você não poderá salvar a árvore de dispositivos.

Salvando seu trabalho

Quando terminar de adicionar e modificar itens na árvore, clique em **Salvar**  para salvar a configuração.

Para fechar o Editor de dispositivos, clique em **Arquivo** > **Sair**.

8.1 Modos de configuração e substituições

Modo de configuração é o estado padrão dos dispositivos de controle de acesso no editor de dispositivos. No modo de configuração, um usuário autorizado do AMS ou BIS ACE pode fazer alterações nos dispositivos no editor de dispositivos, e o ACS propaga as alterações imediatamente para os dispositivos subordinados.

Um operador pode **substituir** o modo de configuração enviando comandos de fora do editor de dispositivos diretamente para os dispositivos de controle de acesso. Isso é comum, por exemplo, quando um operador lida com mensagens e alarmes recebidos. Até o operador enviar o comando **Restaurar configuração**, o dispositivo continua no Modo de operação .

Se um usuário de configuração selecionar um dispositivo no editor durante o modo de operação, a página de propriedade principal do dispositivo exibirá a notificação:

Este dispositivo não está no modo de configuração.

O usuário pode fazer e salvar alterações de configuração, mas as alterações são armazenadas e não entram em vigor até o modo de operação de alarme terminar e o modo de configuração ser restaurado.

9 Configuração de áreas de controle de acesso

Introdução às Áreas

Instalações de segurança podem ser divididas em Áreas. As áreas podem ser de qualquer tamanho: um ou vários edifícios, andares individuais ou até mesmo salas individuais.

Alguns usos de Áreas são:

- A localização de pessoas individuais dentro das instalações de segurança.
- A estimativa do número de pessoas dentro de uma determinada área, em caso de uma evacuação ou outra emergência.
- A limitação do número de pessoas ou veículos em uma área:
  Quando o limite da população predefinido é atingido, outras admissões podem ser rejeitadas até que algumas pessoas ou veículos deixem a área.
- Implementação do controle da sequência de acesso e anti-passback

O sistema distingue entre dois tipos de áreas com controle de acesso

- Áreas para pessoas
- Áreas para veículos (estacionamentos)

Cada área pode ter subáreas para granularidade de controle mais fina. Áreas para pessoas podem ter até três níveis de aninhamento e áreas para estacionamentos somente dois, o estacionamento geral e zonas de estacionamento, entre 1 e 24 em número.

A área padrão, que existe em todas as instalações, é chamada de **Outside (Parte externa)**. Ela serve como pai para todas as áreas de ambos os tipos definidas pelo usuário: para pessoas e estacionamentos.

Uma área não é utilizável a menos que no mínimo uma entrada leve até ela.

O Editor de dispositivos **DevEdit** pode ser usado para atribuir uma área de localização e uma área de destino a qualquer entrada. Quando alguém faz a leitura de um cartão em um leitor que pertence a uma entrada, a nova localização da pessoa torna-se a área de destino daquela entrada.

Aviso!

O controle da sequência de acesso e anti-passback exigem leitores de entrada e saída nas entradas das áreas.

Entradas do tipo catraca são fortemente recomendadas para evitar que uma pessoa entre "a reboque" de outra forma acidental ou deliberada

Procedimento para criação de áreas

Pré-requisitos

Como um operador do sistema, você precisa de autorização do administrador do sistema para criar áreas.

Caminho da caixa de diálogo (AMS)

1. No gerenciador de caixas de diálogo do AMS, selecione **Main menu (Menu principal)** > **Configuration (Configuração)** > **Device data (Dados do dispositivo)**
2. Clique em Áreas 

3. Selecione o nó **Outside (Parte externa)** ou um de seus filhos e clique em  na barra de ferramentas. Como alternativa, clique com o botão direito em **Outside (Parte externa)** para adicionar uma área por meio do menu de contexto.
   Todas as áreas criadas recebem inicialmente um nome exclusivo de **Área** e um sufixo numérico.
4. Na janela pop-up selecione o tipo, isto é, **Area (Área)** para pessoas ou **Parking lot (Estacionamento)** para veículos.
   Observe que somente **Outside (Parte externa)** pode ter filhos de ambos os tipos. Qualquer subárea desses filhos sempre herda o tipo do respectivo pai.
   - **Áreas** para pessoas podem ser aninhadas a três níveis. Para cada área ou subárea você pode definir uma população máxima.
   - **Estacionamentos** são entidades virtuais formadas por pelo menos uma **zona de estacionamento**. Se a população de um estacionamento não precisar ser limitada pelo sistema, é exibido 0. Caso contrário, o número máximo de espaços para estacionar por zona é 9999 e o painel principal do estacionamento exibe a soma de todos os espaços em suas zonas.

Procedimento para edição de áreas

1. Clique em uma área na hierarquia para selecioná-la.
2. Substitua um ou mais dos seguintes atributos no painel principal da caixa de diálogo.

Name (Nome)	O nome padrão, que você pode substituir.
Description (Descrição)	Uma descrição de texto livre da área.
Maximum number of persons / cars (Número máximo de pessoas/ veículos)	O valor padrão 0 (zero) significa sem limites. Caso contrário, insira um número inteiro que representa o número máximo de pessoas.

Observações:

- Não é possível mover uma área arrastando-a e, depois, soltando-a em uma derivação diferente da hierarquia. Se necessário, exclua a área e crie novamente em outra derivação.
- O campo **Division (Divisão)** nessa caixa de diálogo é somente para leitura. Para alterar a divisão de uma área, use a caixa de diálogo **Detector placement (Posicionamento do detector)** e selecione a área no painel **Devices (Dispositivos)**.

Procedimento para exclusão de áreas.

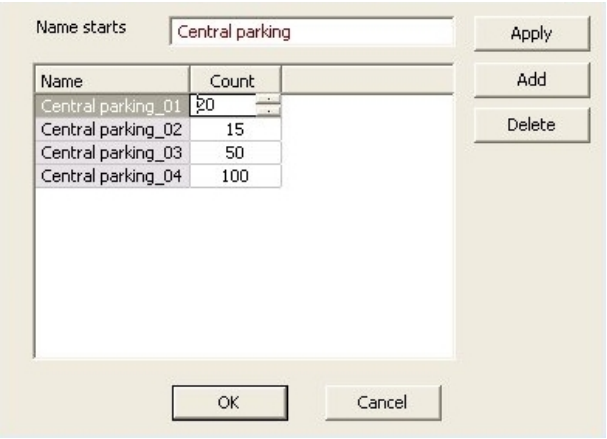
1. Clique em uma área na hierarquia para selecioná-la.
2. Clique em **Delete (Excluir)**  ou clique com o botão direito para excluir por meio do menu de contexto.

Observação: Uma área não pode ser excluída até que todas suas filhas tenham sido excluídas.

9.1 Configuração de áreas para veículos

Criação de áreas para veículos (estacionamento, zona de estacionamento)

Se você selecionar um tipo de área de **Parking lot (Estacionamento)**, é exibida uma janela pop-up.



1. Insira um nome no campo **Name starts with (Nome começa com)** para criar um nome principal para todas suas subáreas de estacionamento ou **zonas de estacionamento**. Até 24 **zonas de estacionamento** podem ser criadas usando o botão **Add (Adicionar)** e cada uma terá o nome principal mais um sufixo de dois dígitos.
2. Se o sistema deve limitar a população dessas áreas, insira o número de espaços para estacionar na coluna **Count (Contagem)**. Se não for necessário um limite, insira 0.

Observação: A população máxima de todo o estacionamento é a soma desses números. Somente zonas de estacionamento podem conter espaços para estacionar. O **estacionamento** é apenas uma entidade virtual formada por uma ou mais **zonas de estacionamento**. O número máximo de espaços para estacionar por zona é 9999.

Criação de entradas para estacionamentos

Da mesma forma que as áreas normais, os estacionamentos também exigem uma entrada. O modelo de porta adequado é **Parking lot 05c (Estacionamento 05c)**.

Para monitorar a população de um estacionamento, são necessárias duas entradas com esse modelo de porta no mesmo AMC, uma para entrada e uma para saída.

Pré-requisito

Crie um estacionamento com pelo menos uma zona de estacionamento, conforme descrito acima.

Caminho da caixa de diálogo

Main menu (Menu principal) > **Configuration (Configuração)** > **Device data (Dados do dispositivo)**

Clique em **LACs/Entrances/Devices (LACs/Entradas/Dispositivos)** 

Procedimento

1. Na hierarquia do dispositivo, crie um AMC ou selecione um AMC sem entradas dependentes.
2. Clique com o botão direito no AMC e selecione **New entrance (Nova entrada)**
3. Na janela pop-up **New entrance (Nova entrada)**, selecione o modelo de entrada **Parking lot 05c (Estacionamento 05c)** e adicione um leitor de entrada do tipo instalado na entrada do estacionamento.
4. Clique em **OK** para fechar a janela pop-up.
5. Selecione essa nova entrada criada na hierarquia do dispositivo.
   – Observe que o sistema designou automaticamente o leitor como um leitor de entrada.
6. No painel de edição principal, na guia **Parking lot 05c (Estacionamento 05c)**, selecione o estacionamento criado anteriormente no menu suspenso **Destination (Destino)**.

7. Clique com o botão direito no AMC novamente e crie outra entrada do tipo **Parking lot 05c (Estacionamento 05c)**, como mostrado acima.
   – Observe que dessa vez você só pode selecionar um leitor de saída.
   – Clique em **OK** para fechar a janela pop-up.
8. Selecione essa segunda nova entrada criada na hierarquia do dispositivo
   – Observe que o sistema designou automaticamente o segundo leitor como um leitor de saída.

10 Configuração de painéis e áreas de intrusão

Introdução

O sistema de controle de acesso permite administrar e operar os painéis de intrusão da Bosch. Consulte a ficha técnica do sistema de controle de acesso para obter detalhes dos modelos compatíveis. O sistema de controle de acesso agrega valor especificamente para a administração dos **usuários** do painel de intrusão. Esses usuários são um subconjunto dos titulares de cartão do sistema de controle de acesso em geral. Os administradores do sistema de controle de acesso fornecem a esses titulares autorizações especiais para operar os painéis de intrusão por meio do AMS Dialog Manager.

Os painéis de intrusão são configurados e atualizados como antes por meio do software de programação remota (RPS). O AMS lê dados constantemente do RPS e exibe os painéis incluídos.

O AMS contém caixas de diálogo para criar e atribuir perfis de autorização e para gerenciar os usuários do painel no RPS.

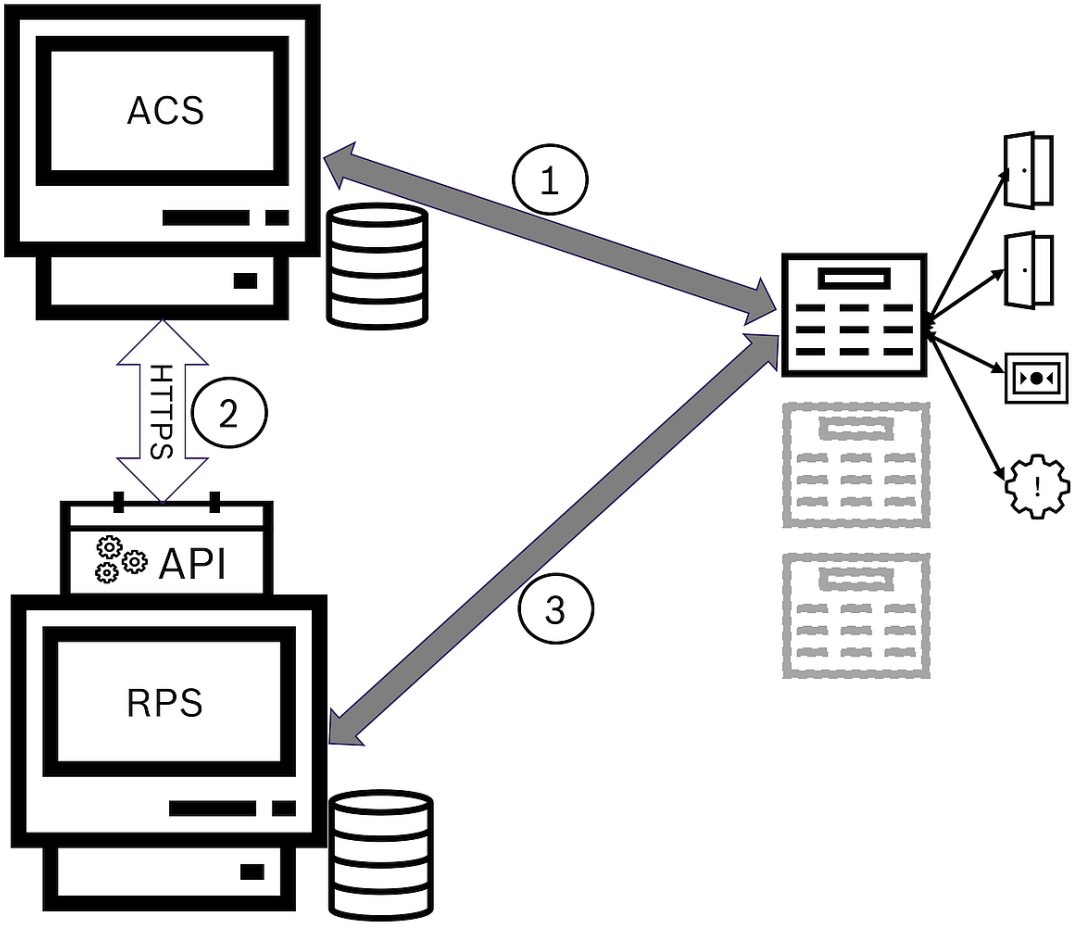


Figura 10.1: Topologia simplificada do sistema de intrusão ACS

ACS	O sistema de controle de acesso principal: AMS ou BIS-ACE
API	A interface de programação de aplicativos
RPS	Sistema de programação remota: o aplicativo para controlar painéis de intrusão

1	ACS para painel: comandos de painel. Painel para ACS: eventos de pontos de intrusão.
2	ACS para RPS: dados do titular do cartão
3	RPS para painel: opções de configuração

Pré-requisitos

- O RPS dos painéis de intrusão da Bosch compatíveis é instalado em um computador separado com uma conexão de rede com o servidor AMS, **não** no servidor AMS em si. Consulte o guia de instalação do RPS para obter instruções de instalação.
- O RPS foi configurado com os painéis de intrusão que pertencerão ao sistema de controle de acesso AMS. Consulte o guia de usuário do RPS ou a ajuda on-line para obter instruções.
- Os relógios nos painéis abrangem 100 dias do relógio no servidor AMS para permitir a sincronização automática.
- O protocolo do Modo 2 é definido em todos os painéis participantes.
- Cartões com uma das seguintes definições de cartão padrão:
  - HID 37 BIT -> Intrusão de 37 bits com um código de instalação/local igual a 32767 ou menos.
  - HID 26 BIT- > Intrusão de 26 bits
  - EM 26 BIT- > Intrusão de 26 bits

Visão geral

O processo de configuração consiste nas seguintes fases, descritas nas próximas seções deste capítulo:

1. Instalação da API do RPS de intrusão no computador do RPS
2. Conexão do sistema de controle de acesso aos painéis de intrusão.
   - Definição da conexão com a API do RPS.
   - Configuração das conexões de painel.
3. Criação de perfis de autorização do painel que governam quais funções dos painéis conectados podem ser usadas.
4. Atribuição de perfis de autorização do painel a titulares de cartão.
   - Assim, esses titulares de cartão tornam-se operadores dos painéis de intrusão.

10.1 Instalação da API do RPS de intrusão no computador do RPS

A API do RPS de intrusão é o canal de comunicação entre os aplicativos AMS e RPS em seus respectivos computadores. Primeiro você deve instalar a API no computador do RPS, depois instalar os certificados que a configuração gera no computador do AMS.

Procedimento

1. Execute o arquivo de configuração da API do RPS de acordo com sua própria documentação.

- O arquivo de configuração e a documentação estão localizados na mídia de instalação do AMS:
  `AddOns\Intrusion-RPS-API\Bosch_RPS_API_Setup_v*.exe`
  `AddOns\Intrusion-RPS-API\RPS-API_Application_note_v*.pdf`
- O programa de configuração gera dois certificados e os salva no computador do RPS:
  `%AppData%\Roaming\Bosch_RPS_API\BoschRpsAPI.cer`
  `%AppData%\Roaming\Bosch_RPS_API\BoschRpsAPI.pfx` (exige que você defina uma senha)

2. Copie os arquivos de certificado para o computador do AMS.
3. No computador do AMS, instale os certificados em **Local de armazenamento**: `Local Machine`, **Loja de certificados**: `Trusted Root Certification Authority`.

10.2 Conexão do sistema de controle de acesso aos painéis de intrusão

Introdução

Esta seção descreve como visualizar os painéis de intrusão e disponibilizá-los para controle por meio do Map View. O sistema de controle de acesso se conecta pela API ao RPS em sua rede. Por meio da API, ele mantém uma lista interna atualizada dos painéis de intrusão compatíveis disponíveis.

Duas etapas são necessárias no AMS para conectá-lo a painéis de intrusão:

– Etapa 1: definição da conexão com a API do RPS
– Etapa 2: configuração das conexões de painel

Caminho da caixa de diálogo

– Menu principal > **Configuração** > **Painéis** e caixas de diálogo secundárias

10.2.1 Etapa 1: definição da conexão com a API do RPS

A etapa 1 fornece o endereço do computador do RPS e informações de login do administrador para o sistema de controle de acesso.

Caminho da caixa de diálogo

Menu principal > **Configuração** > **Painéis > Configuração da API do RPS**

Procedimento

1. Insira as seguintes informações:

Informações	Descrição
Nome do host/Endereço IP	O endereço HTTPS do computador em que o RPS está em execução e o número da porta pela qual o RPS se comunica. O uso de `localhost` não é permitido. O número padrão da porta é `9000`.
Nome de usuário	O nome de usuário do administrador da API do RPS.
Senha	A senha do usuário administrador do RPS.

2. Clique no botão **Testar a conexão** para verificar se o RPS está em execução e se o nome de usuário e a senha são válidos.
3. Clique em  (Salvar) para salvar as alterações.

10.2.2 Etapa 2: configuração das conexões de painel

A etapa 2 configura a quantidade de controle que o sistema de controle de acesso tem em painéis individuais na rede.

Caminho da caixa de diálogo

Menu principal > **Configuração** > **Painéis > Administração do painel**

A caixa de diálogo mantém uma lista dos painéis de intrusão compatíveis que a API do RPS forneceu para o AMS.

A lista é atualizada periodicamente em segundo plano. Depois de abrir a caixa de diálogo, clique em  ocasionalmente para forçar uma atualização imediata manualmente.
A lista é somente leitura, exceto para os controles descritos na próxima seção.

Procedimento

1. Selecione um painel na lista
2. Use os controles abaixo para definir o que o sistema de controle de acesso pode fazer no painel de intrusão selecionado.

Coluna **Administração de usuários** da lista	Marque a caixa de seleção para garantir que os usuários do painel de intrusão dessa linha sejam mantidos no sistema de controle de acesso e **não** no painel em si. **IMPORTANTE**: Essa configuração faz com que todos os usuários do painel criados localmente no RPS sejam substituídos.
Coluna **Map View** da lista	Marque a caixa de seleção para disponibilizar esse painel para comando e controle por meio do Map View.
Ícone de configurações  (cog) na coluna **Dados de acesso**.	Se você marcou a caixa de seleção na coluna **Map View**, clique no ícone para inserir – um endereço IP – um número de porta (padrão `7700`) – a senha do painel individual. A senha é definida no RPS.
Botão: **Excluir painel selecionado**	Se um painel tiver sido excluído no RPS, ele aparecerá com o status **Removido** na lista. Selecione o painel e clique nesse botão para excluí-lo completamente do banco de dados.

10.3 Criação de perfis de autorizações para painéis

Introdução

Esta seção descreve como criar perfis de autorização do painel.
Um perfil de autorização do painel é um conjunto personalizado de autorizações para operar um conjunto personalizado de painéis de intrusão. Um administrador do AMS pode criar vários perfis de autorização do painel para as várias responsabilidades dos vários grupos de titulares de cartão.

Caminho da caixa de diálogo

– Menu principal > **Dados do sistema** > **Perfis de autorização para painéis de intrusão**

Procedimento

1. Clique em  para criar um novo perfil
2. (Obrigatório) Insira um nome para o perfil
3. (Opcional) Insira uma descrição em texto livre do painel
4. Abaixo da lista **Painéis atribuídos**, clique em **Adicionar...** para adicionar um ou mais painéis em uma lista pop-up de painéis disponíveis na rede.
   Por outro lado, selecione um ou mais painéis e clique em **Remover** para removê-los da lista.
5. Clique em um painel na lista **Painéis atribuídos** para selecioná-lo.
   – No painel **Autorizações**, uma lista é exibida com todas as áreas de intrusão que pertencem ao painel selecionado.

6. Na lista **Autorizações**, na coluna **Nível de autoridade**, selecione um nível de autoridade para cada área de intrusão do painel que deve ser incluída nesse perfil.
   – Os níveis de autoridade são definidos e mantidos no RPS. Eles também podem ser personalizados. Verifique se você sabe a definição do nível de autoridade no RPS antes de atribuí-lo a um perfil.
   – Por padrão, **L1** é o nível de autoridade mais alto, com **L2**, **L3** etc. cada vez mais restrito.
   – Se você deixar uma célula em branco, o destinatário desse perfil não terá **nenhuma** autorização na área de intrusão selecionada do painel selecionado.
7. Repita esse processo para todas as áreas de intrusão de todos os painéis a serem incluídos nesse perfil.
8. (Opcional) Na lista **Grupo de usuários**, selecione um grupo de usuários do painel para restringir as autorizações a determinados períodos.
   – Os grupos de usuários são definidos e mantidos no RPS. Eles também podem ser personalizados. Verifique se você sabe a definição do grupo de usuários no RPS antes de atribuí-lo a um perfil.
9. Clique em  (Salvar) para salvar as alterações.

10.4 Atribuição de perfis de autorização do painel a titulares de cartão

Introdução

Esta seção descreve como atribuir diferentes perfis de autorização do painel a diferentes tipos ou grupos de titulares de cartão.

Pré-requisito

Você definiu um ou mais perfis de autorização do painel no sistema de controle de acesso.

Caminho da caixa de diálogo

Menu principal > **Pessoas** > **Cartões**

Procedimento

1. Como faz normalmente, encontre e selecione o titular do cartão desejado no banco de dados.
2. Clique na guia **Intrusão**.
3. Na guia **Intrusão**, marque a caixa de seleção **Usuário do painel**.
4. (Obrigatório) No campo **Senha**, digite uma senha com a qual esse titular vai operar os painéis de intrusão.
   – Se necessário, use o botão para gerar uma nova senha não utilizada.
5. Na lista **Cartão de identificação**, selecione uma das credenciais de controle de acesso que está atribuída a esse titular de cartão.
6. (Opcional) No campo **Número do remoto**, insira o número que está impresso no dispositivo de controle remoto do titular do cartão dos painéis de intrusão.
7. Na lista **Idioma**, selecione o idioma em que o titular do cartão prefere ler as caixas de diálogo do painel.
8. Se o titular do cartão precisar usar o aplicativo de smartphone da Bosch para painéis de intrusão, marque a caixa de seleção **Acesso remoto**.
9. Na lista **Perfil de autorização**, selecione um perfil de autorização do painel adequado para o titular do cartão.
10. Clique em  (Salvar) para salvar as alterações.

– Esse perfil de autorização do painel, com todos os painéis e autorizações, é atribuído ao titular do cartão. O titular do cartão torna-se um operador para os painéis de intrusão.

Também é possível usar os campos de dados nessa caixa de diálogo com o botão para encontrar titulares de cartão no banco de dados.

10.5 Controle de portas pelos módulos B901 em painéis de intrusão

No AMS 4.0.1 e posterior, os Módulos de Interface de Controle de Acesso B901 podem ser controlados pela Map View do AMS.
O B901 é um simples controlador de porta que um administrador de sistema conecta aos painéis de intrusão da Bosch. Você conecta o painel de intrusão correspondente ao AMS, conforme descrito nas seções anteriores.
Você não configura o B901 no Editor de dispositivos.
O B901 pode bloquear/desbloquear, proteger/não proteger e ativar/desativar portas, mas fornece informações limitadas do estado ao sistema de controle de acesso. Por exemplo, ele não informa se uma porta foi fisicamente aberta em vez de apenas desbloqueada.
Como todos os outros dispositivos de intrusão, para enviar comandos para o B901 pela Map View do AMS, você deve ativar a Map View para o painel correspondente na caixa de diálogo do AMS:
Menu principal > **Configuração** > **Painéis > Administração do painel**

Swipe ticker da Map View e portas do B901

Para fornecer informações corretas ao aplicativo **Swipe ticker** na Map View do AMS, os IDs das portas do B901 devem corresponder aos IDs dos pontos de porta. Ou seja, a Porta 1 deve ser atribuída ao Ponto de porta 1, Porta 2 ao Ponto de porta 2 etc.

Doors 1 - 4	Door 1	Door 2	Door 3	Door 4
Door Name Text	Door 1	Door 2	Door 3	Door 4
Door Name Text (Second Language)				
Door Source	SDI2 (B901)	SDI2 (B901)	SDI2 (B901)	SDI2 (B901)
Entry Area	1	1	1	1
Associated Keypad #	Keypad 1	Keypad 1	Keypad 1	Keypad 1
Custom Function	Disabled	Disabled	Disabled	Disabled
Door Point	1	2	3	4
Door Point Debounce	600ms	600ms	600ms	600ms

Faça essas atribuições ao controlador de porta B901 na ferramenta RPS que configura painéis de intrusão e controladores.

11 Configuração de operadores e estações de trabalho

Introdução aos direitos de administrador para controle de acesso

Os direitos de administrador para o sistema de controle de acesso determinam quais caixas de diálogo do sistema podem ser abertas e quais funções podem ser realizadas nele.

Os direitos podem ser atribuídos aos operadores e às estações de trabalho.

Os direitos de uma estação de trabalho podem restringir temporariamente os direitos do operador, pois operações fundamentais para a segurança só devem ser realizadas a partir de estações de trabalho especialmente seguras.

Os direitos são atribuídos aos operadores e às estações de trabalho em pacotes chamados de **Perfis**. Cada perfil é ajustado de acordo com os deveres de um tipo específico de operador ou estação de trabalho.

Cada operador ou estação de trabalho pode ter vários perfis de autorização.

Procedimento geral e caminhos das caixas de diálogo

1. Crie as estações de trabalho no Editor de dispositivos:
   Configuration (Configuração) > **Device data (Dados do dispositivo)** > **Workstations (Estações de trabalho)** 
2. Crie perfis de estação de trabalho na caixa de diálogo:
   Operators and workstations (Operadores e estações de trabalho) > **Workstation profiles (Perfis de estação de trabalho)**.
3. Atribua perfis às estações de trabalho na caixa de diálogo:
   Operators and workstations (Operadores e estações de trabalho) > **Workstation rights (Direitos de estação de trabalho)**
4. Crie perfis de operador na caixa de diálogo:
   Operators and workstations (Operadores e estações de trabalho) > caixa de diálogo **User profiles (Perfis de usuário)**.
5. Atribua perfis aos operadores na caixa de diálogo:
   Operators and workstations (Operadores e estações de trabalho) > caixa de diálogo **User rights (Direitos de usuário)**

11.1 Criação das estações de trabalho

Estações de trabalho são os computadores a partir dos quais os operadores operam o sistema de controle de acesso.

Primeiro uma estação de trabalho deve ser "criada", isto é, o computador deve ser registrado no sistema de controle de acesso.

Caminho da caixa de diálogo

Configuration (Configuração) > **Device data (Dados do dispositivo)** > **Workstations (Estações de trabalho)**

Procedimento

1. Clique com o botão direito em **DMS** e selecione **New object (Novo objeto)** no menu de contexto ou clique em ✚ na barra de ferramentas.
2. Insira valores para os parâmetros:
   – O **Name (Nome)** da estação de trabalho deve corresponder exatamente ao nome do computador

- **Description (Descrição)** é opcional. Ela pode ser usada, por exemplo, para descrever a função e a localização da estação de trabalho
- **Login via reader (Login via leitor)** Deixe essa caixa de seleção desmarcada a menos que os operadores devam fazer login nessa estação de trabalho apresentando cartões a um leitor de cadastramento conectado a essa estação de trabalho. Para obter detalhes, consulte a seção
- **Logout automático depois do tempo de inatividade:** tempo de espera em segundos para encerramento automático de uma sessão de login via leitor de cadastramento. Mantenha em `0` para tempo ilimitado.

11.2 Criação de perfis de estação de trabalho

Introdução aos perfis de estação de trabalho

Dependendo da localização física, uma estação de trabalho de controle de acesso deve ser cuidadosamente configurada quanto ao uso, por exemplo:

- Quais operadores podem usá-la
- Quais credenciais são necessárias para usá-la
- Quais tarefas de controle de acesso podem ser realizadas a partir dela

Um perfil de estação de trabalho é um conjunto de direitos que definem o seguinte:

- Os menus do gerenciador de caixas de diálogo e as caixas de diálogo que podem ser usados em uma estação de trabalho
- Quais perfis de usuário um operador deve ter para fazer login nessa estação de trabalho.

Aviso!
Perfis de estação de trabalho substituem perfis de usuário
Um operador pode empregar somente os direitos do seu perfil de usuário que estão inclusos no perfil de estação de trabalho do computador onde está logado. Se os perfis de estação de trabalho e de operador não tiverem direitos em comum, o usuário não terá nenhum dos direitos da estação de trabalho.

Caminho da caixa de diálogo

Configuration (Configuração) > **Operators and workstations (Operadores e estações de trabalho)** > **Workstation profiles (Perfis de estação de trabalho)**

Criação de um perfil de estação de trabalho

1. Clique em  para criar um novo perfil
2. Insira um nome para o perfil no campo **Profile Name (Nome do perfil)** (obrigatório)
3. Insira uma descrição para o perfil no campo **Description (Descrição)** (opcional, porém recomendado)
4. Clique em  ou **Apply (Aplicar)** para salvar as alterações

Atribuição de direitos de execução para funções do sistema

1. Na lista **Functions (Funções)**, selecione as funções que devem ser acessíveis para essa estação de trabalho e clique duas vezes nelas para definir o valor na coluna **Execute (Executar)** como `Yes`.
   - Da mesma forma, verifique se todas as funções que não deve ser acessíveis estão definidas como `No`.
2. Clique em  ou **Apply (Aplicar)** para salvar as alterações

Atribuição de perfis de usuário para perfis de estação de trabalho
No painel **User Profile (Perfil do Usuário)**.
A lista de **Assigned Profiles (Perfis atribuídos)** contém todos os perfis de usuário autorizados a fazer login em uma estação de trabalho com esse perfil de estação de trabalho.
O campo **Available Profiles (Perfis disponíveis)** contém todos os outros perfis. Esses ainda não estão autorizados a fazer login em uma estação de trabalho com esse perfil de estação de trabalho.

1. Clique nos botões de setas entre as listas para transferir os perfis selecionados de uma lista para a outra.
2. Clique em  ou **Apply (Aplicar)** para salvar as alterações

Aviso!
Os perfis de administrador padrão para o usuário (**UP-Administrador**) e a estação de trabalho (**WP-Administrador**) não podem ser alterados ou excluídos.
O perfil **WP-Administrador** está permanentemente associado à estação de trabalho do servidor. Isso garante que há pelo menos um usuário que pode fazer login na estação de trabalho do servidor.

11.3 Atribuição de perfis de estação de trabalho

Use essa caixa de diálogo para gerenciar as atribuições dos perfis de estação de trabalho para estações de trabalho. Toda estação de trabalho deve ter pelo menos um perfil de estação de trabalho. Se tiver vários perfis, todos os direitos desses perfis se aplicam simultaneamente.

Caminho da caixa de diálogo
Configuration (Configuração) > **Operators and workstations (Operadores e estações de trabalho)** > **Workstation rights (Direitos de estação de trabalho)**

Procedimento
A lista de **Assigned Profiles (Perfis atribuídos)** contém todos os perfis de estação de trabalho que já pertencem a essa estação de trabalho.
A lista de **Available Profiles (Perfis disponíveis)** contém todos os perfis de estação de trabalho que ainda não foram atribuídos a essa estação de trabalho.

1. Na lista de estações de trabalho, selecione a estação de trabalho que deseja configurar
2. Clique nos botões de setas entre as listas **Assigned (Atribuídos)** e **Available (Disponíveis)** para transferir os perfis selecionados de uma lista para a outra.
3. Clique em  ou **Apply (Aplicar)** para salvar as alterações

Aviso!
Os perfis de administrador padrão para o usuário (**UP-Administrador**) e a estação de trabalho (**WP-Administrador**) não podem ser alterados ou excluídos.
O perfil **WP-Administrador** está permanentemente associado à estação de trabalho do servidor. Isso garante que há pelo menos um usuário que pode fazer login na estação de trabalho do servidor.

11.4 Criação de perfis de usuário (operador)

Introdução aos perfis de usuário

Observação: O termo **Usuário** é sinônimo de **Operador** no contexto de direitos de usuário.

Um perfil de usuário é um conjunto de direitos que definem o seguinte:

- Os menus do gerenciador de caixas de diálogo e as caixas de diálogo que estão visíveis ao operador.
- Os recursos do operador nessas caixas de diálogo, basicamente os direitos para executar, alterar, adicionar e excluir os elementos dessas caixas de diálogo.

Os perfis de usuário devem ser cuidadosamente configurados, dependendo da experiência, liberação de segurança e responsabilidades da pessoa:

Caminho da caixa de diálogo

Configuration (Configuração) > **Operators and workstations (Operadores e estações de trabalho)** > **User profiles (Perfis de usuário)**

Procedimento

1. Clique em  para criar um novo perfil
2. Insira um nome para o perfil no campo **Profile Name (Nome do perfil)** (obrigatório)
3. Insira uma descrição para o perfil no campo **Description (Descrição)** (opcional, porém recomendado)
4. Clique em  ou **Apply (Aplicar)** para salvar as alterações

Aviso!

Escolha nomes de perfil que descrevem claramente e com precisão os recursos e as limitações do perfil.

Direitos de adição, edição e execution para funções do sistema

1. No painel da lista, selecione as funções (primeira coluna) e os recursos dentro da função (**Execute (Executar)**, **Change (Alterar)**, **Add (Adicionar)**, **Delete (Excluir)**) que devem ser acessíveis para esse perfil. Clique duas vezes neles para alternar suas definições para `Yes`.
   - Da mesma forma, verifique se todas as funções que não deve ser acessíveis estão definidas como `No`.
2. Clique em  ou **Apply (Aplicar)** para salvar as alterações

11.5 Atribuição de perfis de usuário (operador)

Observação: O termo **Usuário** é sinônimo de **Operador** no contexto de direitos de usuário.

Pré-requisitos

- O operador que deve receber esse perfil de usuário foi definido como uma **Pessoa** no sistema de controle de acesso.
- Um perfil de usuário adequado foi definido no sistema de controle de acesso.
  - Observe que sempre é possível atribuir o perfil de usuário sem restrições **UP-Administrador**, mas essa prática está obsoleta por motivos de segurança.

Caminho da caixa de diálogo
Configuration (Configuração) > **Operators and workstations (Operadores e estações de trabalho)** > **User rights (Direitos de usuário)**

Procedimento
1. Carregue o registro de funcionário do usuário desejado na caixa de diálogo.
2. Se necessário, limite a validade do perfil de usuário inserindo datas nos campos **Valid from (Válido de)** e **Valid until (Válido até)**.

Atribuição de perfis de usuário para operadores
No painel **User Profiles (Perfis de usuário)**:
A lista de **Assigned Profiles (Perfis atribuídos)** contém todos os perfis de usuário que ainda não foram atribuídos a esse usuário.
O campo **Available Profiles (Perfis disponíveis)** contém todos os perfis disponíveis para atribuição.

1. Clique nos botões de setas entre as listas para transferir os perfis selecionados de uma lista para a outra.
2. Marque a caixa de seleção **Global administrator (Administrador global)** para conceder a esse operador acesso de leitura+gravação aos registros de funcionário onde o atributo **administered globally (administrado globalmente)** está ativado. O acesso padrão do operador a tais registros é somente leitura.
3. Clique em  para salvar as alterações.

Atribuição de direitos de uso da API para operadores
Se configurado e licenciado, código de programa externo pode invocar recursos do sistema de controle de acesso por meio de uma Interface de programação de aplicações ou API. O programa externo age através de um operador de proxy dentro do sistema. A lista suspensa **API usage (Uso da API)** controla os recursos do operador atual se for usado como um operador de proxy por código externo.
Configuration (Configuração) > **Operators and workstations (Operadores e estações de trabalho)** > **User rights (Direitos de usuário)**
– Selecione uma configuração na lista **API usage (Uso da API)**.
As opções são:

No access (Sem acesso) O operador não pode ser usado pela API para executar funções do sistema.

Read only (Somente leitura) O operador pode ser usado pela API para ler dados do sistema, mas não adicionar, modificar ou excluir.

Unlimited (Ilimitado) O operador pode ser usado pela API para ler, adicionar, modificar e excluir dados do sistema.

– Clique em  para salvar as alterações

11.6 Definição de senhas para os operadores

Como definir senhas seguras para si e outras pessoas.

Introdução

O sistema requer pelo menos um operador. O operador padrão em uma nova instalação possui o nome de usuário **Administrador** e senha **Administrador**. A primeira etapa ao configurar o sistema sempre deve ser fazer login com essas credenciais e alterar a senha para **Administrador**, de acordo com as políticas de senhas da sua organização.
Depois disso, você pode adicionar outros operadores, com e sem privilégios.

Procedimento para alterar sua própria senha.

Pré-requisitos

Você está logado no gerenciador de caixas de diálogo.

Procedimento

1. No Dialog Manager, selecione o menu: **Arquivo** > **Alterar senha**
2. Na janela pop-up, insira a senha atual, a nova senha e a nova senha outra vez para confirmar.
3. Clique em **Alterar**.

Esse procedimento é a única maneira de alterar a senha de administrador.
No primeiro login depois de uma instalação, o sistema requer a alteração da senha de administrador.

Procedimento para alterar as senhas de outros operadores.

Pré-requisitos

Para alterar as senhas de outros usuários é necessário estar logado no gerenciador de caixas de diálogo usando uma conta com privilégios de Administrador.

Procedimento

1. No menu principal do gerenciador de caixas de diálogo, navegue até **Configuration (Configuração)** > **Operators and Workstations (Operadores e estações de trabalho)** > **User rights (Direitos de usuário)**
2. No painel da caixa de diálogo principal, use a barra de ferramentas para carregar o operador cuja senha você deseja alterar.
3. Clique em **Change password... (Alterar senha...)**
4. Na janela pop-up, insira a nova senha e a nova senha novamente para confirmar.
5. Na janela pop-up, insira o período de validade da nova senha, **Unlimited (Ilimitado)** ou um número de dias.
   – Para ambientes de produção é altamente recomendado definir um período de validade.
6. Clique em **OK** para fechar a janela pop-up.

Na janela de diálogo principal, clique no ícone  para salvar o registro do usuário.

Os seletores de data **Válido de** e **Válido até**, abaixo do botão **Alterar senha...**, referem-se à validade dos direitos de usuário nessa caixa de diálogo, não à senha.

Informações adicionais

Sempre defina senhas de acordo com a política de senhas da sua organização. Para obter orientação sobre a criação de tal política você pode consultar, por exemplo, a orientação fornecida pela Microsoft na seguinte localização.
https://www.microsoft.com/en-us/research/publication/password-guidance/

12 Configurando cartões

12.1 Definição do cartão

Use essa caixa de diálogo para ativar, desativar, modificar ou adicionar as definições de cartão a serem usadas pelo sistema de controle de acesso.

Caminho da caixa de diálogo

– Navegador de configuração > **Infraestrutura** > **Definição do cartão ACE**
– Menu principal do AMS > **Configuração** > **Opções** > **Definição do cartão**

Os seguintes tipos são predefinidos pelo sistema e não podem ser modificados:

– CSN de 32 bits - MIFARE padrão (32 bits)
– HID 26 - Código Wiegand padrão de 26 bits = ativo (**padrão**)
– HID 35 - HID corporate 1000
– HID 37 - Código HID de 37 bits - CN-H10304
– EM 26 - Código EM de 26 bits
– Leitores seriais (AMC 4R4/LACi) - 64 bits
– HID 48 - HID corporate 1000
– CSN de 56 bits - MIFARE Desfire padrão

HID 26 é o tipo de cartão padrão e aparece na lista **Ativar tipos de cartão**

12.1.1 Ativar tipos de cartão

Os tipos de cartão a serem ativados são os tipos que os leitores de cartão do sistema de controle de acesso devem reconhecer e processar. Até 8 definições de cartão podem estar ativas simultaneamente em um sistema.

Para os leitores com protocolos L-Bus ou BG900, a entrada da lista **Leitores seriais** deve ser adicionada a **Ativar tipos de cartão** no Navegador de configuração (**Infraestrutura** > **Definição do cartão ACE**) para disponibilizar a caixa de diálogo de máscara de entrada manual (Bosch) no Access Engine para inserir manualmente os dados do cartão.

12.1.2 Criando e modificando

Clique no botão ✚ (+ verde) acima da caixa de lista à direita para criar uma nova entrada da lista. Diferente dos tipos de cartão predefinidos, os dados dos tipos recém-criados podem ser editados livremente. Clique duas vezes nos campos **Nome**, **Descrição** e **Número de bits** para editá-los.

O nome pode ter, no máximo, 80 caracteres e a descrição 255. O número de bits é limitado a 64 (se um número maior for inserido, será redefinido como o máximo assim que o campo de texto perder o foco de entrada).

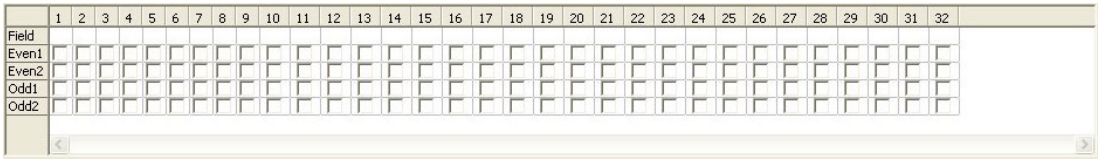
Aviso!

Os comprimentos de bit são usados para diferenciar as definições de Wiegand. Portanto, cada nova definição deve ter um comprimento de bit exclusivo que não tenha sido usado por uma definição existente.

- Para modificar um bit de dados, clique duas vezes no campo relevante. Para excluí-lo, primeiro selecione o bit de dados e, depois, clique no botão (x vermelho).

Aviso!
Somente tipos de cartão que foram criados pelo usuário podem ser modificados ou excluídos.

Quando um único tipo de cartão é selecionado (nas listas à esquerda ou direita), a codificação correspondente é exibida na parte inferior da caixa de diálogo. A tela mostra bits de dados em cinco linhas e na quantidade de colunas equivalente ao número de bits na definição.



Cada coluna da linha **Campo** pode receber um rótulo que determina como essa parte do código deve ser interpretada. Os rótulos disponíveis são os seguintes:

F	Instalação: marca a parte do código para afiliação da instalação	
C	N° do código: parte do código que contém o número do cartão individual	
E1	Par 1: bit para equilibrar a primeira máscara de paridade par	A declaração desses valores ativa a caixa de seleção da linha correspondente.
E2	Par 2: bit para equilibrar a segunda máscara de paridade par	
O1	Ímpar 1: bit para equilibrar a primeira máscara de paridade ímpar	
O2	Ímpar 2: bit para equilibrar a segunda máscara de paridade ímpar	
1	Fixar valores de bit contidos no código	
0		

No caso dos rótulos E1, E2, O1 e O2, basta marcar a caixa de seleção na linha correspondente. A caixa na linha **Campo** será marcado automaticamente conforme necessário.
Explicação:
O sinal enviado por um leitor quando recebe um cartão é composto por uma série de números 0 e 1. Para cada tipo de cartão, o comprimento desse sinal (isto é, o número de bits) é definido exatamente.
Além dos dados reais do usuário, que são salvos como dados de código, o sinal também contém dados do controle para a) identificar o sinal como um sinal de cartão e b) verificar a transmissão correta.

Em geral, os números 0 e 1 fixos são úteis para identificar o tipo de sinal.
Os bits de qualidade, que devem gerar um zero (paridade par) ou um (paridade ímpar) como soma de verificação nos bits selecionados do sinal, são usados para verificar a transmissão correta. Os controladores podem ser configurados para que possam calcular uma ou duas somas de verificação para paridades pares e uma ou duas somas de verificação para paridades ímpares.
No controle da lista, esses bits podem ser marcados nas respectivas linhas para as somas de verificação de paridade (Even1, Even2, Odd1 e Odd2) que devem ser incluídas na soma de verificação. Na linha superior (Campo) de cada soma de verificação usada, um bit é definido para equilibrar a soma de verificação de acordo com o tipo de paridade. Se uma opção de paridade não for usada, a linha correspondente simplesmente continuará vazia.

12.1.3 Ativando/desativando definições de cartão

Até 8 definições de cartão podem estar ativas simultaneamente. As definições a serem ativadas devem ser movidas para a lista à esquerda **Ativar tipos de cartão**. Isso é feito selecionando uma ou mais definições no lado direito e clicando no botão de seta para a esquerda (**<**).
É possível mover no máximo quatro definições de uma vez. Assim que as quatro definições estiverem no lugar, os excedentes serão descartados da movimentação. Para adicionar mais definições a **Ativar tipos de cartão**, será necessário excluir uma ou mais definições presentes selecionando-as e movendo-as para o lado direito usando o botão (**>**) e desativando-as.

Aviso!
Para usar leitores com protocolos L-Bus ou BG900, ative o tipo de cartão **Leitor serial**. Isso disponibiliza a caixa de diálogo de entrada manual **Dialog Bosch** para o gerenciador de caixas de diálogo do sistema de controle de acesso.

12.1.4 Criando dados do cartão no gerenciador de caixas de diálogo

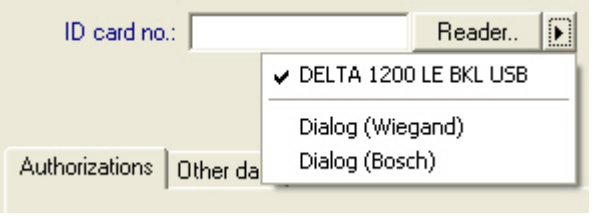
Entradas de dados manual
Diferentes métodos de entrada são usados para cartões Wiegand e Bosch.
Para todas as definições de Wiegand (CSN HID 26, HID 35, HID 37 e 32 bits), a caixa de diálogo **Dialog (Wiegand)** permite inserir o **Código do cliente** e o **N° do cartão** (número do cartão).
Para leitores seriais, a caixa de diálogo **Dialog (Bosch)** contém campos adicionais para **Versão** e **Código do país**.

Entrada de dados pelo leitor de inscrições
Além da entrada de dados manual, qualquer estação de trabalho pode ser equipada com um leitor de caixa de diálogo para coletar dados do cartão. Use um leitor da lista na seguinte caixa de diálogo:
– Navegador de configuração > **Infraestrutura** > **Leitor do cartão ACE**.
– Menu principal do AMS > **Configuração** > **Opções** > **Leitor de cartões**
Se o leitor escolhido for um leitor de entrada de cartões Wiegand, todos os tipos de cartão Wiegand ativos serão listados juntamente com o leitor
– Access Engine > **Dados de pessoal** > **Cartões** > Botão do leitor > ▶ (seta para a direita).
– Menu principal do AMS > **Dados de pessoal** > **Cartões** > Botão do leitor > ▶ (seta para a direita)

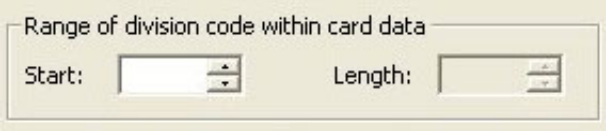
Um desses tipos de cartão deve ser selecionado para garantir o salvamento correto da codificação do cartão. Isso significa que o leitor propriamente dito não pode ser selecionado diretamente. Só é possível selecioná-lo indiretamente pela escolha da definição de Wiegand. Se o tipo de cartão necessário não aparecer na lista suspensa, você deverá ativá-lo na caixa de diálogo de definição do cartão.

– Navegador de configuração > **Infraestrutura** > **Definição do cartão ACE**
– Menu principal do AMS > **Configuração** > **Opções** > **Definição do cartão**

Os leitores de inscrições HITAG, LEGIC e MIFARE podem ser selecionados diretamente na lista.



Definição do cartão para divisões (recurso de várias partes)
Se você tiver licenciado o recurso Divisões para gerenciar várias partes (também conhecidas como "Divisões") com ambientes de acesso controlado, é possível configurar uma área de código no cartão que permite ao operador diferenciar os cartões de várias divisões. Use os campos opcionais (que podem ser selecionados somente onde o recurso Divisões foi licenciado) par definir a posição do bit **inicial** e o **comprimento** da codificação da divisão nos cartões.



12.2 Configurando códigos de cartão

A codificação dos cartões de controle de acesso garante que todos os dados de cartão sejam únicos.

Caminho da caixa de diálogo
Main Menu (Menu principal) > **Configuration (Configuração)** > **Options (Opções)** > **Card coding configuration (Configuração da codificação de cartões)**
Inserindo números na caixa de diálogo
Inserindo números na caixa de diálogo
Por praticidade, é possível inserir números nos formatos decimal ou hexadecimal. Selecione os botões de opção **Hexadecimal** ou **Decimal** de acordo com o formato especificado pelo fabricante dos cartões.
O painel principal da caixa de diálogo é dividido em dois grupos, que são descritos em mais detalhes abaixo:

- **Dados de código padrão do cartão**
- **Verificar valores somente de associação**

Dados de código padrão do cartão

Use esses campos de entrada de texto para definir valores para **Versão**, **Código do país** e **Código da instalação**, que são atribuídos ao número do cartão quando o cartão é inscrito no sistema. Se os campos não puderem ser gravados, eles não serão relevantes para nenhuma definição de cartão ativa. Para o código da Bosch, todos os campos podem ser gravados.
Se o cartão for inscrito manualmente em uma estação de trabalho do operador, uma caixa de diálogo aparecerá mostrando os valores padrão que podem ser personalizados para cada cartão.

Inserindo dados de código:

Se os dados forem fornecidos pelo fabricante como valores decimais, selecione o botão de opção Decimal e insira os valores fornecidos, por exemplo:
Versão: 2
Código do país: 99
Código da instalação: 56720
Clique em **Aplicar** para armazenar os dados.

Observações sobre a inserção de dados de código padrão:

Os dados padrão são armazenados no registro do sistema operacional e cada número do crachá é adicionado durante a codificação. O registro assume o formato de um valor **hexadecimal de 8 dígitos** com zeros iniciais, se necessário.
Se os números do código forem transferidos completamente, o sistema pode converter de decimal para hex, preencher até 8 casas com zeros iniciais e salvar o parâmetro de sistema apropriado.

- Exemplo:
  - Entrada: 56720
  - Conversão: DD90
  - Salvo como: 0000DD90

Se os números do código forem transferidos separadamente (formato dividido), então somente no formato **decimal**. São convertidos para um número decimal de 10 dígitos construído da seguinte forma:

- Versão: 2 dígitos
- Código do país: 2 dígitos
- Código da instalação: 6 dígitos
- Se qualquer um dos 10 dígitos ainda estiver vazio, serão preenchidos com zeros iniciais
  - Exemplo: 0299056720

Esse valor decimal de 10 dígitos é convertido e armazenado como um valor hexadecimal de 8 dígitos.

- Exemplo:
  - decimal: 0299056720
  - hexadecimal: 11D33E50

Aviso!
O sistema valida valores hex em caso de números de código dividido, para evitar a entrada de códigos de país inválidos (acima de 63 hex ou 99 decimal) e códigos de instalação inválidos (acima de F423F hex ou 999.999 decimal)

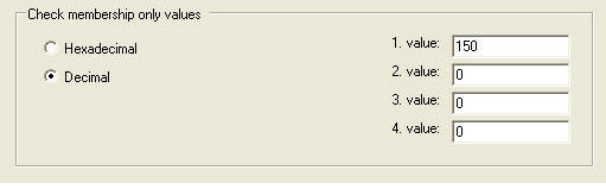
Aviso!
Se a captura do cartão ocorre por meio de um leitor de caixa de diálogo conectado, os valores padrão são atribuídos automaticamente. Não é possível substituir os padrões ao capturar a partir de um leitor.
Para fazer isso, o tipo de captura deve ser alternado para **Dialog (Caixa de diálogo)**

A entrada manual do número do cartão é feita no formato decimal.
Ao salvar os dados, um valor decimal de 10 dígitos (com zeros iniciais) é criado e, em seguida, convertido para um valor hexadecimal de 8 dígitos. Esse valor é armazenado com os dados do código padrão como o número de código de 16 dígitos do cartão.

- Exemplo:
  - Entrada do número do cartão: 415
  - 10 dígitos: 0000000415
  - Convertido para hexadecimal: 0000019F
  - Combinado com os dados de Código padrão (veja acima) e salvo como o número de código do crachá: 11D33E500000019F

Verificar valores somente de associação
Verificar apenas a associação significar que a credencial é verificada somente quanto à associação de uma empresa ou organização, e não para identificar um indivíduo. Portanto, não use **Membership check only (Somente verificação de associação)** para leitores que dão acesso às áreas de alta segurança.

Use esse grupo de opções para inserir até quatro códigos de empresa ou cliente. Os dados podem ser inseridos como decimal ou hexadecimal, mas são armazenados como valores decimais no registro do sistema operacional.



Selecione o leitor no Editor de dispositivos, DevEdit, e ative o parâmetro do leitor **Membership check (Verificação de associação)**.
Somente os códigos de empresa ou cliente dentro dos dados do cartão são lidos e verificados em relação aos valores armazenados.

Aviso!
A **Membership check (Verificação de associação)** funciona apenas com definições de cartão predefinidas no sistema (histórico cinza), não com definições personalizadas.

13 Configuração dos controladores

Introdução

Os controladores no sistema de controle de acesso são os dispositivos físicos e virtuais que enviam comandos ao hardware periférico em entradas (leitores e portas) e enviam solicitações dos leitores e portas de volta ao software de tomada de decisão central.
Os controladores armazenam cópias de algumas informações de dispositivo e usuário do cartão do software central e, se assim configurados, podem tomar decisões de controle de acesso mesmo quando temporariamente isolados do software central.
O software de tomada de decisões é o Sistema de gerenciamento de dados.
Os controladores são de dois tipos:

- Controladores de acesso principal, conhecidos como MACs, e seu par de backup redundante RMAC.
- Controladores de acesso locais, conhecidos como LACs ou AMCs.

Os controladores são configurados no editor de dispositivos, DevEdit

Caminho da caixa de diálogo do editor de dispositivos
Main menu (Menu principal) > **Configuration (Configuração)** > **Device data (Dados do dispositivo)** > **Device tree (Árvore de dispositivos)**

Uso do editor de dispositivos, DevEdit

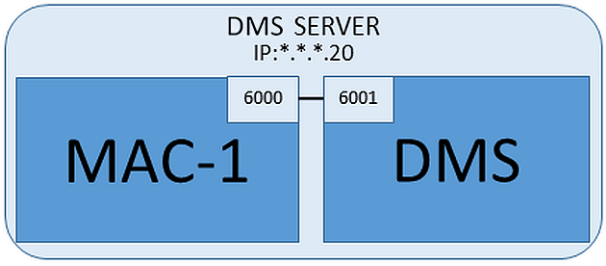
O uso básico do DevEdit está descrito na seção **Uso do editor de dispositivos** no link abaixo.

Consulte

- *Usando o Editor de dispositivos, página 22*

13.1 Configuração de MACs e RMACs

13.1.1 Configuração de um MAC no servidor DMS



É necessário um MAC para uma configuração mínima do sistema. Nesse caso, o MAC pode residir no servidor DMS.

Procedimento

No servidor DMS, abra o Editor de dispositivos e crie um MAC na árvore de dispositivos, conforme descrito na seção **Uso do editor de dispositivos**.
Selecione o MAC no Editor de dispositivos. Na guia **MAC**, forneça os seguintes valores de parâmetros:

Parâmetro	Descrição
Name (Nome)	O nome que deve aparecer na árvore de dispositivos, Por exemplo, MAC-1.
Descrição	Descrição opcional para benefício dos operadores do sistema

Parâmetro	Descrição
With RMAC (Com RMAC) (caixa de seleção)	**<Deixe em branco>**
RMAC Port (Porta RMAC)	**<Deixe em branco>**
Active (Ativo) (caixa de seleção)	**Desmarque** essa caixa de seleção para suspender temporariamente a sincronização em tempo real entre esse MAC e o DMS. Isso é vantajoso após atualizações do DMS em sistemas grandes, para evitar a reinicialização de todos os MACs de uma só vez.
Load devices (Carregar dispositivos) (caixa de seleção)	**Desmarque** essa caixa de seleção para suspender temporariamente a sincronização em tempo real entre esse MAC e seus dispositivos subordinados. Isso encurta o tempo necessário para abrir um MAC no editor de dispositivos.
IP address (Endereço IP)	`Localhost 127.0.0.1`
Time zone (Fuso horário)	**IMPORTANTE:** o fuso horário do MAC e de todos seus AMCs subordinados.
Division (Divisão)	(Se aplicável) A divisão à qual o MAC pertence.

Como esse MAC local não tem MAC de failover redundante, não é necessário executar a ferramenta MACInstaller para ele. Basta deixar os dois parâmetros do RMAC na guia **MAC** em branco.

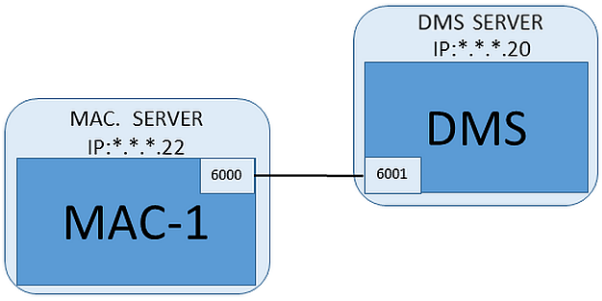
13.1.2 Preparação de computadores do servidor MAC para executar MACs e RMACs

Esta seção descreve como preparar computadores para se transformarem em servidores MAC. Por padrão, o primeiro MAC no sistema de controle de acesso é executado no mesmo computador do Data Management Server (DMS). No entanto, para maior resiliência, é recomendado que o MAC seja executado em outro computador, que poderá assumir tarefas de controle de acesso se o computador do DMS parar de funcionar.
Computadores separados onde MACs ou RMACs residem são conhecidos como servidos MAC, independentemente de hospedarem um MAC ou um RMAC.
Para fornecer o recurso de failover, MACs e RMACs **devem** ser executados em servidores MAC separados.
Verifique se as condições a seguir são atendidas em todos os servidores MAC participantes:

1. Os sistemas operacionais de todos os servidores MAC devem ter suporte da Microsoft no momento e ter as últimas atualizações instaladas.
2. O usuário Administrator em todos os servidores possui a mesma senha
3. Você está logado como Administrador (se estiver usando MSTC, use apenas sessões / Admin /Console)
4. Desative IP V6. Anote com cuidado o endereço IP V4 de cada servidor.
5. Habilite .NET 3.5 em todos os computadores participantes.
   Observação: nos sistemas operacionais Windows 10 e Windows Server já está habilitado como um recurso.

6. Reinicie o computador.

13.1.3 Configuração de um MAC em seu próprio servidor MAC



– O computador do servidor MAC foi preparado conforme descrito na seção

1. No computador do servidor DMS, no editor de dispositivos:
   – Clique com o botão direito no MAC e selecione **Desativar todos os LACs**.
   – Desative o MAC desmarcando as caixas de seleção **Ativar** e **Carregar dispositivos** para esse MAC.
2. No computador do servidor MAC, usando o programa do Windows `services.msc`
   – Pare o serviço MAC **AUTO_MAC2**
   – Defina o **Tipo de inicialização** desse serviço MAC como **Manual**.
3. Inicie o `MACInstaller.exe`
   – Para ACE, ele pode ser encontrado na mídia de instalação do BIS `\AddOns\ACE\MultiMAC\MACInstaller` (consulte a seção Uso da ferramenta MACInstaller abaixo).
   – Para AMS, ele pode ser encontrado na mídia de instalação do AMS `\AddOns\MultiMAC\MACInstaller` (consulte a seção Uso da ferramenta MACInstaller abaixo).
4. Percorra as telas da ferramenta, fornecendo valores para os parâmetros a seguir.

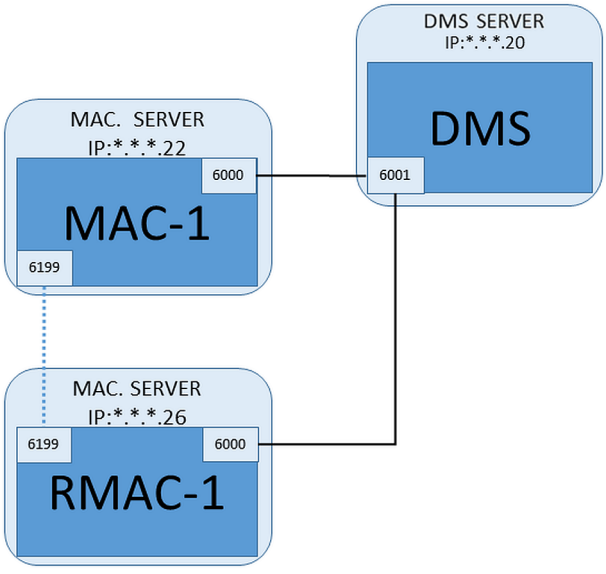
Nº da tela	Parâmetro	Descrição
3	**Destination Folder (Pasta de destino)**	O diretório local onde o MAC deve ser instalado. Escolha o padrão sempre que possível.
4	**Server (Servidor)**	O nome ou o endereço IP do servidor onde o DMS está em execução.
4	**Port (Porta) (porta para o DMS)**	A porta no servidor DMS que será usada para receber comunicação do MAC**.** Use 6001 para o primeiro MAC no DMS e incremente em 1 para cada MAC subsequente.
4	**Number (Número) (número do sistema MAC)**	Defina 1 para esse e todos os MACs (ao contrário dos RMACs)**.**
4	**Twin (Gêmeo) (nome ou endereço IP do MAC associado)**	Deixe esse campo em branco desde que esse MAC não venha a ter RMACs.

5. No servidor DMS, selecione o MAC no Editor de dispositivos.
6. Na guia **MAC**, forneça valores para os seguintes parâmetros:

Parâmetro	Descrição
Name (Nome)	O nome que deve aparecer na árvore de dispositivos, por exemplo, MAC-1.
Descrição	Descrição opcional para benefício dos operadores do sistema
With RMAC (Com RMAC) (caixa de seleção)	**<Deixe em branco>**
RMAC Port (Porta RMAC)	**<Deixe em branco>**
Active (Ativo) (caixa de seleção)	Marque essa caixa de seleção agora
Load devices (Carregar dispositivos) (caixa de seleção)	Marque essa caixa de seleção agora
IP address (Endereço IP)	O endereço IP do computador do servidor MAC.
Time zone (Fuso horário)	**IMPORTANTE:** O fuso horário do MAC e de todos os AMCs subordinados.
Division (Divisão)	(Se aplicável) A **divisão** do ACE à qual o MAC pertence.

13.1.4 Adição de RMACs aos MACs

Aviso!
Não adicione RMACs para MACs comuns até que o os MACs comuns estejam instalados em funcionando corretamente.
Caso contrário, a replicação de dados poderá ser impedida ou danificada.



- O MAC para esse RMAC foi instalado conforme descrito nas seções anteriores e está funcionando corretamente.
- O computador do servidor MAC para o RMAC foi preparado conforme descrito na seção

Os MACs podem ser geminadas com MACs redundantes (RMACs) para fornecer capacidade de failover e, consequentemente, controle de acesso resiliente. Nesse caso, os dados de controle de acesso são replicados automaticamente entre os dois. Se um dos pares falhar, o outro assume o controle dos controladores de acesso locais abaixo dele.

No servidor do DMS, no Navegador de configuração

1. No Editor de dispositivos, selecione o MAC para o qual o RMAC deve ser adicionado.
2. Na guia **MAC**, altere os valores para os seguintes parâmetros:

Parâmetro	Descrição
With RMAC (Com RMAC) (caixa de seleção)	**Desmarque** essa caixa de seleção até ter instalado o RMAC correspondente no servidor de conexão de failover redundante
Active (Ativo) (caixa de seleção)	**Desmarque** essa caixa de seleção para suspender temporariamente a sincronização em tempo real entre esse MAC e o DMS. Isso é vantajoso após atualizações do DMS em sistemas grandes, para evitar a reinicialização de todos os MACs de uma só vez.
Load devices (Carregar dispositivos) (caixa de seleção)	**Desmarque** essa caixa de seleção para suspender temporariamente a sincronização em tempo real entre esse MAC e seus dispositivos subordinados. Isso encurta o tempo necessário para abrir um MAC no editor de dispositivos.

3. Clique no botão **Apply (Aplicar)**
4. Mantenha o Editor de dispositivos aberto pois você retornará a ele.

No servidor MAC para o RMAC

Para configurar o RMAC, faça o seguinte:

– No próprio computador do servidor MAC preparado, execute a ferramenta MACInstaller (consulte Uso da ferramenta MACInstaller) e defina os seguintes parâmetros:
  – **Server (Servidor)**: o nome ou endereço IP do computador do servidor DMS
  – **Port (Porta)**: `6001` (a mesma do MAC)
  – **Number (Número)**: `2` (todos os RMACs têm número 2)
  – **Twin (Gêmeo)**: o endereço IP do computador onde o MAC gêmeo está em execução.

Volte ao Editor de dispositivos no servidor DMS

1. **IMPORTANTE:** verifique se o MAC e o RMAC, em seus respectivos computadores, estão em execução e visíveis uns aos outros na rede.
2. Na guia **MAC**, altere os parâmetros da seguinte forma:

Parâmetro	Descrição
With RMAC (Com RMAC) (caixa de seleção)	**Selecionado** Uma nova guia rotulada **RMAC** aparece ao lado da guia **MAC**.
RMAC Port (Porta RMAC)	`6199` (o padrão estático) Todos os MACs e RMACs usam essa porta para verificar se os seus parceiros estão em execução e acessíveis**.**

Parâmetro	Descrição
Active (Ativo) (caixa de seleção)	**Selecionado** Isso habilita a sincronização em tempo real entre esse MAC e seus dispositivos subordinados.
Load devices (Carregar dispositivos) (caixa de seleção)	**Selecionado** Isso encurta o tempo necessário para abrir um MAC no editor de dispositivos.

3. Na guia **RMAC**, forneça valores para os seguintes parâmetros:

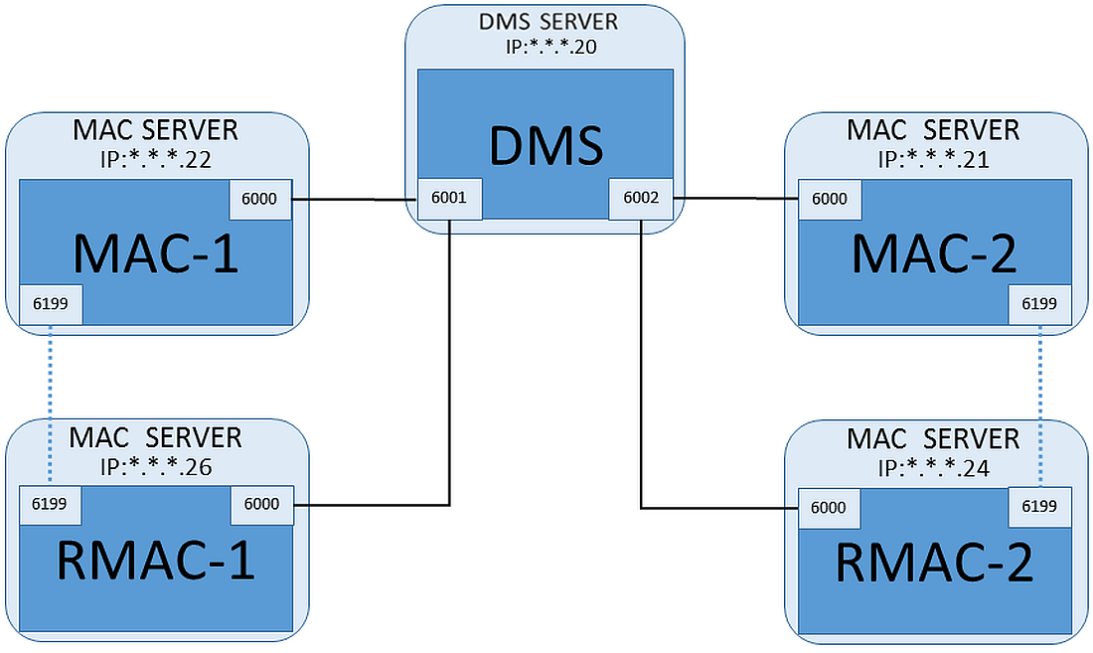
Parâmetro	Descrição
Name (Nome)	O nome que deve aparecer na árvore de dispositivos. Por exemplo, se o MAC correspondente for chamado de MAC-01, esse RMAC deverá ser chamado de RMAC-01.
Descrição	Documentação opcional para operadores de controle de acesso.
IP address (Endereço IP)	O endereço IP do RMAC.
MAC Port (Porta MAC)	`6199` (o padrão estático) Todos os MACs e RMACs usam essa porta para verificar se os seus associados estão em execução e acessíveis**.**

Consulte

– *Uso da ferramenta MACInstaller, página 52*

13.1.5 Adição de pares MAC/RMAC adicionais

Dependendo do número de entradas a serem controladas e do grau de tolerância a falhas necessário, um número grande pares MAC/RMAC pode ser adicionado à configuração do sistema. Para obter o número exato compatível com a sua versão, consulte a folha de dados correspondente.



Para cada par MAC/RMAC adicional...

1. Prepare os computadores separados para MAC e RMAC, conforme descrito na seção
2. Configure o MAC conforme descrito na seção
3. Configure o RMAC para esse MAC conforme descrito na seção

Observe que cada par MAC/RMAC transmite a uma porta separada no servidor DMS. Portanto, para o parâmetro **Port (Porta) (porta para o DMS)** no `MACInstaller.exe`, use:
– `6001` para ambos os computadores no primeiro par MAC/RMAC
– `6002` para ambos os computadores no segundo par MAC/RMAC
– etc.
No Editor de dispositivos, a porta `6199` sempre pode ser usada para os parâmetros **MAC Port (Porta MAC)** e **RMAC Port (Porta RMAC)**. Esse número de porta é reservado para o "aperto de mãos" entre cada par MAC/RMAC, pela qual cada um sabe se o parceiro está acessível ou não.

Aviso!
Reativação de MACs após atualizações do sistema
Após uma atualização do sistema, MACs e seus AMCs são desativados por padrão. Lembre-se de reativá-los no navegador de configuração marcando as caixas de seleção relevantes no editor de dispositivos.

13.1.6 Uso da ferramenta MACInstaller

`MACInstaller.exe` é a ferramenta padrão para instalar MACs e RMACs em seus respectivos computadores (servidores MAC). Ela coleta valores de parâmetros para um MAC ou RMAC e faz as alterações necessárias no Registro do Windows.

Aviso!
Como a ferramenta faz alterações no Registro do Windows, é necessário interromper qualquer processo do MAC em execução antes de reconfigurá-lo.

A ferramenta MACInstaller pode ser encontrada na mídia de instalação no seguinte caminho:
– `\AddOns\ACE\MultiMAC\MACInstaller.exe`
– `\AddOns\MultiMAC\MACInstaller.exe`
Por meio de uma série de telas, ela coleta valores dos parâmetros abaixo.

Nº da tela	Parâmetro	Descrição
3	**Destination Folder (Pasta de destino)**	O diretório local onde o MAC deve ser instalado.
4	**Server (Servidor)**	O nome ou o endereço IP do servidor onde o DMS está em execução.
4	**Port (Porta) (porta para o DMS)**	O número da porta no servidor DMS que será usada para comunicação entre o MAC e o DMS. **Veja os detalhes abaixo.**
4	**Number (Número) (número do sistema MAC)**	Defina 1 para todos os MACs originais. Defina 2 para todos os MACs de failover redundantes (RMACs).

Nº da tela	Parâmetro	Descrição
4	**Twin (Gêmeo) (nome ou endereço IP do MAC associado)**	O endereço IP do computador onde o parceiro de failover redundante para esse servidor MAC deverá ser executado. Se não se aplicar, deixe esse campo em branco.

Parâmetro: porta (porta para DMS)

Os números de porta têm o seguinte esquema de numeração:

– Em um sistema não hierárquico, onde existe apenas um servidor DMS, cada MAC e o RMAC correspondente são transmitidos do mesmo número de porta, geralmente 6000. O DMS pode se comunicar com apenas um de cada par MAC/RMAC por vez.
– O DMS recebe sinais do primeiro MAC ou par MAC/RMAC na porta 6001, do segundo MAC ou par MAC/RMAC na porta 6002 e assim por diante.

Parâmetro: Number (Número) (número do sistema MAC)

Esse parâmetro serve para distinguir MACs originais de RMACs:

– Todos os MACs originais têm o número 1.
– Todos os MACs de failover redundantes (RMACs) têm o número 2

Parâmetro: Configure Only (Somente configuração) (botão de opção)

Selecione essa opção para alterar a configuração de um MAC existente no servidor DMS principal, especialmente para informar sobre um RMAC recém-instalado em um computador diferente.

Neste caso, insira o endereço IP ou nome do host do RMAC no parâmetro **Twin (Gêmeo)**.

Parâmetro: Update Software (Atualizar software) (botão de opção)

Selecione essa opção em um computador diferente do servidor DMS principal, seja para instalar um RMAC ou para alterar a sua configuração.

Neste caso, insira o endereço IP ou nome do host do MAC gêmeo do RMAC no parâmetro **Twin (Gêmeo)**.

13.2 Configuração dos LACs

Criação de um controlador de acesso local AMC

Os Controladores modulares de acesso (AMCs) são subordinados aos Controladores de acesso principal (MACs) no editor de dispositivos.

Para criar um AMC:

1. No Editor de dispositivos, clique com o botão direito em um MAC e escolha **New Object (Novo objeto)** no menu de contexto
   ou
2. Clique no botão ✚.
3. Escolha um dos seguintes tipos de AMC na caixa de diálogo exibida:

AMC 4W (padrão)	com quatro interfaces de leitor Wiegand para conectar até quatro leitores
AMC 4R4	com quatro interfaces de leitor RS485 para conectar até oito leitores

Resultado: uma entrada de novo AMC do tipo escolhido é criada na hierarquia do DevEdit

AMC2 4W	**A**ccess **M**odular **C**ontroller (Controlador de acesso modular) com quatro leitores Wiegand.	Um máximo de quatro leitores Wiegand podem ser configurados para conectar até quatro entradas. O controlador oferece suporte para oito sinais de entrada e oito sinais de saída. Se necessário, placas de extensão podem fornecer até 48 sinais de entrada e saída adicionais.
AMC2 4R4	**A**ccess **M**odular **C**ontroller (Controlador de acesso modular) com quatro interfaces de leitor RS485	Um máximo de oito leitores RS485 podem ser configurados para conectar até oito entradas. O controlador oferece suporte para oito sinais de entrada e oito sinais de saída. Se necessário, placas de extensão podem fornecer até 48 sinais de entrada e saída adicionais.
AMC2 8I-8O-EXT	Placa de extensão para o AMC com oito sinais de entrada e saída	Disponibilize sinais adicionais. Podem ser ligadas até três placas de extensão a um AMC
AMC2 16I-16O-EXT	Placa de extensão para o AMC com 16 sinais de entrada e saída	
AMC2 8I-8O-4W	Placa de extensão para AMC Wiegand com oito sinais de entrada e saída	

Ativação/Desativação de controladores

Ao ser criado, um novo controlador tem a seguinte opção marcada (caixa de seleção): **Communication to host enabled (Comunicação com host habilitada)**.

Isso abre a conexão de rede entre o MAC e os controladores, para que qualquer dado de configuração alterado ou estendido seja propagado aos controladores automaticamente. Desative essa opção para economizar largura de banda da rede e, portanto, melhorar o desempenho, enquanto cria vários controladores e seus dispositivos dependentes (entradas, portas, leitores, placas de extensão). No editor de dispositivos, os dispositivos são marcados com ícones em cinza.

IMPORTANTE: lembre-se de reativar essa opção assim que a configuração dos dispositivos for concluída. Isso sempre manterá os controladores atualizados com qualquer alteração da configuração feita em outros níveis.

Mistura de tipos de controladores dentro de uma instalação

Os sistemas de controle de acesso normalmente são equipados com apenas um tipo de controlador e leitor.

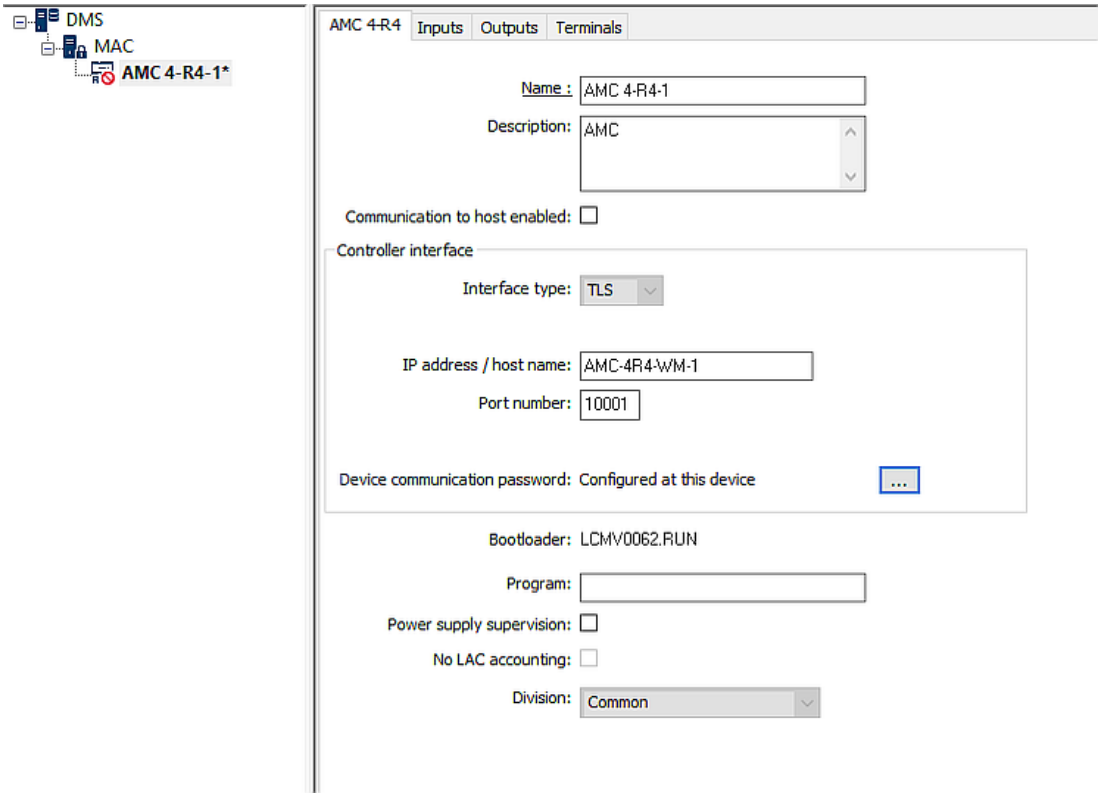
Atualizações de software e instalações em crescimento podem exigir que os componentes de hardware existentes sejam complementados com novos componentes. Mesmo configurações que combinam variantes do RS485 (AMC 4R4) com variantes do Wiegand (AMC 4W) são possíveis, desde que as seguintes ressalvas sejam consideradas:

– Os leitores RS485 transmitem um "telegrama" que contém o número de código conforme lido.

- Os leitores Wiegand transmitem seus dados de modo que devem ser codificados com a ajuda da definição de crachás para preservar o número de código no formato correto.
- A operação de controlador misturado só funciona se ambos os números de códigos forem construídos da mesma forma.

13.2.1 Parâmetros e configurações do AMC

Parâmetros gerais do AMC



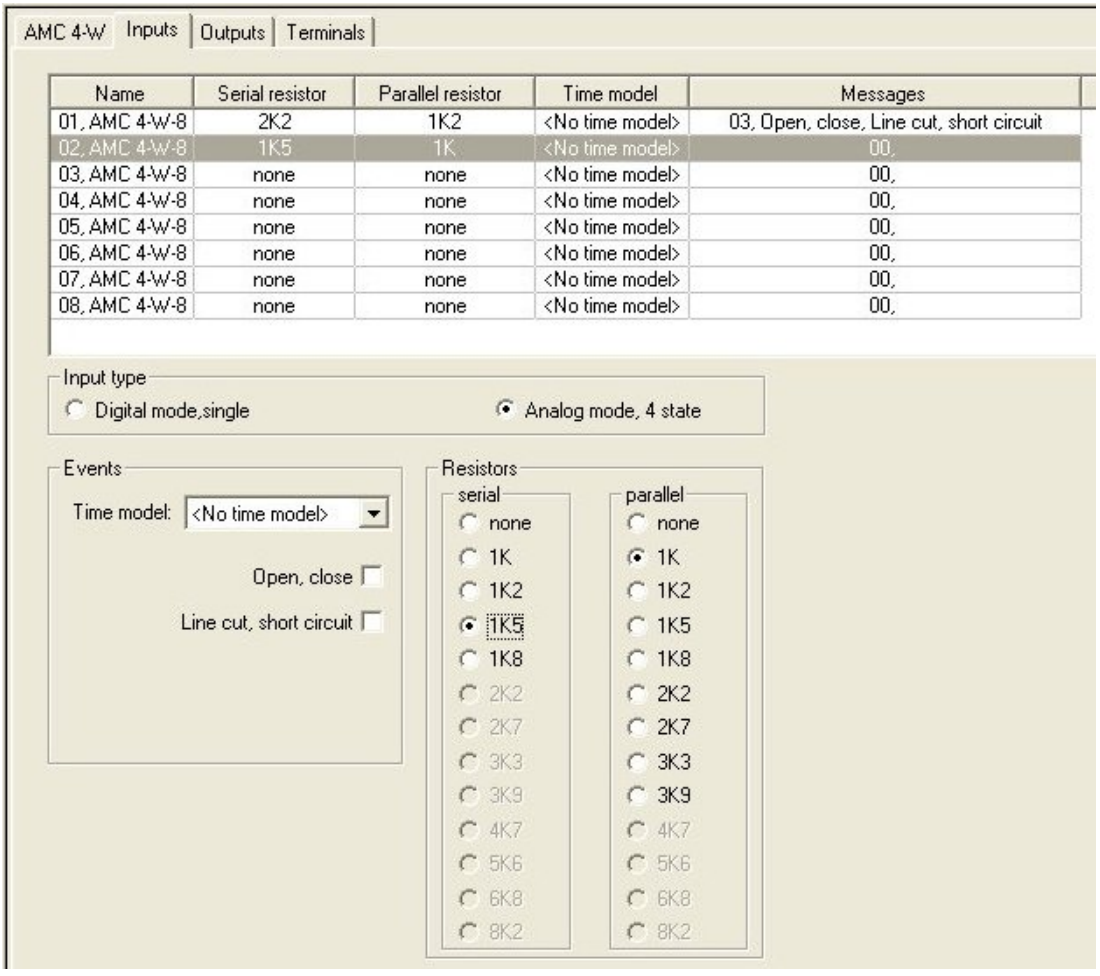
Configurando parâmetros de AMC

Parâmetro	Valores possíveis	Description (Descrição)
Nome do controlador	Restrição alfanumérica: 1 a 16 dígitos	A geração da ID (padrão) garante nomes exclusivos, mas os usuários podem substituí-los. Se você substituir um nome, garanta que os IDs sejam exclusivos.
Descrição do controlador	Alfanumérico: 0 a 255 dígitos	Texto livre.
Comunicação com host ativada	0 = desativado (a caixa de seleção está desmarcada) 1 = ativado (a caixa de seleção está marcada)	Padrão = ativado Os ícones de sobreposição nos controladores na árvore de dispositivos indicam o status da conexão do host (ativado/desativado). Desmarcar a caixa de seleção deixa o AMS temporariamente off-line, além de ser útil para reconfiguração e teste.

		A atualização do sistema de controle de acesso para uma nova versão desmarca as caixas de seleção de todos os controladores automaticamente. Marque e desmarque as caixas de seleção dos AMCs para testá-los individualmente no software atualizado.
		Marque a caixa de seleção ao usar o editor de dispositivos para definir uma DCP (senha de comunicação do dispositivo) no AMC durante a implementação "de cima para baixo" do DTLS. Essa ação abre uma janela de 15 minutos para propagar a DCP para os AMCs. Desmarque e marque a caixa de seleção para reiniciar a janela de tempo.
Interface do controlador		
Tipo de interface	UDP TLS	UDP (= protocolo do datagrama do usuário) onde a conexão é feita pela rede e nenhuma DCP (senha de comunicação do dispositivo) foi definida no AMC. TLS (= segurança da camada de transporte): quando você define uma DCP (senha de comunicação do dispositivo) para o AMC, a comunicação com o MAC é feita via DTLS com segurança aprimorada. Para UDP e TLS, verifique se os comutadores DIP 1 e 5 do AMC estão ativados.
Endereço IP/nome do host	Nome da rede ou endereço IP do AMC	Este campo de texto só estará ativo se **UDP** for selecionado como tipo de porta. Se os endereços IP forem alocados por DHCP, o nome da rede do AMC deverá ser fornecido para que o AMC possa ser localizado após uma reinicialização, mesmo que o endereço IP tenha mudado. Para redes sem DHCP, insira o endereço IP.
Número da porta	numérico: 10001 (padrão)	É a porta do AMC que receberá as mensagens do MAC.
Outros parâmetros		
Programa	Alfanumérico	Nome do arquivo do programa a ser carregado no AMC. Os programas disponíveis estão localizados no diretório BIN do MAC e

		podem ser selecionados em uma lista. Por praticidade, o protocolo e a descrição também são exibidos. Esse parâmetro é definido automaticamente conforme os programas são carregados automaticamente, dependendo dos leitores conectados, e o parâmetro é substituído em caso de incompatibilidade entre leitor e programa.
Supervisão da fonte de alimentação	0 = desativado (a caixa de seleção está desmarcada) 1 = ativado (a caixa de seleção está marcada)	Supervisão da tensão da fonte. Se a fonte de alimentação cair, uma mensagem informativa será gerada. A função de supervisão presume o pré-requisito de uma fonte de alimentação ininterrupta (UPS/No-break), para que uma mensagem possa ser gerada. 0 = sem supervisão 1 = supervisão ativada
Sem contabilidade de LAC	0 = desativado (a caixa de seleção está desmarcada) 1 = ativado (a caixa de seleção está marcada)	Marque essa caixa de seleção para dispositivos AMC que funcionam em conjunto para fornecer acesso a estacionamentos, onde apenas o MAC pai contabiliza o número de unidades entrando e saindo. **Observe** que, se essa opção for selecionada e o AMC ficar off-line, o AMC não conseguirá impedir o acesso a áreas lotadas, pois não tem acesso à contagem total da população.
Divisão	Valor padrão "Comum"	Relevante somente se o recurso **Divisões** for licenciado.

Configuring AMC inputs (Configuração de entradas do AMC)



Esta caixa de diálogo é dividida em quatro painéis:
- Lista das entradas por nome
- Os tipos de entrada
- Os eventos que serão assinalados pelas entradas
- Os tipos de resistores usados no modo analógico

Parâmetros das entradas

Os parâmetros das entradas do AMC estão descritos na seguinte tabela:

Nome da coluna	**Descrição**
Name (Nome)	Numeração da entrada (de 01 a 08) e nome do AMC ou AMC-EXT apropriado.
Serial resistor (Resistor em série)	Exibição do valor de resistor definido para o resistor em série. "nenhum" ou "---" = modo digital
Parallel resistor (Resistor em paralelo)	Exibição do valor de resistor definido para o resistor em paralelo. "nenhum" ou "---" = modo digital

Time model (Modelo de tempo)	Nome do modelo de tempo selecionado
Messages (Mensagens)	Número da escritura e designação das mensagens que serão geradas 00 = nenhuma mensagem 01 = se os eventos **Aberto** e **Fechado** foram ativados 02 = se os eventos **Corte de linha** e **Curto-circuito** foram ativados 03 = se ambas as opções de eventos foram ativadas
Atribuído	Usando o Modelo de entrada 15, o nome do sinal do DIP é exibido.

Use as teclas Ctrl e Shift ao clicar para selecionar várias entradas simultaneamente. Todos os valores alterados serão aplicados a todas as entradas selecionadas.

Eventos e modelos de tempo
Dependendo do modo de operação, os seguintes estados de porta são detectados e relatados: **Aberto**, **Fechado**, **Corte de linha** e **Curto-circuito**.
Selecione as respectivas caixas de seleção para permitir que o AMC transmita esses estados como eventos ao sistema geral.
Selecione um **Modelo de tempo** na lista suspensa com o mesmo nome para restringir a transmissão dos eventos aos tempos definidos pelo modelo. Por exemplo, o evento **Aberto** poderá ser significativo apenas fora do horário de funcionamento normal.

Tipo de entrada
Os resistores podem ser operados no **Modo digital** ou **Modo analógico (quatro estados)**.
O padrão é **Modo digital**: somente os estados de porta **aberto** e **fechado** são detectados.
No modo analógico, os estados de fio **Corte de linha** e **Curto-circuito** também são detectados.

Porta aberta	soma dos valores de resistores em série (R_S) e em paralelo (R_P): $R_S + R_P$
Porta fechada	igual aos valores dos resistores em série: R_S
Quebra de circuito	soma dos valores de resistores em série (R_S) e em paralelo (R_P) tendendo ao infinito.
Curto-circuito	soma dos valores de resistores em série (R_S) e em paralelo (R_P) é igual a zero.

Resistores
Os resistores são definidos como "nenhum" ou "---" no **Modo digital** padrão.
No **Modo analógico**, os valores dos resistores em série e em paralelo podem ser definidos selecionando os respectivos botões de opções.
nenhum, 1K, 1K2, 1K5, 1K8, 2K2, 2K7, 3K3, 3K9, 4K7, 5K6, 6K8, 8K2 (em 100 ohms)
Dependendo do valor de resistor selecionado, somente intervalos restritos estarão disponíveis para o resistor correspondente.
As tabelas a seguir mostram os valores selecionados nas colunas da esquerda e os intervalos disponíveis do outro resistor nas colunas da direita.

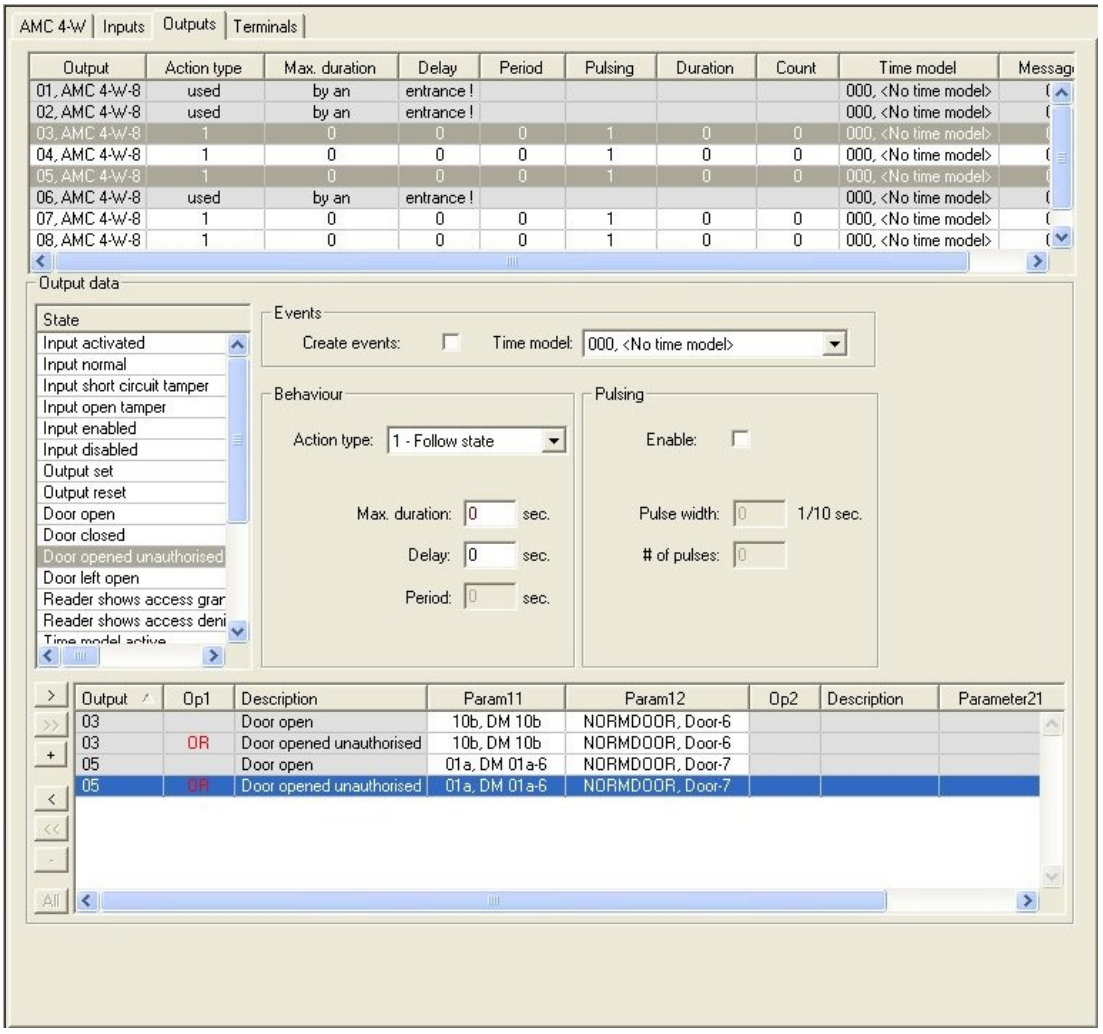
Série	**Intervalo**		**Paralelo**	**Intervalo**
"nenhum" ou "---"	1K até 8K2		"nenhum" ou "---"	1K até 8K2
1K	1K até 2K2		1K	1K até 1K8

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

Configuração de saídas do AMC – Visão geral

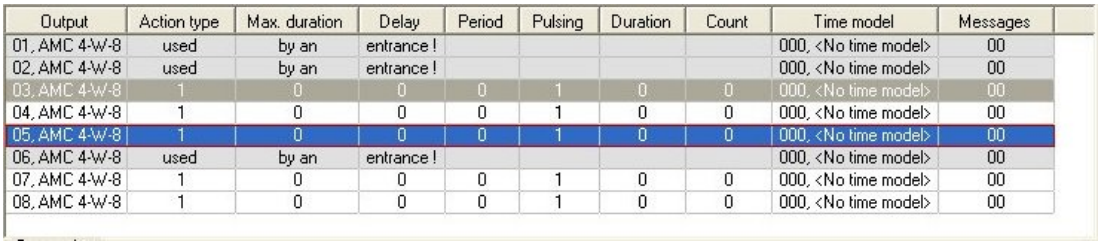
Essa página de caixa de diálogo fornece a configuração de cada saída em um AMC ou AMC-EXT, e contém três áreas principais:

– caixa de listagem com uma visão geral do parâmetro definido para toda saída
– opções de configuração para as saídas selecionadas na lista
– definição das condições para ativação das saídas



Seleção de saídas do AMC na tabela

Para configurar contatos de saída, primeiro selecione a linha correspondente na tabela superior. Use as teclas Ctrl e Shift para selecionar várias linhas, se necessário. As alterações feitas na parte inferior da janela afetarão somente as saídas selecionadas.



As linhas cujas saídas já foram atribuídas por meio de um modelo de porta, ou em outro lugar, são mostradas em cinza claro com a informação "**usado por uma entrada!**". Essas saídas não podem mais ser configuradas.

As linhas selecionadas estão em cinza escuro.

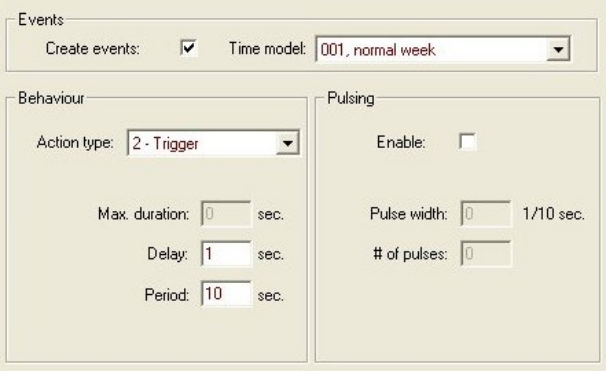
Parâmetros das saídas do AMC

Nome da coluna	Descrição
Output (Saída)	numeração atual das saídas no AMC ou AMC-EXT respectivo 01 a 08 com AMC e AMC_IO08

	01 a 16 com AMC_IO16
Action type (Tipo de ação)	indicação do tipo de ação selecionado 1 = Acompanhar estado 2 = Acionador 3 = Alternado
Max. duration (Duração máx.)	duração, em segundos, do sinal [1 a 9999; 0 = sempre, se a mensagem inversa não aparecer] – somente com o tipo de ação "1"
Delay (Atraso)	atraso, em segundos, até que o sinal seja fornecido [0 a 9999] – somente com os tipos de ação "1" e "2"
Period (Período)	período, em segundos, em que o sinal é fornecido – somente com o tipo de ação "2"
Pulsing (Pulsação)	ativação do impulso – caso contrário, o sinal é fornecido constantemente
Duration (Duração)	comprimento do impulso
Count (Contagem)	número de impulsos por segundo
Time model (Modelo de tempo)	nome do modelo de tempo selecionado
Messages (Mensagens)	marcação da atividade da mensagem 00 = nenhuma mensagem 03 = eventos são relatados
Atribuído	Usando o Modelo de entrada 15, o nome do sinal do DOP é exibido.

Saídas: Eventos, Ação, Pulsação

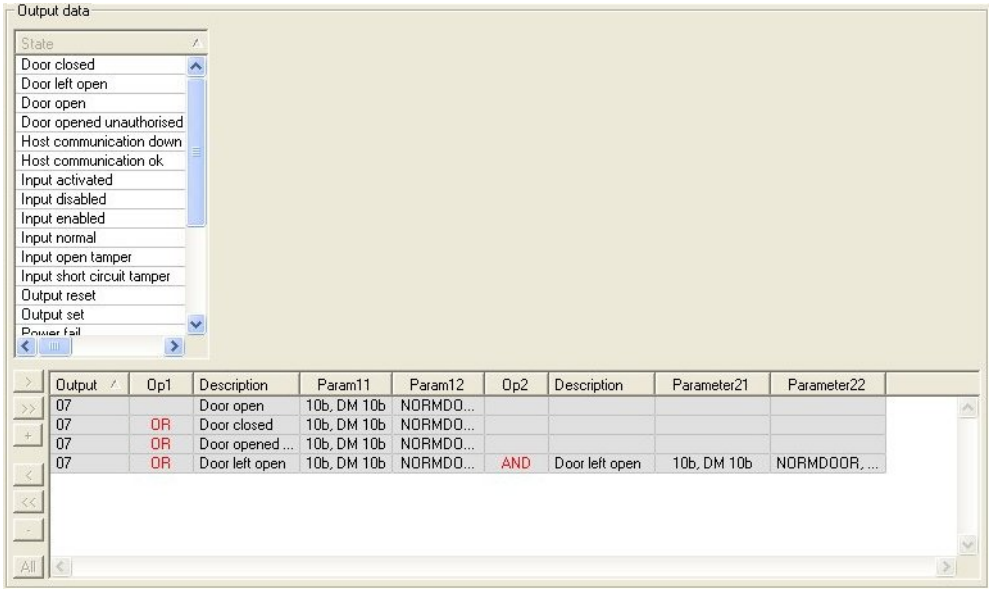
Todas as entradas da lista acima são geradas usando as caixas de seleção e campos de entrada nas áreas de caixa de diálogo **Events (Eventos)**, **Action (Ação)** e **Pulsing (Pulsação)**. Selecionar uma entrada da lista indica as configurações respectivas nessas áreas. Isso também vale para a seleção de várias entradas da lista, desde que os parâmetros de todas as saídas selecionadas sejam iguais. Alterações nas configurações do parâmetro são adotadas para todas as entradas selecionadas na lista.



Selecione a caixa de seleção **Create events (Criar eventos)** caso a mensagem deva ser enviada para a saída ativada. Se essas mensagem forem ser enviadas somente durante períodos especiais, por exemplo, à noite ou aos finais de semana, atribua um **modelo de tempo** adequado.
Os seguintes parâmetros podem ser definidos para os tipos de ações individuais:

Action type (Tipo de ação)	**Max. duration (Duração máx.)**	**Delay (Atraso)**	**Period (Período)**	**Pulsing/Enable (Pulsação/ Ativar)**	**Pulse width (Largura do pulso)**	**Number of pulses (Número de pulsos)**
Acompanhar estado	0 = sempre 1 - 9999	0 - 9999	não	sim	1 - 9999	Nenhum
Acionador	não	0 - 9999	0 a 9999 se a pulsação **não** estiver ativada	sim desativa o período	1 - 9999	1 - 9999
Alternado	não	não	não	sim	1 - 9999	não

Dados da saída do AMC
A parte inferior da caixa de diálogo **Outputs (Saídas)** contém:
– Uma caixa de listagem com os **estados** disponíveis para as saídas selecionadas.
– Uma tabela com as saídas e os estados configurados para acionar essas saídas.



Configuração de saídas a serem acionadas por determinados estados
Você pode configurar as saídas selecionadas acima para serem acionadas por estados individuais ou combinações lógicas de estados.
– Selecione uma ou mais saídas na caixa de listagem superior.
– Selecione um estado na lista **Estado**.
– Se houver vários dispositivos ou instalações para um status selecionado capaz de transmitir esse estado, o botão » será ativado ao lado do botão ›.
Clique em › (ou clique duas vezes no estado) para criar, para cada saída selecionada, uma entrada com esse estado com o primeiro dispositivo (por exemplo, AMC, primeira entrada) e a instalação (por exemplo, primeiro sinal, primeira porta).

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

Ao clicar em », o status selecionado é transferido para a lista e criado junto com um operador lógico OR para todos os dispositivos instalados (por exemplo, todas as entradas do AMC).

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

– Vários estados podem ser atribuídos por um atalho OR.

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	<< !!! >>

Atalhos com AND também são possíveis:

– Um estado já deve estar atribuído, ao qual outra condição é adicionada selecionando-a em uma coluna arbitrária.
– Em seguida, outro estado é selecionado e conectado ao status marcado clicando em ·.

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	<< !!! >>

Aviso!
Até 128 condições OR podem ser atribuídas a qualquer saída.
Cada condição pode ter **uma** condição AND dentro dela.

Assim que um status é atribuído a uma dispositivo ou instalação, também poderá se atribuído a todos os dispositivo e instalações existentes.

– Selecione a entrada atribuída em uma coluna arbitrária.
– Esse status é criado para todos os dispositivos e instalações existentes clicando em All.

Modificação de parâmetros das saídas

Você pode modificar linhas na lista
Com vários dispositivos ou instalações aos quais o status atribuído pode se corresponder, os primeiros dispositivos e instalações deste tipo sempre serão definidos.

Nas colunas **Param11** e **Param21** (com atalhos AND), os dispositivos (por exemplo, AMC, entrada) são exibidos. As colunas **Param12** e **Param22** contêm instalações especiais (por exemplo, sinal de entrada, porta, leitor).
Se existirem diversos dispositivos (por exemplo, placas de E/S) ou instalações (por exemplo, sinais adicionais, leitores), o ponteiro do mouse muda ao apontar para essa coluna.

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	<< !!! >>

Um clique duplo na entrada da coluna adiciona um botão que exibe uma lista suspensa das entradas válidas para o parâmetro.

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

Alterar as entradas nas colunas **Param11** e **Param21** atualiza as entradas nas colunas **Param12** e **Param22**:

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

Aviso!
Isso só é possível para as colunas **Param11**, **Param12**, **Param21** e **Param22**.
Se não houver outras opções (por exemplo, pois apenas uma entrada foi configurada), o ponteiro do mouse não muda e todos campos são cinzas. Se clicar duas vezes nessa entrada, isso será interpretado como um comando de exclusão e a caixa de mensagens para verificação da exclusão é exibida.

Exclusão dos estados que acionam saídas
As atribuições selecionadas podem ser removidas clicando em "**<**" (ou clicando duas vezes na entrada da lista). Uma caixa de mensagens solicitará confirmação para a exclusão.

Se vários estados foram associados a uma saída, todos eles poderão ser excluídos juntos da seguinte forma:
- Selecione a primeira entrada da lista (aquela sem entrada na coluna **Op1**) e, em seguida, clique no botão "**<<**".
- Como alternativa, clique duas vezes na primeira entrada.
  - Uma janela pop-up é exibida. Confirme ou aborte a exclusão.

– Se você confirmar a exclusão, um segundo pop-up pergunta se você deseja excluir todas as entradas associadas (resposta **Yes (Sim)**) ou apenas a entrada selecionada (repostas **No (Não)**).

Para excluir estados adicionais que qualificam o primeiro estado por operador AND na coluna **Op2**, clique em qualquer lugar da linha e, em seguida, clique no botão "menos" , que só estará ativo se um estado AND qualificado estiver presente na linha.

Descrição do estado

A tabela a seguir fornece uma visão geral de todos os estados selecionáveis, o número de tipo e a descrição.

O campo de lista **Estado** contém esses parâmetros também; eles são indicados ao rolar para a direita na lista.

Estado	Tipo	Descrição
Entrada ativada	1	Entrada local
Entrada normal	2	Entrada local
Falsificação de curto-circuito de entrada	3	Entrada local com resistor configurado
Falsificação de abertura de entrada	4	Entrada local com resistor configurado
Entrada desativada	5	Entrada local desativada por modelo de tempo
Entrada ativada	6	Entrada local ativada por modelo de tempo
Saída definida	7	Saída local, não saída atual
Saída redefinida	8	Entrada local, não entrada atual
Porta aberta	9	GID da entrada, número da porta
Porta fechada	10	GID da entrada, número da porta
Porta aberta não autorizada	11	GID da entrada, número da porta, substitui "Porta aberta" (9)
Porta deixada aberta	12	GID da entrada, número da porta
O leitor mostra acesso concedido	13	Endereço do leitor
O leitor mostra acesso negado	14	Endereço do leitor
Modelo de tempo ativo	15	Modelo de tempo configurado
Leitor de violação	16	Endereço do leitor
AMC violado	17	---
Placa de E/S violada	18	---
Falha de alimentação	19	somente para AMC com bateria
Alimentação adequada	20	somente para AMC com bateria

Comunicação com o host OK	21	---
Comunicação com o host perdida	22	---
Mensagem do leitor	23	Endereço do leitor
Mensagem do LAC	24	Número da placa
Controle do cartão	25	Endereço do leitor, função de controle do cartão.

Configurando saídas

Além da atribuição de sinal com modelos de porta ou com atribuição individual, é possível definir condições para saídas que ainda não foram alocadas. Se essas condições ocorrerem, a saída será ativada de acordo com o parâmetro definido.

Você deve decidir o que será trocado na saída. Diferente dos sinais que podem ser associados a um modelo de porta específico, portas e leitores, nesse caso, os sinais de todos os dispositivos e instalações conectados a um AMC podem ser aplicados.

Se, por exemplo, um sinal óptico acústico ou uma mensagem para um dispositivo externo precisar ser acionado pelos sinais de entrada **Falsificação do curto-circuito de entrada** e **Porta aberta não autorizada**, essas entradas ou entradas que podem ser consideradas são atribuídas à saída de destino correspondente.

Exemplo em que somente um contato foi selecionado em cada caso:

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	<< !!! >>

Exemplo com todos os contatos:

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

Exemplo com contatos selecionados:

Uma única entrada é criada para cada contato clicando em » ou removendo os contatos desnecessários depois de atribuir todos os contatos:

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

As mesmas condições podem ser instaladas em várias saídas. Se, por exemplo, além de um sinal óptico, você também precisar de um sinal acústico, uma mensagem deverá ser enviada para o dispositivo externo ao mesmo tempo:

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

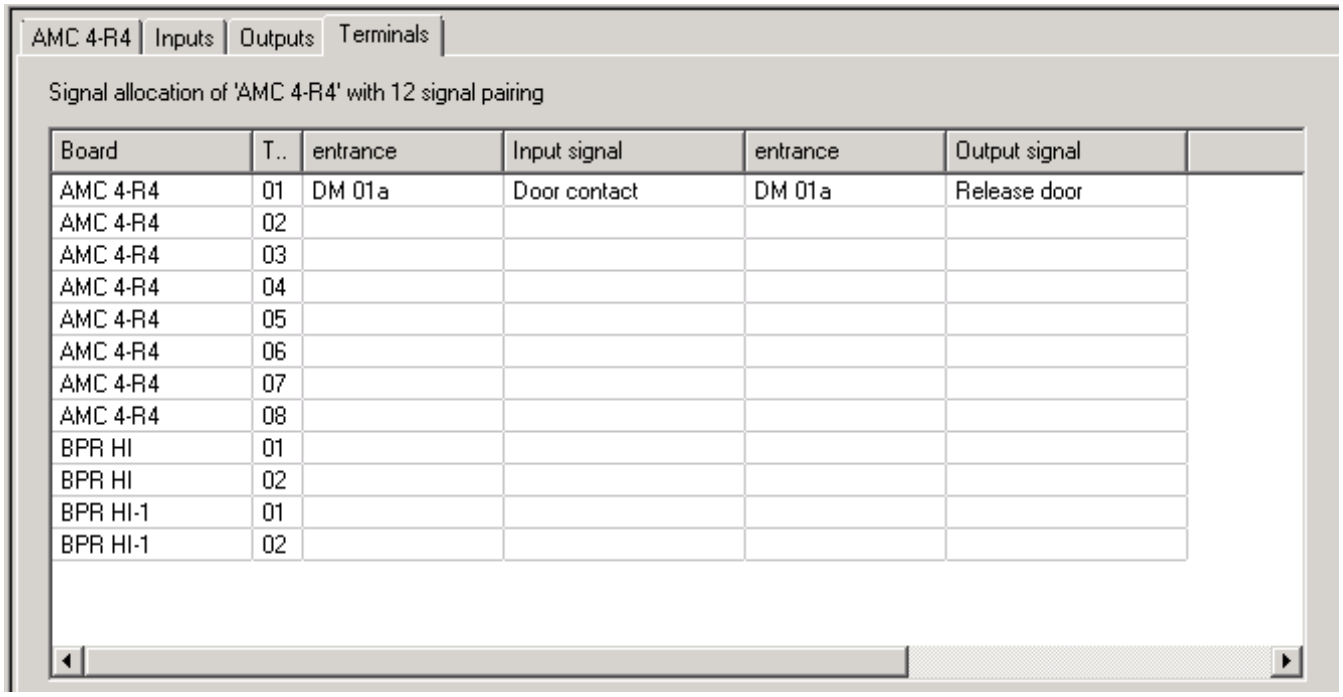
Lista de todos os estados existentes com os valores padrão para o parâmetro 11/21 e 12/22:

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	---	---

Definição de sinais na guia Terminais

A guia **Terminals (Terminais)** lista a alocação de contatos em um AMC ou AMC-EXT. Assim que as entradas forem criadas, as atribuições de sinais são indicadas de acordo com o modelo de porta selecionado.

Você não pode fazer modificações na guia **Terminals (Terminais)** do controlador ou das placas de extensão. As edições só são possíveis na guia de terminais da página de entrada. Por esse motivo as configurações do terminal são exibidas em um fundo cinza. As entradas exibidas em vermelho indicam as configurações dos sinais das saídas respectivas.



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				

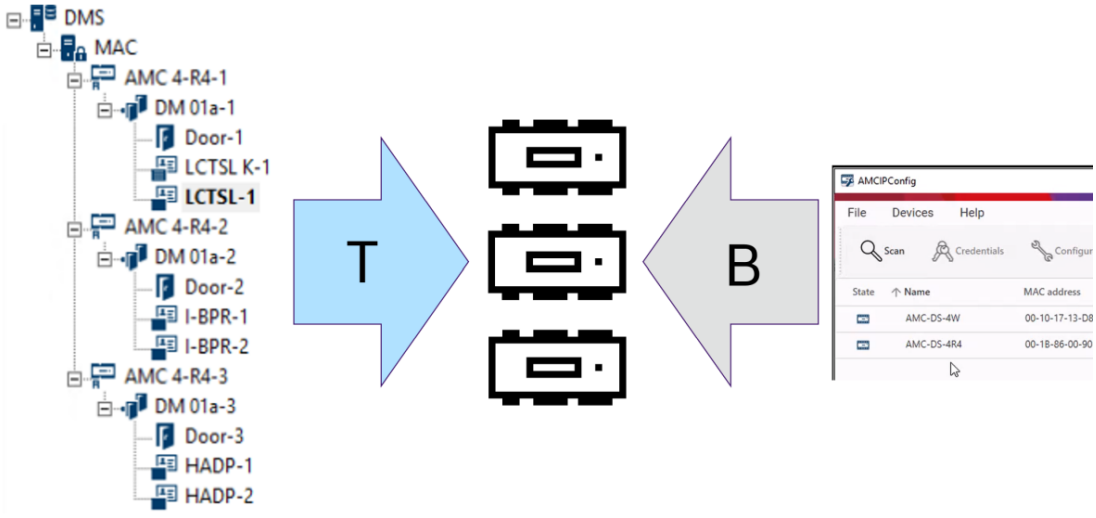
14 Configuração de DTLS para comunicação segura

Introdução

O sistema de controle de acesso (ACS) oferece comunicação entre dispositivos extremamente segura, protegida por DTLS. Existem duas maneiras principais de implantar a comunicação DTLS entre os dispositivos no ACS:

A **implantação de cima para baixo** (T) é feita no editor de dispositivos no ACS.

A **implantação de baixo para cima** (B) é feita principalmente na ferramenta AMCIPConfig, mas requer o editor de dispositivos para conclusão.



- (T) A implantação de cima para baixo pode ser feita de duas maneiras alternativas no editor de dispositivos:
  - Usando uma única senha de comunicação de dispositivo (DCP) no nível DMS para todos os AMCs.
  - Usando vários DCPs para diferentes ramificações da árvore de dispositivos, começando nos respectivos MACs ou AMCs.
- (B) A implantação de baixo para cima também pode ser iniciada de duas maneiras alternativas na ferramenta AMCIPConfig:
  - Uso de uma chave de hardware do AMC
  - Uso de uma chave de LCD aleatória

Aviso!

A implantação de baixo para cima ainda requer a configuração de DCPs no editor de dispositivos.

A implantação de baixo para cima permite configurar um DCP no dispositivo AMC. No entanto, é necessário configurar o mesmo DCP no mesmo AMC no editor de dispositivos também para permitir a comunicação DTLS total entre o MAC e o AMC.

Resumo das opções de implantação de DTLS

	Descrição breve	Vantagens	Desvantagens
De cima para baixo	O administrador do sistema insere uma senha forte no **Editor de dispositivos**. A partir dessa senha, o sistema gera uma **Chave**	Implantação rápida e simples.	Durante a propagação da chave mestre para os controladores de porta AMC, a

	Descrição breve	Vantagens	Desvantagens
	mestre que é propagada de cima para baixo na árvore de dispositivos de controle de acesso, do DMS até os MACs e os controladores de porta AMC. É possível definir uma senha para a árvore de dispositivos inteira ou senhas diferentes para ramificações diferentes da árvore de dispositivos.		comunicação do dispositivo não é protegida por DTLS.
De baixo para cima usando a chave de hardware do AMC	O administrador do sistema usa a ferramenta **AMC IPConfig** para implantar DTLS no nível dos controladores de porta AMC.	Maior diferenciação e flexibilidade de implantação. Esse método evita a principal desvantagem da implantação de cima para baixo, ou seja, a comunicação esporádica sem proteção da chave mestre. No entanto, isso requer que a conexão da ferramenta AMCIPConfig com o AMC seja protegida durante a configuração do DCP.	Quando a ferramenta IPConfig configura o DCP no AMC, é necessário proteger a comunicação por outros meios. Por exemplo, conecte o AMC diretamente ao computador quando a IPConfig estiver em execução. Os DCPs configurados na ferramenta IPConfig também devem ser configurados nos mesmos AMCs por meio do editor de dispositivos.
De baixo para cima usando a chave de LCD aleatória		Maior diferenciação e flexibilidade de implantação. O nível mais alto de segurança porque a chave de LCD não é transmitida pela rede; portanto, a propagação de credenciais sempre é protegida.	Implantação mais complicada e demorada. Você deve transferir a chave de LCD aleatória de 27 símbolos por algum meio que não seja pela rede para a ferramenta IPConfig.
Os detalhes e as instruções estão disponíveis nas próximas seções deste capítulo.			

Tecnologia DTLS	
DCP (senha de comunicação de dispositivo)	Uma única senha forte a partir da qual o ACS gera uma chave mestre interna. A senha deve ser guardada porque não é armazenada no ACS.
Chave mestre	Um código que o sistema gera a partir do DCP e usa para proteger os dispositivos de controle de acesso. A chave mestre nunca fica visível para nenhum usuário.
Chave de LCD aleatória	Um código alfanumérico temporário que o AMC gera sempre que é iniciado. A chave pode ser exibida no visor de cristal líquido (LCD) do AMC e pode ser solicitada por ferramentas de software para autenticar a comunicação de rede.
Chave de hardware do AMC.	Um código de autenticação interno que o AMC gera a partir de determinados parâmetros de hardware. Não fica visível para o usuário.

14.1 Implantação de DTLS de cima para baixo

Pré-requisitos

– AMS 4.0 ou BIS-ACE 4.9.1 ou posterior.
– A árvore de dispositivos de controle de acesso de DMS para AMCs é configurada fisicamente e conectada à rede, mas os AMCs não estão ativados. Com a ativação, as caixas de seleção **Comunicação com host ativada** dos AMCs estão marcadas.
– O DTLS ainda não foi configurado nos AMCs por um dos métodos de baixo para cima pela ferramenta IPConfig.

Procedimento: um DCP para tudo

1. No ACS, inicie o Editor de dispositivos
– Navegador de navegação do BIS > **Connections (Conexões)**
– Menu principal do AMS > **Configuração** > **Dados do dispositivo** > **Árvore de dispositivos**

– Uma caixa de diálogo é exibida e solicita a inserção de uma senha forte de comunicação do dispositivo (DCP).
2. Para configurar um único DCP para todos os AMCs na árvore de dispositivos, insira e confirme uma senha forte de acordo com as políticas de senha locais.
– A caixa de diálogo fornece feedback sobre a intensidade da senha, com base na entropia da senha.
3. Anote a senha, pois ela não é armazenada no ACS.
4. Clique em **OK** para fechar a caixa de diálogo.

Procedimento alternativo: vários DCPs para diferentes ramificações da árvore de dispositivos

1. No ACS, inicie o Editor de dispositivos
– Navegador de navegação do BIS > **Connections (Conexões)**

– Menu principal do AMS > **Configuração** > **Dados do dispositivo** > **Árvore de dispositivos**

– Uma caixa de diálogo é exibida e solicita a inserção de uma senha forte de comunicação do dispositivo (DCP).

2. Clique em **Cancelar** para definir DCPs diferentes em diferentes ramificações da árvore de dispositivos (MACs e AMCs).

– Uma caixa de diálogo pop-up informa quantos AMCs no sistema ainda não têm nenhum DCP.
– A árvore de dispositivos é aberta no Editor de dispositivos.

3. Desdobre a árvore de dispositivos para selecionar o MAC ou AMC para o qual deseja configurar um DCP.

– Se você configurar o DCP no nível de um MAC, ele será configurado para todos os AMCs subordinados do MAC.
– Se você configurar o DCP no nível de um AMC, ele será configurado somente para o AMC em questão.

4. Clique no botão de reticências ... ao lado do campo de texto **Senha de comunicação do dispositivo:**
5. Insira e confirme uma senha forte de acordo com as políticas de senha locais.
6. Anote a senha e a ramificação à qual ela se aplica, pois isso não é armazenado no ACS.
7. Repita esse procedimento para cada MAC ou AMC para o qual deseja configurar um DCP separado.
8. Clique em **OK** para fechar a caixa de diálogo.

Resultado da implantação de cima para baixo

O ACS usa DCPs para gerar chaves internas para todos os AMCs abaixo do DMS ou MAC selecionado.

Não é necessário repetir esse procedimento, a não ser que você altere o DCP posteriormente em um ou mais AMCs usando a ferramenta AMC IPConfig (consulte a implantação "de baixo para cima"). Nesse caso, você deve configurar imediatamente o mesmo DCP de cima para baixo nos mesmos AMCs no editor de dispositivos.

Se, depois, você adicionar dispositivos à árvore subornados aos DMSs e MACs que já possuem DCPs, os novos dispositivos herdarão automaticamente o mesmo DCP dos dispositivos superiores.

15 Configuração de entradas

15.1 Entradas – Introdução

O termo Entrada denota em sua totalidade o mecanismo de controle de acesso em um ponto de entrada:
Os elementos da entrada incluem:

- Leitores de acesso – entre 1 e 4
- Alguma forma de barreira, por exemplo, uma porta, catraca, eclusa ou canaleta.
- O procedimento de acesso conforme definido por sequências predefinidas de sinais eletrônicos transmitidos entre os elementos de hardware.

Um Modelo de porta é um modelo para um tipo específico de entrada. Ela descreve os elementos de porta presentes (número e tipo de leitores, tipo de porta ou barreira, etc.) e força um processo de controle de acesso específico com sequências de sinais predefinidos. Modelos de porta facilitam muito a configuração de um sistema de controle de acesso.

Modelo de porta 1	porta simples ou comum
Modelo de porta 3	catraca bidirecional para entrada e saída
Modelo de porta 5	entrada ou saída de estacionamento
Modelo de porta 6	Leitores de entrada/saída para tempo e presença
Modelo de porta 7	controle de elevador
Modelo de porta 9	canaleta para veículos e portão rolante
Modelo de porta 10	porta simples com arme/desarme do IDS
Modelo de porta 14	porta simples com arme/desarme do IDS e direitos de acesso especial
Modelo de porta 15	sinais de entrada e saída independentes

- Os modelos de porta 1, 3, 5, 9 e 10 incluem uma opção para leitores de cartões adicionais nos lados de entrada e saída.
- Um controlador de acesso local usado dentro do modelo de porta 05 (estacionamento) ou 07 (elevador) não pode ser compartilhado com outro modelo de porta.
- Ao configurar e salvar uma entrada com um modelo de porta, o modelo de porta não pode mais ser trocado por outro. Se for necessário um modelo de porta diferente, a entrada deve ser excluída e configurada novamente do zero.

Alguns modelos de porta têm variantes (a, b, c, r) com as seguintes características:

a	leitores de entrada **e** saída
b	leitor de entrada e botão de destrave de saída

c	leitor de entrada **OU** saída (não ambos, o que seria a variante **a**)
r	(Somente modelo de porta 1). um leitor com a finalidade exclusiva de registrar pessoas em um ponto de encontro, por exemplo, no caso de uma evacuação. Este modelo de porta não requer nenhuma barreira física.

O botão **OK** para concluir a configuração só se torna ativa quando todos os valores obrigatórios forem inseridos. Por exemplo, modelos de porta da variante (a) exigem leitores de entrada **e** saída. As entradas não podem ser salvas até que um tipo para ambos os leitores seja selecionado.

15.2 Criação de entradas

A lista de leitores apresentada para seleção se adequará ao tipo de controlador escolhido.

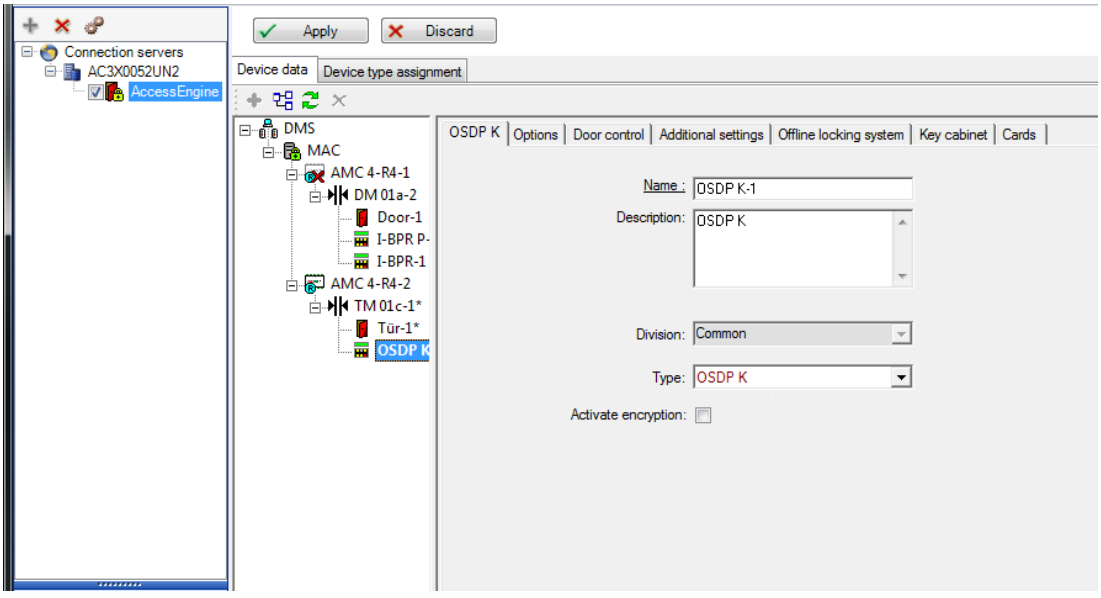
– Para os **tipos AMC 4W**, somente leitores Wiegand estão disponíveis, com e sem teclado.
– Para **AMC 4R4**, estão disponíveis os leitores da seguinte tabela. Não misture protocolos no mesmo controlador.

Nome do leitor	Protocolo de Wiegand	Protocolo BPR(*)	Protocolo I-BPR	Protocolo HADP	Protocolo OSDP
WIE1	X				
WIE1K (teclado)	X				
BPR MF		X			
Teclado BPR MF		X			
BPR LE		X			
Teclado BPR LE		X			
BPR HI		X			
Teclado BPR HI		X			
TA40 LE		X			
TB15 HI1		X			
TB30 LE		X			
INTUS 1600			X		
I-BPR			X		
I-BPR K (teclado)			X		
DT 7020			X		
OSDP					X
OSDP K (teclado)					X
OSDP KD (teclado + monitor)					X
HADP				X	
HADP K (teclado)				X	

HADP KD (teclado + monitor)				X	
RKL 55 (teclado + LCD)				X	
RK40 (teclado)				X	
R15				X	
R30				X	
R40				X	
RK40				X	
RKL55				X	

(*) O protocolo BPR foi desativado e está incluído aqui apenas por motivos de compatibilidade.

No caso de um **leitor OSDP**, a caixa de diálogo aparece da seguinte forma:



Comunicação segura com OSDP

Por padrão, a caixa de seleção **Ativar criptografia** está desmarcada. Marque-a se estiver usando leitores com suporte para **OSDPv2 seguro**.

Se você desativar a criptografia depois desmarcando a caixa de seleção, redefina o hardware do leitor de acordo com as instruções do fabricante.

Como precaução de segurança adicional, qualquer tentativa de trocar uma unidade configurada de leitor OSDP por uma unidade diferente vai gerar um alarme no sistema de controle de acesso. O operador pode confirmar o alarme no cliente e, ao mesmo tempo, dar permissão para a troca.

Mensagem de alarme: **Troca de leitor OSDP recusada**

Comando: **Permitir a troca do leitor OSDP**

Os seguintes tipos de leitores OSDP estão disponíveis:

OSDP	Leitor OSDP padrão
Teclado OSDP	Leitor OSDP com teclado

Teclado + visor OSDP	Leitor OSDP com teclado e visor

Os seguintes leitores OSDP foram testados:

OSDPv1 - modo não seguro	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 - modos seguro e não seguro	LECTUS secure 2000 RO LECTUS secure 4000 RO LECTUS secure 5000 RO

Aviso!

Ressalvas para o OSDP

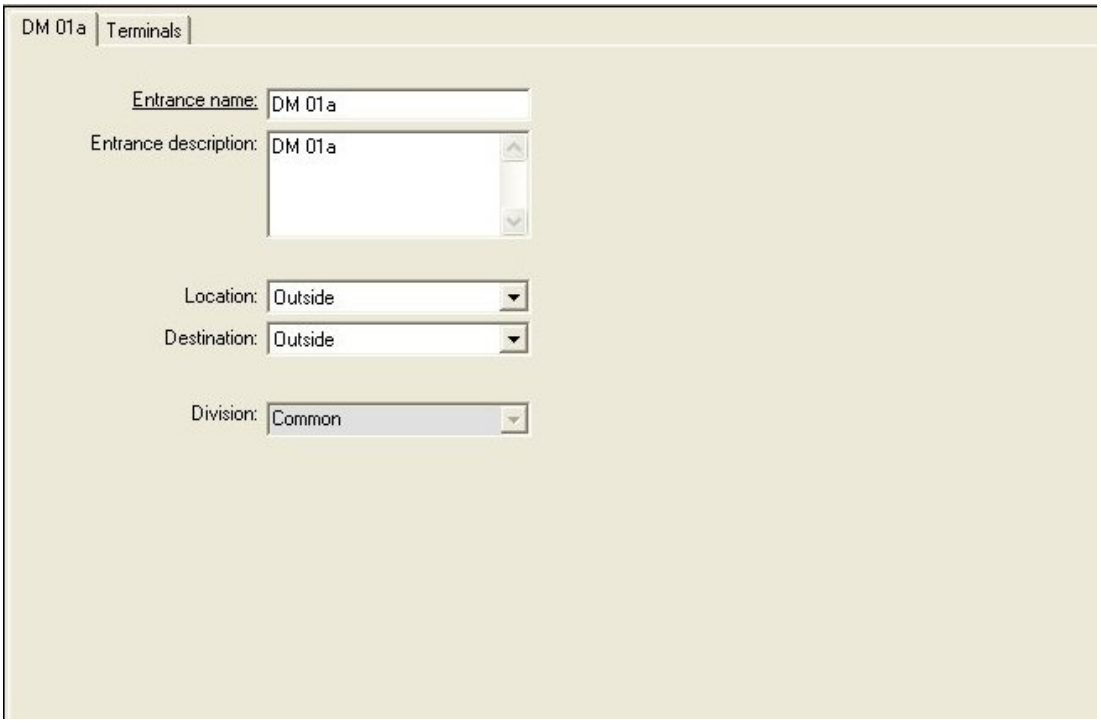
Não misture famílias de produtos, por exemplo, **LECTUS duo** e **LECTUS secure** no mesmo barramento OSDP.

Uma chave específica ao cliente é gerada e usada para a transmissão de dados criptografados ao leitor OSDP. Verifique se o sistema está com o backup adequado.

Mantenha as chaves seguras. Chaves perdidas não podem ser recuperadas, o leitor só poderá ser redefinido para os padrões de fábrica.

Por motivos de segurança, não misture modos criptografados e não criptografados no mesmo barramento OSDP.

Se você desativar a criptografia desmarcando a caixa de seleção na guia OSDP do leitor no Editor de dispositivos, redefina o hardware do leitor de acordo com as instruções do fabricante.



Parâmetro	Valores possíveis	Descrição
Nome da entrada	Alfanumérico, entre 1 e 16 caracteres	A caixa de diálogo gera um nome exclusivo para a entrada, mas esse nome pode ser substituído pelo operador que configura a entrada, se desejar.
Descrição da entrada	alfanumérico: 0 a 255 caracteres	Um texto descritivo arbitrário para exibição no sistema.
Localização	Qualquer área definida (não estacionamento)	A área nomeada (conforme definido no sistema) onde o leitor está localizado. Essas informações são usadas para controle da sequência de acesso: se uma pessoa tentar usar esse leitor, mas o local atual dessa pessoa (conforme rastreado pelo sistema) for diferente da localização do leitor, o leitor negará o acesso para a pessoa.
Destino	Qualquer área definida (não estacionamento)	A área nomeada, conforme definido no sistema, à qual o leitor permite o acesso. Essas informações são usadas para controle da sequência de acesso: se uma pessoa usar esse leitor, a localização será atualizada para o valor de **Destino**.
Tempo de espera pela decisão de acesso externo	Número de décimos de um segundo	O tempo que um controlador de acesso espera por uma decisão de um sistema ou dispositivo externo que está conectado a uma das entradas.
Divisão	A divisão à qual o leitor pertence. O valor padrão é **Comum**	Relevante somente se o recurso **Divisões** for licenciado.
Área de acionamento (somente para modelo de entrada 14)	Uma letra: A até Z	As entradas de um grupo de IDS serão ativadas juntas pela ativação dos leitores da área.

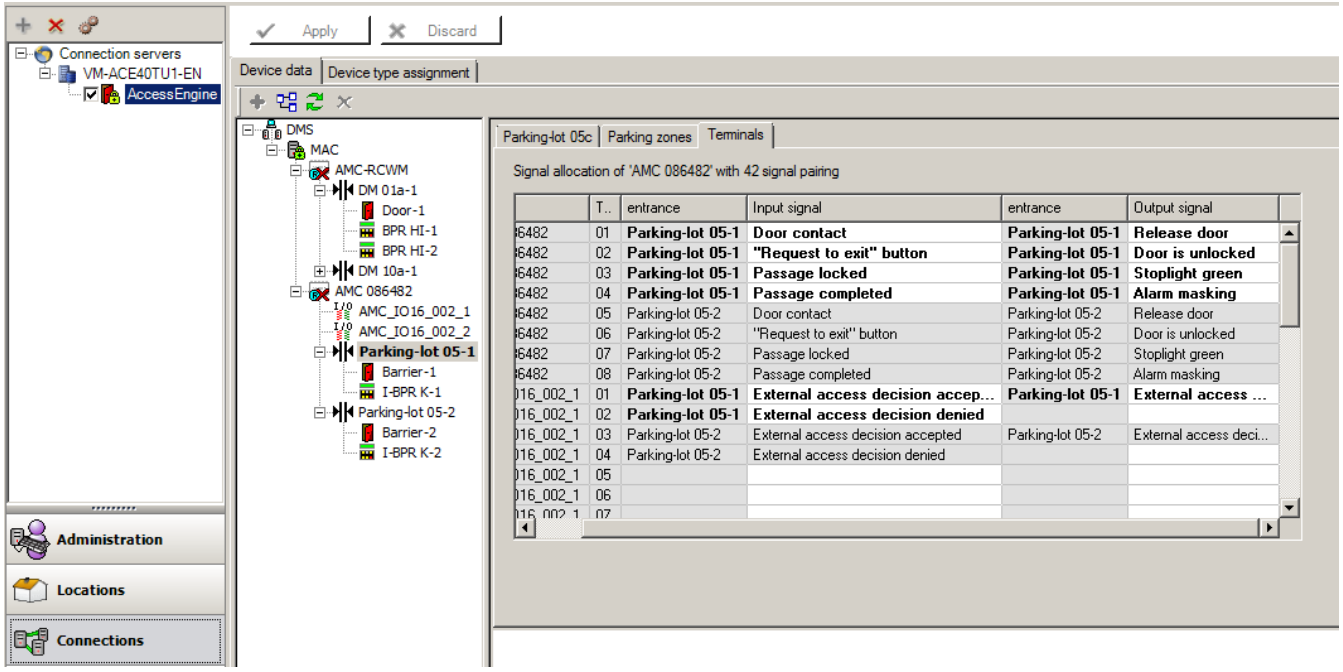
15.3 Verificações de E/S adicionais

As verificações de E/S adicionais, por exemplo, ajudam a identificar um visitante com base no Reconhecimento de número da placa automatizado (ANPR).

O AMC recebe uma entrada por meio do contato de E/S do AMC:

– Verificação de E/S adicional de visitante autorizado

O AMC impede o acesso em caso de um sinal "não autorizado".

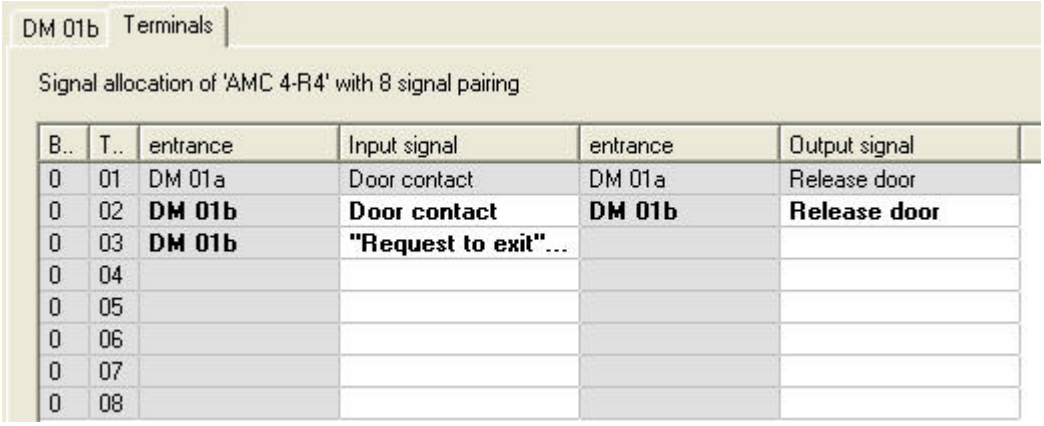


Status do cartão	Sinal = 1: autorizado por ANPR	Sinal = 0: não autorizado por ANPR
Cartão autorizado	Acesso	Evento de número de veículo inválido
Cartão na lista negra	Não autorizado – lista negra	Não autorizado – lista negra
Cartão expirou	Não autorizado – expirou	Não autorizado – expirou
Cartão não autorizado para este leitor	Não autorizado	Não autorizado

É possível abrir a barreira manualmente mesmo que o visitante não seja reconhecido.
Para essa função, um comutador é conectado aos contatos de E/S do AMC.
O AMC define um sinal de saída **Verificação adicional ativa** antes da análise do sinal de entrada.
Se o proprietário do veículo e a placa ainda forem desconhecidos para o sistema de controle de acesso, o operador deverá registrá-los agora.

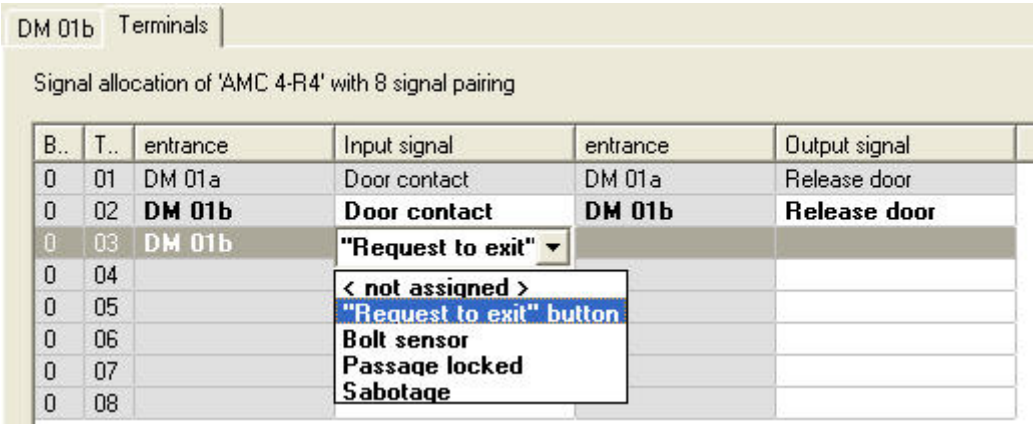
15.4 Configuração de terminais do AMC

Quanto ao conteúdo e à estrutura, esta guia é idêntica à guia **Terminals (Terminais)** do AMC.

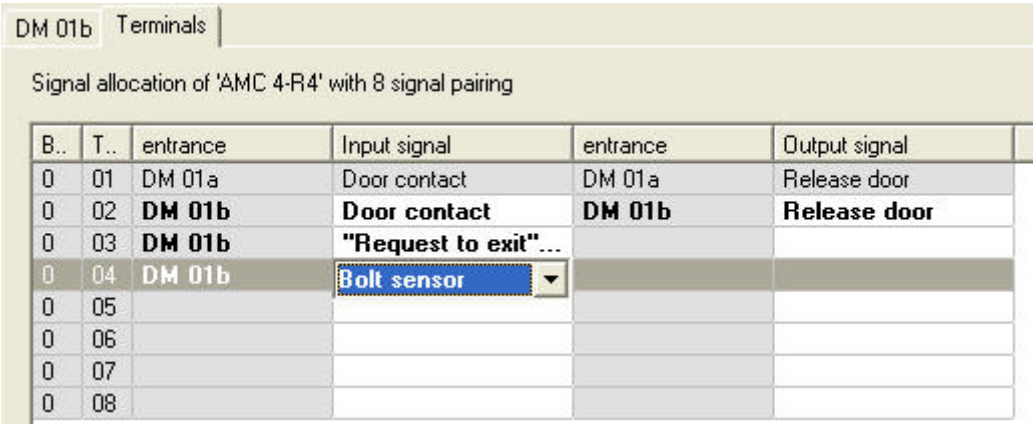


B..	T..	entrance	Input signal	entrance	Output signal
0	01	DM 01a	Door contact	DM 01a	Release door
0	02	**DM 01b**	**Door contact**	**DM 01b**	**Release door**
0	03	**DM 01b**	**"Request to exit"...**		
0	04				
0	05				
0	06				
0	07				
0	08				

Aqui, no entanto, é possível fazer alterações na atribuição de sinais para o modelo de entrada selecionado. Clicar duas vezes nas colunas **Output signal (Sinal de saída)** ou **Input signal (Sinal de entrada)** abre caixas de combinação.



De forma semelhante, é possível criar sinais adicionais para a entrada respectiva. Clicar duas vezes em uma linha vazia exibe a caixa de combinação apropriada:

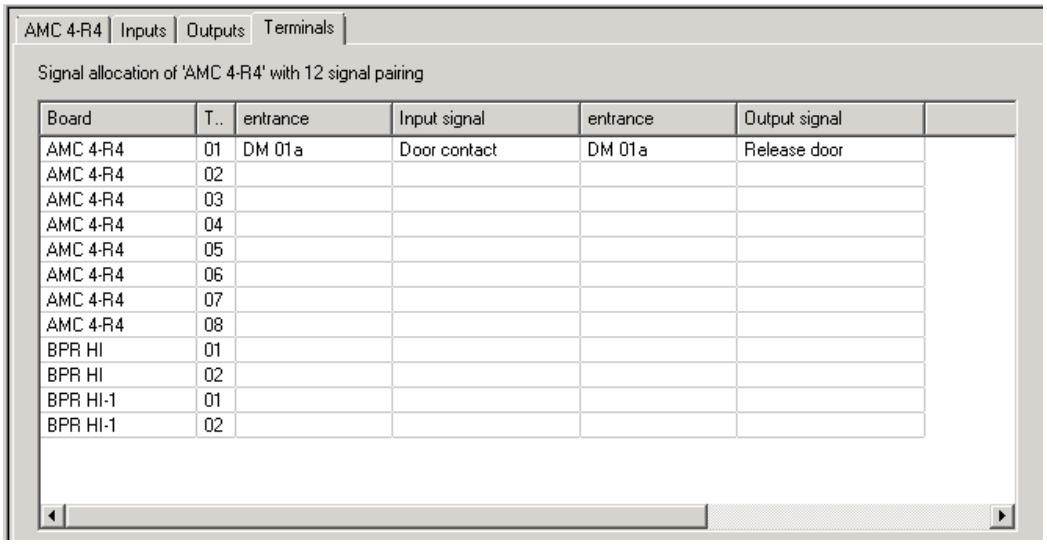


Atribuições de sinais inadequadas para a entrada em edição são somente leitura, com um fundo em cinza. Elas só podem ser editadas enquanto a entrada correspondente estiver selecionada.
Um fundo cinza semelhante e uma cor pálida de primeiro plano são aplicados a essas saídas que foram parametrizadas na guia **Outputs (Saídas)** do AMC.

Aviso!
As caixas de combinação não são 100% sensíveis ao contexto, portanto, é possível selecionar sinais que não funcionarão na vida real. Se você adicionar ou remover sinais na guia **Terminals (Terminais)**, teste-os para garantir que são física e logicamente compatíveis com a entrada.

Atribuição de terminal
Para cada AMC e cada entrada, uma guia **Terminal** lista todos os oito sinais do AMC em oito linhas separadas. Sinais não utilizados são marcados em branco e os utilizados são marcados em azul.
A lista contém a seguinte estrutura:

– **Board (Placa)**: numeração da extensão Wiegand do AMC (0) ou da placa de extensão de E/S (1 a 3)

- **Terminal**: número do contato no AMC (01 até 08) ou na placa de extensão Wiegand (09 a 16).
- **Entrance (Entrada)**: nome da entrada
- **Output signal (Sinal de saída)**: nome do sinal de saída
- **Entrance (Entrada)**: nome da entrada
- **Input signal (Sinal de entrada)**: nome do sinal de entrada
- 

Alteração da atribuição de sinal

Na guia de terminais dos controladores, a atribuição dos sinais separados é apenas exibida (somente leitura). Nas guias de terminais das entradas respectivas, no entanto, é possível alterar ou reposicionar os sinais das entradas selecionadas.

Clicar duas vezes na coluna **Output signal (Sinal de saída)** ou **Input signal (Sinal de entrada)** da entrada a ser alterada ativa uma lista suspensa, para que um valor diferente possa ser selecionado como o sinal do modelo de entrada. Se você selecionar **Not assigned (Não atribuído)**, o sinal é liberado e poderá ser usado para outras entradas.

Portanto, você pode não apenas alterar sinais, mas também atribuir sinais a outros contatos para otimizar o uso da tensão disponível. Qualquer contato livre ou liberado poderá ser usado posteriormente para novos sinais ou como novas posições para sinais existentes.

Aviso!

A princípio, todos os sinais de entrada e saída podem ser selecionados livremente, mas nem todas as seleções fazem sentido para todos os modelos de porta. Por exemplo, não faria sentido atribuir sinais do IDS a um modelo de porta (por exemplo, 01 a 03) que não oferece suporte ao IDS. Para obter mais detalhes, consulte a tabela na seção Atribuição de sinais aos modelos de porta.

Atribuição de sinais aos modelos de porta

Para evitar a parametrização incorreta dos menus suspensos para atribuição de sinais aos modelos de porta, os menus oferecem somente os sinais compatíveis com o modelo de porta selecionado.

Tabela de sinais de entrada

Sinais de entrada	Descrição
Door contact (Contato de porta)	

Botão "Solicitação de saída"	Botão para abrir a porta.
Sensor do parafuso	É usado somente para mensagens. Não há nenhuma função de controle.
Entrada bloqueada	É usado para bloquear a porta oposta em eclusas temporariamente. Mas também pode ser usado para travar por muito tempo.
Adulterar	Sinal de adulteração de um controlador externo.
Catraca na posição normal	A catraca está fechada.
Passagem concluída	Uma passagem foi concluída. É um pulso de um controlador externo.
IDS: pronto para armar	Será definido pelo IDS, se todos os detectores estiverem em repouso e o IDS puder ser armado.
IDS: está armado	O IDS está armado:
IDS: botão de solicitação para armar	Botão para armar o IDS.
Suprimir alarme de abertura não autorizada	Será usado se um esquema de portas abrir a porta sem envolver o AMC. O AMC não envia nenhuma mensagem de inclusão, mas "porta local aberta".
Decisão de acesso externo aceita	O sinal será definido, se um sistema externo aceitar o acesso
Decisão de acesso externo negado	O sinal será definido, se um sistema externo negar o acesso

Tabela de sinais de saída

Sinais de saída	**Descrição**
Liberar porta	
Eclusa: bloquear direção oposta	Bloqueia o outro lado da eclusa. O sinal é enviado quando a porta abre.
Supressão de alarme	... para o IDS. Definido desde que a porta esteja aberta, para evitar que o IDS crie uma mensagem de intrusão.
Semáforo verde	Lâmpada indicadora – será controlada assim que a porta abrir.
Tempo máximo de abertura da porta decorrido ou segurança da porta comprometida	Se a porta for mantida aberta ou ficar aberta por muito tempo
Conexão de câmera	A câmera será ativada no início de uma passagem.
Liberar entrada da catraca	

Liberar saída da catraca	
A porta está destravada	Sinal para destravar a porta durante um período prolongado.
IDS: armar	Sinal para armar o IDS.
IDS: desarmar	Sinal para desarmar o IDS.
Decisão de acesso externo ativada	O sinal deve ser definido para ativar o sistema de acesso externo

Tabela de mapeamento dos modelos de porta para sinais de entrada e saída

A tabela a seguir lista atribuições relevantes de sinais e modelos de porta.

Modelo de porta	Descrição	Sinais de entrada	Sinais de saída
01	Porta simples com leitor de entrada e saída Leitores de frequência Decisão de acesso externo disponível	- Door contact (Contato de porta) - Botão "Solicitação de saída" - Sensor do parafuso - Entrada bloqueada - Adulterar - Abertura local habilitada - Decisão de acesso externo aceita - Decisão de acesso externo negado	- Liberar porta - Eclusa: bloquear direção oposta - Supressão de alarme - Semáforo verde - Conexão de câmera - Tempo máximo de abertura da porta decorrido ou segurança da porta comprometida - Decisão de acesso externo ativada
03	Porta giratória com leitor de entrada e saída Leitores de frequência Decisão de acesso externo disponível	- Catraca na posição de descanso - Botão "Solicitação de saída" - Entrada bloqueada - Adulterar - Decisão de acesso externo aceita - Decisão de acesso externo negado	- Eclusa: bloquear direção oposta - Liberar entrada da catraca - Liberar saída da catraca - Supressão de alarme - Conexão de câmera - Tempo máximo de abertura da porta decorrido ou - Segurança da porta comprometida - Decisão de acesso externo ativada
05	Entrada ou saída de estacionamento – máximo de 24 zonas de estacionamento Leitores de frequência Decisão de acesso externo disponível	- Door contact (Contato de porta) - Botão "Solicitação de saída" - Entrada bloqueada - Passagem concluída - Decisão de acesso externo aceita	- Liberar porta - Supressão de alarme - Semáforo verde - Tempo máximo de abertura da porta decorrido ou - Segurança da porta comprometida

		- Decisão de acesso externo negado	- A porta está destravada - Decisão de acesso externo ativada
06	Leitores de frequência		
07	Elevador – máximo de 56 andares		
09	Leitor de entrada ou saída de veículo e botão de destrave Leitores de frequência Decisão de acesso externo disponível	- Door contact (Contato de porta) - Botão "Solicitação de saída" - Entrada bloqueada - Passagem concluída - Decisão de acesso externo aceita - Decisão de acesso externo negado	- Liberar porta - Supressão de alarme - Semáforo verde - Tempo máximo de abertura da porta decorrido ou - Segurança da porta comprometida - A porta está destravada - Decisão de acesso externo ativada
10	Porta simples com leitor de entrada e saída e arme/ desarme do IDS Leitores de frequência Decisão de acesso externo disponível	- Door contact (Contato de porta) - Botão "Solicitação de saída" - IDS: pronto para armar - IDS: está armado - Adulterar - IDS: solicitação para armar - Decisão de acesso externo aceita - Decisão de acesso externo negado	- Liberar porta - Conexão de câmera - IDS: armar - IDS: desarmar - Tempo máximo de abertura da porta decorrido ou - Segurança da porta comprometida - Decisão de acesso externo ativada
14	Porta simples com leitor de entrada e saída e arme/ desarme do IDS Leitores de frequência	- Door contact (Contato de porta) - Botão "Solicitação de saída" - IDS: pronto para armar - IDS: está armado - Adulterar - IDS: solicitação para armar	- Liberar porta - Conexão de câmera - IDS: armar - Tempo máximo de abertura da porta decorrido ou - Segurança da porta comprometida
15	Contatos digitais		

Atribuição de sinais aos leitores

Os leitores seriais (por exemplo, leitores em um AMC2 4R4) e leitores OSDP podem ser aprimorados com sinais de E/S locais. Dessa forma, sinais adicionais podem ser disponibilizados e os caminhos elétricos até os contatos da porta podem ser encurtados. Quando um leitor serial é criado, a guia **Terminals (Terminais)** da entrada correspondente mostra dois sinais de entrada e dois de saída para cada leitor abaixo do controlador e, se presente, os sinais da placa de extensão.

Aviso!
Essas entradas da lista são criadas para cada leitor serial, independentemente se têm ou não E/Ss locais.

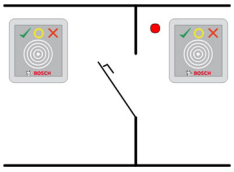
Esses sinais locais do leitor não podem ser atribuídos a funções e parametrizados como aqueles de controladores e placas. Eles também não aparecem nas guias **Input signal (Sinal de entrada)** e **Output signal (Sinal de saída)**, nem podem ser usados para elevadores (por exemplo, para exceder o limite de 56 andares). Por esse motivo, eles são mais indicados para o controle direto de portas (por exemplo, fechadura eletromagnética de porta ou liberação). No entanto, isso liberta os sinais do controlador para funções parametrizadas mais complexas.

Edição de sinais
Quando uma entrada é criada, a guia **Terminals (Terminais)** da entrada correspondente mostra dois sinais de entrada e dois de saída para cada leitor abaixo do controlador. A coluna de Placa exibe o nome do leitor. Os sinais padrão da entrada são atribuídos, por padrão, aos primeiros sinais livres do controlador. Para movê-los para os próprios sinais do leitor, primeiro eles precisam ser excluídos das posições originais. Para fazer isso, selecione a entrada da lista **<Not assigned> (<Não atribuído>)**
Clique duas vezes na coluna **Input signal (Sinal de entrada)** ou **Output signal (Sinal de saída)** do leitor para exibir uma lista dos possíveis sinais para o modelo de porta escolhido e, assim, reposicionar o sinal. Como todos os sinais, esses podem ser visualizados na guia **Terminals (Terminais)** do controlador, mas não podem ser editados nela.

Aviso!
O status dos sinais do leitor não pode ser monitorado.
Eles só podem ser usados para a porta à qual o leitor pertence.

15.5 Sinais predefinidos para modelos de porta

Modelo de entrada 01



Variantes do modelo:

01a	Porta normal com leitor de entrada **e** saída
01b	Porta normal com leitor de entrada e botão de destrave
01c	Porta normal com leitor de entrada **ou** saída

Sinais possíveis:

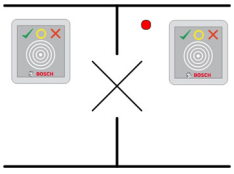
Sinais de entrada	**Sinais de saída**
Door contact (Contato de porta)	Liberar porta
Botão "Solicitação de saída"	Eclusa: bloquear direção oposta

Adulterar	Semáforo verde
Suprimir alarme de abertura não autorizada	Conexão de câmera
	Tempo máximo de abertura da porta decorrido ou segurança da porta comprometida

Aviso!
As funções onde apenas uma pessoa pode acessar por vez, especialmente o bloqueio da direção oposta, podem ser parametrizadas somente com DM 03.

A supressão de alarme somente é ativada quando, antes da abertura da porta, o tempo de supressão de alarme for superior a 0.
Este modelo de entrada também pode ser vantajoso para entradas de veículos, em que também é recomendado um leitor secundário para caminhões e carros.

Modelo de entrada 03



Variantes do modelo:

03a	Catraca bidirecional com leitor de entrada **e** saída
03b	Catraca bidirecional com leitor de entrada e botão de destrave
03c	Catraca com leitor de entrada **ou** saída

Sinais possíveis:

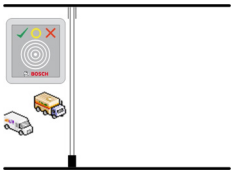
Sinal de entrada	**Sinais de saída**
Catraca na posição normal	Liberar entrada da catraca
Botão "Solicitação de saída"	Liberar saída da catraca
Adulterar	Entrada bloqueada
Suprimir alarme de abertura não autorizada	Conexão de câmera
	Tempo máximo de abertura da porta decorrido ou segurança da porta comprometida
Sinais adicionais usando a opção de **eclusa**:	
Entrada bloqueada	Eclusa: bloquear direção oposta
	Supressão de alarme

Notas de configuração para eclusas:
Quando a catraca está na posição normal, o primeiro sinal de entrada de todos os leitores conectados é ligado. Se um cartão é apresentado e se o proprietário possui direitos de acesso para essa entrada, então:

– Se, no leitor de entrada, o primeiro sinal de saída for definido no leitor de entrada para a duração do tempo de ativação.
– Se, no leitor de saída, o segundo sinal de saída for definido no leitor de saída para a duração do tempo de ativação.

Quando o botão Solicitação de saída (REX) é pressionado, o segundo sinal de entrada e o segundo sinal de saída são definidos. Durante este período, a porta giratória pode ser usada no sentido habilitado.

Modelo de entrada 05c



Variante do modelo:

05c	Leitor de acesso ao estacionamento de entrada **ou** saída

Sinais possíveis para esse modelo de entrada:

Sinais de entrada	**Sinais de saída**
Door contact (Contato de porta)	Liberar porta
Botão "Solicitação de saída"	A porta está destravada
Entrada bloqueada	Semáforo verde
Passagem concluída	Supressão de alarme
	Tempo máximo de abertura da porta decorrido ou segurança da porta comprometida

A entrada e a saída do estacionamento devem ser configuradas no mesmo controlador. Se o acesso ao estacionamento foi atribuído a um controlador, esse controlador não poderá governar outros modelos de porta. Para a entrada do estacionamento, somente um leitor de entrada (nenhum leitor de saída) pode ser atribuído. Assim que a entrada for atribuída, selecionar o modelo de porta novamente permite que você apenas defina o leitor de saída. Você pode definir até 24 subáreas para cada estacionamento, das quais uma deve estar contida nas autorizações do cartão para que o cartão funcione.

Modelo de entrada 06


Variantes de modelo

06a	Leitor de entrada **e** saída para tempo e participação
06c	Leitor de entrada **ou** saída para tempo e participação

Os leitores que são criados com esse modelo de porta não controlam portas ou barreiras, mas apenas encaminham dados do cartão para um sistema de tempo e participação. Esses leitores costumam ficar em lugares aos quais o acesso já foi controlado.
Portanto, nenhum sinal é definido.

Aviso!
Para que pares de registro válidos (hora de entrada mais hora de saída) possam ser criados no sistema de frequência, é necessário parametrizar dois leitores separados com o modelo de porta 06: um para sincronia de entrada e outro para saída

Use a variante **a** quando entrada e saída não forem separadas. Use a variante **c** se a entrada e a saída forem separadas fisicamente ou se não for possível anexar os leitores ao mesmo controlador. Lembre-se de definir um dos leitores como leitor de entrada e um como leitor de saída.
Assim como em qualquer entrada, é necessário criar e atribuir autorizações. A guia **Controle de tempo** nas caixas de diálogo **Autorizações de acesso** e **Autorizações de área/tempo** lista todos os leitores de tempo e participação que foram definidos. Ative pelo menos um leitor na direção de entrada e um leitor na direção de saída. As autorizações para leitores de tempo e participação podem ser atribuídas junto com outras autorizações de acesso ou como autorizações separadas.
Se existir mais de um leitor de tempo e participação para uma determinada direção, é possível atribuir determinados titulares de cartão a determinados leitores. Somente o tempo de participação de usuários atribuídos e autorizados será registrado e armazenado pelo leitor.

Aviso!
Outros recursos de controle de acesso também afetam o comportamento dos leitores de frequência. Logo, listas negras, modelos de tempo ou datas de validade também podem impedir que um leitor de frequência registre os horários de acesso.

As horas registradas de entrada e saída são armazenadas em um arquivo de texto no diretório:
`<SW_installation_folder>\AccessEngine\AC\TAExchange\`
com o nome `TAccExc_EXP.txt` e ficam com a exportação pendente para um sistema de tempo e participação.
Os dados de reserva são transmitidos no seguinte formato:
`ddMMyyyy;hhmm[s];Direction [0,1]; AbsenceReason; Personnel-Nr.`
d = dia, M = mês, a = ano, h = hora, m = minuto, s = horário de verão, 0 = saída, 1 = entrada
O arquivo de exportação contém todas as reservas em ordem cronológica. O separador de campo dentro do arquivo é um ponto e vírgula.

Variantes do modelo de entrada 07:

Variantes do modelo:

07a	Elevador com, no máximo, 56 andares
07c	Elevador com, no máximo, 56 andares e modelo de hora

Modelo de entrada 07a
Sinais:

Sinal de entrada	Sinais de saída
	Liberar <nome do andar>
	Um sinal de saída por andar definido, com um máximo de 56.

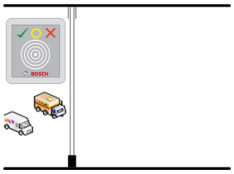
Ao chamar o elevador, o proprietário do cartão pode selecionar somente os andares para os quais seu cartão está autorizado.
Os modelos de porta de elevador não podem ser misturados com outros modelos de porta no mesmo controlador. Usando placas de extensão, até 56 andares podem ser definidos para cada elevador em um AMC. As autorizações do cartão devem conter o próprio elevador e pelo menos um andar.

Modelo de entrada 07c
Sinais:

Sinal de entrada	Sinal de saída
Chave de entrada <nome do andar>	Liberar <nome do andar>
Para cada andar definido, existe uma entrada e uma saída – até 56.	

Ao chamar o elevador e pressionar o botão de seleção do andar (logo, a necessidade de sinais de entrada), as autorizações do cartão são verificadas para ver se incluem o andar escolhido. Além disso, com esse modelo de porta é possível definir qualquer andar atendido como **acesso público**, isto é, nenhuma verificação de autorização será realizada para esse andar e qualquer pessoa pode levar o elevador até ele. Contudo, o próprio acesso público pode ser governado por um **modelo de tempo** que o limita a determinadas horas de determinados dias. Fora desses intervalos, as verificações de autorização serão realizadas normalmente.
Os modelos de porta de elevador não podem ser misturados com outros modelos de porta no mesmo controlador. Usando placas de extensão, até 56 andares podem ser definidos para cada elevador em um AMC. As autorizações do cartão devem conter o próprio elevador e pelo menos um andar.

Modelo de entrada 09

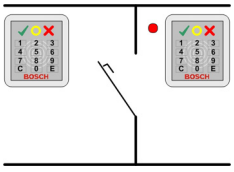


Sinais possíveis:

Sinais de entrada	Sinais de saída
Door contact (Contato de porta)	Liberar porta
Botão "Solicitação de saída"	Porta aberta por muito tempo
Entrada bloqueada	Semáforo verde
Passagem concluída	Supressão de alarme
	Tempo máximo de abertura da porta decorrido ou segurança da porta comprometida

Para o controle da barreira, utiliza-se um controle subjacente (SPS). Ao contrário do **modelo de porta 5c**, você pode configurar essa entrada e saída em diferentes AMCs. Além disso, não existem subáreas, apenas uma autorização geral para área de estacionamento.

Modelo de entrada 10



Variantes do modelo:

10a	Porta normal com leitor de entrada **e** saída **e** arme/desarme do IDS (Sistema de detecção de intrusão)
10b	Porta normal com leitor de entrada, botão REX (solicitação de saída) e arme/desarme do IDS
10e	Porta normal com leitor de entrada, botão REX e arme/desarme do IDS descentralizado

Sinais possíveis:

Sinais de entrada	Sinais de saída
Door contact (Contato de porta)	Liberar porta
IDS: está armado	IDS: armar
IDS: pronto para armar	IDS: desarme [somente DM 10e]
Botão "Solicitação de saída"	Conexão de câmera

Sensor do parafuso	Tempo máximo de abertura da porta decorrido ou segurança da porta comprometida
Adulterar	
Suprimir alarme de abertura não autorizada	
IDS: botão de solicitação para armar	

Aviso!
Esse modelo de porta requer leitores com teclado. titulares de cartões exigem **códigos PIN** para armar/desarmar o IDS.

Diferentes procedimentos são necessários dependendo dos leitores instalados.

Leitores seriais (incluindo I-BPR, HADP e OSDP)
Acione pressionando a tecla **7** e confirmando com Enter (#). Em seguida, apresente o cartão, insira o código PIN e confirme novamente com a tecla Enter (#).
Desarme apresentando o cartão, inserindo o código PIN e confirmando com Enter (#).

Leitores Wiegand (incluindo o protocolo serial BPR)
Arme pressionando 7, apresentando o cartão e inserindo o código PIN. Não é necessário confirmar usando a tecla Enter.
Desarme apresentando o cartão e inserindo o código PIN. O desarme e a liberação da porta ocorrem simultaneamente.

Recursos especiais do DM 10e:
Enquanto nos modelos de porta 10a e 10b toda entrada é sua própria área de segurança, no 10e várias entradas podem ser agrupadas em unidades. Qualquer leitor desse grupo é capaz de armar ou desarmar a unidade toda. Um sinal de saída **Disarm IDS (Desarmar IDS)** é necessário para redefinir o status definido por qualquer um dos leitores no grupo.
Sinais:
- Modelos de porta 10a e 10b:
  - - O arme é acionado por um sinal contínuo
  - - O desarme é acionado pela descontinuação do sinal contínuo.
- Modelo de porta 10e:
  - - O arme e o desarme são acionados por um pulso de sinal com duração de um segundo.

[Usando um relé biestável, é possível controlar o IDS de várias portas. Para fazer isso, os sinais de todas as portas exigem uma operação OR no relé. Os sinais **IDS armed (IDS armado)** e **IDS ready to arm (IDS pronto para armar)** devem ser replicados em todas as portas participantes.]

Entradas especiais
Para modelos de entrada com recursos especiais, como:
- Elevadores
- Detecção de intrusão
- Switches digitais ou binários genéricos
- Eclusas

consulte o capítulo dedicado sobre entradas especiais.

Consulte

– *Entradas especiais, página 93*

15.6 Entradas especiais

15.6.1 Elevadores (DM07)

Observações gerais sobre elevadores (modelo de entrada 07)

Os elevadores não podem ser combinados com outros modelos de porta no mesmo controlador AMC.

Os elevadores não podem ser usados com as opções **Group access (Acesso de grupo)** ou **Attendant required (Atendedor necessário)** do leitor

Até 8 andares podem ser definidos em um AMC. Uma placa de extensão do AMC oferece 8 ou 16 saídas adicionais por placa de extensão.

Logo, usando o número máximo das maiores placas de extensão é possível configurar até 56 andares com leitores RS485 e 64 andares com leitores Wiegand, se uma placa de extensão Wiegand especial for usada adicionalmente.

Diferenças entre os modelos de entrada 07a e 07c

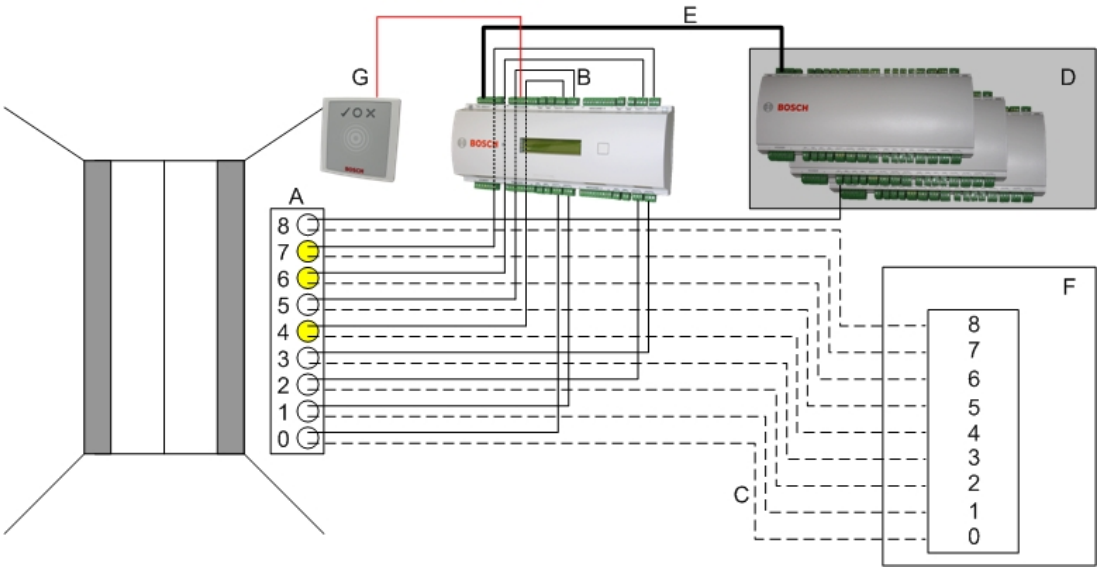
Nas caixas de diálogo de autorização de acesso, é possível atribuir pisos específicos para a autorização de uma pessoa.

Se o elevador tiver sido criado com o modelo de entrada **07a**, um titular de cartão apresentará seu cartão de identificação e os pisos para os quais ele tem permissão.

Com o modelo de entrada **07c**, o sistema verifica a autorização do piso selecionado depois que a pessoa tiver escolhido. Os pisos marcados como **públicos** estão disponíveis para cada pessoa independentemente da autorização. Junto com um modelo de tempo, a função pública pode ser restrita ao modelo de tempo especificado. Fora desse período, a autorização será marcada para o piso selecionado.

Esquema de fiação para elevadores:

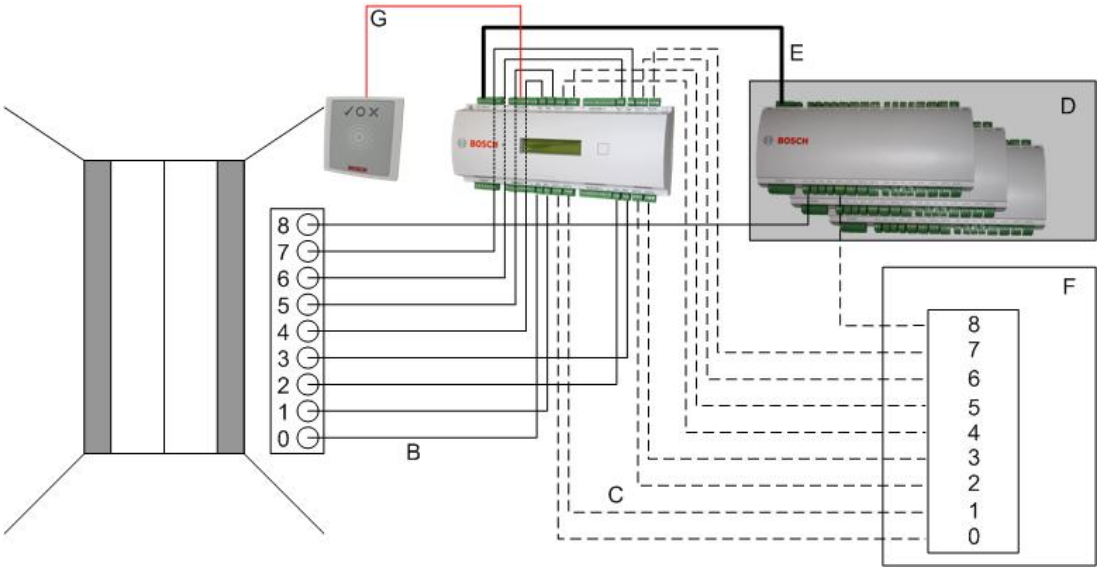
A figura a seguir mostra o esquema de conexão de um elevador usando o modelo de porta 07a.



Legenda:

- A = teclado do elevador
- B = (linha contínua) sinais de saída do AMC
- C = (linha tracejada) conexão aos controles do elevador
- D = até três placas de E/S podem ser conectadas a um AMC se as oito entradas e saídas não forem suficientes.
- E = Dados e fonte de alimentação do AMC para as placas de E/S
- F = o seletor de andares do elevador
- G = leitor. Dois leitores podem ser configurados para cada elevador.

A figura a seguir mostra o esquema de conexão de um elevador usando o modelo de porta 07c.



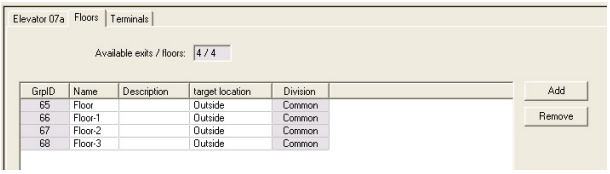
Legenda:

- B = (linha contínua) sinais de saída do AMC
- C = (linha tracejada) conexão aos controles do elevador
- D = até três placas de E/S podem ser conectadas a um AMC se as oito entradas e saídas não forem suficientes.
- E = Dados e fonte de alimentação do AMC para as placas de E/S
- F = o seletor de andares do elevador

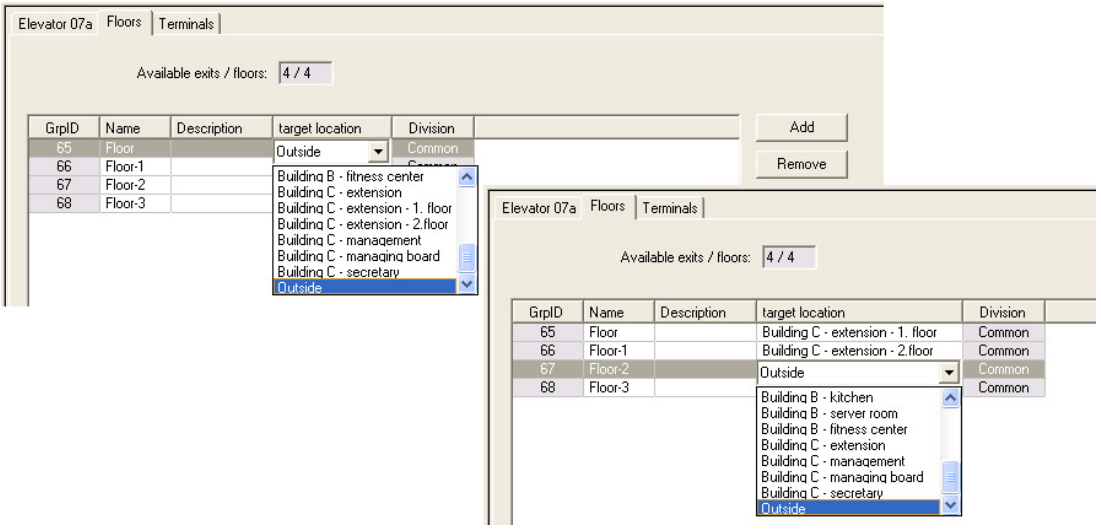
– G = leitor. Dois leitores podem ser configurados para cada elevador.

Igual aos estacionamentos, os elevadores também têm o parâmetro **Public (Público).** Esse parâmetro pode ser definido individualmente para cada andar. Se o parâmetro **Public (Público)** for ativado, as autorizações de acesso não será verificadas. Portanto, qualquer titular de cartão no elevador poderá selecionar o andar.
Se desejado, defina um modelo de tempo para o modelo de entrada: fora dos intervalos de tempo definidos, as autorizações serão verificadas.

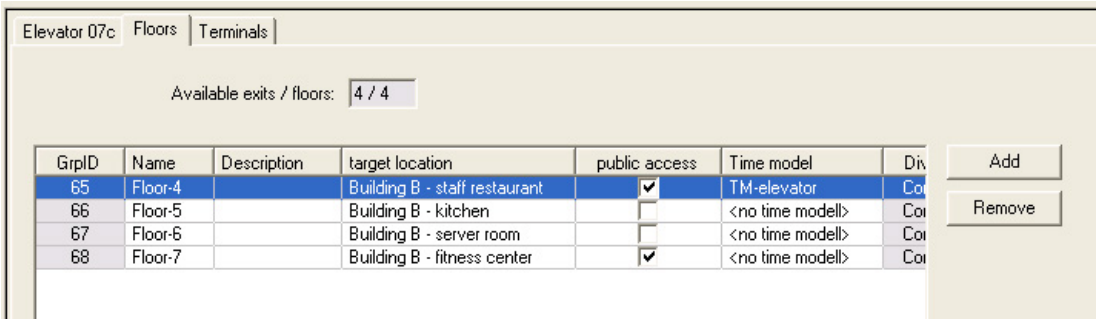
Pisos para o modelo de entrada 07
Use a guia **Pisos** para adicionar e remover pisos do elevador, usando os botões **Adicionar** e **Remover**.



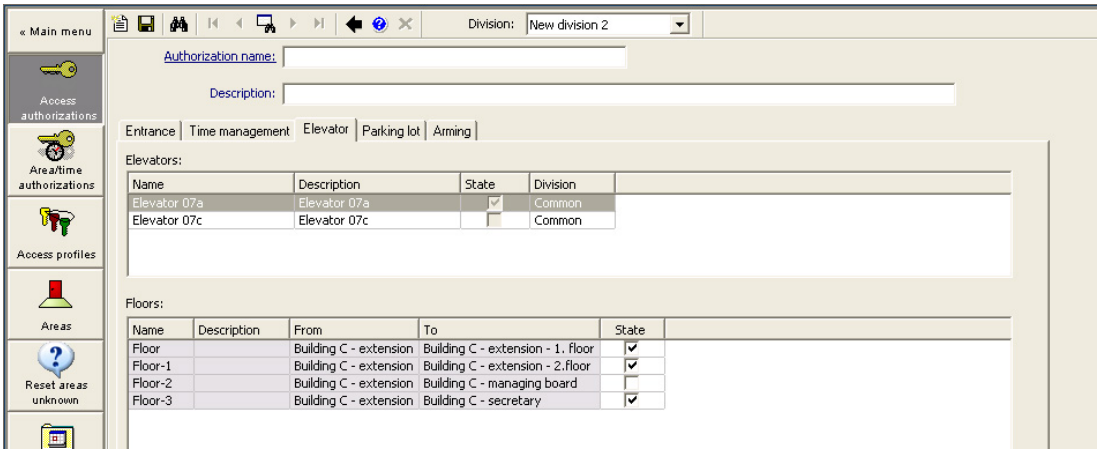
Os locais de destino de um piso podem ser qualquer **Área**, exceto áreas de estacionamento. Somente uma área pode ser atribuída a um piso individual. A escolha das áreas oferecidas nas caixas combinadas é, portanto, reduzida depois de cada atribuição, impedindo atribuições duplas não intencionais.



Ao usar o modelo de entrada 07a, é possível deixar pisos individuais publicamente acessíveis marcando a caixa **Acesso público**. Nesse caso, não ocorre nenhuma verificação de autorizações. A atribuição adicional de um **Modelo de tempo** também acabaria restringindo o acesso a períodos predefinidos.



Na guia **Elevador** acima da caixa de lista superior nas caixas de diálogo **Autorizações de acesso** e **Autorizações de área/tempo**, selecione primeiro o elevador necessário e, abaixo, os pisos aos quais o titular do cartão tem acesso permitido.



15.6.2 Modelos de porta com alarmes de intrusão (DM14)

Introdução

Ao contrário do modelo de entrada 10 (DM10), o **DM14** é capaz de armar e desarmar um sistema de alarme de intrusão ou IDS para uma área de armação específica. Uma entrada DM14 também pode ser configurada para conceder acesso ao titular de cartão que desarmar dela, desde que o titular tenha todas as outras permissões necessárias.

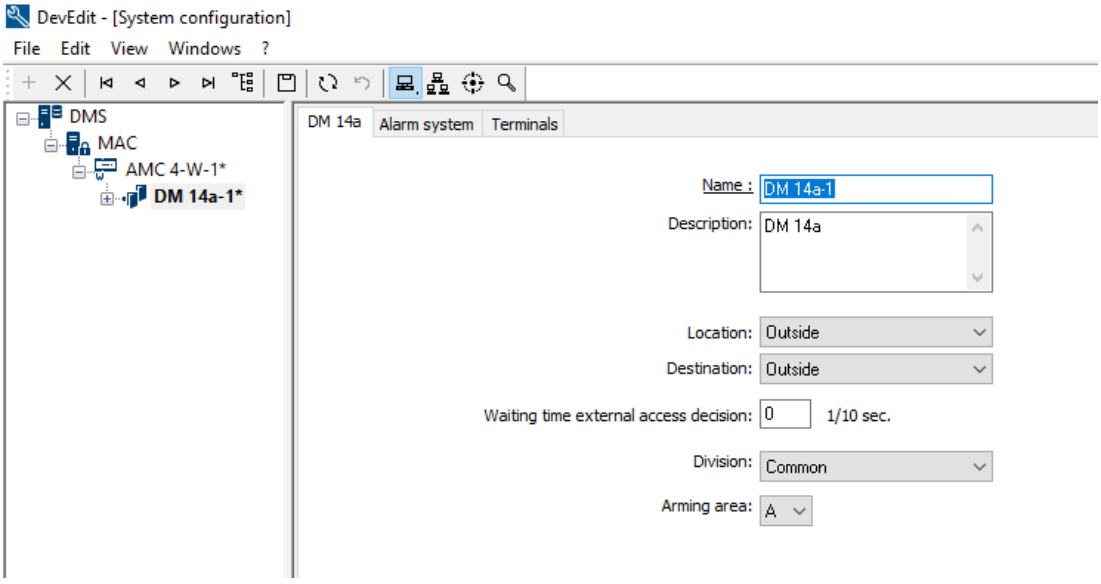
O procedimento de configuração para o DM14 no editor de dispositivos e no gerenciador de caixas de diálogo inclui estas tarefas:

1. Definir parâmetros gerais para identificar a entrada e a respectiva área de armação.
2. Definir parâmetros específicos para implantar o procedimento exato de desarme da área.
3. Definir sinais de entrada e saída específicos do IDS nos terminais do controlador de porta da entrada.
4. Incluir permissões de armação/desarme nas autorizações de acesso dos titulares de cartões que deverão operar as entradas DM14.

As tarefas estão descritas nas seções a seguir.

Parâmetros gerais

Na primeira guia, **DM14a** ou **DM14b**, defina os parâmetros a seguir.

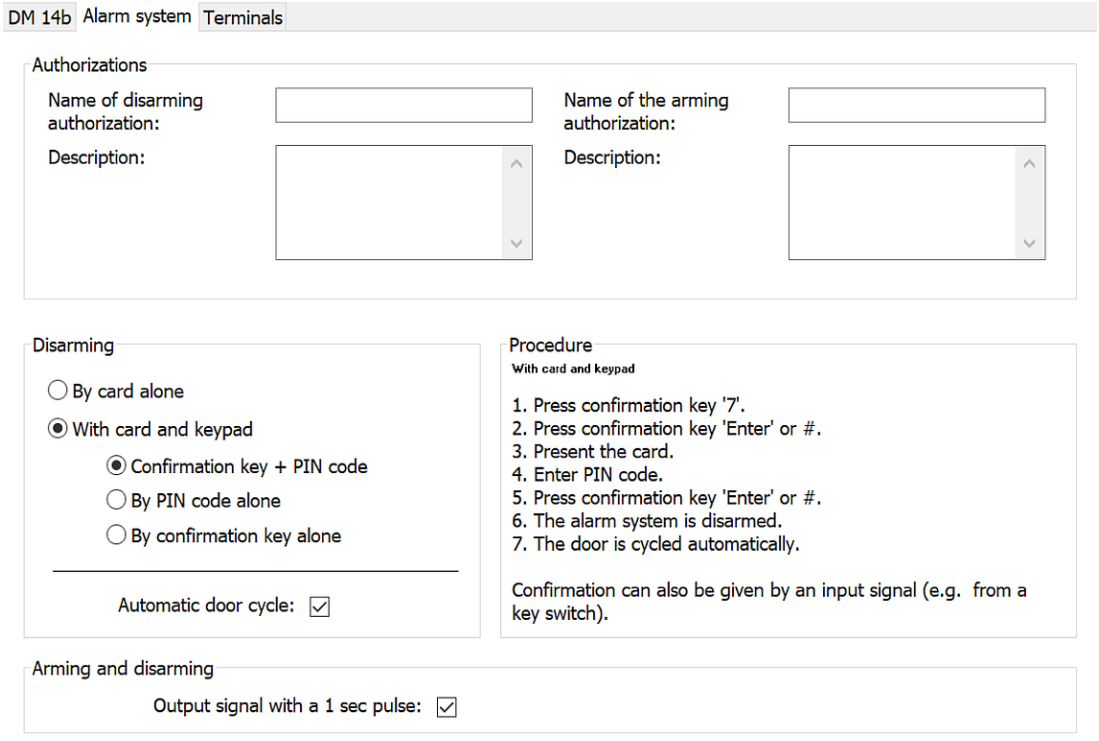


Parâmetro	Value type (Tipo de valor)	Descrição
Name (Nome)	Texto livre	O nome da entrada.
Description (Descrição)	Texto livre, opcional	Uma descrição da entrada.
Location (Local)	Lista das áreas definidas, se usada	A área de acesso em que a entrada está localizada.
Destination (Destino)	Lista das áreas definidas, se usada	A área de acesso à qual a entrada leva.
Division (Divisão)	Lista das divisões definidas, se usada	A divisão ou o locatário dentro do sistema de controle de acesso ao qual a entrada pertence.

Parâmetro	Value type (Tipo de valor)	Descrição
Waiting time external access decision (Tempo de espera para decisão de acesso externa)	Décimos de segundo	Se você conectou um sistema externo aos terminais do AMC, para tomar decisões de acesso por ele, esse parâmetro limita o tempo de espera por uma resposta do sistema externo. Observação: A decisão de acesso requer o cumprimento de **todas** as condições definidas no sistema de controle de acesso, por exemplo, autorizações de acesso, modelos de tempo e divisões (se usados). O valor padrão é 0, ou seja, o parâmetro é ignorado.
Arming area (Área de armação)	Lista de letras maiúsculas A...Z	Uma letra para agrupar entradas DM14 em áreas de armação.

Parâmetros do sistema de alarme

Na segunda guia, **Alarm system (Sistema de alarme)**, defina os parâmetros a seguir. Esses parâmetro governam as credenciais e o procedimento para desarmar o IDS e o desarme afeta todas as entradas dentro da mesma área de armação, conforme definido na primeiro guia.



Parâmetro	Value type (Tipo de valor)	Descrição
Painel de autorizações		

Parâmetro	Value type (Tipo de valor)	Descrição
Name of disarming authorization (Nome da autorização de desarme)	Texto livre	Um nome que aparecerá em protocolos e relatórios quando um titular de cartão desarmar o IDS nessa entrada.
Name of arming authorization (Nome da autorização de armação)	Texto livre	Um nome que aparecerá em protocolos e relatórios quando um titular de cartão armar o IDS nessa entrada.
Descrição (um para cada autorização)	Texto livre, opcional	Descrições das autorizações de armação
Desarme de painel		
Somente por cartão	Botão de opção	Selecione essa opção para permitir que o IDS seja desarmado pela apresentação de um cartão no leitor, sem autenticação adicional.
Por cartão e teclado	Botão de opção	Selecione essa opção para permitir que o IDS seja desarmado pela apresentação de um cartão no leitor e autenticação adicional no teclado do leitor. A autenticação exata e o procedimento de desarme são determinados pelos seguintes subparâmetros:
Tecla de confirmação + código PIN	Botão de opção	Os titulares de cartões devem se autenticar usando um cartão, uma tecla de confirmação e um código PIN.
Somente por código PIN	Botão de opção	Os titulares de cartão devem se autenticar usando um cartão e um código PIN.
Somente por tecla de confirmação	Botão de opção	Os titulares de cartão devem se autenticar usando um cartão e uma tecla de confirmação.
Ciclo automático da porta	Caixa de seleção	Marque esta caixa de seleção se quiser aplicar um ciclo de bloqueio da porta mediante desarme, para permitir que o titular do cartão desarme e entre simultaneamente. **Observação:** Só será realizado o ciclo do bloqueio se o titular do cartão tiver permissão de acesso para essa porta.
Painel de procedimento		

Parâmetro	Value type (Tipo de valor)	Descrição
Dependendo dos parâmetros definidos no painel **Disarming (Desarme)**, ele mostrará um procedimento padrão para desarme do IDS. Comunique este procedimento aos titulares de cartões que utilizarão as entradas DM14 nesta área de armação.		
Painel de armação e desarme		
Sinal de saída com pulso de 1 s	Caixa de seleção	Marque esta caixa de seleção se estiver usando um painel de intrusão **B Series ou G Series da Bosch**. O efeito é enviar um sinal de pulso único para alternar o estado de armação da área de intrusão da entrada, em vez de definir o sinal como 1 (armar) ou 0 (desarmar) constante.

Terminais de controladores de portas

Para possibilitar a armação e o desarme com uma entrada DM14, é necessário definir a entrada do IDS e os sinais de saída que você deseja usar nos terminais do controlador de porta da entrada.

Essa etapa é necessária somente uma vez para cada controlador que tiver entradas DM14. Todas as entradas DM14 subsequentes definidas no mesmo controlador e nas respectivas placas de extensão herdarão os sinais do controlador compartilhado.

Os sinais padrão estão descritos na tabela a seguir.

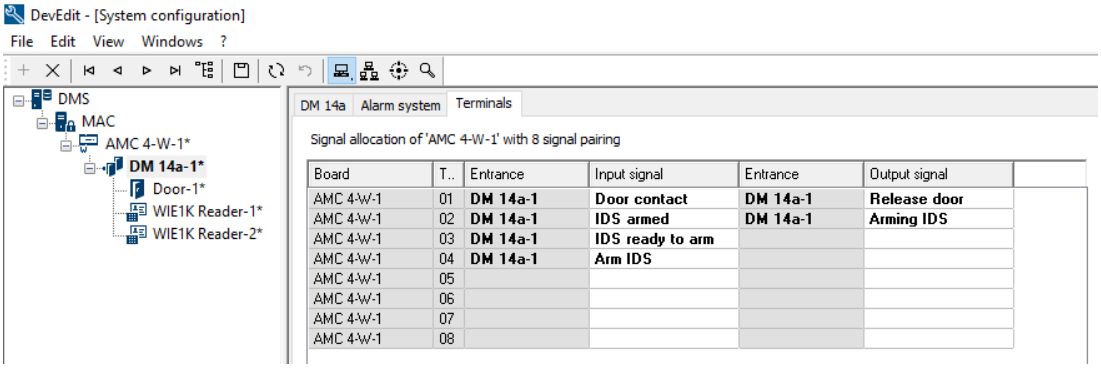
Sinal	Entrada/ Saída	Descrição
IDS armado	Entrada	O IDS está armado para esta área de intrusão.
IDS: pronto para armar	Entrada	Nenhum ponto do IDS está em estado de falha (aberto ou não preparado).
Armar IDS	Entrada	Solicitação para armar o IDS.
Botão "Solicitação de saída" (REX)	Entrada	
Sensor do parafuso	Entrada	Um sensor está monitorando a trava da porta.
Adulterar	Entrada	A adulteração foi detectada.
Suprimir alarme de abertura não autorizada	Entrada	Suprima o alarme por um número configurado de segundos extras se um sinal REX tiver sido emitido por um detector de movimento. Consulte o recurso de espera REX para obter mais detalhes.
Liberar porta	Saída	Realizar um ciclo do mecanismo da porta, para desbloqueada e de volta para bloqueada, a fim de permitir o acesso.

Sinal	Entrada/ Saída	Descrição
Armação do IDS	Saída	Armar ou desarmar o IDS, dependendo do estado atual (alternância).
Conexão de câmera	Saída	Ative uma câmera conectada à entrada.
Tempo máx. de abertura de porta esgotado ou **Segurança da porta comprometida**	Saída	A porta está mantida aberta ou o sistema suspeita de uma violação de segurança na porta.

Procedimento para atribuir sinais aos terminais

1. Abra a terceira guia, **Terminals (Terminais)**.

– Os terminais do controlador de porta dessa entrada, bem como as placas de extensão associadas, são exibidos em uma tabela.



2. Selecione a linha que corresponde ao terminal que deseja usar para o sinal de entrada.
3. Na célula correspondente, na coluna **Input signal (Sinal de entrada)**, selecione o sinal desejado na lista suspensa. Observe que somente os sinais não atribuídos até agora aparecerão na lista.
4. Repita as etapas anteriores para adicionar outros sinais de entrada necessários para essa entrada.
5. Repita o procedimento quantas vezes forem necessárias para adicionar os sinais de saída necessários à coluna **Output signal (Sinal de saída)**.

Definição de autorizações para armar e desarmar entradas DM14

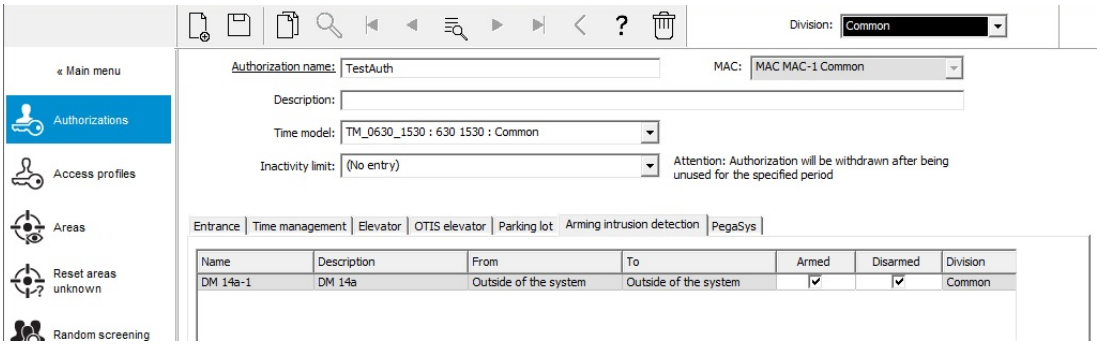
Depois de criar uma entrada DM14 no editor de dispositivos, a entrada estará disponível para inclusão nas autorizações de acesso.

1. No gerenciador de caixas de diálogo, navegue até:

– Main menu (Menu principal) > **System data (Dados do sistema)** > **Authorizations (Autorizações)** > guia: **Arming Intrusion detection (Armar detecção de intrusão)**

2. Carregue uma autorização de acesso existente na caixa de diálogo ou clique em  (Nova) para criar uma.

3. Encontre a entrada DM14 desejada na lista e marque as caixas de seleção **Armed (Armada)** e/ou **Disarmed (Desarmada)**.

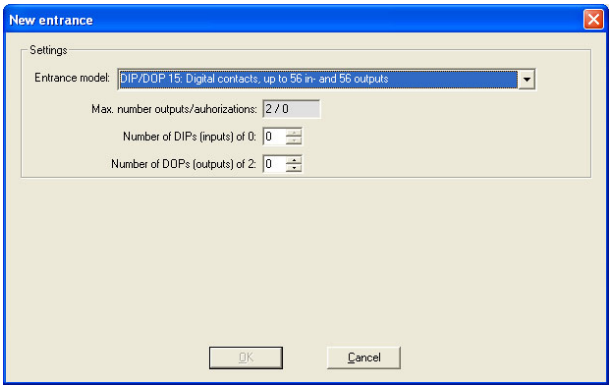


4. Clique em  (Salvar) para salvar a autorização de acesso com as permissões selecionadas.
5. Atribua essa autorização de acesso aos titulares de cartões que deverão operar as entradas DM14.

15.6.3 DIPs e DOPs (DM15)

Criação do modelo de entrada 15:

Esse modelo de entrada oferece sinais de entrada e saída independentes.



Se todas as interfaces do leitor estão ocupadas, somente esse modelo de entrada se torna disponível. Você pode definir esse modelo de entrada desde que haja pelo menos dois sinais livres.

Para AMCs de elevadores (modelo 07) ou estacionamentos (modelo 05c), não é possível atribuir esse modelo de entrada.

Modelo de entrada 15

Possíveis sinais: esses nomes padrão podem ser substituídos.

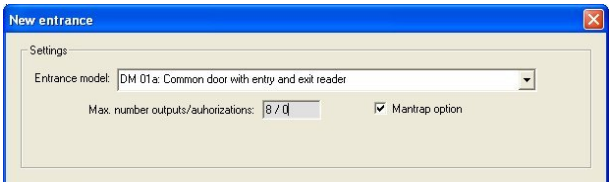
Sinal de entrada	Sinal de saída
DIP	DOP
DIP-1	DOP-1
...	...
DIP-63	DOP-63

Diferente de outros modelos de porta, o modelo de entrada 15 gerencia as entradas e saídas de um controlador que ainda estão livres e as coloca como entradas genéricas e saídas sem tensão à disposição do sistema inteiro.
Diferente dos contatos de saída de outros modelos de porta, os contatos do modelo de entrada 15 podem ser procurados individualmente no editor de dispositivos.

Reestabelecimento de DOPs após reinicializações
Ao reiniciar um MAC ou AMC, normalmente os valores de estado dos DOPs subordinados são redefinidos para o valor padrão 0 (zero).
Para garantir que uma reinicialização sempre redefina um DOP para o última estado atribuído manualmente a ele, selecione o DOP na árvore de dispositivos e marque a caixa de seleção **Keep state (Manter estado)** na janela principal.

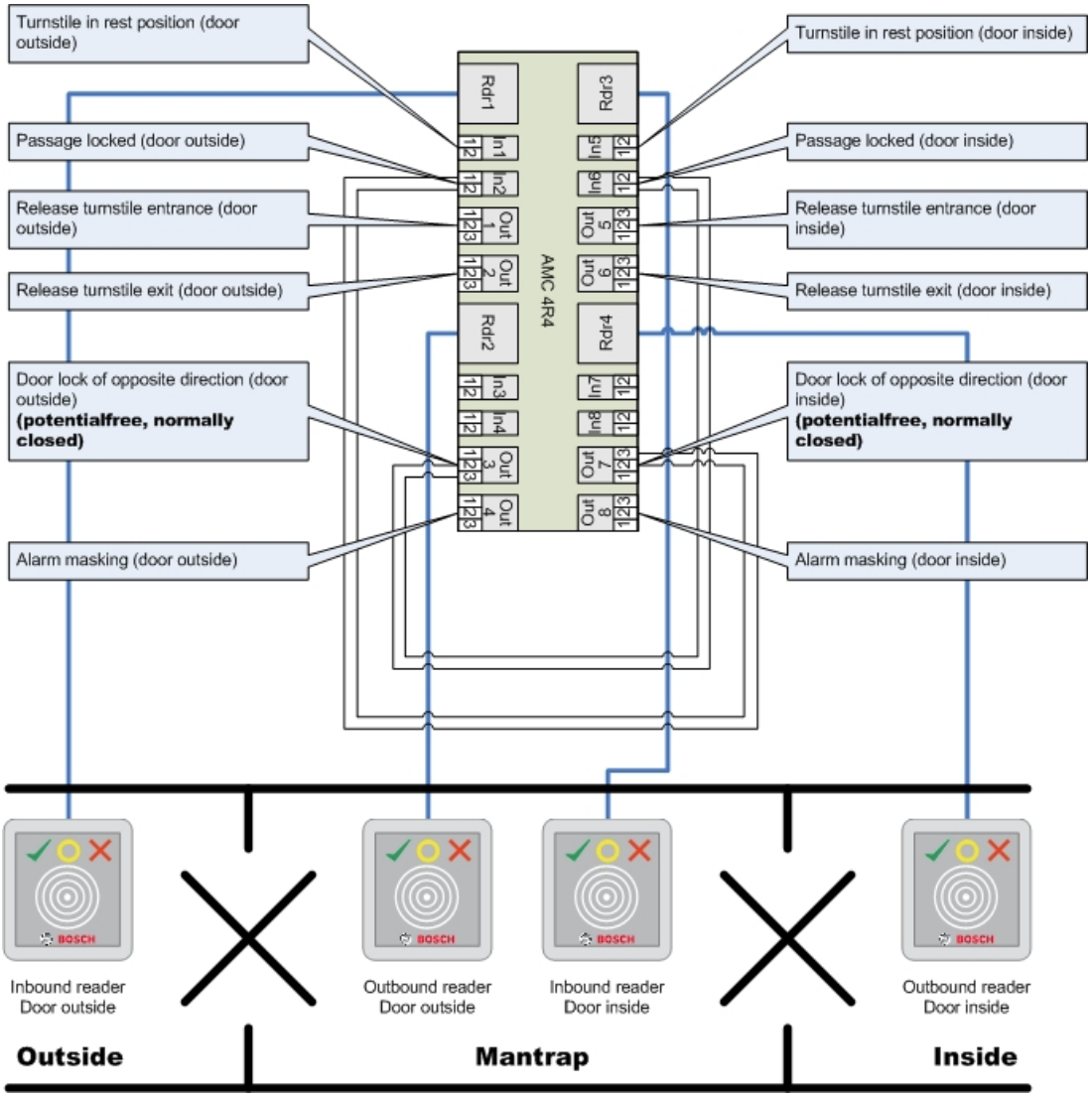
15.6.4 Modelos de porta de eclusa

Criação de uma eclusa
Os modelos de entrada 01 e 03 podem ser usados como "eclusas" para permitir o acesso de um titular de cartão por vez. Use a caixa de seleção **Mantrap option (Opção de eclusa)** para disponibilizar os sinais adicionais necessários.



Você pode combinar todos os tipos dos modelos 01 e 03, porém definir essa opção em ambas as entradas pertencentes à eclusa.
Junto com as atribuições de sinais usuais para o modelo de porta, a opção de eclusa requer atribuições adicionais próprias.

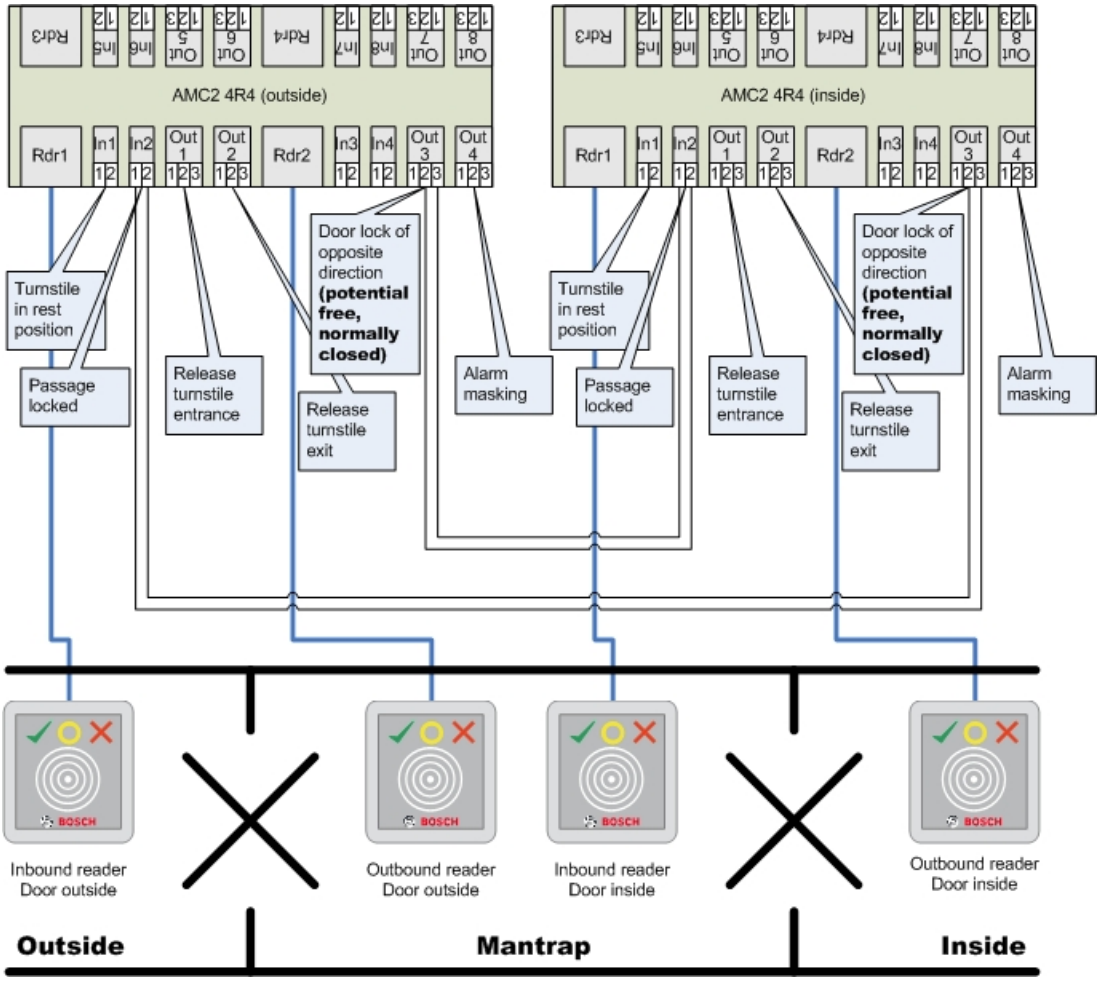
Exemplo: eclusa em um controlador
As catracas são os dispositivos mais comuns para permitir o acesso de um titular de cartão por vez. Assim, utilizamos nos seguintes exemplos o modelo de porta 3a (catraca com leitor de entrada e saída).
Configuração de eclusa com duas catracas (DM 03a):



As conexões aos bloqueios da porta para o sentido oposto asseguram que apenas uma das catracas possa ser aberta por vez.

Aviso!
Os sinais de saída (Out) 3 e 7 devem ser definidos sem potencial (modo seco)
O sinal "bloqueio da porta do sentido oposto" está ativo em 0. Deve ser usado para as saídas 3 e 7 "normalmente fechadas".

Exemplo: eclusa em dois controladores
Configuração de eclusa com duas catracas (DM 03a) distribuídas em dois controladores:



As conexões aos bloqueios da porta para o sentido oposto asseguram que apenas uma das catracas possa ser aberta por vez.

Aviso!
O sinal de saída (Out) 3 deve ser definido sem potencial (modo seco)
O sinal "bloqueio da porta do sentido oposto" está ativo em 0. Deve ser usado para a saída 3 "normalmente fechada".

15.7 Portas

Guia: Porta

Parâmetro	Valores possíveis	Descrição
Nome	Alfanumérico, até 16 caracteres	O valor padrão gerado pode ser substituído por um nome exclusivo (opcional).
Descrição	Alfanumérico, até 255 caracteres	
Divisão	A divisão padrão é "Comum"	Relevante somente se o recurso **Divisões** for licenciado.
Somente para os modelos de porta 01 e 03 se uma área de inspeção estiver configurada:		

Opção de área de inspeção	0 = desativado (a caixa de seleção está desmarcada) 1 = ativado (a caixa de seleção está marcada)	Existe uma área de inspeção onde duas portas combinadas usam o modelo de porta 01 ou 03. Ative a opção de área de inspeção para as **duas** portas. As portas também precisarão de fiação física especial.

Guia: Opções

Parâmetro	**Valores possíveis**	**Observações**
Gerar mensagem para aberto/fechado	0 = caixa de seleção desmarcada 1 = caixa de seleção marcada.	0 = Nenhuma mensagem é gerada quando a porta é aberta (em um ângulo com o batente da porta) ou fechada (totalmente presa no batente da porta). 1 = as mensagens correspondentes são geradas no registro de eventos.
Porta definida como manual	0 = caixa de seleção desmarcada 1 = caixa de seleção marcada.	0 = a porta está no modo normal (padrão, isto é, está sujeita ao controle de acesso realizado pelo sistema geral. 1 = a porta não faz parte do sistema de controle de acesso. A porta não é controlada e não gera mensagens. Só pode ser trancada ou destrancada manualmente. Todos os outros parâmetros dessa porta estão desligados. Esse parâmetro deve ser definido a porta e para o leitor separadamente.
Modo da porta	0 = porta está no modo normal 1 = porta está destravada 2 = porta é destravada dependendo do modelo de tempo 3 = porta é aberta dependendo do modelo de tempo após primeira passagem 5 = porta é bloqueada por muito tempo 6 = porta é bloqueada dependendo do modelo de tempo	0 = modo normal (padrão), a porta será trancada ou destrancada dependendo dos direitos de acesso das credenciais. 1 = destravar durante período estendido, o controle de acesso é suspenso durante o período. 2 = destravar durante um período definido pelo modelo de tempo. O controle de acesso é suspenso durante o período. 3 = travada a partir da ativação do modelo de tempo até a primeira pessoa obter acesso, depois aberta enquanto o modelo estiver ativo. 5 = bloqueada (excluída do sistema de controle de acesso) até ser desbloqueada manualmente. 6 = bloqueada (excluída do sistema de controle de acesso), desde que o modelo de tempo esteja ativado; não há controle da porta, e ela não poderá ser usada enquanto o modelo de tempo estiver ativo.

Time model (Modelo de tempo)	um dos modelos de tempo disponíveis	Modelo de tempo para os horários de abertura da porta. Se os modos de porta 2, 3, 4, 6 e 7 forem selecionados, a caixa de listagem dos modelos de tempo estará disponível. A seleção de um modelo de tempo é obrigatória.
Duração máxima do pulso para acionamento da porta:	0 - 9999	Duração máxima do sinal de desbloqueio. Unidade: décimos de segundo. Valores padrão: 50 para portas, 10 para portas giratórias (modelo de porta 03) e 200 para barreiras (modelos de porta 05c ou 09c).
Duração mínima do pulso para acionamento da porta:	0 - 9999	Duração mínima do sinal de desbloqueio em décimos de segundo. Padrão: 10.
Supressão de alarme prefixado	0 - 9999	Supressão adicional de alarme **antes** do pulso para acionamento da porta. (`$PARAMETER_WAITEMA`) Em casos muito raros em que um acionamento de porta pode reagir mais lentamente do que um alarme de intrusão, é possível suprimir o alarme temporariamente antes de enviar o sinal de desbloqueio para a porta. Unidade: décimos de segundo. Padrão 0. Um valor de 20, que equivale a 2 segundos, normalmente é suficiente até mesmo para portas muito lentas.
Supressão de alarme sufixado	0 - 9999	Supressão adicional de alarme **depois** do pulso para acionamento da porta. (`$PARAMETER_OPENINRT`) Depois que o pulso para acionamento da porta (o sinal de desbloqueio) tiver passado, a porta poderá ser aberta dentro desse tempo, sem disparar um alarme. Unidade: décimos de segundo. Padrão: 0.
Door strike mode (Modo de funcionamento porta)	Entrada da caixa de lista	0 = botão REX (solicitação de saída) é desabilitado após o tempo de ativação 1 = botão REX (solicitação de saída) é habilitado imediatamente (= padrão)
O sensor de batente da porta está presente	0 = desativado (a caixa de seleção está desmarcada)	0 = porta sem contato da estrutura

	1 = ativado (a caixa de seleção está marcada)	1 = porta tem um contato da estrutura. Um contato fechado normalmente significa que a porta está fechada. (= padrão)
O sensor de trava da fechadura está presente	0 = desativado (a caixa de seleção está desmarcada) 1 = ativado (a caixa de seleção está marcada)	0 (padrão) = a porta não tem sensor de trava da fechadura 1 = a porta tem um sensor de trava da fechadura. Uma mensagem é emitida quando a porta é travada ou destravada.
Extended door open time (Tempo estendido de abertura da porta) (pessoas com deficiência)	0 = desativado (a caixa de seleção está desmarcada) 1 = ativado (a caixa de seleção está marcada)	0 = o sinal de desbloqueio tem a duração padrão, que é definida no parâmetro “Tempo máximo de ativação de trava” da **porta**, ou seja, a duração do pulso para acionamento da porta. 1 (padrão) = a duração do sinal de desbloqueio é multiplicada pelo fator definido no parâmetro “**Fator de tempo para pessoas com deficiência**” do **MAC** (guia: **Configurações de acesso global**). Um valor de 0 nesse parâmetro do MAC coloca tempos estendidos de abertura da porta fora de operação.

Guia: Segurança da porta

Parâmetro	**Valores possíveis**	**Observações**
Gerar mensagem para “Abertura forçada da porta”	0 = desativado (a caixa de seleção está desmarcada) 1 = ativado (a caixa de seleção está marcada)	0 = sem mensagem de intrusão. Isso é útil se uma porta puder ser aberta livremente pelo lado de dentro. 1 = (padrão) Após a abertura não autorizada, uma mensagem será emitida, seguida de outra mensagem quando a porta se fechar.
Gerar mensagem para “Porta mantida aberta” depois de:	0 - 9999	Se a porta ficar aberta após esse horário, uma mensagem será emitida para avisar que a porta permaneceu aberta por muito tempo. Unidade: décimos de segundo. Padrão: 300. 0 = Sem tempo limite, sem mensagem.
Extensão da supressão de alarme para “Abertura forçada da porta”	0 - 9999	Usado no recurso “Espera REX”: Unidade: décimos de segundo. Padrão 0. Depois de um sinal REX de um detector de movimento, se a porta se fechar novamente dentro desse tempo, a mensagem `Unauthorized opening of door N` usual será substituída pela mensagem: `Door N opened (in alarm suppression mode)` onde N é o número da porta.

Gerar alarme local para “Abertura forçada da porta”	0 = desativado (a caixa de seleção está desmarcada) 1 = ativado (a caixa de seleção está marcada)	Pré-requisito: a caixa de seleção **Gerar mensagem para “Abertura forçada da porta”** nesta caixa de diálogo é marcada (veja acima). 0 = (padrão) os leitores conectados a esta porta não emitem um alarme local. 1 = os leitores conectados a esta porta emitirão um alarme local se a porta for forçada a abrir.
Gerar alarme local para “Porta mantida aberta” depois de:	0 - 9999	Se a porta ficar aberta após esse tempo, os leitores conectados a esta porta emitirão um alarme local. Unidade: décimos de segundo. 0 = (padrão) Sem alarme local.

15.7.1 Espera REX

Introdução

Nas entradas onde não há risco de segurança em abrir uma porta manualmente por dentro, um detector de movimento costuma tomar o lugar de um botão REX, para destrancar a porta. Para este cenário comum, o ACS fornece um meio simples de estender a duração do sinal REX do detector de movimento, ao mesmo tempo que aciona espera (suspensão) para o alarme `Door forced open` .

Este recurso é conhecido como “Espera REX”.

Quando o recurso estiver em operação, os titulares de cartão que saírem pela porta durante o período de espera gerarão o evento de acesso `Door N opened (in alarm suppression mode)` em vez do evento `Unauthorized opening of door N`.

Aviso!

Espera REX em combinação com sistemas de detector de intrusão armados

O recurso de espera REX suspende alarmes pela duração definida no parâmetro:

Editor de dispositivos > ... > **Porta** > guia: **Segurança da porta** > **Extensão da supressão de alarme para “Abertura forçada da porta”**

independentemente da porta estar atualmente armada como parte de um sistema de alarme de roubo.

Pré-requisitos

- Portas configuradas dos seguintes tipos: 01a, 01b, 01c, 03a, 03b, 03c, 10a, 10b, 10e, 14a, 14b
- A porta física é equipada com um detector de movimento, em vez de um botão REX, para destrancar a porta. Defina a duração do sinal do detector de movimento como pelo menos 1 segundo.

Caminho da caixa de diálogo

- **Main menu (Menu principal)** > **Configuration (Configuração)** > **Device data (Dados do dispositivo)**
- **Navegador de configuração do BIS** > **Connections (Conexões)** > **Device data (Dados do dispositivo)**

Procedimento

1. No editor de dispositivos, navegue até a entrada desejada (um nó filho direto de um controlador de porta).
2. Na guia **Terminais** da entrada, crie um sinal de entrada do tipo:
   `Suppress alarm from unauthorized opening`
3. Clique em  (Salvar) para salvar as alterações.
4. Selecione a porta que está dentro da entrada desejada
5. Na guia **Segurança da porta**, defina um valor para o parâmetro **Extensão da supressão de alarme para "Abertura forçada da porta"**

– O valor está em décimos de segundo.
– O valor padrão é `0`. Ou seja, por padrão, não há extensão da supressão do alarme depois que o titular do cartão deixa a área sensível do detector de movimento.

6. Clique em  (Salvar) para salvar as alterações.

15.7.2 Configuração das portas para emitir alarmes locais

Introdução

Para os seguintes estados de porta, o ACS fornece um meio de emitir os alarmes em todos os leitores conectados à porta.

Estado	Resposta de alarme local
Abertura forçada da porta	O alarme soa por 17 segundos ou até a porta se fechar.
Porta mantida aberta	O alarme soa até a porta se fechar.

Pré-requisitos

– Os leitores usam o protocolo OSDP ou Wiegand
– As campainhas de alarme estão presentes nos leitores e eletricamente conectadas ao controlador da porta.
– Versão do firmware do AMC 02.38 ou posterior.

Os seguintes tipos de leitor **não** são compatíveis:

– Leitores IDEMIA
– Leitores Suprema com protocolo Wiegand
– Leitores LBUS
– Leitores BG900

Caminho da caixa de diálogo

– **Main menu (Menu principal)** > **Configuration (Configuração)** > **Device data (Dados do dispositivo)**
– **Navegador de configuração do BIS** > **Connections (Conexões)** > **Device data (Dados do dispositivo)**

Procedimento para Abertura forçada da porta

1. Na árvore de dispositivos, selecione a porta que deseja configurar.
2. Na guia **Segurança da porta**, marque a caixa de seleção **Gerar mensagem para "Abertura forçada da porta"**

3. Marque a caixa de seleção **Gerar alarme local para “Abertura forçada da porta”**
   O valor padrão é `0` (a caixa de seleção está desmarcada). Isso significa que, por padrão, nenhum alarme local será emitido.
4. Clique em (Salvar) para salvar as alterações.

Procedimento para Porta mantida aberta

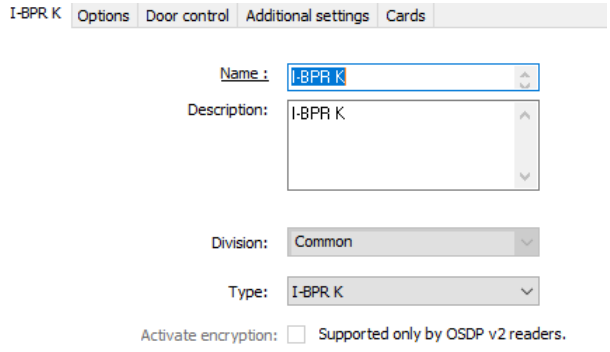
1. Na árvore de dispositivos, selecione a porta que deseja configurar.
2. Na guia **Segurança da porta**, defina um valor diferente de zero para **Gerar alarme local para “Porta mantida aberta” depois de:**

– O valor está em décimos de segundo.
– O valor padrão é `0`. Isso significa que, por padrão, nenhum alarme local será emitido.

3. Clique em (Salvar) para salvar as alterações.

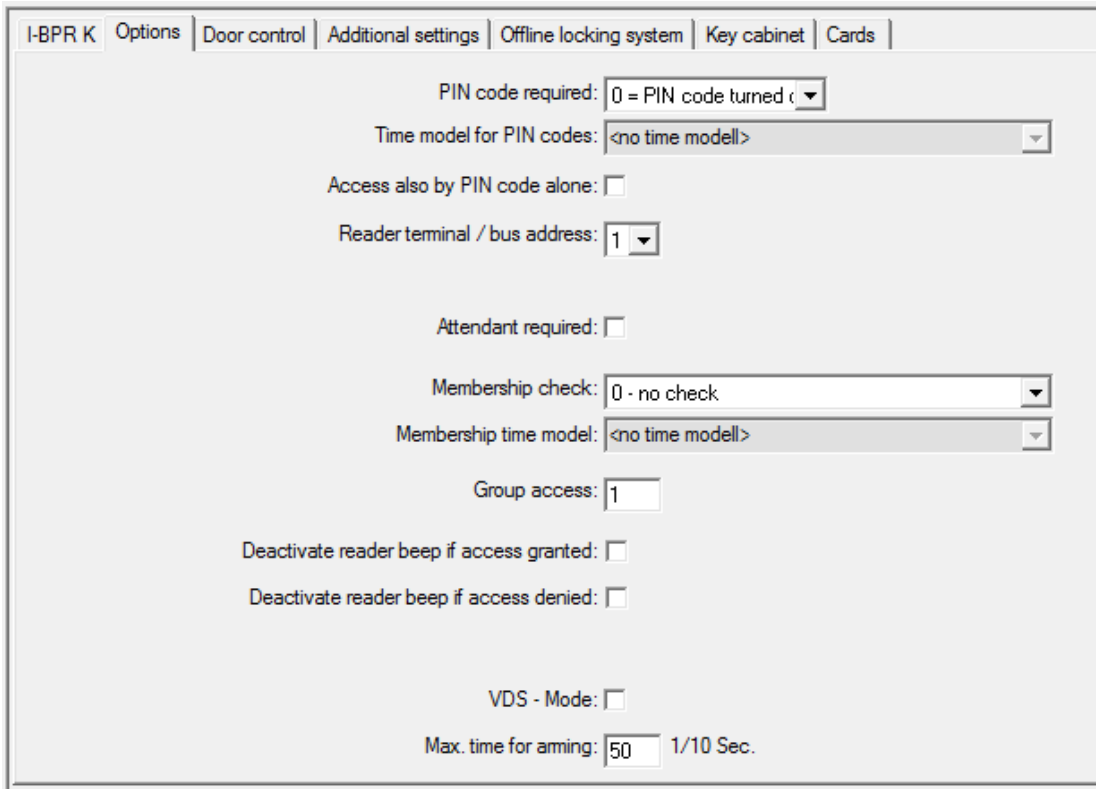
15.8 Leitores

Configuração de um leitor: parâmetros gerais



Parâmetro	Valores possíveis	Descrição
Reader name (Nome do leitor)	alfanumérico, restringido entre 1 e 16 caracteres	O valor padrão pode ser substituído por um nome exclusivo.
Reader description (Descrição do leitor)	alfanumérico: 0 a 255 caracteres	Uma descrição de texto livre.
Division (Divisão)	Divisão "Comum" padrão.	Somente as divisões relevantes estão licenciadas e em uso.
Type (Tipo)	alfanumérico, restringido entre 1 e 16 caracteres	Tipo de leitor ou grupo de leitores

Configuração de um leitor: opções



Parâmetro	Valores possíveis	Description (Descrição)
PIN code required (Código PIN obrigatório)	0 = código PIN desligado – nenhuma entrada é necessária (padrão) 1 = código PIN ligado – a entrada sempre é necessária 2 = código PIN controlado por modelo de tempo – entrada necessária somente se estiver fora do modelo de tempo	Este campo só está habilitado se o leitor tiver um dispositivo de entrada. Observe que as verificações no cartão, como suas autorizações e sequência de acesso (se habilitada), têm prioridade em relação à exatidão do PIN.
Time model for PIN codes (Modelo de tempo para códigos PIN)	um dos modelos de tempo disponíveis	A seleção de um modelo de tempo aqui é obrigatória se o parâmetro **PIN code required (Código PIN obrigatório)** estiver definido como 2.

Access also by PIN code alone (Acesso também só com código PIN)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	Determina se esse leitor também pode permitir o acesso apenas com base no PIN, ou seja, sem um cartão, se o sistema de controle de acesso estiver configurado dessa forma. Consulte
Reader terminal / bus address (Endereço do terminal/barramento do leitor)	1 - 4	Para AMC 4W: numerado correspondente às interfaces Wiegand. Para AMC 4R4: numerado como endereço jumpeado do leitor.
Attendant required (Atendedor necessário)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	0 = o visitante não precisa de atendedor (padrão) 1 = o atendedor também deve usar o leitor
Membership check (Verificação de associação)	List box entry (Entrada da caixa de listagem)	A verificação de associação geralmente é usada nas fases iniciais, antes que um sistema de controle de acesso entre em operação. Aqui, o acesso é concedido com base no ID de empresa genérico da credencial, em vez do ID pessoal único. **IMPORTANTE** A verificação de associação funciona apenas com credenciais físicas em que as definições de cartões estejam predefinidas no sistema (histórico cinza), **não** com definições personalizadas nem credenciais biométricas. **0 – sem verificação** A verificação de associação está desligada, mas o cartão é verificado quanto às autorizações normalmente (padrão) **1 – verificar** O cartão é verificado somente quanto ao ID de empresa, para a associação do sistema. **2 – dependente do modelo de tempo** O cartão é verificado quanto ao ID de empresa (associação), mas somente durante o período definido no modelo de tempo da associação.
Membership time model (Modelo de tempo da associação)	um dos modelos de tempo disponíveis	O modelo de tempo ativa/desativa a verificação de associação. A seleção de um modelo de tempo é obrigatória para a opção 2 da **Membership check (Verificação de associação)**.
Group access (Acesso de grupo)	1 - 10	**Para leitores com teclado:**

		O número mínimo de cartões válidos que devem ser apresentados ao leitor de cartões antes que a porta seja aberta. O grupo pode consistir de mais cartões que esse número. Nesse caso, a tecla ENTER/# é usada para sinalizar que o grupo está completo. Então, a porta é aberta. **Para leitores sem teclado:** O número exato de cartões válidos que devem ser apresentados ao leitor de cartões antes que a porta seja aberta. O valor padrão é 1.
Deactivate reader beep if access granted (Desativar bipe do leitor em caso de acesso concedido)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	Se ativado (1), o leitor permanece em silêncio se um usuário autorizado receber acesso.
Deactivate reader beep if access not granted (Desativar bipe do leitor em caso de acesso não concedido)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	Se ativado (1), o leitor permanecerá em silêncio quando um usuário não autorizado tiver o acesso negado.
 As funções "Desativar bipe do leitor" dependem do firmware do leitor. O firmware de alguns leitores pode não oferecer suporte à essa função.		
VDS mode (Modo VDS)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	Se ativada (1), a sinalização do leitor é desligada.
Max. time for arming (Tempo máx. para armar)	1 a 100 [1/s]	Tempo máximo para feedback do painel de intrusão sobre a conclusão do arme.

Rede e modos de operação

Esta guia só é exibida para leitores biométricos em rede.

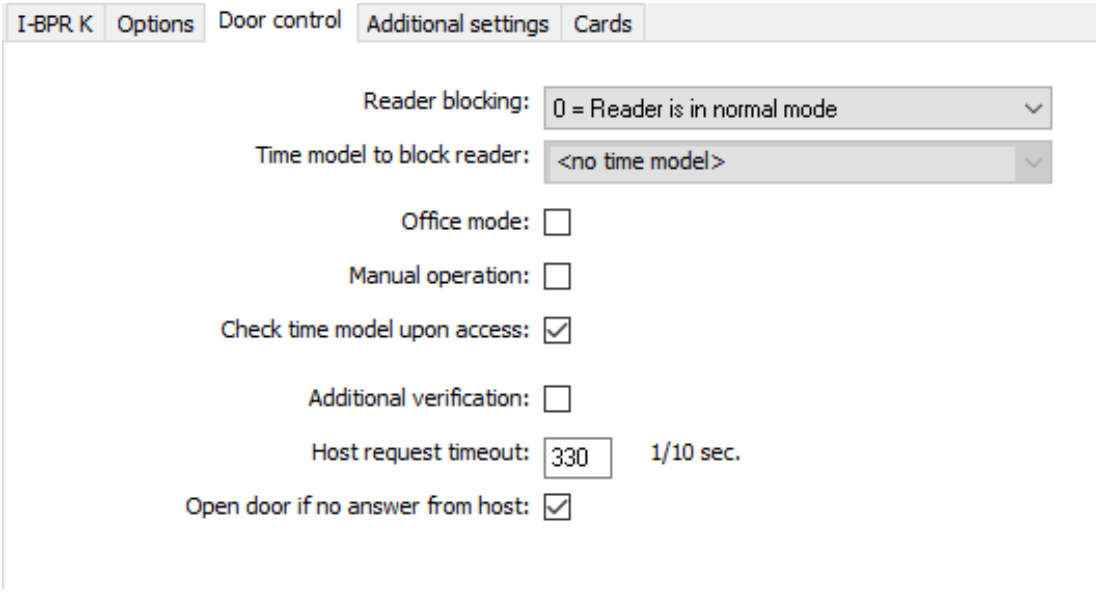
Modelos são padrões armazenados. Podem ser dados de cartão ou dados biométricos.

Os modelos podem ser armazenados em dispositivos acima do leitor na árvore de dispositivos e no próprio leitor. Os dados no leitor são atualizados periodicamente pelos dispositivos superiores.

O leitor pode ser configurado para usar seus próprios modelos ao tomar decisões de acesso ou somente para usar os modelos dos dispositivos acima dele.

Parâmetro	**Descrição**
IP address: (Endereço IP:)	O endereço IP deste leitor em rede
Port: (Porta:)	A porta padrão é `51211`
Templates on server (Modelos no servidor)	
Card only (Somente cartão)	O leitor lê apenas dados de cartão. Ele os autentica em relação aos dados do sistema geral.
Card and fingerprint (Cartão e impressão digital)	O leitor lê dados de cartão e dados de impressões digitais. Ele os autentica em relação aos dados do sistema geral.
Templates on device (Modelos no dispositivo)	
Person dependent verification (Verificação dependente da pessoa)	O leitor permite configurações do titular de cartão individual para determinar qual **Modo de identificação** será usado. Os dados de funcionários oferecem as seguintes opções: – Fingerprint only (Somente impressão digital) – Card only (Somente cartão) – Card and fingerprint (Cartão e impressão digital) Serão descritos posteriormente nesta tabela.
Fingerprint only (Somente impressão digital)	O leitor lê apenas dados de impressões digitais. Ele os autentica em relação aos seus próprios dados armazenados.
Card only (Somente cartão)	O leitor lê apenas dados de cartão. Ele os autentica em relação aos seus próprios dados armazenados.
Card and fingerprint (Cartão e impressão digital)	O leitor lê dados de cartão e dados de impressões digitais. Ele os autentica em relação aos seus próprios dados armazenados.
Card or fingerprint (Cartão ou impressão digital)	O leitor lê dados de cartão ou dados de impressões digitais, dependendo do que o titular de cartão fornecer primeiro. Ele os autentica em relação aos seus próprios dados armazenados.

Configuração de um leitor: controle de porta

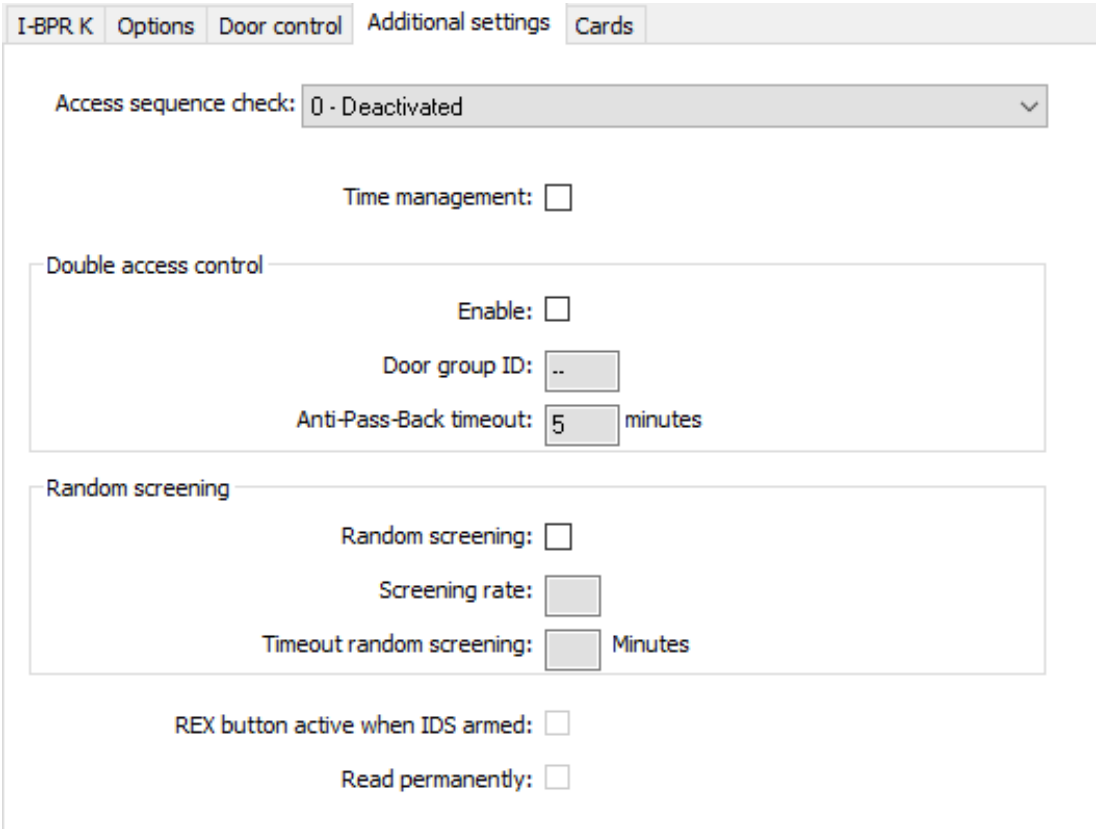


Parâmetro	Valores possíveis	Observações
Bloqueio do leitor	Entrada da caixa de lista	0 = Leitor no modo normal - sem bloqueio (= padrão) 1 = O leitor está bloqueado permanentemente - bloqueio permanente 2 = O leitor é bloqueado dependendo do modelo de tempo - bloqueio de acordo com o modelo de tempo definido com Modelo de tempo para bloquear leitor
Modelo de tempo para bloquear leitor	um dos modelos de tempo definidos no sistema.	Bloqueia o leitor de acordo com o modelo de tempo selecionado.
Modo de escritório	0 = desativado (a caixa de seleção está desmarcada) 1 = ativado (a caixa de seleção está marcada)	Permite que este leitor defina uma entrada como Modo escritório. O leitor deve ter um teclado. Quando esse parâmetro é ativado, um titular de cartão devidamente autorizado ativa e desativa o Modo escritório pressionando a tecla 3 antes de apresentar seu cartão. Consulte *Autorizar pessoas a ativarem o modo Escritório, página 204*
Operação manual	0 = desativado (a caixa de seleção está desmarcada) 1 = ativado (a caixa de seleção está marcada)	0 = leitor no modo normal (= padrão) 1 = o leitor foi removido do sistema de controle de acesso, ou seja, está "fora de serviço".

		Nenhum comando é recebido. Todos os outros parâmetros desse leitor são desativados. O parâmetro deve ser definido independentemente para o leitor e a porta.
Verificar modelos de tempo após acesso	0 = desativado (a caixa de seleção está desmarcada) 1 = ativado (a caixa de seleção está marcada)	0 = Os modelos de tempo não serão verificados. Não há restrição de tempo para acesso. 1 = Se o titular do cartão tiver um modelo de tempo atribuído, diretamente ou como uma autorização de área/tempo, o modelo de tempo será verificado. (= padrão)
Verificação adicional	0 = desativado (a caixa de seleção está desmarcada) 1 = ativado (a caixa de seleção está marcada)	0 = a verificação do host não é necessária 1 = a verificação do host é necessária (padrão) **IMPORTANTE**: a ativação dessa opção é necessária para verificação de vídeo adicional pelo operador de um Bosch BVMS ou sistema de controle de acesso da Bosch.
Tempo limite de solicitação do host	0 = desativado	0 = o AMC funciona sem verificação do host (não funciona com Alteração de área ou Contagem de pessoas). Esse controle só estará ativo se a verificação do host estiver desativada (0) e Abrir porta se não houver resposta do host estiver ativado (1) 1 a 9999 x 1/10 de um segundo. (Padrão = 330 =33 segundos). O leitor solicita a confirmação do sistema de controle de acesso. Se a confirmação não for recebida nesse tempo, o AMC marcará o parâmetro **Abrir porta se não houver resposta do host** e concederá ou negará o acesso conforme necessário.
Abrir porta se não houver resposta do host	0 = desativado (a caixa de seleção está desmarcada) 1 = ativado (padrão) (a caixa de seleção está marcada)	Esse controle só estará ativo se o parâmetro **Verificação do host** estiver definido. 0 = não abrirá a porta se o sistema do host não confirmar antes do tempo limite. 1 (padrão) = abrirá a porta depois do tempo limite se o sistema do host não confirmar antes do tempo limite.
Verificar créditos de ticket de estacionamento	0 = desativado (a caixa de seleção está desmarcada)	Se ativado (1), os créditos de ticket de estacionamento serão verificados.

	1 = ativado (a caixa de seleção está marcada)	
Verificar permanência prolongada no estacionamento	0 = desativado (a caixa de seleção está desmarcada) 1 = ativado (a caixa de seleção está marcada)	Se ativado (1), será verificado se o período de estacionamento foi muito longo.

Configuração de um leitor: configurações adicionais

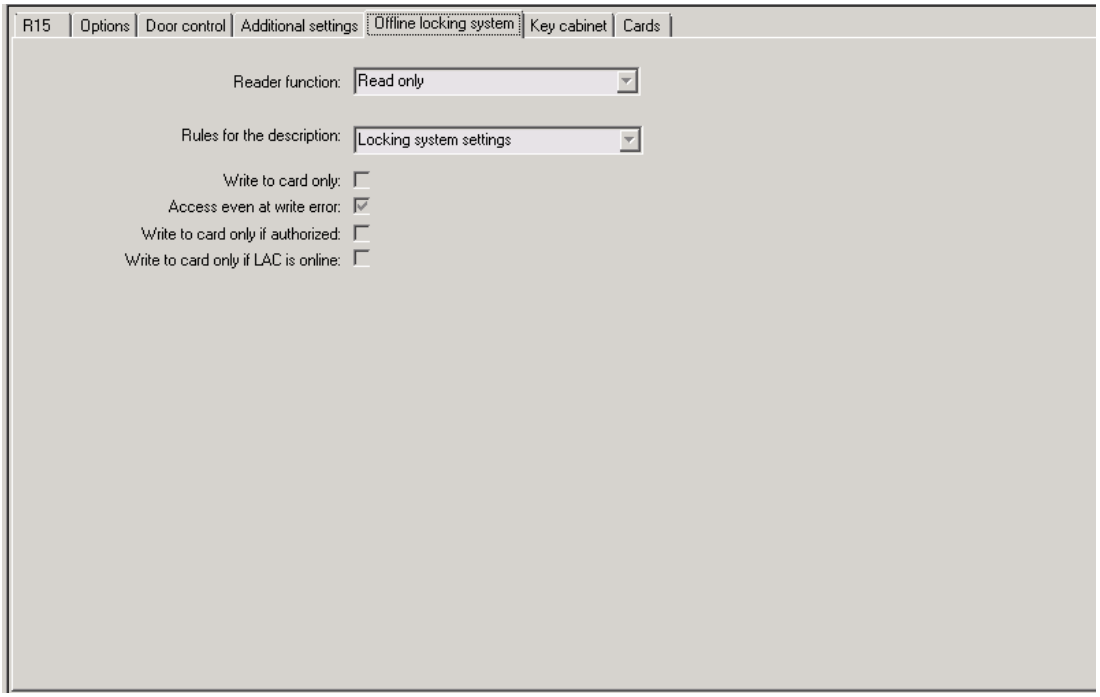


Parâmetro	Valores possíveis	Observações
Verificação da sequência de acesso	0 - Desativado 1 - Ativado; desativar após falha de LAC 2 - Ativado; deixar ativo após falha de LAC 3 - Ativada; use a verificação de sequência rígida mesmo quando o LAC	0 = o leitor não participa da verificação da sequência de acesso (= padrão) Uma verificação de sequência ativada pode manipular pessoas DESCONHECIDAS das seguintes maneiras: 1 = A primeira leitura do cartão não será feita sem a verificação do local. Todos os controladores devem estar on-line. 2 = A primeira leitura do cartão não será feita sem a verificação do local. 3 = A verificação do local não será feita para cada leitura do cartão durante a falha de LAC.

	falhar (observação: atualize o local da pessoa manualmente)	
 Há um comando do MAC para ativar ou desativar todas as verificações de sequência de acesso em geral. Para desativar a verificação da sequência de acesso por um período, um valor é fornecido em minutos com, no máximo, 2880 (= 48 horas). Definir o valor como "0" desativa a verificação da sequência de acesso por completo. **Observação:** esse comando pode modificar a verificação da sequência de acesso somente para os leitores com o parâmetro **Ativar sequência de acesso** definido. Isso não desativa/ativa a verificação da sequência de acesso de todos os leitores.		
Controle de tempo	0 = desativado (a caixa de seleção está desmarcada) 1 = ativado (a caixa de seleção está marcada)	Se selecionado, o sistema de controle de acesso coletará dados para gerenciamento de tempo e participação.
Controle de acesso duplo (controle contra entrada)		
Ativar	0 = desativado (a caixa de seleção está desmarcada) 1 = ativado (a caixa de seleção está marcada)	0 = sem controle de acesso duplo (= padrão) 1 = com controle de acesso duplo Dentro do período definido pelo parâmetro **Duração**, esse leitor e outros leitores do grupo não poderão ser usados com o mesmo cartão. Se esse parâmetro estiver ativado, um ID do grupo de portas deverá ser usado, mesmo que somente um leitor seja usado.
ID do grupo de portas	Letras A - Z e a - z, e "-" 2 caracteres	Os leitores podem ser agrupados com um ID do grupo de portas. A apresentação de um cartão em um leitor bloqueará as próximas reservas em todos os leitores do grupo de portas (Padrão = **--**) até o tempo acabar.
Tempo limite contra entrada	1 - 120	O leitor pode ser usado com o mesmo cartão depois que o tempo acabar. Assim que o cartão for usado em um leitor fora do grupo, o bloqueio será removido imediatamente. Os valores são em minutos - padrão = 5.

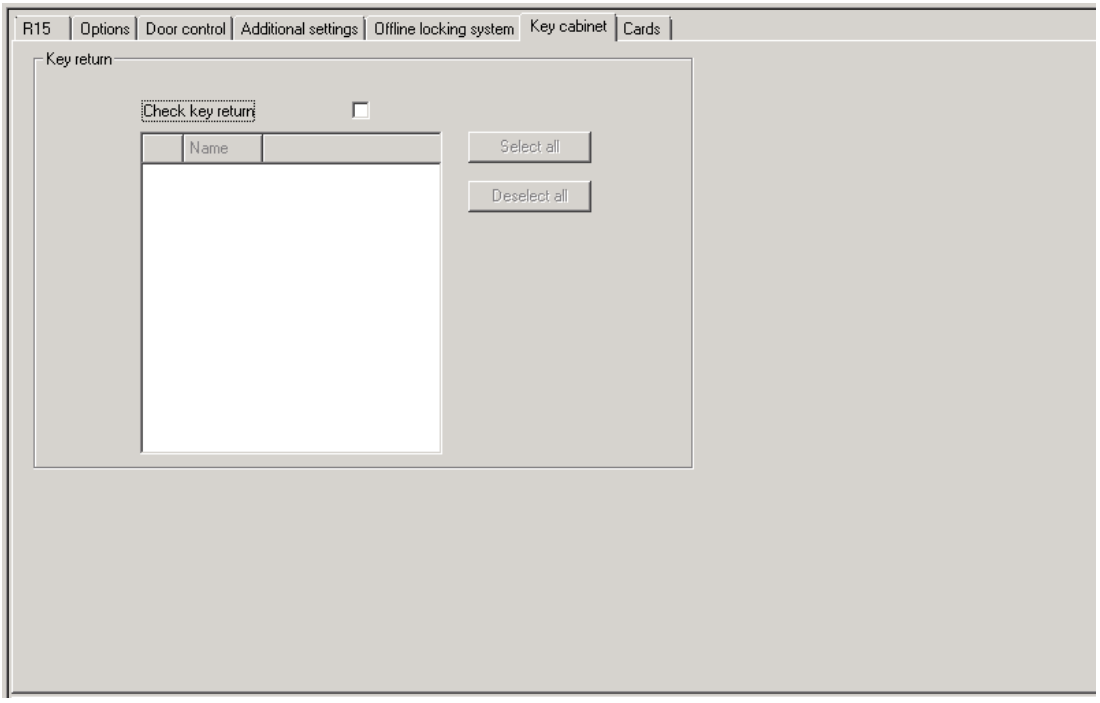
Revista aleatória	0 = desativado (a caixa de seleção está desmarcada) 1 = ativado (a caixa de seleção está marcada)	0 = sem revista aleatória 1 = a revista aleatória de acordo com o fator não será aceita até ser desbloqueada pela caixa de diálogo **Bloqueio**.
Taxa de revista	1 - 100	Porcentagem de revista aleatória para uma verificação estendida. Disponível se a revista aleatória estivar ativada.
Tempo limite da revista aleatória	1 - 120	Dentro do tempo definido, o usuário é submetido à revista aleatória. Os valores são em minutos - padrão = 5.
Botão REX ativado quando IDS é armado	0 = desativado (a caixa de seleção está desmarcada) 1 = ativado (a caixa de seleção está marcada)	Somente para **DM10** e **DM14**: os botões REX são desativados, por padrão, quando o IDS é armado. Isso impossibilitaria a saída da área monitorada. Esse novo parâmetro do leitor ativa o botão REX mesmo quando o IDS é armado.
Ler permanentemente	0 = desativado (a caixa de seleção está desmarcada) 1 = ativado (a caixa de seleção está marcada)	A leitura será permanente se o leitor tiver o respectivo firmware do fabricante.

Configuração de um leitor: sistema de bloqueio offline



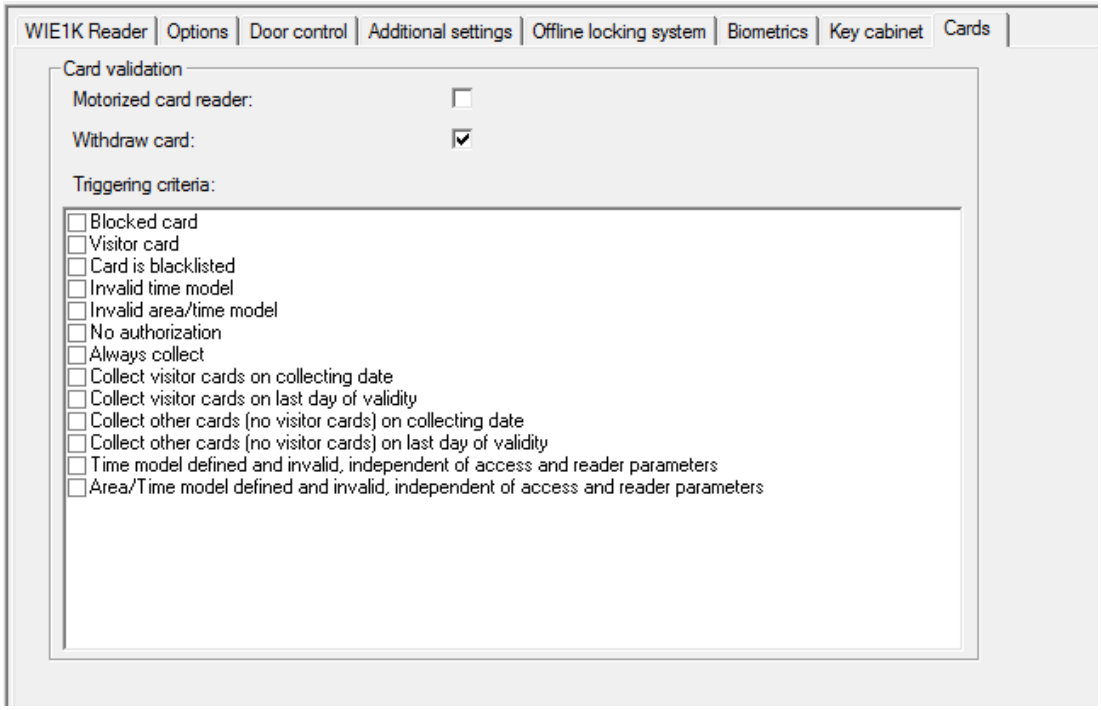
Parâmetro	Valores possíveis	Observações
Reader function (Função do leitor)		Esta caixa deve ser marcada se um leitor de cartões motorizado for usado
Regras para a descrição		"Retirar" significa tornar o cartão inválido.
Write to card only (Gravar somente no cartão)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	
Access even on write error (Acessar mesmo em caso de erro de gravação)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	
Write to card only if authorized (Gravar somente no cartão se autorizado)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	
Write to card only if LAC is online (Gravar somente no cartão se o LAC estiver online)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	

Configuração de um leitor: armário de chaves



Parâmetro	Valores possíveis	Observações
Check key return (Verificar devolução de chave)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	Instrui o sistema de controle de acesso a garantir que uma chave for devolvida a um armário de chaves Kemas antes de permitir que o portador da chave deixe o local.

Configuração de um leitor: cartões



Parâmetro	Valores possíveis	Observações
Motorized card reader (Leitor de cartões motorizado)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	Marque essa caixa de seleção se um leitor de cartões motorizado for usado
Withdraw card (Retirar cartão)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	No caso de um leitor de cartões motorizado, Retirar significa reter fisicamente o cartão. No caso de outros leitores de cartões, Retirar significa que o sistema torna o cartão inválido.
Triggering criteria (Critérios de acionamento)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	Selecione nessa lista qualquer critério que deve acionar a ação **Retirar cartão**.

Aviso!
Leitores de cartões motorizados só podem ser usados com leitores IBPR.

Consulte

– *Autorizar pessoas a ativarem o modo Escritório, página 204*

15.8.1 Configuração da triagem aleatória

A triagem aleatória é um método comum para aprimorar a segurança do local selecionando os funcionários aleatoriamente para verificações de segurança adicionais.

Pré-requisitos:

– A entrada deve ser do tipo eclusa ou catraca para impedir que uma pessoa entre junto com outra, "a reboque", sem exibir sua própria identificação.
– Um leitor de cartões deve estar presente em pelo menos um dos sentidos de passagem.
– Os leitores devem ser configurados para o controle de acesso normal.
– A seleção aleatória pode ser configurada separadamente para cada leitor.
– Deve haver uma estação de trabalho nas proximidades para liberar quaisquer bloqueios feitos pelo sistema.

Procedimento

1. Localize o leitor desejado no editor de dispositivos DevEdit
2. Na guia **Settings (Configurações)**, marque a caixa de seleção **Random screening (Triagem aleatória)**.
3. Na caixa **Screening percentage (Percentual de triagem)**, digite a porcentagem de pessoas a serem triadas.
4. Salve suas configurações.

15.9 Acesso apenas com código PIN

Plano de fundo

Os leitores de teclado podem ser configurados para permitir o acesso somente por PIN. Quando os leitores também são configurados, o operador de controle de acesso pode atribuir PINs individuais ao pessoal selecionado. Na verdade, esse pessoal recebe um "cartão virtual" que consiste apenas em um PIN. É chamado de PIN de identificação. Por outro lado, um PIN de verificação é um PIN usado em combinação com um cartão para impor maior segurança.

O operador pode inserir PINs de pessoal manualmente ou atribuir PINs gerados pelo sistema. O mesmo pessoal pode continuar acessando com qualquer cartão físico que também tenha sido atribuído.

Pré-requisito de autorização para operadores

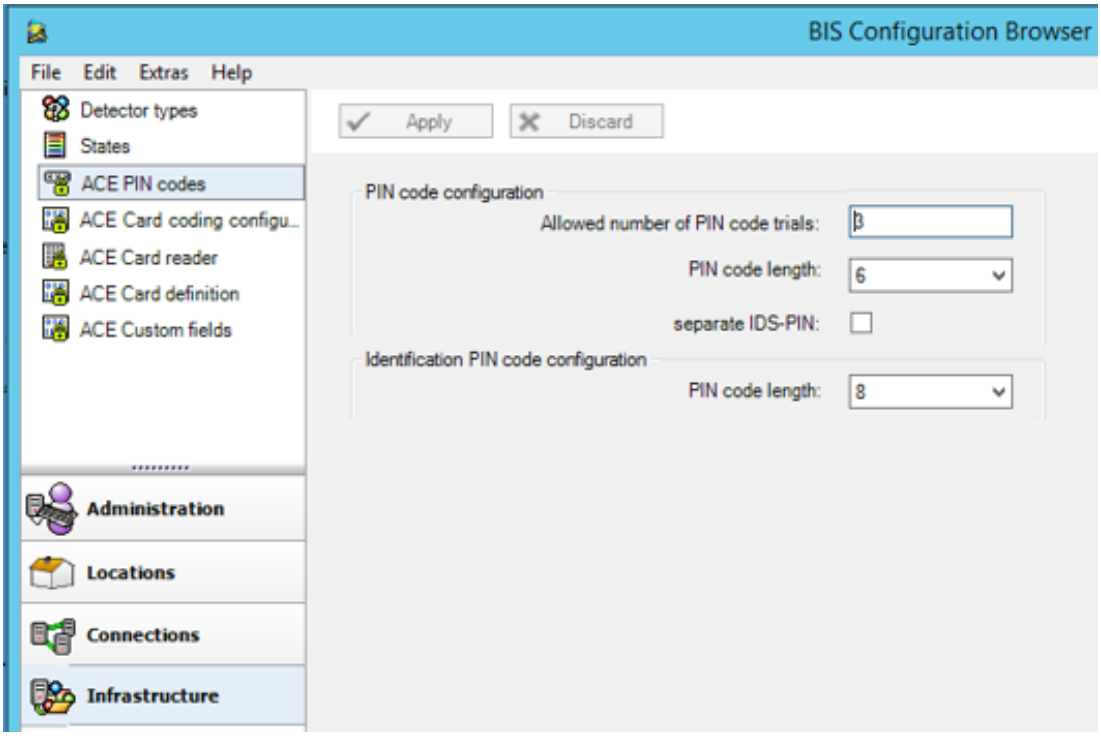
A autorização para um titular de cartão acessar apenas com código PIN só pode ser concedida por operadores com autorização especial para atribuir cartões virtuais. Para conceder essa autorização a um operador, faça o seguinte.

1. No Navegador de configuração do BIS, navegue até **Administration (Administração) > ACE User profiles (Perfis de usuário do ACE)**
2. Navegue até o Main menu (Menu principal) > **Configuration (Configuração)** > **Operators and workstations (Operadores e estações de trabalho)** > **User profiles (Perfis de usuário)**
3. Selecione o Perfil de usuário que deve receber a autorização:
   Insira-o no campo de texto **Profile name (Nome do perfil)** ou use a instalação de busca para encontrar o perfil desejado.

4. Na lista de caixas de diálogo, clique na célula que contém **Cards (Cartões)**
   Uma janela pop-up chamada **Special functions (Funções especiais)** aparece próximo da parte inferior do painel da janela principal.
5. No painel de Funções especiais, marque a caixa de seleção **Assign virtual cards (PIN) (Atribuir cartões virtuais (PIN))**
6. Clique em ou **Apply (Aplicar)** para salvar as alterações

Definição do comprimento do PIN de identificação para os tipos de leitores compatíveis
O comprimento de PINs inseridos manualmente ou gerados pelo sistema é governado pelo parâmetro definido na configuração do sistema.

– Caixa de diálogo do Navegador de configuração do BIS
  Infrastructure (Infraestrutura) > **ACE PIN Codes (Códigos PIN do ACE)** > (o painel da caixa de diálogo inferior) **Identification PIN code configuration (Configuração do código PIN de identificação)** > **PIN code length (Comprimento do código PIN)**
– Main menu (Menu principal) > **Configuration (Configuração)** > **Options (Opções)** > **PIN codes (Códigos PIN)** > **PIN code length (Comprimento do código PIN)**



Configuração de um leitor para acesso apenas com código PIN

1. No Navegador de configuração do BIS, navegue até **Infrastructure (Infraestrutura)** > **ACE Card reader (Leitor de cartões do ACE)**.
2. Navegue até o Main menu (Menu principal) > **Configuration (Configuração)** > **Device data (Dados do dispositivo)** > árvore **Workstations (Estações de trabalho)**
3. No painel **Workstation (Estação de trabalho)**, selecione a estação de trabalho à qual o leitor está fisicamente conectado.

4. Clique com o botão direito na estação de trabalho e adicione um leitor do tipo **Dialog Enter PIN (Caixa de diálogo Inserir PIN)** ou **Dialog Generate PIN (Caixa de diálogo Gerar PIN)**.
5. Selecione o leitor no painel **Workstations (Estações de trabalho)**.
   Um painel de configuração de leitor personalizado é exibido à direita do painel **Workstations (Estações de trabalho)**.
6. Verifique se a lista suspensa **Card usage default (Utilização do cartão predefinida)** contém o valor padrão **Virtual card (Cartão virtual). Usar PIN como cartão**.
7. Clique em  ou **Apply (Aplicar)** para salvar as alterações
8. No Navegador de configuração do BIS, navegue até **Connections (Conexões)**.
9. No editor de dispositivos DevEdit, navegue até a árvore **Device configuration (Configuração do dispositivo)** 
10. Selecione o leitor na entrada em que deseja configurar o acesso apenas com código PIN.
11. Na guia **Options (Opções)**, marque a caixa de seleção **Access also by PIN code alone (Acesso também só com código PIN)**.
12. Clique em  ou **Apply (Aplicar)** para salvar as alterações

15.10 Placas de extensão do AMC

Criação de um AMC-I/O-EXT (Placa de extensão de E/S)

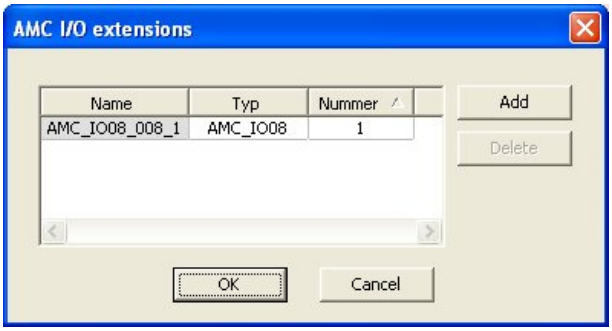
As placas de extensão fornecem sinais de entrada e saída adicionais, caso os oito contatos localizados no AMC não forem suficientes para a conexão dos contatos necessários (por exemplo, com elevadores).

Essas extensões são conectadas fisicamente ao AMC associado e podem ser instaladas apenas abaixo dos AMCs respectivos no Editor de dispositivos. A entrada do AMC correspondente é selecionada no explorador para a criação de um AMC-EXT e a entrada **New Extension Board (Nova placa de extensão)** é escolhida no menu de contexto **New Object (Novo objeto)**.

Aviso!

Clicar no botão **+**  na barra de ferramentas do Editor de dispositivos cria apenas novas entradas. As placas de extensão podem ser selecionadas usando o menu de contexto.

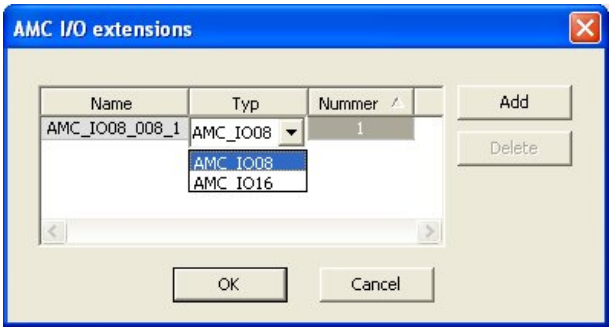
Uma caixa de diálogo de seleção para a criação das extensões aparece.



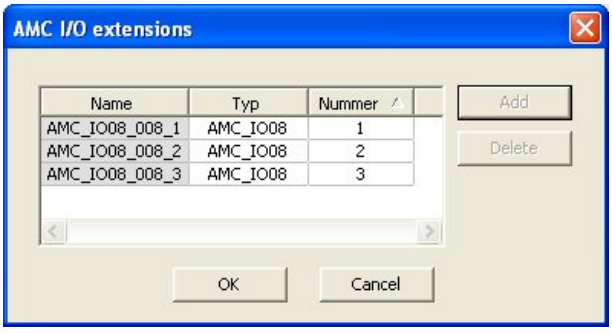
AMC-EXT está disponível em duas variantes:

- AMC_IO08: com 8 entradas e 8 saídas
- AMC_IO16: com 16 entradas e 16 saídas
- Extensão AMC_4W: com 8 entradas e 8 saídas

A caixa de diálogo de seleção contém uma entrada com um AMC_IO08. Ao clicar duas vezes na caixa de listagem na coluna **Type (Tipo)**, você também pode colocar um AMC_IO16.



Conecte até três extensões a um AMC. É possível misturar as duas variantes. Clique em **Add (Adicionar)** para criar mais entradas da lista. Todas as entradas da coluna podem ser personalizadas.



As placas de extensão são numeradas 1, 2 ou 3 conforme são criadas. A numeração dos sinais começa, para cada placa, em 01. O número do sinal, combinado com o número da placa, fornece uma identificação única. Os sinais das placas de extensão também podem ser vistos na guia do AMC ao qual eles pertencem.
Junto com os sinais de entrada e saída no AMC, até 56 pares de sinais podem ser fornecidos. Placas de extensão podem ser adicionadas individualmente, conforme necessário, ou posteriormente até o número máximo (três por AMC).

Criação de um AMC2 4W-EXT

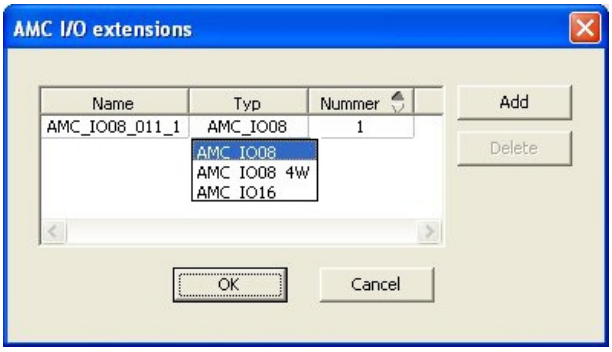
É possível configurar placas de extensão especiais (AMC2 4W-EXT) para controladores com interfaces de leitor Wiegand (AMC2 4W). Esse módulos oferecem quatro conexões de leitor Wiegand adicionais, além de oito contatos de entrada e oito de saída cada. Logo, o número máximo de leitores e portas conectáveis por AMC2 4W pode ser dobrado para oito.

Aviso!
O AMC2 4W-EXT não pode ser usado como um controlador autônomo, apenas como uma extensão ao AMC2-4W. As portas são controladas e as decisões do controle de acesso são feitas somente pelo AMC2 4W.

O AMC2 4W-EXT só pode ser usado conectado a um AMC2 4W. Como ele só tem interfaces de leitor Wiegand, não pode ser utilizado com a variante AMC2 4R4 do AMC.
Como as placas de extensão de E/S (AMC2 8I-8O-EXT e AMC2 16I-16O-EXT), o AMC2 4W-EXT é conectado por meio da interface de extensão do AMC2 4W. A placa de extensão não tem memória ou visor próprios, mas é totalmente controlada pelo AMC2 4W.
Um AMC2 4W-EXT e um máximo de três extensões de E/S podem ser conectados a cada AMC2-4W.
Para criar um AMC2 4W-EXT no sistema, clique com o botão direito no AMC2 4W pai desejado no Explorador e selecione **New object (Novo objeto)** > **New extension board (Nova placa de extensão)** no menu de contexto.

Aviso!
O botão ✚ na barra de ferramentas do Editor de dados do dispositivo só pode ser usado para adição de entradas. As placas de extensão só podem ser adicionadas por meio do menu de contexto.

A mesma caixa de diálogo de seleção para criação de extensões de E/S é exibida, exceto que a lista para um AMC2 4W contém o elemento adicional AMC_IO08_4W.



A entrada de lista AMC2 4W só pode ser adicionada uma vez, enquanto até três extensões de E/S podem ser adicionadas.
O botão **Add (Adicionar)** adiciona novas entradas de lista. No caso de um AMC2 4W o número máximo é quatro, onde a quarta entrada é criada como uma placa AMC2 4W-EXT.
As placas de extensão são numeradas de acordo com a ordem de criação 1, 2 ou 3. O AMC2 4W-EXT recebe o número 0 (zero). A numeração dos sinais para o AMC2 4W-EXT continua a partir da numeração do controlador, a saber 09 a 16, enquanto para cada placa de E/S a numeração começa com 01. Os sinais de todas as placas de extensão também são mostrados na guia do AMC2 4W relevante.

Junto com os sinais de entrada e saída do AMC2 4W, até 64 pares de sinais podem ser fornecidos.

Modificação e exclusão de placas de extensão

A primeira guia contém os controles a seguir para configuração de placas de extensão.

Parâmetro	Valores possíveis	Descrição
Nome da placa	Restrição alfanumérica: 1 a 16 dígitos	A identificação padrão garante um nome exclusivo, mas pode ser substituída manualmente. Verifique se o ID é exclusivo. As conexões de rede com servidores DHCP devem usar o nome da rede.
Descrição da placa	Alfanumérico: 0 a 255 dígitos	Esse texto é exibido na ramificação OPC.
Número da placa	1 - 3	Número da placa conectada ao AMC. Somente campo de exibição.
Fonte de alimentação	0 = desativado (a caixa de seleção está marcada) 1 = ativado (a caixa de seleção está marcada)	Supervisão da tensão da fonte. Com interrupções de tensão, uma mensagem é gerada no final de um atraso. A função de supervisão presume o uso de um USV, para que uma mensagem possa ser gerada. 0 = sem supervisão 1 = supervisão ativada
Divisão	Valor padrão **Comum**	Relevante somente onde o recurso **Divisões** é licenciado.

As guias Inputs (Entradas), Outputs (Saídas) e Signal Settings (Configurações do sinal) têm o mesmo layout e função que as guias correspondentes dos controladores.

Exclusão de placas de extensão

Só é possível excluir uma placa de extensão quando nenhuma das interfaces estiver ocupada. Os sinais associados devem primeiro ser configurados em uma placa diferente antes que o botão de exclusão  e a opção **Delete object (Excluir objeto)** do menu de contexto possam ser utilizadas.

AMC2 4W-EXT

Como os leitores que ocupam placas de extensão não podem ser removidos ou reconfigurados individualmente, eles precisam ser excluídos junto com suas entradas correspondentes. Enquanto isso não acontecer o AMC2 4W-EXT também não pode ser removido.

16 Configurações de leitor personalizadas

16.1 Introdução

No BIS 4.9 e no AMS 4.0, os sistemas de controle de acesso da Bosch permitem o uso de configurações personalizadas do MIFARE DESFire. É possível criar arquivos de parâmetro criptografados usando a ferramenta auxiliar `Bosch.ReaderConfigTool.exe`. Essa ferramenta é incluída nas configurações do BIS ACE 4.9, do AMS 4.0 e em versões posteriores com sua documentação própria. Consulte essa documentação para ver a lista atual de leitores compatíveis

As seções a seguir descrevem como usar o Editor de dispositivos para importar um arquivo de parâmetro criptografado e aplicá-lo a todos os leitores compatíveis na hierarquia de dispositivos de controle de acesso.

16.2 A propriedade do leitor: Parâmetros de leitor estendidos

Os conjuntos disponíveis de parâmetros estendidos para leitores compatíveis são exibidos nas páginas de propriedade do editor de dispositivos, com o rótulo **Parâmetros de leitor estendidos**.

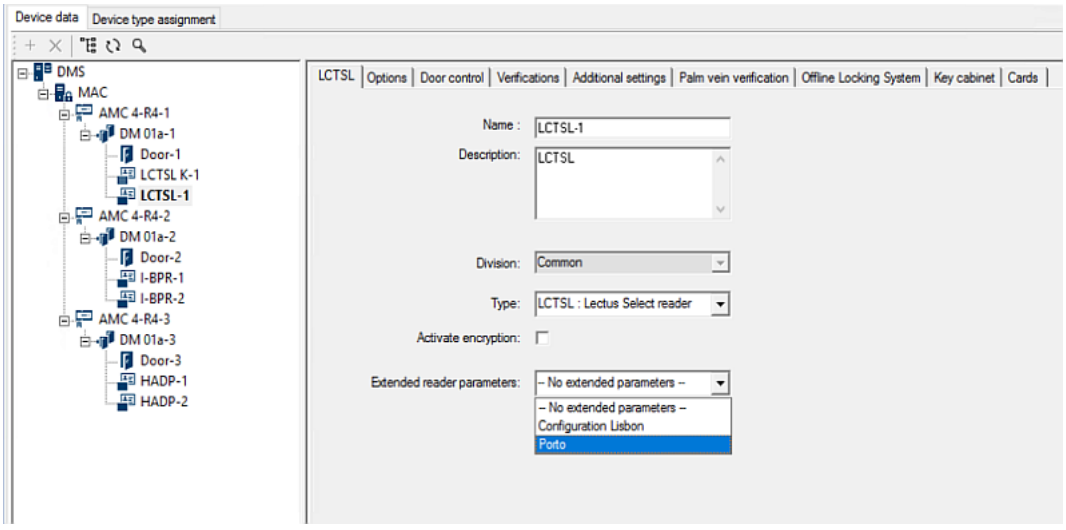


Figura 16.1: Parâmetros de leitor estendidos

O valor padrão da lista suspensa é `No extended parameters`. Esse é o único valor possível, a não ser que você importe outros conjuntos de parâmetros.

Procedimento

Para aplicar um conjunto de parâmetros importado a um leitor individual compatível:

1. No Editor de dispositivos, selecione o leitor na árvore de dispositivos
2. Selecione a primeira guia de propriedade
3. Selecione o conjunto de parâmetros necessário na lista **Parâmetros de leitor estendidos**
4. Clique em **Aplicar** ou 

16.3 Importação de um conjunto de parâmetros do leitor

É possível importar e excluir arquivos de parâmetro somente no nível DMS da hierarquia de dispositivos.

Pré-requisitos

Acesso a um arquivo de parâmetro aprovado do sistema de controle de acesso. Por padrão, o arquivo é do tipo `.ReaderConfigSave`

Procedimento

1. No Editor de dispositivos, clique com o botão direito no nó DMS e selecione **Importar conjuntos de parâmetros do leitor** no menu de contexto.
   A janela pop-up **Importar conjuntos de parâmetros do leitor** é exibida.
2. Clique em **Arquivo** e localize o arquivo de parâmetro usando o explorador de arquivos.
3. Quando solicitado, insira a senha do arquivo de parâmetro.
   Se a senha estiver correta, a metade inferior da janela pop-up será preenchida com as seguintes informações:

– Uma lista dos tipos de leitor aos quais o conjunto de parâmetros se aplica.
– O nome do conjunto de parâmetros. É possível editá-lo nessa caixa de diálogo.
– Uma descrição de texto livre, se o criador do conjunto de parâmetros tiver fornecido uma. É possível adicionar ou editar uma descrição nessa caixa de diálogo.

4. Clique em **Importar** para importar o conjunto de parâmetros para possível uso futuro por parte do sistema de controle de acesso.

– O conjunto de parâmetros é importado e armazenado no sistema de controle de acesso.
– Ele é adicionado à lista de conjuntos de parâmetros disponíveis na parte superior da janela pop-up.

5. Clique em **Sair** para sair da janela pop-up **Importar conjuntos de parâmetros do leitor**.

16.4 Aplicação de um conjunto de parâmetros aos leitores

Introdução

A importação de um conjunto de parâmetros para o sistema de controle de acesso o armazena para uso futuro, mas não o aplica aos leitores no sistema. A aplicação do conjunto de parâmetros é uma etapa extra que pode ser realizada em diferentes níveis da hierarquia de dispositivos:

– DMS
– MAC
– AMC

Quando você aplica um conjunto de parâmetros no nível do DMS, MAC ou AMC, ele só poderá ser aplicado aos leitores subordinados dos tipos de leitor para os quais o conjunto foi criado. Nenhum outro leitor subordinado é afetado.

Pré-requisitos

Você importou um conjunto de parâmetros do leitor.

Procedimento

1. No Editor de dispositivos, clique com o botão direito em um leitor ou dispositivo (DMS, MAC ou AMC) cujos leitores deseja parametrizar.
2. Selecione **Gerenciar conjuntos de parâmetros do leitor** no menu de contexto.
3. No painel de lista superior, **Conjuntos de parâmetros para tipos de leitor**, selecione o conjunto de parâmetros que deseja aplicar.
   Os leitores aplicáveis são listados no painel inferior esquerdo: **Leitores parametrizáveis com esse conjunto de parâmetros**.
4. Na lista **Leitores parametrizáveis com esse conjunto de parâmetros**, selecione os leitores aos quais deseja aplicar o conjunto de parâmetros selecionado.

– Se o número de leitores for grande, use as listas suspensas para restringir a exibição a subordinados de um determinado MAC ou AMC.

5. Use os botões de seta para mover os leitores selecionados até o painel inferior direito, **Todos os leitores parametrizados com o conjunto de parâmetros selecionado**.

Aviso!
Exibição de leitores compatíveis
Somente os leitores compatíveis com o conjunto de parâmetros serão listados. Se você marcar a caixa de seleção **Mostrar todos os leitores**, os leitores que tiverem outros conjuntos de parâmetros também serão exibidos. Eles têm o plano de fundo cinza para marcá-los como somente leitura para o conjunto de parâmetros selecionado.

6. Clique em **OK** para fechar a janela pop-up.
7. Novamente no Editor de dispositivos, clique em **Aplicar** ou
   O conjunto de parâmetros é aplicado a todos os leitores que sobrarem na lista **Todos os leitores parametrizados com o conjunto de parâmetros selecionado** na janela pop-up.

16.5 Gerenciamento de conjuntos de parâmetros do leitor

Introdução
É possível alterar a aplicação de conjuntos de parâmetros em diferentes níveis da hierarquia de dispositivos:
– DMS
– MAC
– AMC
As alterações no nível do DMS, MAC ou AMC só podem ser aplicadas aos leitores subordinados dos tipos de leitor para os quais o conjunto foi criado. Nenhum outro leitor subordinado é afetado.

Pré-requisito
Você importou um conjunto de parâmetros do leitor.

Procedimento
1. No Editor de dispositivos, clique com o botão direito em um leitor ou dispositivo (DMS, MAC ou AMC).
2. Selecione **Gerenciar conjuntos de parâmetros do leitor** no menu de contexto.
3. No painel de lista superior, **Conjuntos de parâmetros para tipos de leitor**, selecione o conjunto de parâmetros que deseja aplicar.
– Os leitores aplicáveis são listados no painel inferior esquerdo: **Leitores parametrizáveis com esse conjunto de parâmetros**.
– Os leitores aos quais o arquivo de parâmetro já foi aplicado são listados no painel inferior direito: **Todos os leitores parametrizados com o conjunto de parâmetros selecionado**.
4. Selecione os leitores em qualquer lista. Use as teclas de seta para adicionar e remover os leitores da lista inferior direita, **Todos os leitores parametrizados com o conjunto de parâmetros selecionado**.
– IMPORTANTE: anote os leitores retirados da lista para a última etapa deste procedimento.
5. Quando concluir as alterações, clique em **OK** para fechar a janela pop-up.
6. Novamente no Editor de dispositivos, clique em **Aplicar** ou
– O conjunto de parâmetros é aplicado a todos os leitores que sobrarem na lista **Todos os leitores parametrizados com o conjunto de parâmetros selecionado**.
– Ele é removido dos leitores retirados dessa lista.
7. Realize um destes procedimentos em todos os leitores retirados da lista:

– Redefina os padrões de fábrica usando os interruptores DIP no hardware do leitor.
– Aplique um conjunto de parâmetros diferente a eles.

Aviso!
A exclusão de um conjunto de parâmetros não reconfigura os leitores que o utilizaram.
A configuração de leitor excluída continuará nos leitores que a utilizaram até você redefinir o hardware do leitor ou aplicar um conjunto de parâmetros diferente.

16.6 Exclusão de conjuntos de parâmetros do leitor

É possível importar e excluir arquivos de parâmetro somente no nível DMS da hierarquia de dispositivos.

Pré-requisitos
Pelo menos um arquivo de parâmetro já foi importado para o sistema de controle de acesso.

Procedimento
1. No Editor de dispositivos, clique com o botão direito no nó DMS e selecione **Excluir conjuntos de parâmetros do leitor** no menu de contexto.
   A janela pop-up **Excluir conjuntos de parâmetros do leitor** é exibida.
2. Na lista **Conjuntos de parâmetros para tipos de leitor**, selecione o conjunto de parâmetros que deseja excluir.
– No canto inferior direito da janela pop-up, uma lista será exibida com todos os leitores atualmente parametrizados (configurados) com o conjunto de parâmetros selecionado.
– Anote esses leitores. Eles precisarão ser redefinidos ou reconfigurados após a exclusão do conjunto de parâmetros. Consulte a última etapa deste procedimento para ver os detalhes.
3. Clique em **Excluir**
4. Clique em **Sair**
5. Novamente no Editor de dispositivos, clique em **Aplicar** ou 
6. Realize um destes procedimentos em todos os leitores que estavam usando o conjunto de parâmetros excluído:
– Redefina os padrões de fábrica usando os interruptores DIP no hardware do leitor.
– Aplique um conjunto de parâmetros diferente a eles.

Aviso!
A exclusão de um conjunto de parâmetros não reconfigura os leitores que o utilizaram.
A configuração de leitor excluída continuará nos leitores que a utilizaram até você redefinir o hardware do leitor ou aplicar um conjunto de parâmetros diferente.

17 Campos personalizados para dados de funcionários

Introdução

Os campos de dados de funcionários podem ser personalizados de várias maneiras:

- Quanto à **visibilidade**, ou seja, se serão exibidos no cliente
- Quanto à **obrigatoriedade**, ou seja, se um registro de dados pode ser armazenado sem dados válidos no campo
- Se os valores que eles contêm devem ser mantidos **únicos** dentro do sistema
- Quais tipos de dados eles contêm (texto, data e hora, inteiro etc.)
- Onde (em qual guia, em qual coluna e em qual linha) no cliente eles aparecerão
- Com que tamanho serão exibidos
- Se e onde os dados serão usados em relatórios padrão

Ainda é possível definir campos de dados totalmente novos com todos os atributos listados aqui.

17.1 Pré-visualização e edição de campos personalizados

Caminho da caixa de diálogo

- No Navegador de configuração, navegue até o menu **Infrastructure (Infraestrutura)** > **ACE Custom fields (Campos personalizados do ACE)**.
- Main menu (Menu principal) > **Configuration (Configuração)** > **Options (Opções)** > **Custom fields (Campos personalizados)**

A janela principal é dividida em duas guias

Overview (Visão geral) Esta guia e suas subguias (**Address (Endereço), Contact (Contato), Additional person data (Dados pessoais adicionais), Additional Company data (Dados adicionais da empresa), Remarks (Observações), Card Control (Controle do cartão)** e **Extra Info (Informações adicionais)**) são somente leitura e contêm visão geral WYSIWYG aproximada de quais dados aparecerão em quais guias no software cliente.

Details (Detalhes) Esta guia contém uma lista dos editores, um para cada campo de dados predefinido ou definido pelo usuário.

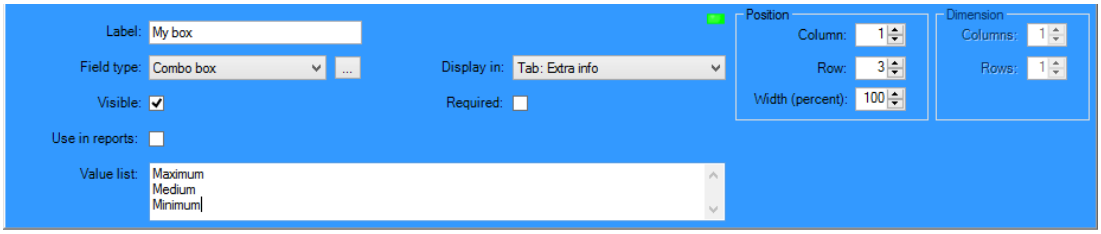
Pré-visualização

Para visualizar, no Navegador de configurações, o efeito de qualquer alteração feita na guia **Details (Detalhes)**, clique no botão **Apply (Aplicar)** e vá até a guia **Overview (Visão geral)**. Para ver, no cliente do ACE, o efeito dessas alterações, clique no botão **Apply (Aplicar)** e abra a caixa de diálogo relevante no cliente do ACE. Não é necessário recarregar a configuração ou reiniciar o cliente do ACE. No entanto, se a caixa de diálogo modificada estiver aberta no cliente do ACE, será necessário fechar e abrir novamente essa caixa.

Edição de campos de dados existentes

Na guia **Custom fields (Campos personalizados)** > **Details (Detalhes)**, cada campo de dados, predefinido ou definido pelo usuário, tem sua própria janela de editor onde os atributos podem ser modificados.

Clique no editor do campo que deseja modificar. O editor ativo será destacado.



Os atributos editáveis dos campos personalizados são explicados na tabela a seguir.

Texto do rótulo	Descrição
Label (Rótulo)	**Label (Rótulo)** é o rótulo do campo de dados conforme ele aparece no cliente. Pode ser substituído livremente para refletir a terminologia usada no seu local.

Field type (Tipo de campo)	**Field type (Tipo de campo)** é o tipo de dado e determina o controle da caixa de diálogo que o operador usará para realizar entradas no cliente. Cada tipo de campo fornece verificações de consistência para seus valores de entrada específicos, para garantir datas, horas, comprimentos de texto e limites numéricos válidos.
	– **Text field (Campo de texto)**
	  – Clique no botão de elipse ao lado dele para especificar o número de caracteres permitidos.
	– **Check box (Caixa de seleção)**
	– **Date field (Campo de data)**
	– **Time (Hora)**
	– **Date-time field (Campo de data/hora)**
	– **Combo box (Caixa de combinação)**
	  – Insira os valores válidos para a caixa de combinação no campo de texto fornecido. Separe-os com vírgulas ou quebras de linha.
	– **Numerical input (Entrada numérica)**
	  – Insira valores mínimo e máximo para a entrada numérica nas caixas de rotação fornecidas.
	– **Building control 1 (Controle de edifício 1)** e **Building control 2 (Controle de edifício 2)**
	  – São controles especiais que podem ser rotulados novamente aqui (no campo **Label (Rótulo)**) e vinculados a comandos na UI do cliente. Logo, você pode conceder permissão para usuários específicos, através de seus cartões, para realizar operações especiais no local. Exemplos de tais operações são a ativação de holofotes ou o controle de equipamentos especiais.

Visible (Visível)	Desmarque essa caixa de seleção para evitar que o campo de dados apareça no cliente.
Unique (Exclusivo)	Marque essa caixa de seleção para garantir a exclusividade dos valores inseridos neste campo. O sistema rejeitará a entrada de qualquer valor que já tenha sido armazenado para esse campo no banco de dados. Por exemplo, os números de funcionários devem ser únicos para cada funcionário, bem como as placas veiculares para veículos.

Texto do rótulo	Descrição
	A luz verde indica que o campo de dados **não** está sendo usado atualmente no banco de dados. A luz vermelha indica que o campo de dados está sendo usado atualmente no banco de dados.
Display in (Exibir em)	Use esta lista suspensa para selecionar a guia de cliente em que o campo de dados deve aparecer.
Required (Obrigatório)	Marque essa caixa de seleção para tornar o campo de dados obrigatório. Por exemplo, é necessário um sobrenome para cada registro de funcionários. Sem um sobrenome, o registro de dados não pode ser armazenado. Observe que o editor não permitirá que um campo de dados obrigatório seja definido como invisível pela caixa de seleção **Visible (Visível)**. Para facilitar o uso no cliente, é altamente recomendado que todos os campos obrigatórios sejam colocados na primeira guia.
Position (Posição)	Use as caixas de rotação em **Column (Coluna)** e **Row (Linha)** para posicionar o campo de dados na guia nomeada na lista suspensa **Display in (Exibir em)**. Observe que o editor não permitirá que você selecione uma posição que já está em uso ou sobreponha campos de dados existentes. Use a caixa de rotação **Width (percent) (Largura (porcentagem))** para definir o tamanho de determinados controles redimensionáveis, como campos de textos. 100% indica que o controle ocupará todo o espaço que ainda não estiver ocupado pelo rótulo do campo de dados.
Dimension (Dimensão)	Use as caixas de rotação em **Column (Coluna)** e **Row (Linha)** para especificar o número de colunas e linhas a serem ocupadas na guia nomeada na lista suspensa **Display in (Exibir em)**. Observe que o editor não permitirá que você sobreponha campos de dados existentes.

Criação e edição de novos campos de dados

Na guia **Custom fields (Campos personalizados)** > **Details (Detalhes)**, cada campo de dados, predefinido ou definido pelo usuário, tem seu próprio painel de editor onde os atributos podem ser modificados.

Clique no botão **New field (Novo campo)** para criar um novo campo personalizado em seu próprio editor. O painel do editor ativo será destacado.

O editor tem os mesmos controle de caixa de diálogo para edição de campos de dados existentes (veja a tabela acima) e dois adicionais:

Use in reports (Usar em relatórios) (caixa de seleção)	Selecione essa caixa de seleção para permitir que o novo campo de dados apareça em relatórios padrão.
Sequence number (Número de sequência) (caixa de rotação)	O número de sequência determina a coluna que o campo de dados ocupará em relatórios padrão.

Aviso!
No momento, somente os números sequenciais de 1 a 10 são endereçáveis por **Badge Designer (Criador de crachá)** e **Reports (Relatórios)**.

17.2 Regras para campos de dados

- Localização dos campos de dados
  - Cada campo só pode aparecer em uma guia.
  - Cada campo personalizado pode aparecer em qualquer guia selecionável.
  - Os campos podem ser movidos para outras guias alterando a entrada na lista suspensa **Display in (Exibir em)**.
- O rótulo pode conter qualquer texto: comprimento máximo de 20 caracteres.
- Os campos de texto personalizados podem conter qualquer texto: comprimento máximo de 2.000 caracteres.
- Qualquer campo pode se tornar um campo obrigatório, mas a sua caixa de seleção **Visible (Visível)** deve ser marcada.

Aviso!
Recomendações urgentes antes do uso produtivo
Concorde e finalize os tipos de campo e seus usos antes de usá-los para armazenas dados pessoais:
Cada campo de entrada de dados é atribuído a um campo específico do banco de dados, para que os dados possam ser localizados manualmente e por geradores de relatórios. Uma vez que os registros de dados de campos personalizados forem armazenados no banco de dados, esses campos não poderão mais ser movidos ou alterados sem risco de perda de dados.

18 Configuração do gerenciamento de nível de ameaça

Introdução

O objetivo do gerenciamento do nível de ameaça é responder de forma eficiente a situações de emergência, promovendo uma mudança instantânea no comportamento das entradas em toda a área afetada.

18.1 Conceitos do gerenciamento de nível de ameaça

- Uma **Threat (Ameaça)** é uma situação crítica que requer resposta imediata e simultânea de algumas ou de todas as entradas em um sistema de controle de acesso.
- Um **Threat level (Nível de ameaça)** é a resposta do sistema a uma situação prevista. Cada nível de ameaça deve ser configurado cuidadosamente para que cada uma das entradas do MAC saiba como responder.
  Os níveis de ameaça são totalmente personalizáveis. Por exemplo, os níveis altos de ameaça comuns podem ser configurados desta maneira:
  - **Lockout (Bloqueio)**: somente socorristas, com altos níveis de segurança, podem entrar.
  - **Lockdown (Isolamento)**: todas as portas são trancadas. Tanto a entrada quanto a saída são negadas a todas as credenciais abaixo de um nível de segurança configurado.
  - **Evacuation (Evacuação)**: todas as portas de saída são destrancadas.
- Os níveis baixos de ameaça comuns podem ser configurados desta maneira:
  - **Sports event (Evento esportivo)**: as portas das áreas esportivas são destrancadas; todas as outras áreas ficam protegidas.
  - **Parents' evening (Reunião de pais e mestres)**: apenas salas de aula selecionadas e a entrada principal ficam acessíveis.
- Um **Threat alert (Alerta de ameaça)** é um alarme que aciona um nível de ameaça. Pessoas devidamente autorizadas podem acionar um alerta de ameaça com uma ação momentânea, por exemplo, pela interface do usuário do operador, por um sinal de hardware (por exemplo, botão de destrave) ou pela apresentação de um cartão de alerta especial em qualquer leitor.
- Um **Security level (Nível de segurança)** é um atributo dos **Security profiles (Perfis de segurança)** dos usuários de cartão e leitores, expresso como um número inteiro 0–100. Cada nível de ameaça define os leitores de seu MAC (Main Access Controller) para os níveis de segurança indicados. Então, esses leitores concedem acesso apenas a credenciais de pessoas com um nível de segurança igual ou maior em seus perfis de segurança.
- Um **Security profile (Perfil de segurança)** é um conjunto de atribuições que podem ser designadas a um **Person type (Tipo de pessoa)** (**Person security profile (Perfil de segurança de pessoas)**), a uma porta (**Door security profile (Perfil de segurança da porta)**) ou a um leitor (**Reader security profile (Perfil de segurança do leitor)**). Os perfis de segurança controlam os seguintes comportamentos de controle de acesso:
  - **Security level (Nível de segurança)**, como definido acima, para tipo de pessoa, porta ou leitor
  - **Screening rate (Taxa de triagem)**. A probabilidade percentual de que a triagem aleatória seja acionada por esse tipo de pessoa ou leitor.

18.2 Visão geral do processo de configuração

O gerenciamento de nível de ameaça exige as seguintes etapas de configuração, que serão explicadas em detalhes após esta visão geral

1. No Editor de dispositivos
   - Definição de níveis de ameaça
   - Definição de perfis de segurança da porta
   - Definição de perfis de segurança do leitor
   - Atribuição de perfis de segurança da porta a entradas
2. Nas caixas de diálogos de dados do sistema
   - Definição de perfis de segurança de pessoas
   - Atribuição de perfis de segurança de pessoas a tipos de pessoas
3. Nas caixas de diálogo de dados pessoais
   - Atribuição de tipos de pessoas a pessoas
   - Atribuição de tipos de pessoas a grupos de pessoas

Após a configuração do gerenciamento do nível de ameaça, os alarmes e os estados do dispositivo do MAC poderão ser monitorados e controlados pelo aplicativo Map View. Consulte a ajuda online do Map View para obter mais informações.

18.3 Etapas de configuração no Editor de dispositivos

Esta seção descreve as etapas prévias de configuração que devem ser seguidas no editor de dispositivos.

Aviso!
Os dados de dispositivo não poderão ser modificados no editor de dispositivos enquanto um nível de ameaça estiver ativo.

18.3.1 Criação de um nível de ameaça

Esta seção descreve como criar níveis de ameaça para uso no local. Até 15 níveis podem ser criados.

Caminho da caixa de diálogo

- **Main menu (Menu principal)** > **Configuration (Configuração)** > **Device data (Dados do dispositivo)**
- **Navegador de configuração do BIS** > **Connections (Conexões)** > **Device data (Dados do dispositivo)**

Procedimento

1. Selecione a guia secundária **Threat levels (Níveis de ameaça)**
   - A tabela Threat levels (Níveis de ameaça) será exibida. Ela pode ter até 15 níveis de ameaça, cada um com um nome, uma descrição e uma caixa de seleção para ativação do nível de ameaça após a configuração.
2. Clique na linha **Please enter a name for the threat level (Insira um nome para o nível de ameaça)**
3. Insira um nome que seja significativo para os operadores do sistema.
4. (Opcional) Na coluna **Description (Descrição)**, insira uma descrição mais completa do comportamento das entradas quando o nível de ameaça em questão estiver em operação.
5. **Não** marque a caixa de seleção **Active (Ativar)** agora. Primeiro, conclua todas as outras etapas de configuração para esse nível de ameaça, conforme descrito nas seções a seguir.
6. Clique em (Salvar) para salvar o novo nível de ameaça.

18.3.2 Criação de um perfil de segurança da porta

Esta seção descreve como criar perfis de segurança para diferentes tipos de portas e como definir o estado para o qual todas as portas desse perfil serão alteradas quando um nível de ameaça entrar em operação.

Caminho da caixa de diálogo

- **Main menu (Menu principal)** > **Configuration (Configuração)** > **Device data (Dados do dispositivo)**
- **Navegador de configuração do BIS** > **Connections (Conexões)** > **Device data (Dados do dispositivo)**

Pré-requisitos

- Pelo menos um nível de ameaça deve ter sido definido
- Pelo menos uma entrada deve ter sido configurada na árvore de dispositivos.

Procedimento

1. Selecione a guia secundária **Door security profiles (Perfis de segurança das portas)**
   - A janela de diálogo principal tem dois painéis: **Selection (Seleção)** e **Door security profile (Perfil de segurança da porta)** (nome padrão)
2. Clique em **New (Novo)**.
   - Um novo perfil de segurança da porta é criado com um nome padrão
   - A tabela **Threat level (Nível de ameaça)** no painel **Door security profile (Perfil de segurança da porta)** é preenchida com os níveis de ameaça que já foram criados e com um valor **undefined (não definido)** para cada um na coluna **State (Estado)**.
3. No painel **Door security profile (Perfil de segurança da porta)**, insira um nome para o tipo de porta ao qual o perfil será atribuído.
   - O novo nome do perfil será exibido no painel **Selection (Seleção)**. Se desejar, poderá excluí-lo da configuração clicando em **Delete (Excluir)** nesse painel.
4. (Opcional) Insira uma descrição do perfil para ajudar os operadores a atribuírem o perfil corretamente.
5. Se esse perfil for atribuído a catracas, marque a caixa de seleção **Turnstile (Catraca)**.
   - Isso fornecerá mais opções para o estado de destino da porta em diferentes níveis de ameaças. Por exemplo, as opções para permitir a entrada ou a saída desacompanhado ou as duas situações.
6. Na coluna **State (Estado)** da tabela **Threat level (Nível de ameaça)**, para cada nível de ameaça, selecione um estado de destino pertinente, para todas as portas desse perfil, sempre que esse nível de ameaça for acionado.
7. Clique em  (Salvar) para salvar as alterações.

Repita o procedimento para criar perfis de segurança da porta para todos os tipos de portas em sua configuração. Os tipos comuns de portas podem ser:

- Porta pública principal
- Acesso de evacuação para o lado de fora
- Acesso a salas de aula
- Acesso público à arena esportiva

18.3.3 Criação de um perfil de segurança do leitor

Esta seção descreve como criar perfis de segurança para diferentes tipos de leitores. Os perfis de segurança do leitor definem os seguintes atributos do leitor **para cada nível de ameaça**:

- O nível mínimo de segurança exigido por uma credencial para obter acesso ao leitor.
- A taxa de triagem, ou seja, a porcentagem de usuários de cartões que serão selecionados aleatoriamente para uma triagem de segurança adicional.
  - **Observação**: Uma taxa de triagem definida em um perfil de segurança do leitor substitui uma taxa de triagem definida no próprio leitor.

Caminho da caixa de diálogo

- **Main menu (Menu principal)** > **Configuration (Configuração)** > **Device data (Dados do dispositivo)**
- **Navegador de configuração do BIS** > **Connections (Conexões)** > **Device data (Dados do dispositivo)**

Pré-requisitos

- Pelo menos um nível de ameaça deve ter sido definido
- Pelo menos uma entrada deve ter sido configurada na árvore de dispositivos.

Procedimento

1. Selecione a guia secundária **Reader security profiles (Perfis de segurança do leitor)**
   - A janela de diálogo principal tem dois painéis: **Selection (Seleção)** e **Reader security profile (Perfil de segurança do leitor)** (nome padrão)
2. Clique em **New (Novo)**.
   - Um novo perfil de segurança do leitor é criado com um nome padrão
   - A tabela **Threat level (Nível de ameaça)** no painel **Reader security profile (Perfil de segurança do leitor)** é preenchida com os níveis de ameaça que já foram criados, com um valor padrão de **0** para cada um nas colunas **Security level (Nível de segurança)** e **Screening rate (Taxa de triagem)**.
3. No painel **Reader security profile (Perfil de segurança do leitor)**, insira um nome para o tipo de leitor ao qual o perfil será atribuído.
   - O novo nome do perfil será exibido no painel **Selection (Seleção)**. Se desejar, poderá excluí-lo da configuração clicando em **Delete (Excluir)** nesse painel.
4. (Opcional) Insira uma descrição do perfil para ajudar os operadores a atribuírem o perfil corretamente.
5. Na coluna **Security level (Nível de segurança)** da tabela **Threat level (Nível de ameaça)**, para cada nível de ameaça, selecione um nível de segurança mínimo (número inteiro 0–100) que um operador deverá ter para operar um leitor desse perfil sempre que esse nível de ameaça for acionado.
6. Na coluna **Screening rate (Taxa de triagem)** da tabela **Threat level (Nível de ameaça)**, para cada nível de ameaça, selecione a porcentagem de usuários de cartões que serão selecionados aleatoriamente pelo leitor para verificações de segurança adicionais sempre que o nível de ameaça for acionado.
7. Clique em  (Salvar) para salvar as alterações.

18.3.4 Atribuição de perfis de segurança da porta e do leitor a entradas

Esta seção descreve como atribuir os perfis de segurança da porta e do leitor às portas e aos leitores em entradas específicas.

O primeiro subprocedimento é identificar e filtrar o conjunto de entradas que você deseja atribuir, já o segundo é fazer as atribuições.

Além disso, você pode visualizar os estados, os níveis de segurança e as taxas de triagem das entradas selecionadas, pois seriam definidas pelos vários níveis de ameaças que você definiu.

Caminho da caixa de diálogo

- **Main menu (Menu principal)** > **Configuration (Configuração)** > **Device data (Dados do dispositivo)**
- **Navegador de configuração do BIS** > **Connections (Conexões)** > **Device data (Dados do dispositivo)**

Pré-requisitos

- Pelo menos um nível de ameaça deve ter sido definido
- Pelo menos uma entrada deve ter sido configurada na árvore de dispositivos.

Procedimento

1. Selecione o **DMS** na árvore de dispositivos (a raiz da árvore de dispositivos)
2. No painel de diálogo principal, selecione a guia **Threat level management (Gerenciamento do nível de ameaça)**
   - O painel de diálogo principal recebe várias guias secundárias.

Subprocedimento 1: selecionar entradas para atribuição

1. Selecione a guia secundária **Entrances (Entradas)**
   - A janela de diálogo principal tem dois painéis: **Filter conditions (Filtrar condições)** e uma tabela com todas as entradas que foram criadas no sistema até o momento.
2. (Opcional) No painel **Filter conditions (Filtrar condições)**, insira critérios para restringir o conjunto de entradas que aparecem na tabela na metade inferior da caixa de diálogo, por exemplo:
   - Marque ou desmarque as caixas de seleção que determinam se as opções **Inbound readers (Leitores de entrada)**, **Outbound readers (Leitores de saída)** e/ou **Doors (Portas)** serão exibidas na tabela.
   - Insira strings de caracteres que devem aparecer nos nomes das entradas, áreas, nomes de perfis ou nomes de leitores de todas as entradas informadas na tabela.
   - Marque ou desmarque a caixa de seleção que determina se as portas e os leitores que ainda não foram configurados também devem aparecer na tabela
3. Clique em **Apply filter (Aplicar filtro)** para filtrar a lista Entrances (Entradas) ou **Reset filter (Redefinir filtro)** para definir os controles de filtros de volta para os valores padrão.

Subprocedimento 2: atribuir perfis de segurança às entradas selecionadas

Pré-requisito: As entradas a serem atribuídas devem ter sido identificadas e aparecerem na tabela na metade inferior da caixa de diálogo.

Note que cada entrada geralmente tem uma porta ou barreira e um ou mais leitores de cartão. No entanto, alguns tipos de entrada especializados, como **Assembly points (Pontos de encontro)**, podem não ter esses itens.

1. Na coluna **Door or reader security profile (Perfil de segurança da porta ou do leitor)**, clique na célula correspondente à porta ou ao leitor que você deseja atribuir.
2. Selecione um perfil de segurança da porta ou do leitor na lista suspensa da célula.

(Opcional) Visualização do comportamento das portas e leitores em níveis de ameaça

As colunas no lado direito da tabela são somente para leitura. Elas mostram como seriam o status de bloqueio (**Mode [Modo]**), o **Security level (Nível de segurança)** e a **Screening rate (Taxa de triagem)** das portas e dos leitores na tabela se o nível de ameaça selecionado na lista **Select threat level for details (Selecionar o nível de ameaça para obter detalhes)** estivesse em operação.

Pré-requisito: As entradas que você deseja visualizar devem ter sido identificadas e aparecerem na tabela na metade inferior da caixa de diálogo.

- ▸ Na lista **Select threat level for details (Selecionar o nível de ameaça para obter detalhes)**, selecione o nível de ameaça que você deseja visualizar.

P A tabela mostra como seriam o status de bloqueio (**Mode [Modo]**) das portas e o **Security level (Nível de segurança)** e as **Screening rates (Taxas de triagem)** dos leitores se o nível de ameaça selecionado estivesse em operação.

18.3.5 Atribuição de um nível de ameaça a um sinal de hardware

Esta seção descreve como atribuir um sinal de entrada de hardware para acionar ou cancelar um alerta de ameaça.

Caminho da caixa de diálogo

- **Main menu (Menu principal)** > **Configuration (Configuração)** > **Device data (Dados do dispositivo)**
- **Navegador de configuração do BIS** > **Connections (Conexões)** > **Device data (Dados do dispositivo)**

Pré-requisitos

- Pelo menos um nível de ameaça deve ter sido definido
- Pelo menos uma entrada deve ter sido configurada na árvore de dispositivos.

Procedimento

1. Na árvore de dispositivos, selecione uma **entrada** abaixo do controlador AMC cujos sinais de entrada você deseja atribuir.
2. Na janela de diálogo principal, selecione a guia **Terminals (Terminais)**.
   - A tabela de entradas e sinais é exibida.
3. Na linha do sinal que você deseja atribuir, clique na célula de **Input signal (Sinal de entrada)**.
   - A lista suspensa contém um comando **Threat level: Deactivate (Nível de ameaça: desativar)** e
     um **Threat level (Nível de ameaça)** `<name>` para cada nível de ameaça definido anteriormente.
   - O comando **Threat level: Deactivate (Nível de ameaça: desativar)** cancelará qualquer nível de ameaça atualmente em operação.
4. Atribua os comandos aos sinais de entrada desejados.
5. Clique em  (Salvar) para salvar as alterações.

Aviso!
Restrição para DM 15
No momento, o modelo de porta 15 (DIP/DOP) não pode ser usado para acionar um nível de ameaça.

18.4 Etapas de configuração em caixas de diálogo de dados do sistema

Esta seção descreve como criar **perfis de segurança de pessoas** e atribuí-los a **tipos de pessoas**.

18.4.1 Criação de um perfil de segurança de pessoas

Caminho da caixa de diálogo

- **Main menu (Menu principal)** > **System data (Dados do sistema)** > **Person security profile (Perfil de segurança de pessoas)**
- **ACE client (Cliente ACE)** > **System data (Dados do sistema)** > **Person security profile (Perfil de segurança de pessoas)**

Pré-requisitos

Os perfis de segurança de pessoas exigem planejamento e especificação cuidadosos com antecedência, pois terão consequências importantes no funcionamento do sistema em situações críticas.

Procedimento

1. Se a caixa de diálogo já contiver dados, clique em  (New, Novo) para apagá-los.
2. Insira um nome para o novo perfil no campo de texto Security profile name (Nome do perfil de segurança):
3. (Opcional) Insira uma descrição do perfil para ajudar os operadores a atribuir o perfil corretamente.
4. Insira um número inteiro entre 0 e 100 na caixa **Security level (Nível de segurança)**.
   - Como o usuário do cartão está autorizado a usar uma entrada, 100 é suficiente para obter acesso a qualquer leitor, mesmo que o nível de segurança também esteja atualmente definido como 100
   - Caso contrário, o nível de segurança no perfil de segurança de pessoas do usuário do cartão deverá ser igual ou superior ao nível de segurança atual do leitor.
5. Insira um número inteiro entre 0 e 100 na caixa **Screening rate (Taxa de triagem)**.
   - **Observação**: A taxa de triagem do perfil da pessoa é secundária à do perfil do leitor. A tabela abaixo descreve a interação entre as duas taxas de triagem do perfil.
6. Clique em  (Salvar) para salvar as alterações.

Interação de taxas de triagem para perfis de segurança de pessoas e do leitor

Taxa de triagem (%) em Reader security profile (Perfil de segurança do leitor) R	Taxa de triagem (%) em Person security profile (Perfil de segurança de pessoas) P	Pessoa selecionada para verificações de segurança adicionais?
0	Qualquer	**Não**
100	Qualquer	**Sim**
1..99	0	**Não**
1..99	100	**Sim**
1..99	1..99	**Possibilidade** Probabilidade = MAX(R,P)

18.4.2 Atribuição de um perfil de segurança de pessoas a um tipo de pessoa

Caminho da caixa de diálogo

- **Main menu (Menu principal)** > **System data (Dados do sistema)** > **Person Type (Tipo de pessoa)**
- **ACE client (Cliente ACE)** > **System data (Dados do sistema)** > **Person Type (Tipo de pessoa)**

Procedimento

Observação: Por motivos históricos, **Employee ID (Identificação do funcionário)** aqui é sinônimo de **Person type (Tipo de pessoa)**

1. Na tabela **Predefined employee IDs (IDs de funcionário predefinidos)** ou na tabela **User-defined employee IDs (IDs de funcionário definidos pelo usuário)**, selecione a célula na coluna **Security profile name (Nome do perfil de segurança)** que corresponde ao tipo de pessoa desejado.
2. Selecione um perfil de segurança de pessoas na lista suspensa.
   - Repita o procedimento para todos os tipos de pessoas que exigem um perfil de segurança de pessoas
3. Clique em  (Salvar) para salvar as atribuições

18.5 Etapas de configuração em caixas de diálogo de dados pessoais

Esta seção descreve como os novos registros de **pessoa** criados no sistema recebem um **Person security profile (Perfil de segurança de pessoa)** pelo **Person type (Tipo de pessoa)**.

Caminhos da caixa de diálogo

- **Main menu (Menu principal)** > **Personnel data (Dados de funcionários)** > **Persons (Pessoas)**
- **Main menu (Menu principal)** > **Personnel data (Dados de funcionários)** > **Group of Persons (Grupo de pessoas)**

Observação: Por motivos históricos, **Employee ID (Identificação do funcionário)** aqui é sinônimo de **Person type (Tipo de pessoa)**

Procedimento

Todos os registros de **pessoa** criados no sistema devem ter um **Person type (Tipo de pessoa)**.

1. Os operadores do sistema devem atribuir apenas **tipos de pessoas** que foram vinculados a um **Person security profile (Perfil de segurança de pessoa)** na caixa de diálogo **Main menu (Menu principal)** > **System data (Dados do sistema)** > **Person Type (Tipo de pessoa)**
2. Para obter mais informações sobre a vinculação de **perfis de segurança de pessoas** e a criação de registros de **pessoa**, clique nos links a seguir.

Consulte

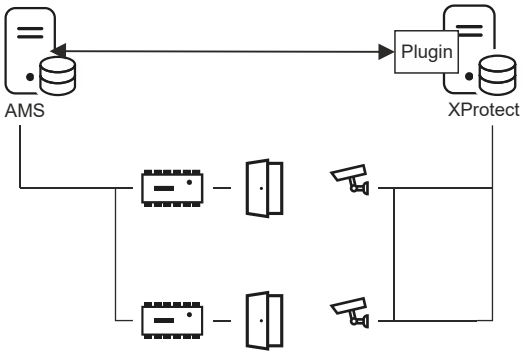
- *Atribuição de um perfil de segurança de pessoas a um tipo de pessoa, página 145*
- *Criação e gerenciamento de dados de funcionários, página 189*

19 Configuração do Milestone XProtect para usar AMS

Introdução

Este capítulo descreve como configurar o Milestone XProtect para usar os recursos de controle de acesso do AMS.

Um plug-in fornecido pelo AMS, mas instalado no servidor XProtect, transmite eventos e comandos para o AMS e envia os resultados de volta para o XProtect.



A configuração tem três estágios, descritos nestas seções:

- Instalação do certificado público do AMS no servidor XProtect.
- Instalação do plug-in do AMS no servidor XProtect.
- Configuração do AMS no aplicativo XProtect.

Aviso!

Incompatibilidade em potencial de plug-ins de diferentes fontes

Os plug-ins Milestone XProtect não possuem sandbox, ou seja, eles não estão completamente isolados um do outro. Por essa razão, poderão ocorrer erros de software se você executar vários plug-ins com diferentes versões do .NET e suas dependências no mesmo servidor XProtect. A BOSCH só poderá garantir o funcionamento correto do plug-in AMS se for o único plug-in instalado.

Pré-requisitos

- O AMS deve estar instalado e licenciado.
- O XProtect deve estar instalado e licenciado no mesmo computador ou em seu próprio computador.
- Deve haver uma conexão de rede entre os dois sistemas.

Instalação do certificado público do AMS no servidor XProtect

Este procedimento só será necessário se o AMS estiver sendo executado em outro computador.

1. Copie o arquivo de certificado do servidor AMS
   `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Certificates\Access Management System Internal CA.cer`
   para o servidor XProtect.
2. No servidor XProtect, clique duas vezes no arquivo de certificado.
   O Assistente de certificados será exibido.
3. Clique em **Install Certificate... (Instalar certificado...)**
   O Assistente de importação de certificados será exibido.

4. Selecione **Local Machine (Máquina local)** como **Store Location (Local de armazenamento)** e clique em **Next (Próximo)**
5. Selecione **Place all certificates... (Colocar todos os certificados...)**
6. Clique em **Browse... (Procurar...)**
7. Selecione **Trusted Root Certification Authorities (Autoridades de certificação raiz confiáveis)** e clique em **OK**
8. Clique em **Next (Próximo)**
9. Analise o resumo das configurações e clique em **Finish (Concluir)**

Instalação do plug-in do AMS no servidor XProtect

1. Copie o arquivo de configuração
   `AMS XProtect Plugin Setup.exe`
   da mídia de instalação do AMS para o servidor XProtect.
2. Execute o arquivo no servidor XProtect.
   O Assistente de configuração será exibido.
3. No Assistente de configuração, verifique se o plug-in do AMS XProtect está marcado para instalação e clique em **Next (Próximo)**.
   O Contrato de licença do usuário final será exibido. Caso deseje prosseguir, clique em **Accept (Aceitar)** para aceitar o contrato.
4. O assistente exibirá o caminho de instalação padrão do plug-in. Clique em **Next (Próximo)** para aceitar o caminho padrão ou em **Browse (Procurar)** para alterá-lo antes de clicar em **Next (Próximo)**.
   O assistente confirma que está prestes a instalar o plug-in do AMS XProtect.
5. Clique em **Install (Instalar)**.
6. Aguarde a confirmação de instalação concluída e clique em **Finish (Concluir)**.
7. Reinicie o serviço do Windows chamado **Milestone XProtect Event Server**.

Configuração do AMS no aplicativo XProtect

1. No aplicativo de gerenciamento XProtect, acesse **Advanced Configuration (Configuração avançada)** > **Access Control (Controle de acesso)**
2. Clique com o botão direito em **Access Control (Controle de acesso)** e selecione **Create new... (Criar novo...)**
   O Assistente de plug-in será exibido.
3. Insira as seguintes informações no Assistente de plug-in:
   - **Name (Nome)**: uma descrição desta integração AMS-XProtect para diferenciá-la de outras integrações no mesmo sistema XProtect
   - **Integration plug-in (Plug-in de integração)**: `AMS - XProtect Plugin` (Este nome estará disponível na lista suspensa após a instalação do plug-in)
   - **AMS API discovery endpoint (Endpoint de descoberta de API do AMS)**: `https://<hostname of the AMS system>:44347/`
     , em que `44347` é a porta padrão selecionada ao instalar a API do AMS.
   - **Operator name (Nome do operador)**: o nome de usuário de um operador AMS com pelo menos permissões para operar as portas nas quais as câmeras XProtect serão mapeadas.
   - **Operator password (Senha do operador)**: a senha do AMS desse operador.

4. Clique em **Next (Próximo)**
   O plug-in AMS estabelece conexão com o servidor AMS especificado e informa os elementos de controle de acesso que descobre (portas, unidades, servidores, estados e comandos de eventos)
5. Quando a barra de progresso for concluída, clique em **Next (Próximo)**
   A página do assistente **Associate cameras (Associar câmeras)** será exibida.
6. Para associar câmeras a portas, arraste as câmeras da lista **Cameras (Câmeras)** para os pontos de acesso na lista **Doors (Portas)**.
7. Após finalizar, clique em **Next (Próximo)**.
   O XProtect salva a configuração e confirma quando ela é salva com sucesso.

20 Integração do Otis Compass

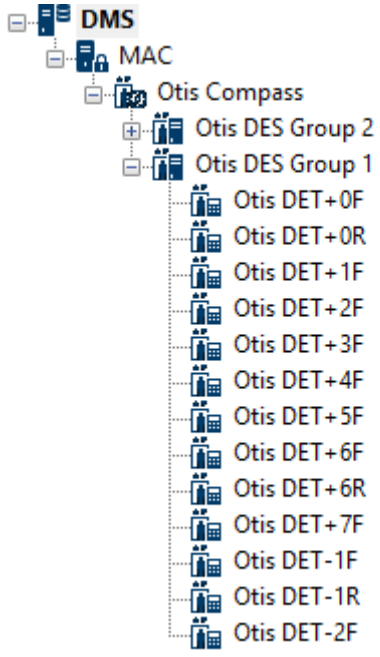
Introdução

Compass é um sistema de gerenciamento de destinos da Otis Elevator Company. Sua função é gerenciar vários bancos de elevadores, enviando os elevadores aos passageiros para que eles cheguem ao destino da maneira mais eficiente possível. Para fornecer os dados necessários, os passageiros não precisam mais apenas pressionar as teclas **Para cima** ou **Para baixo**, mas solicitar o destino nos terminais de leitor de cartão, tela de toque ou teclado.

A integração com os sistemas de controle de acesso da Bosch aumenta a segurança. Com base nas credenciais e nos modelos de hora em operação, os passageiros são transportados até o andar inicial e outros destinos autorizados com eficiência. O sistema não aceitará a solicitação de andares que não estiverem nos perfis de autorização do passageiro ou uma hora do dia fora do modelo de hora atual.

Topologia de hardware de um sistema Compass

O hardware de um sistema Compass é configurado de cima para baixo como uma hierarquia de três níveis com um único MAC no Editor de dispositivos.



A hierarquia acima mostra:
Um sistema **Otis Compass** em um MAC dedicado
Um único grupo de elevadores governado por um **DES**
Alguns terminais (**DET**), cada um com um número de andar de -2 a +7 e F ou R em referência às portas dianteiras ou traseiras.

Primeiro nível: (Otis Compass)
O Sistema de gerenciamento de destinos. Cada sistema **Compass** pode governar até oito grupos de elevadores (também conhecidos como bancos de elevadores).
Parâmetros: a variedade de andares, endereços de rede,
números de porta e tempos limite.

Segundo nível: (Otis DES/DER)
Até oito grupos de elevadores, cada um gerenciado por um Servidor de entrada de destino (DES) lógico que é composto por um ou dois dispositivos físicos.
Além disso, esse nível pode ter até dois dispositivos opcionais para otimização, conhecidos como Redirecionadores de entrada de destino (DER).
Parâmetros: um ID de grupo por grupo de elevadores.
Um endereço IP por dispositivo.
A tabela de andares com portas de elevador e se elas são de acesso público.

Terceiro nível: Otis DET
Os Terminais de entrada de destino (DET)
Parâmetros: um endereço IP por terminal. Os andares acessíveis com portas de elevador em cada terminal.

Visão geral da integração no sistema de controle de acesso

Os administradores do sistema de controle de acesso integram o Compass nos seguintes estágios, descritos em detalhes posteriormente no capítulo:

1. Configure o hardware do Compass com um único MAC no Editor de dispositivos.
2. Configure campos personalizados para propriedades de titular de cartão específicas da Otis, como andar inicial.
3. Crie perfis de autorização que governem o acesso a destinos de elevador específicos.
4. Atribua perfis de autorização aos titulares de cartão apropriados

– (consulte o guia de operação do ACE para ver esses procedimentos padrão).

20.1 Configuração de um sistema Compass no Editor de dispositivos

Esta seção descreve as etapas para configurar um sistema Otis Compass no Editor de dispositivos.

Caminho da caixa de diálogo

– **Main menu (Menu principal)** > **Configuration (Configuração)** > **Device data (Dados do dispositivo)**
– **Navegador de configuração do BIS** > **Connections (Conexões)** > **Device data (Dados do dispositivo)**

20.1.1 Nível 1: configuração do sistema Compass

Procedimento do Nível 1: configuração do sistema Compass

1. Selecione o MAC desejado na visualização em árvore do Editor de dispositivos
2. Clique com o botão direito e selecione **Novo Otis Compass**. A página de propriedades tem duas guias.
   – **Otis Compass**
   – **Andares**
3. Na guia **Otis Compass**, os parâmetros mais importantes a serem definidos são
   – **Nome** (o nome que deve aparecer na árvore de dispositivos)
   – **Endereço IP do MAC** (o endereço IP de retorno de chamada do sistema Compass, em um cartão de rede dedicado, por meio do qual o sistema Compass se comunica com o MAC).
   OBSERVAÇÃO: este **não** é o endereço IP do MAC propriamente dito.
   – **Divisão** (se, e somente se, divisões estiverem licenciadas e forem usadas na instalação)

Deixe os demais parâmetros com os valores padrão, a não ser que você seja instruído a alterá-los pelo suporte técnico especializado. A tabela a seguir contém uma breve explicação:

Parâmetro	Valor padrão	Descrição
Endereço do grupo MC	234.46.30.7	Endereço IP do grupo multicast
Porta MC para DES/DER remota Porta MC para DES/DER local	48307 47307	Portas multicast
Porta UDP para DES/DER remota	46303 45303	Portas UDP para os dispositivos DES e DER

Parâmetro	Valor padrão	Descrição
Porta UDP para DES/DER local		
Porta UDP para DET remota Porta UDP para DET local	45308 46308	Portas UDP para os dispositivos DET
Multicast time-to-live (TTL)	5 segundos	
Intervalo de batimentos cardíacos	1 segundo	O tempo entre os sinais de batimento cardíaco. Esses sinais mostram para os outros dispositivos que um dispositivo está "vivo", ou seja, funcionando
Número máx. de batimentos cardíacos perdidos	3	O número de batimentos cardíacos que podem ser perdidos antes que um dispositivo seja considerado "morto" (não funcionando mais)
Tempo limite da mensagem	1 segundo	
Tentativas de mensagem	3	

1. Na guia **Andares**, clique em **Alterar intervalo de andares**
2. Insira os números dos andares mais baixo e mais alto a serem atendidos por todos os bancos de elevadores do sistema Otis Compass.
   – O intervalo máximo vai de -127 a +127
3. Clique em (Salvar) para salvar as alterações.

20.1.2 Nível 2: grupos de elevadores, dispositivos DES e DER

Procedimento do Nível 2: configuração dos grupos de elevadores (dispositivos DES/DER)
Introdução
O DES (Servidor de entrada de destino) é o computador que gerencia um grupo de elevadores. Se desejar, dois dispositivos DES físicos com endereços IP separados podem ser combinados em um DES lógico, com capacidade de failover.
O DER (Redirecionador de entrada de destino) conecta grupos de elevadores e permite DETs em um ponto de entrada comum no edifício (por exemplo, o saguão) para aceitar solicitações de destino em qualquer andar do edifício. O DER não é configurado para operar no modo de failover.

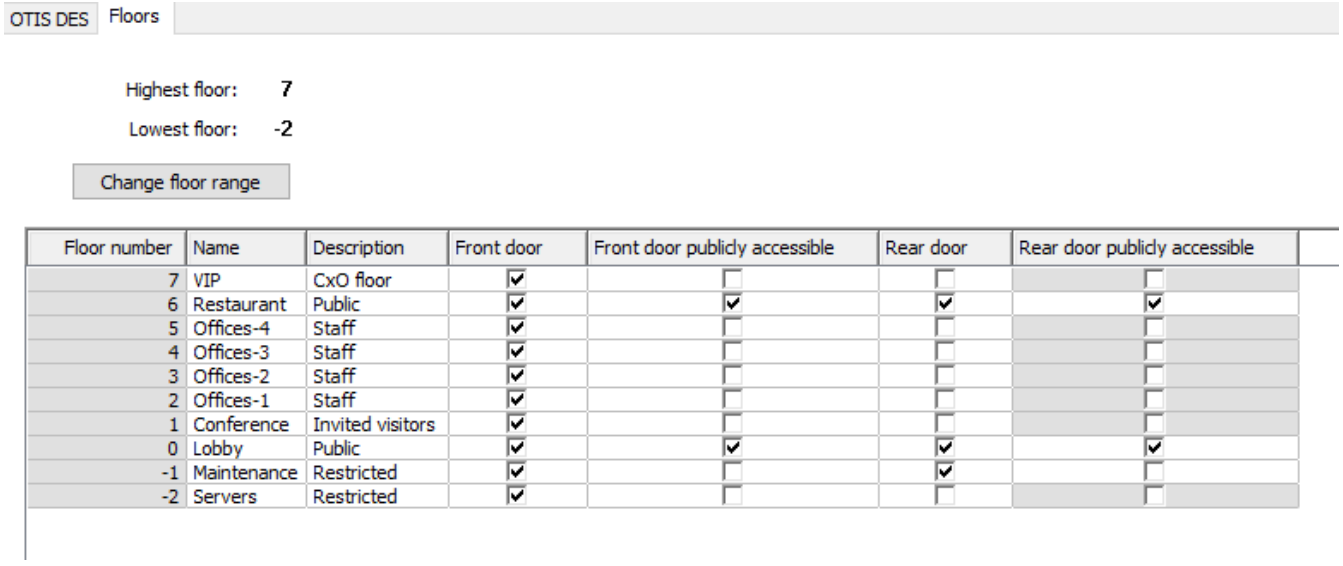
Criação de dispositivos DES na árvore de dispositivos:
1. Selecione o Otis Compass desejado na visualização em árvore do Editor de dispositivos
2. Clique com o botão direito e selecione **Novo Otis DES**. A página de propriedades tem duas guias:
   – **Otis DES**
   – **Andares**
3. Na guia **Otis DES**, defina os seguintes parâmetros:

- **Nome**: o nome que deve aparecer na árvore de dispositivos.
  Use um esquema de nomeação sistemático que fornecerá orientação clara para os configuradores dos dispositivos DES e DET posteriormente no processo de configuração.
- **Descrição:** (opcional) uma descrição em texto livre do dispositivo.
- **Grupo:** um inteiro de 1 a 10**.** Esse número inteiro deve ser exclusivo entre todos os grupos de elevadores (designados pelos dispositivos DES/DER) nesse sistema Otis Compass. Não será possível salvar as edições no dispositivo se o mesmo número de **Grupo** for usado mais de uma vez.
- **1° endereço IP:** o endereço IP desse dispositivo DES.
- **2° endereço IP:** se esse DES tiver uma cópia redundante, insira o endereço IP correspondente aqui.
- **Divisão** (se, e somente se, divisões estiverem licenciadas e forem usadas na instalação)

Na guia **Andares**, os andares definidos para o Nível 1 (o sistema Compass) são apresentados como uma tabela de células editáveis.

Criação de dispositivos DER na árvore de dispositivos:
Os dispositivos DER são criados quase da mesma maneira que os dispositivos DES. A única diferença é que o DER não precisa de nenhum dispositivo de failover e, portanto, não tem um parâmetro para **2° endereço IP**.

Exemplo de grupo de elevadores.
O exemplo abaixo mostra os andares de um grupo de elevadores de 10 andares, com portas dianteiras e traseiras, e o térreo e seis andares de acesso público.



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

1. Na coluna **Porta dianteira**, marque as caixas de seleção de todos os andares em que o elevador oferece o uso da porta dianteira.
2. Marque as caixas de seleção de maneira semelhante para a coluna **Porta traseira**, se aplicável.
3. Para a coluna **Porta dianteira de acesso público**, marque as caixas de seleção dos andares que podem ser acessados por todos os passageiros do elevador sem restrição.
4. Marque as caixas de seleção de maneira semelhante para a coluna **Porta traseira de acesso público**, se aplicável.

5. (opcional) Clique em **Alterar intervalo de andares** nessa guia para restringir ainda mais o intervalo de andares que foi definido no nível do **Otis Compass**.
6. Substitua os nomes padrão nas colunas **Nome** e **Descrição** por alternativas significativas.
7. Clique em  (Salvar) para salvar as alterações.

20.1.3 Nível 3: dispositivos DET

Procedimento do Nível 3: configuração dos terminais (dispositivos DET)
Introdução:
Um DET (também conhecido como DEC - Computador de entrada de destino) lê credenciais físicas ou códigos PIN. Um DET pode estar localizado em um determinado andar fora da porta dianteira ou traseira de um elevador ou dentro da cabine do elevador.

Criação de dispositivos DET na árvore de dispositivos:
1. Selecione o dispositivo Otis DES/DER desejado na visualização em árvore do Editor de dispositivos.
2. Clique com o botão direito e selecione **Novo terminal Otis**.
   – A janela pop-up **Criar terminais Otis** é exibida
3. Insira o número de terminais que deseja configurar nesse DES/DER.
4. Aceite os valores padrão ou insira novos valores iniciais para os quatro octetos do endereço IP.
   – Para qualquer octeto, mas normalmente para o quarto, marque a caixa de seleção **Incremento automático** se desejar que o sistema configure um endereço IP exclusivo para cada terminal aumentando o octeto.
5. Clique em **OK**.
   – O número desejado de dispositivos DET é criado na árvore de dispositivos.
   – Os endereços IP são aumentados conforme determinado na etapa anterior.

Configuração de dispositivos DET
A página de propriedades de cada DET tem duas guias:
– **Terminal Otis**
– **Andares**
1. Na guia **Terminal Otis**, defina os seguintes parâmetros:
   – **Nome:** o nome que deve aparecer na árvore de dispositivos
   – **Descrição** (opcional) uma descrição em texto livre do dispositivo.
   – **Endereço IP** O endereço IP desse dispositivo DET
   – **Modo operacional:** `1..4`
   Determina como o terminal solicita destinos ao passageiro do elevador e transmite as solicitações ao DES/DER para validação. A tabela a seguir fornece detalhes:

Modo op.	Descrição	Comportamento
1	Andar padrão	(O modo operacional padrão) O passageiro apresenta a credencial ou insere um código PIN. Se a credencial ou o PIN for válido e o passageiro não inserir mais nada, o DET solicitará ao DES o andar padrão ou "inicial" do passageiro.

Modo op.	Descrição	Comportamento
		Se o passageiro inserir um andar de destino diferente, o DET solicitará esse destino ao DES.
2	Acesso aos andares autorizados	O passageiro apresenta a credencial ou insere um código PIN e insere um andar de destino. O DET solicita esse destino ao DES. O sistema de controle de acesso concede ou nega o acesso ao destino solicitado.
3	Entrada do andar de destino pelo usuário	O passageiro insere um andar de destino. Se o destino for de acesso público, o DET solicitará o destino ao DES. Caso contrário, o DET pedirá que o passageiro apresente a credencial para validação.
4	Andar padrão ou entrada do andar de destino pelo usuário.	O passageiro apresenta a credencial ou insere um código PIN. Se a credencial ou o PIN for válido, o DET solicitará ao DES o andar padrão ou "inicial" do passageiro. Dentro do período de tempo limite definido, o passageiro pode substituir a seleção do andar padrão e escolher um destino diferente.

- **Registros de auditoria:** marque essa caixa de seleção para registrar a entrada de passageiros nesse terminal para o log de eventos.
- **Código PIN:** marque essa caixa de seleção para permitir o uso de um código PIN de identificação nesse terminal como uma alternativa para as credenciais físicas.
  Observação: use leitores de inscrição do tipo **Diálogo cartão PIN (introduzir)** para inscrever códigos PIN para uso em terminais Otis.
- **Modelos de hora:** marque essa caixa de seleção para permitir que modelos de hora restrinjam as horas em que esse terminal pode ser usado.
- **Divisão** (se, e somente se, divisões estiverem licenciadas e forem usadas na instalação)

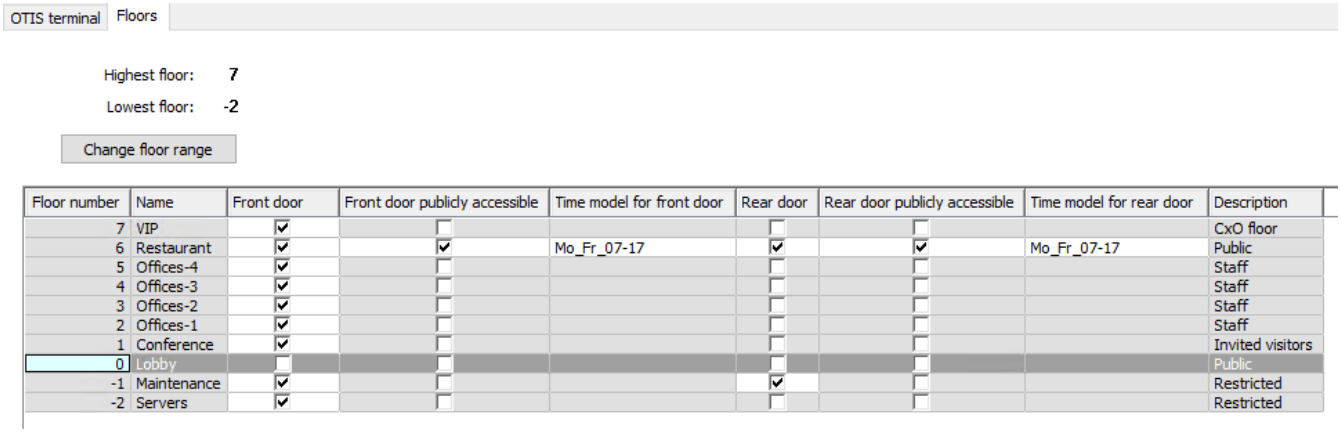
Na guia **Andares** da página de propriedades **Terminal Otis**, os andares definidos para o Nível 2 (o DES/DER) são apresentados como uma tabela de células editáveis.
Observação: o esquema de nomeação definido para o Nível 2 acima deve fornecer orientação suficiente. Caso isso não aconteça, recomendamos salvar o trabalho e voltar ao Nível 2 para concluir o esquema de nomeação.

1. Selecione cada DET que acabou de criar na árvore de dispositivos e abra a guia **Andares**.
   - A tabela **Andares** é exibida
2. Na coluna **Porta dianteira**, marque a caixa de seleção para cada andar que pode ser acessado pelo DET atual.
3. Na coluna **Porta dianteira de acesso público**, marque a caixa de seleção de cada porta dianteira que deve ser de acesso público, isto é, sem autorização explícita.

4. (opcional) Na coluna **Modelo de hora da porta dianteira**, selecione um modelo de hora para restringir o acesso público à porta dianteira nesse andar, se necessário. Por exemplo, o andar do restaurante pode ser acessado apenas em determinados horários do dia.
5. Refaça as etapas anteriores, se necessário, para as colunas **Porta traseira**, **Porta traseira de acesso público** e **Modelo de hora da porta traseira.**
6. Clique em (Salvar) para salvar as alterações.

Exemplo:

O exemplo abaixo mostra os andares de um grupo de elevadores de 10 andares, com esses andares e portas acessados pela porta dianteira do elevador no saguão. O acesso ao andar do restaurante, pelas portas dianteira e traseira do elevador, é limitado por um modelo de hora.



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

20.2 Configuração de campos personalizados para propriedades de titular de cartão específicas da Otis

Introdução

Esta seção descreve como criar campos personalizados onde o operador pode inserir as propriedades específicas da Otis para um titular de cartão, especificamente o destino "inicial" ou padrão do titular do cartão. Esse andar "inicial" deve ser definido por **três coordenadas**:

1. Grupo de elevadores
2. Andar
3. Porta

Ao especificar um andar inicial para um titular de cartão no cliente do sistema de controle de acesso, o operador deve inserir os dados na mesma ordem: grupo de elevadores, andar e porta. Por esse motivo, os três campos personalizados devem estar posicionados em ordem de leitura, de preferência de cima para baixo.

Clique em **OK** para confirmar os lembretes pop-up da criação das três coordenadas.

Defina os três campos personalizados necessários, além das opções especiais da Otis de que você precisa, para exibição na guia **Elevadores** da interface do cliente de controle de acesso.

Para informações gerais sobre como configurar campos personalizados, consulte a ajuda de configuração do ACE/AMS para **Campos personalizados para dados de pessoal**.

Caminho da caixa de diálogo

Menu principal > **Configuração** > **Opções** > **Campos personalizados**

Navegador de configuração do BIS > **Infraestrutura** > **Campos personalizados do ACE**

Procedimento

Na página de propriedade **Campos personalizados**, selecione a guia **Elevadores**.

Primeira coordenada: grupo de elevadores

1. Clique duas vezes em uma célula na guia e clique em **Sim** para criar um novo campo de entrada.
2. Na lista **Tipo de campo**, selecione **Seleção do Otis DES**.
3. No campo **Rótulo**, insira `Elevator Group`
4. Na lista **Exibir em**, selecione `Tab:Elevators`
5. No grupo **Posição**, selecione um local exclusivo na guia **Elevadores**, onde esse campo personalizado deve aparecer.

Segunda coordenada: andar inicial

1. Clique em **Novo campo** para criar um novo campo personalizado
2. Na lista **Tipo de campo**, selecione **Andar inicial**.
3. No campo **Rótulo**, insira `Home floor`
4. Na lista **Exibir em**, selecione `Tab:Elevators`
5. No grupo **Posição**, selecione um local exclusivo na guia **Elevadores**, onde esse campo personalizado deve aparecer. Para facilitar o uso por parte dos operadores do sistema, ela deve estar abaixo da coordenada anterior.

Terceira coordenada: porta de saída

1. Clique em **Novo campo** para criar um novo campo personalizado
2. Na lista **Tipo de campo**, selecione **Porta de saída**.
3. No campo **Rótulo**, insira `Exit door`
4. Na lista **Exibir em**, selecione `Tab:Elevators`
5. No grupo **Posição**, selecione um local exclusivo na guia **Elevadores**, onde esse campo personalizado deve aparecer. Para facilitar o uso por parte dos operadores do sistema, ela deve estar abaixo da coordenada anterior.

Opções especiais da Otis para titulares de cartão

Introdução

Oito opções binárias específicas da Otis são fornecidas de acordo com a funcionalidade padrão da Otis. Se definidas como campos personalizados na guia **Elevadores**, elas aparecem como caixas de seleção na guia **Dados do elevador** dos titulares de cartão na caixa de diálogo **Pessoas** (Menu principal > **Dados pessoais** > **Pessoas**). Elas podem ser marcadas e desmarcadas pelos operadores do sistema de controle de acesso.

Configure essas opções somente conforme instruído pelo representante da Otis.

Procedimento

1. Clique em **Novo campo** para criar um novo campo personalizado
2. Na lista **Tipo de campo**, selecione **Opções da Otis**.
3. No campo **Rótulo**, insira seu próprio rótulo, por exemplo, `Otis flag 1` ou de acordo com a documentação da Otis.
4. Na lista **Exibir em**, selecione `Tab:Elevators`
5. Na lista **Tipo de função**, selecione uma das opções de `OTIS option 1` a `OTIS option 8`
6. No grupo **Posição**, selecione um local exclusivo na guia **Elevadores**, onde essa caixa de seleção deve aparecer.
7. Clique em  (Salvar) para salvar as alterações.

20.3 Criação e configuração de autorizações para elevadores Otis

Introdução

Esta seção descreve como incluir direitos de acesso para grupos de elevadores Otis, andares e portas de elevador em uma **Autorização**.

Autorizações são atribuídas diretamente a titulares de cartão ou, o mais comum, combinadas com outras autorizações em **Perfis de acesso**, que são atribuídos aos titulares de cartão.

Pré-requisitos

Um sistema Otis Compass foi definido em um MAC no editor de dispositivos. Ele é completo com um grupo de elevadores (representado pelo DES) e por pares de andar + porta (representados pelos DETs).

Caminho da caixa de diálogo

Menu principal > **Dados do sistema** > **Autorizações**

Procedimento

1. No campo **Nome da autorização**, insira o nome de uma autorização existente ou clique em  (Novo) para criar uma nova autorização.
2. Na lista **MAC**, selecione o nome do MAC em que o sistema Otis Compass foi criado.
3. Clique na guia **Elevador Otis**
4. Na lista **Elevadores Otis**, selecione o DES/DER do grupo de elevadores que deseja adicionar à autorização (uma autorização pode conter somente um DES/DER).
   – Os andares do grupo de elevadores selecionado é exibido no painel **Andares**.
5. Nas colunas **Porta dianteira** e **Porta traseira** do painel **Andares**, selecione as portas nos andares que devem ser incluídos nessa autorização.
   – Os andares e portas que **não** foram selecionados para esse grupo de elevadores quando definido no editor de dispositivos serão desativados e não poderão ser selecionados nessa caixa de diálogo.
6. Como alternativa, clique nos botões **Atribuir todos os andares** e **Remover todos os andares** para marcar e desmarcar todos os andares e portas de uma vez.
7. Clique em  (**Salvar**) para salvar a autorização.

21 Configuração do IDEMIA Universal BioBridge

Esta seção descreve a configuração dos dispositivos biométricos IDEMIA para trabalhar com os sistemas de controle de acesso da Bosch por meio de **MorphoManager** e **BioBridge**.
As subseções abrangem as tarefas de configuração necessárias nestas áreas:

- O sistema de controle de acesso da Bosch
- MorphoManager
- O cliente de inscrição BioBridge no MorphoManager
- Adaptações para vários formatos e tecnologias de cartão

21.1 Configuração do BioBridge no sistema de controle de acesso da Bosch

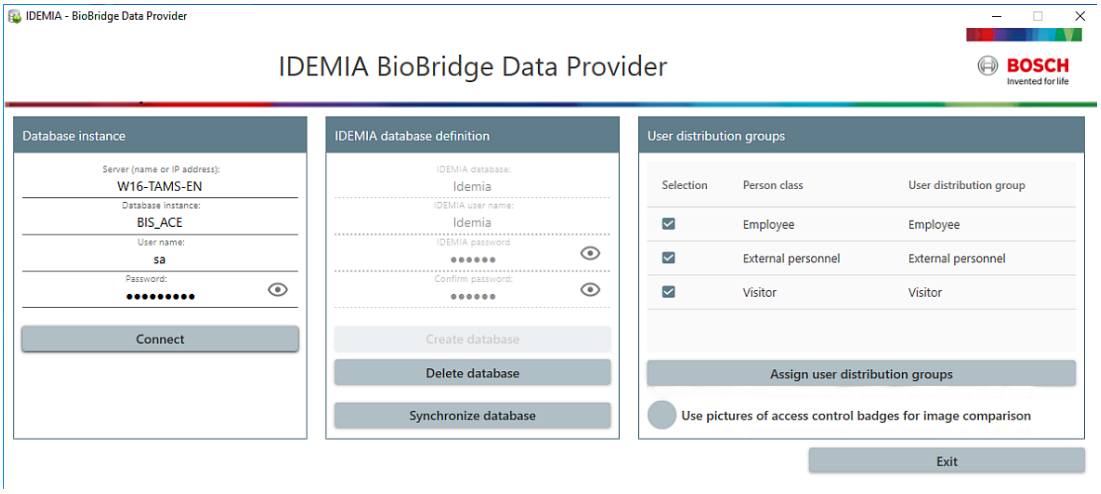
As etapas a seguir são realizadas no ACS para criar o banco de dados que vincula os dispositivos biométricos IDEMIA ao sistema de controle de acesso da Bosch. O banco de dados mapeia as seguintes entidades de banco de dados uma para a outra:

- **Classe de pessoa** (Bosch) e
- **Grupo de distribuição de usuários** (IDEMIA).

Caminho da caixa de diálogo

- **Navegador de configuração do BIS** > **Ferramentas** > **Banco de dados IDEMIA de configuração do ACE**
- Menu principal do AMS > **Configuração** > **Ferramentas** > **Banco de dados IDEMIA de configuração**

1. Clique em **Banco de dados IDEMIA de configuração**
   A caixa de diálogo **Provedor de dados IDEMIA BioBridge** é exibida.



2. No painel **Instância do banco de dados**, insira as seguintes informações:

- **Servidor**: o nome do host ou endereço IP do computador em que a instância do banco de dados SQL Server do ACS está em execução. Pode ser o nome do host local, caso o SQL Server esteja em execução no local.
- **Instância do banco de dados**: a instância do ACS (padrão: `ACE`).
- **Nome de usuário**: o nome da conta do administrador da instância do banco de dados do ACS (padrão: `sa`)
- **Senha**: a senha da conta do administrador, conforme configurada durante a instalação do AMS

No painel de definição do banco de dados IDEMIA

Os dois primeiros campos são somente leitura:

– **Banco de dados IDEMIA**: o nome do banco de dados que une os dados da Bosch e da IDEMIA.
– **Nome de usuário IDEMIA**: o nome do usuário do banco de dados em cujo nome o software executa comandos no banco de dados.

1. Insira e confirme uma senha forte para **Nome de usuário IDEMIA**.
2. Anote a senha com cuidado. Ela será necessária em futuras tarefas de configuração e, caso seja perdida, não será possível restaurá-la.
3. Clique em **Criar banco de dados**.
   Uma caixa de mensagem confirmará se a criação foi bem-sucedida. Clique em **OK**
4. Clique em **Conectar** para testar a conexão do banco de dados.
5. Quando os testes forem concluídos, clique em **Sair** para fechar a caixa de diálogo.

No painel Grupos de distribuição de usuários

Os grupos de distribuição de usuários são objetos do MorphoManager que mapeiam usuários (titulares de credencial) para grupos de leitores biométricos ou clientes do MorphoManager. Nós os mapeamos para as **Classe da pessoa** dos sistemas de controle de acesso da Bosch.

1. Na coluna Selecionar, marque a caixa de seleção de cada **Classe da pessoa** do AMS usada por sua instalação.
2. Para cada linha selecionada, copie o nome da classe de pessoa para a célula correspondente na coluna **Grupo de distribuição de usuários**.

– Observe que os nomes da **Classe da pessoa** e do **Grupo de distribuição de usuários** devem corresponder exatamente.

3. Quando o mapeamento terminar, clique em **Atribuir grupos de distribuição de usuários**.

Fornecimento de fotos de identidade para reconhecimento facial VisionPass

para permitir que os leitores IDEMIA realizem o reconhecimento facial VisionPass usando fotos de identidade dos titulares de cartão do banco de dados AMS:

- Clique em **Usar fotos de crachás de controle de acesso para comparação de imagens** e confirme na janela pop-up.
  A janela **Provedor de dados IDEMIA BioBridge** confirma que a sincronização está em andamento.
  Dependendo da quantidade de dados de imagem envolvidos, a transferência pode levar um tempo considerável.

21.2 Configuração do BioBridge no MorphoManager

Pré-requisitos

O MorphoManager é instalado em um servidor do MorphoManager em sua rede. Consulte o guia de instalação e a ajuda on-line do próprio MorphoManager.

Visão geral

Para usar a interface do BioBridge entre os sistemas de controle de acesso da Bosch e o MorphoManager, configure o seguinte no MorphoManager:

– **Configuração do dispositivo biométrico**
– **Dispositivo biométrico**
– **Perfis de Wiegand**
– **Configuração do usuário**
– **Grupo de distribuição de usuários**

– **Modo de autenticação do usuário**
– **Configuração do sistema**

Além disso, é necessário configurar o protocolo Open Database Connectivity (ODBC) para comunicação entre o MorphoManager BioBridge e o banco de dados compartilhado com AMS. Todas essas tarefas de configuração são descritas nas próximas seções.

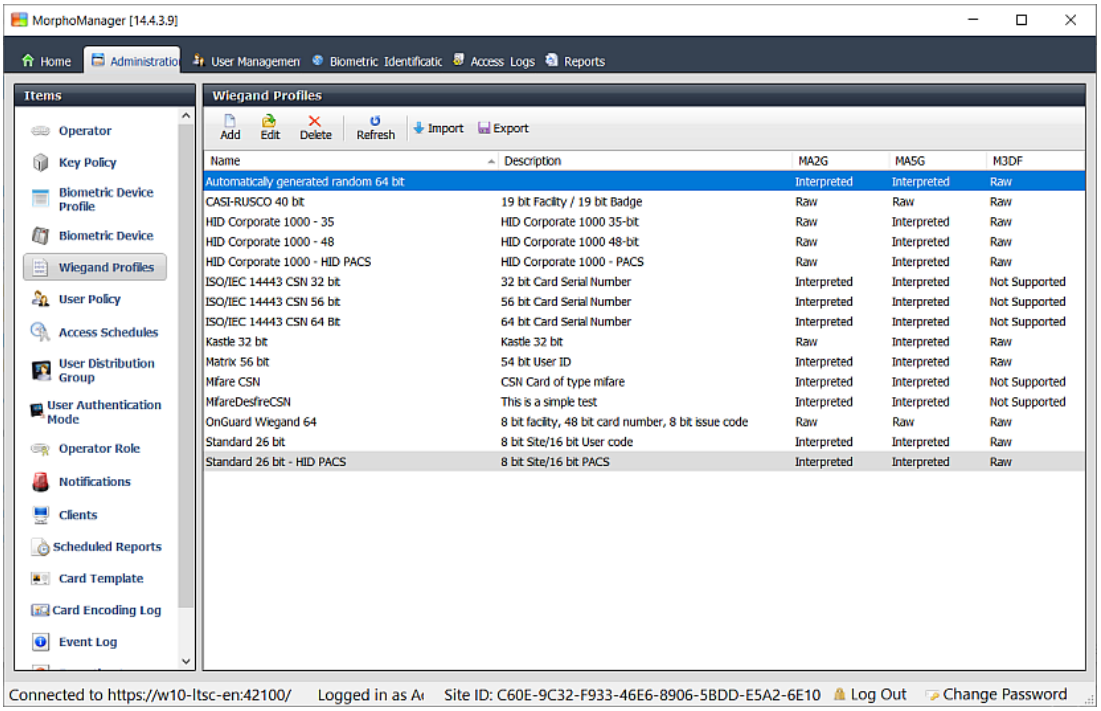
21.2.1 Perfis de Wiegand

Aviso!
Apesar do nome, os perfis de Wiegand se aplicam a todos os tipos de leitor, incluindo os leitores OSDP.

Os perfis de Wiegand definem quais informações são enviadas pelos dispositivos biométricos pela interface de saída de Wiegand quando um usuário é identificado. Essas informações vão para o sistema de controle de acesso da Bosch, que as utiliza para tomar uma decisão de acesso.

Procedimento:

1. No MorphoManager, navegue até **Administração** > **Perfil de Wiegand**.
2. Selecione um dos perfis de Wiegand predefinidos ou clique em **Adicionar** para criar um perfil personalizado.
   Em geral, todos os perfis CSN são adequados para uso com os sistemas de controle de acesso da Bosch, além dos perfis de 26 bits padrão. Se o instalador tiver fornecido um perfil para o seu sistema, clique em **Importar** para localizar e importar o arquivo fornecido e selecione-o na lista.



3. Na caixa de diálogo, insira as informações exigidas pelo sistema de controle de acesso dos dispositivos biométricos.

4. Anote o nome do perfil de Wiegand selecionado ou criado aqui. Ele deve ser mencionado nas definições da **Configuração do usuário** e **Configuração do dispositivo biométrico** do MorphoManager.

21.2.2 Configuração do dispositivo biométrico

A configuração do dispositivo biométrico define configurações e parâmetros comuns para um ou mais dispositivos biométricos. Ao adicionar dispositivos biométricos ao sistema posteriormente na seção **Dispositivo biométrico** de **Administração**, você aplica uma configuração a eles.
O procedimento a seguir presume que você está implantando leitores biométricos da IDEMIA com tecnologia adicional de leitura de cartão.

Procedimento:

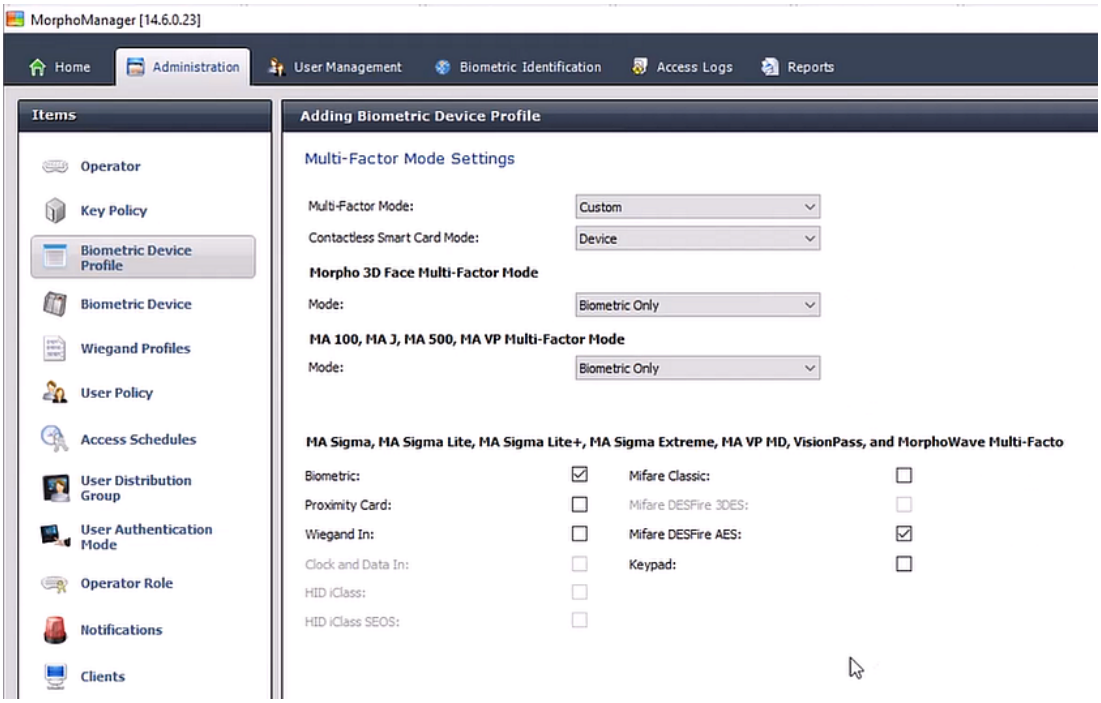
1. No MorphoManager, navegue até **Administração** > **Configuração do dispositivo biométrico**.
2. Clique em **Adicionar** para criar uma configuração de dispositivo biométrico.
3. Na próxima tela, insira um nome para o perfil e uma descrição (opcional). Se você não usar o campo de descrição, recomendamos um nome que descreva o tipo e os modos de identificação (biometria e/ou cartão) do grupo de leitores.
4. Clique em **Próximo** até chegar a **Configurações de dispositivo biométrico**

– Selecione o perfil de Wiegand criado anteriormente para a instalação.

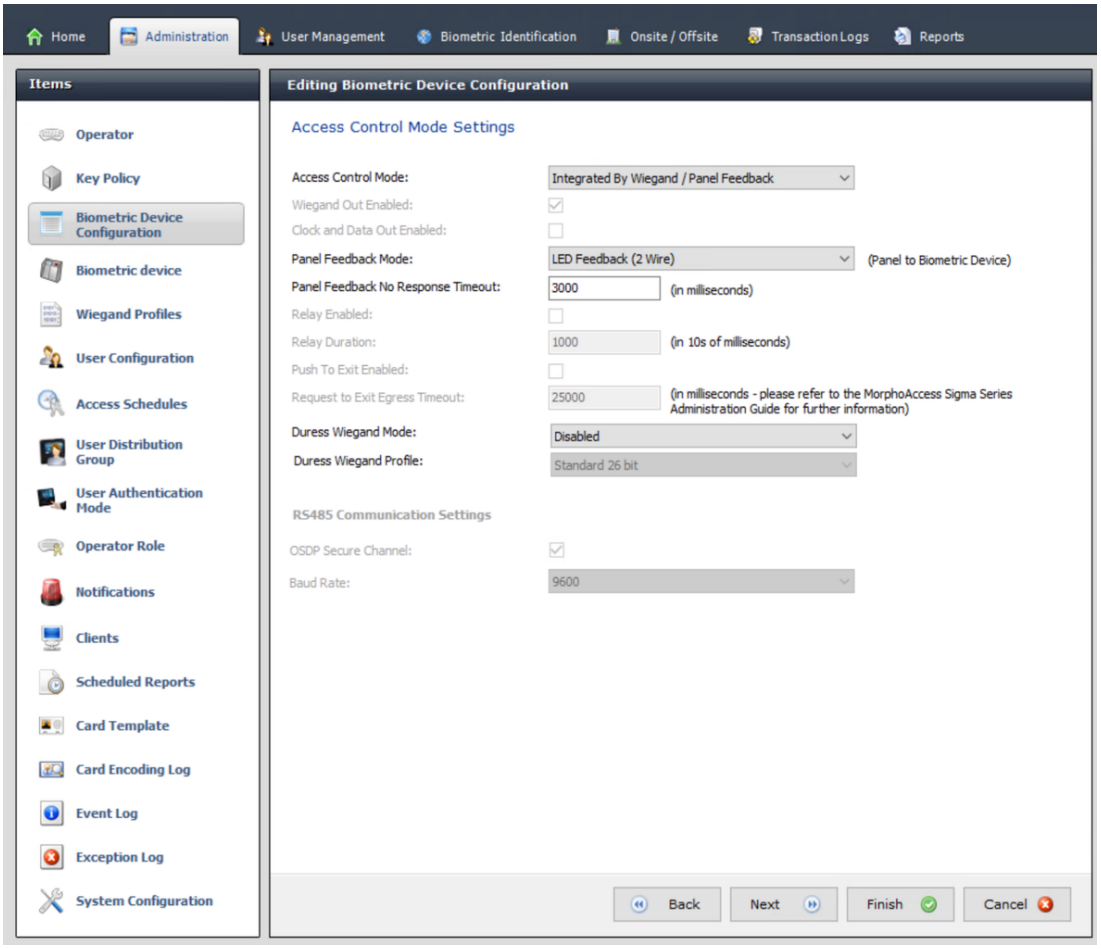
5. Clique em **Próximo** até chegar a **Configurações de modo multifatorial**

– Em **Modo multifatorial**: isto é, uma combinação de capacidade biométrica e de leitura de cartão de acesso, selecione `Custom` na lista.

– Em **Modo de cartão inteligente sem contato**: selecione `Device` na lista.



6. Clique em **Próximo** até chegar à página **Configurações de modo de controle de acesso**.



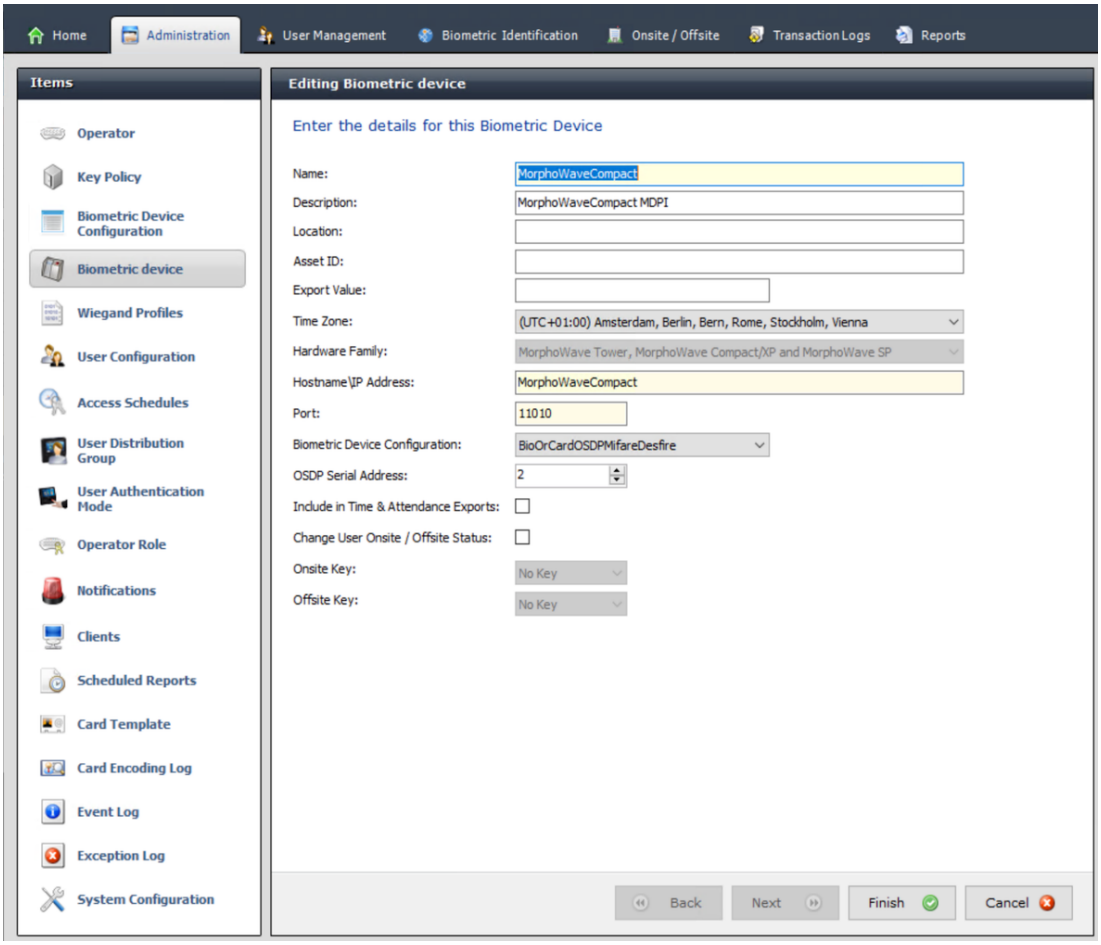
Nesse momento, os procedimentos para AMCs Wiegand e OSDP divergem. Siga o procedimento abaixo que corresponde ao tipo de controlador AMC:

Para AMCs Wiegand

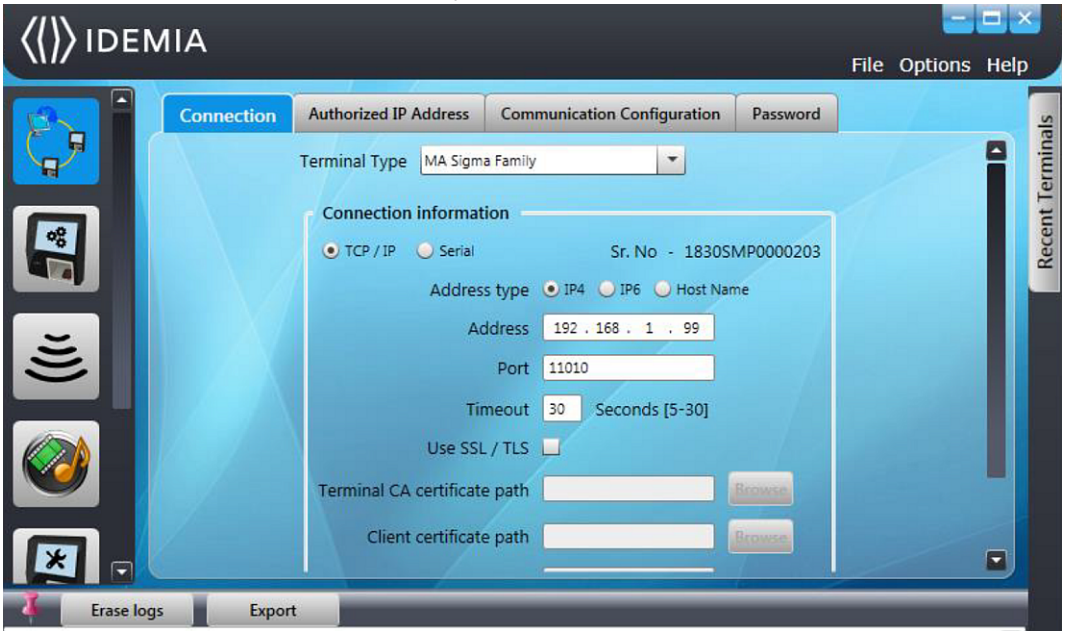
1. Defina **Modo de controle de acesso** como `Integrated by Wiegand`
2. Defina **Modo de feedback de painel** como `LED Feedback (2 wire)`
3. Clique em **Concluir**

Para AMCs OSDP

1. Defina **Modo de controle de acesso** como `Integrated by OSDP`
2. Defina **Modo de feedback de painel** como `LED Feedback (2 wire)`
3. Marque a caixa de seleção **OSDP Secure Channel**
4. Defina a taxa de baud `9600`
5. Navegue até **Administração** > **Dispositivo biométrico**
6. No painel **Edição de dispositivo biométrico**, selecione seu dispositivo biométrico IDEMIA e insira o **Endereço serial OSDP**



7. Clique em **Concluir** para sair do MorphoManager.
8. Inicie o programa **MorphoBioToolBox (MBTB)** separado
9. Na guia **Conexão**, defina o endereço IP do leitor biométrico



1. No programa MorphoBioToolBox, vá até **Rede e comunicação segura** > guia: **Configuração de comunicação**

1. Defina as seguintes configurações no painel **Configurações de série**:
– **Tipo**: `Half Duplex`
– **Taxa** de transmissão: `9600`
– **Bits de dados**: `8`
– **Bits de parada**: `1`
– **Bit de paridade**: `No parity`
– **Identificador de terminal**: `0`.
2. Se você alterar algum valor, clique em **Gravar** para enviar as alterações ao dispositivo.

Solução de problemas das chaves OSDP

Se você não puder estabelecer uma conexão segura com o leitor OSDP, tente redefinir a chave básica da seguinte forma:

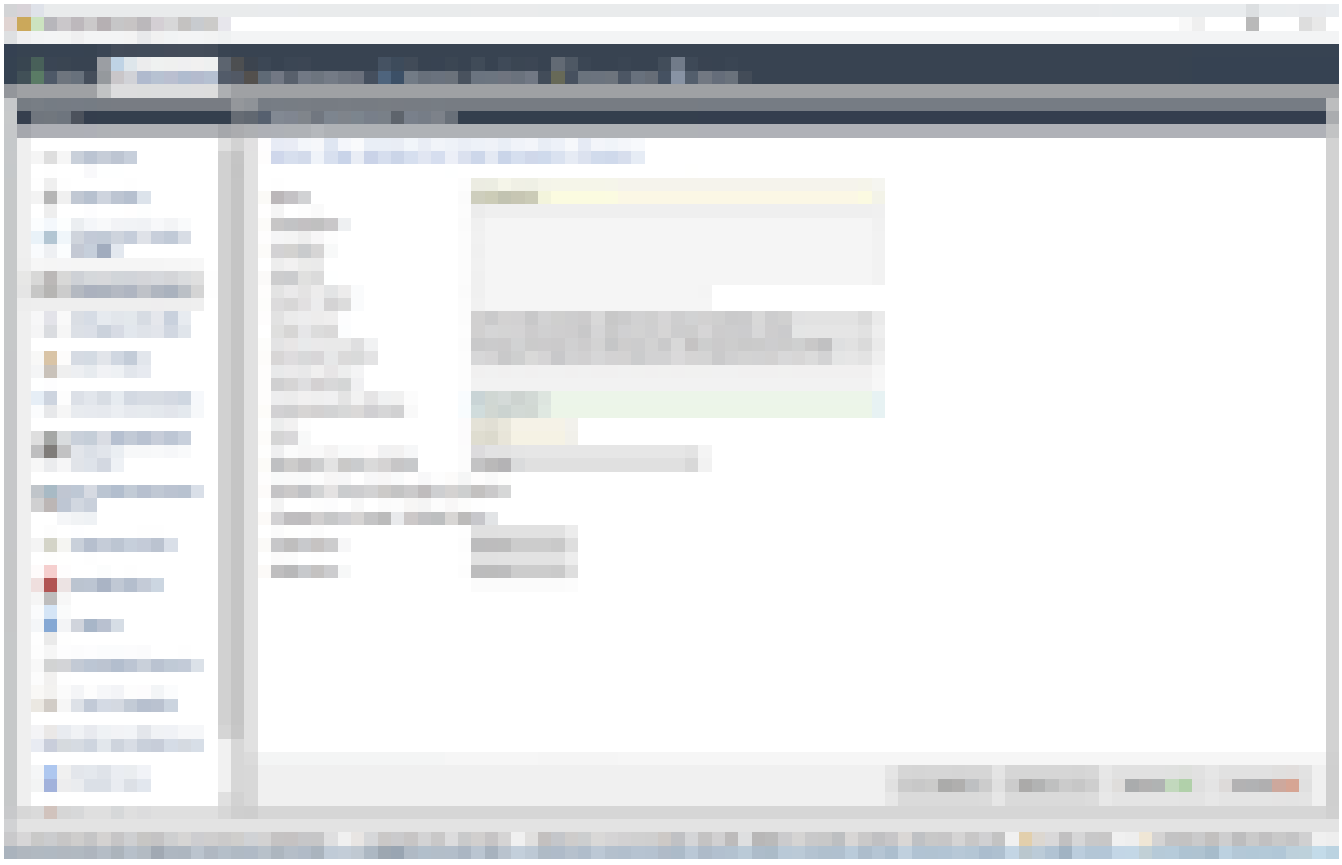
1. No programa MorphoBioToolBox, vá até **Configurações de dispositivo** > **Redefinir**
2. Selecione a chave OSDP básica
3. Clique em **Redefinir chaves criptográficas**
4. Saia do MorphoBioToolBox

21.2.3 Dispositivo biométrico

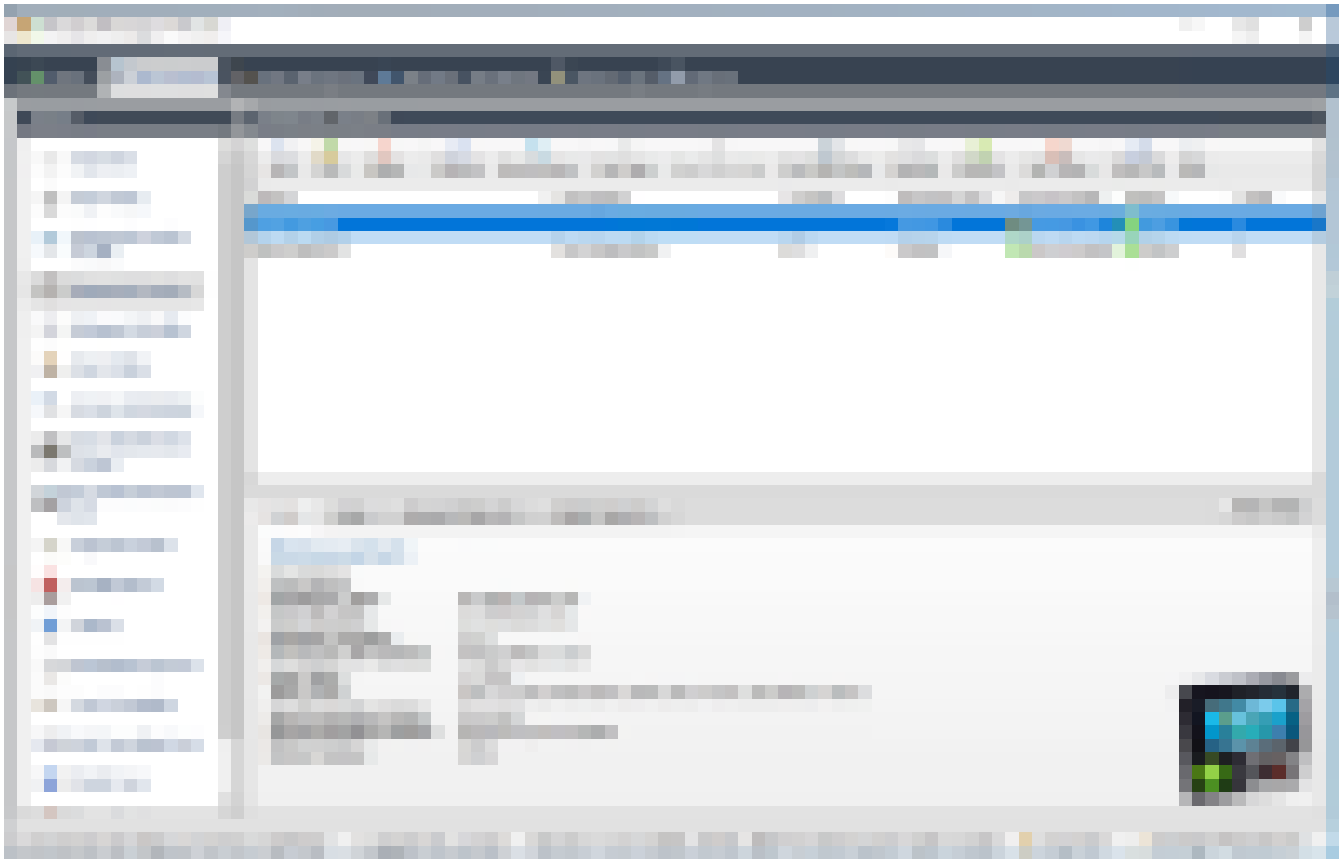
Os dispositivos biométricos testam se as credenciais biométricas lidas correspondem aos registros no banco de dados. Eles também mantêm um registro de todo evento de uso.

Procedimento:

1. No MorphoManager, navegue até **Administração** > **Dispositivo biométrico**.
2. Clique em **Adicionar** para criar um dispositivo biométrico.
3. Insira pelo menos os detalhes básicos do dispositivo:
– (na lista) **Família de hardware**
– **Nome do host/endereço IP**
– (na lista) a **Configuração do dispositivo biométrico** definida anteriormente



4. Clique em **Concluir**
   A caixa de diálogo Dispositivo biométrico agora lista os dispositivos já configurados:



21.2.4 Configuração do usuário

Configurações de usuário são pacotes de direitos de acesso que você atribui aos usuários com os mesmos requisitos de acesso, isto é, quais dispositivos biométricos eles podem usar em quais modos e em quais horários.

Procedimento:

1. No MorphoManager, navegue até **Administração** > **Configuração do usuário**
2. Clique em **Adicionar** para criar uma configuração de usuário.

3. Na caixa de diálogo **Adicionando política de usuário**, insira o seguinte:

– Um **Nome** para a política de usuário e uma descrição (opcional)
– O **Modo de acesso** `Per User`
– Uma **Programação de acesso** que governa os dias e horários em que o acesso é permitido
– O mesmo **Perfil de Wiegand** definido e usado para o **Perfil do dispositivo biométrico**.
– Um **Modo de autenticação do usuário**, dependendo de como os dispositivos serão usados (por impressão digital, dedo, rosto, cartões etc.). Consulte o Manual do usuário do MorphoManager para obter detalhes.

4. Clique em **Concluir**

A política de usuário padrão terá um modo de autenticação do usuário de `(1: Many)`. Para usar outros modos de autenticação, crie políticas de usuário adicionais. Consulte o Manual do usuário do MorphoManager para obter mais detalhes sobre todas as diversas propriedade que podem ser atribuídas a uma política do usuário.

21.2.5 Grupos de distribuição de usuários

Os grupos de distribuição de usuários mapeiam usuários para grupos de leitores biométricos ou clientes do MorphoManager.

Pré-requisitos:

Os usuários do grupo de distribuição devem ter uma política de usuário em que **Modo de acesso** seja definido como `Per User`.

Cada grupo de distribuição de usuários deve ser mapeado para pelo menos uma classe de pessoa no AMS. Portanto, crie pelo menos um grupo de distribuição de usuários para cada classe de pessoa utilizada.

Procedimento:

1. No MorphoManager, navegue até **Administração** > **Grupo de distribuição de usuários**.
2. Clique em **Adicionar** para criar um novo grupo de distribuição de usuários.

3. Clique em **Próximo** até chegar à página **Selecionar dispositivos biométricos**.
4. Marque as caixas de seleção dos dispositivos biométricos que as pessoas desse grupo de distribuição de usuários devem usar.

5. Clique em **Concluir**

21.2.6 Configuração do ODBC para BioBridge

Introdução

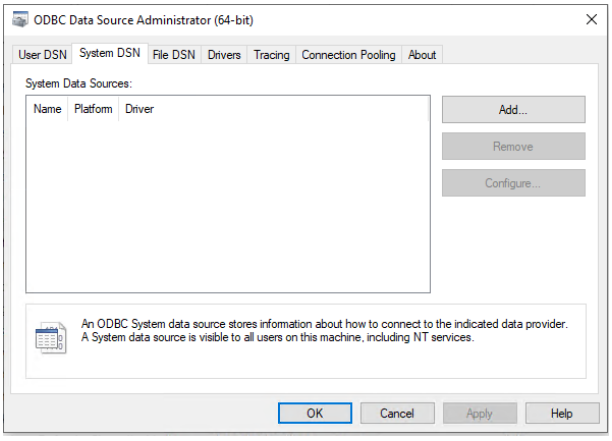
Open Database Connectivity (ODBC) é um pré-requisito para uso do MorphoManager BioBridge. O ODBC é uma interface de programação padrão para acessar bancos de dados diferentes. O driver recomendado é `OdbCDriver17SQLServer`

- Para o BIS, o driver está localizado na mídia de instalação do BIS em `BIS\3rd_Party\OdbCDriver17SQLServer`
- Para o AMS, baixe o driver em `www.microsoft.com`

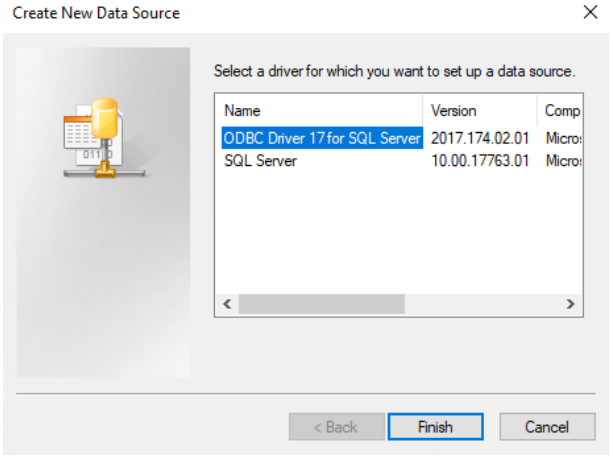
Criação de uma fonte de dados

Criação de um nome de fonte de dados (DSN) para ODBC

1. No Painel de controle do Windows, selecione **Ferramentas administrativas**.
2. Selecione `ODBC Data Sources (64-bit)` na lista.
3. Selecione a guia **DSN do sistema**.



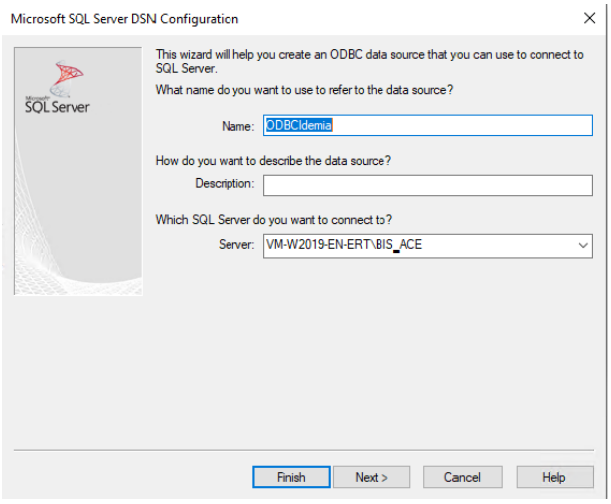
4. Clique em **Adicionar** para selecionar um driver.
5. Selecione `ODBC Driver 17 for SQL Server` como driver e clique em **Concluir**.



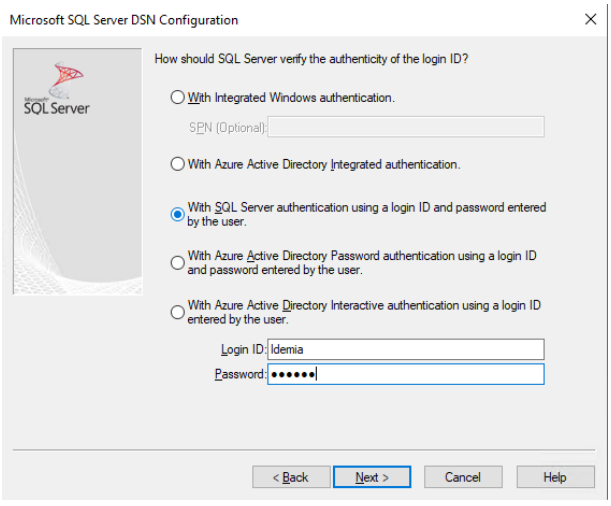
6. Insira estes detalhes para a fonte de dados.

- **Nome**: um nome para a fonte de dados

– **Descrição** (opcional)
– **Servidor**: o nome do computador em que o banco de dados AMS é instalado e o nome do banco de dados (padrão: <MyACS server>\ACE)



7. Clique em **Próximo >**
   Uma caixa de diálogo aparece para coletar informações de login



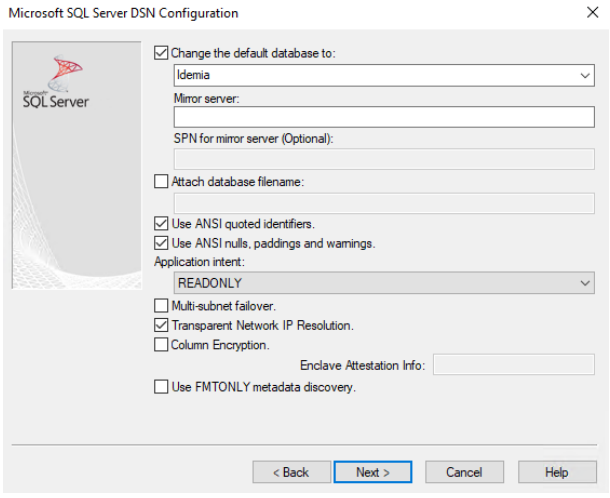
8. Selecione **Com autenticação do SQL Server usando um ID de login...**
9. Insira as seguintes informações:

– **ID de login**: o nome de usuário definido para o usuário do banco de dados IDEMIA conforme configurado no ACS. É sempre `Idemia`.
– **Senha**: a senha que foi definida para o usuário do banco de dados IDEMIA, quando configurado no ACS.

10. Clique em **Next (Próximo)>**
11. Na próxima caixa de diálogo, marque as caixas de seleção:

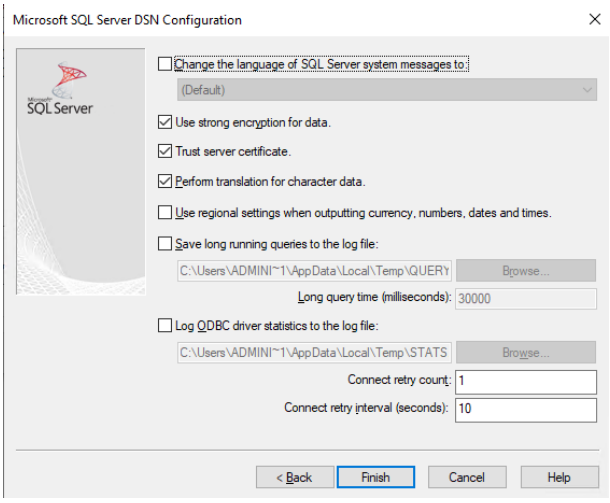
– **Altere o banco de dados padrão para:** e selecione `Idemia`
– **Usar identificadores ANSI entre aspas**
– **Usar valores novos ANSI, preenchimentos e avisos**
– **Resolução IP de rede transparente**

12. Defina **Intenção do aplicativo** como `READONLY`

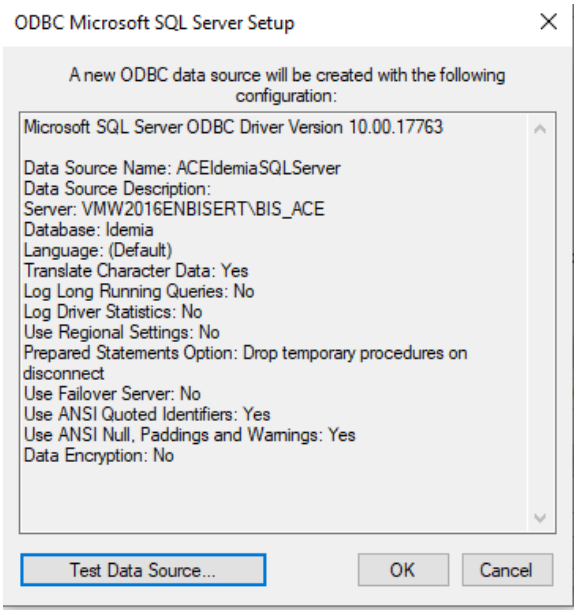


13. Clique em **Next (Próximo)>**
14. Na próxima caixa de diálogo, marque as caixas de seleção

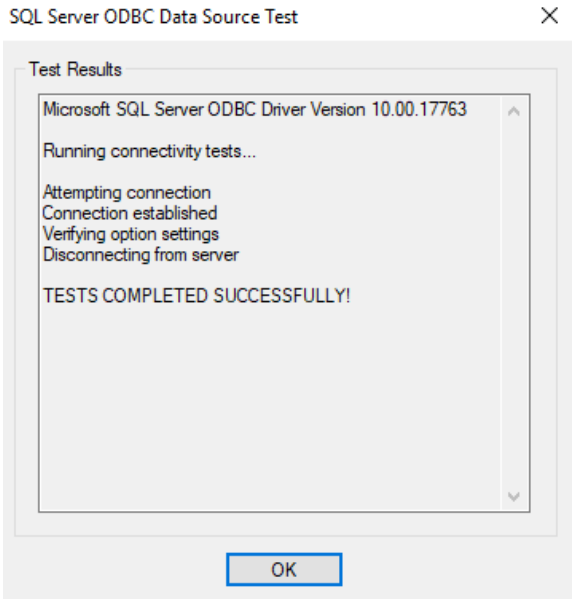
– **Usar criptografia forte para dados**
– **Realizar tradução de dados de caractere**
– **Certificado do servidor confiável**



15. Clique em **Concluir**
16. Na próxima caixa de diálogo, revise os dados de resumo



17. Clique em **Testar fonte de dados...** e verifique se os testes são concluídos com sucesso



18. Salve todas as alterações e saia do assistente de configuração ODBC.

21.2.7 Configuração do sistema BioBridge

Esta seção descreve as configurações restantes necessárias para os sistemas de controle de acesso usarem a interface BioBridge.

Pré-requisito

ODBC é configurado para BioBridge. Consulte *Configuração do ODBC para BioBridge, página 167*

Procedimento:

1. No MorphoManager, navegue até **Administração** > **Configuração do sistema**.
2. Selecione a guia **BioBridge**

3. Na lista suspensa **Sistema**, selecione `MorphoManager Universal BioBridge`
4. Clique em **Configurar**
   Uma caixa de diálogo pop-up é exibida.

Na janela pop-up

1. Na lista suspensa **Provedor**, selecione `ODBC`
2. Insira o DSN (nome da fonte de dados) na configuração de ODBC.
3. Em **Detalhes de login**, insira o nome de usuário (`Idemia`) e a senha conforme definido na configuração de ODBC.
4. Clique em **OK** para voltar para a caixa de diálogo **Configuração do sistema**.

Na caixa de diálogo **Configuração do sistema**

1. Em **Perfil de Wiegand**: selecione na lista o perfil de Wiegand definido anteriormente.

Modo de agrupamento:

Essa configuração determina como o MorphoManager deve mapear os usuários do MM Universal BioBridge para os grupos de distribuição de usuários do MorphoManager. Selecione uma das seguintes opções:

- **Automático**: esse modo associará automaticamente os **Grupos de nível de acesso** do MM Universal BioBridge aos **Grupos de distribuição de usuários** do MorphoManager, se eles tiverem a mesma convenção de nomeação.
- **Manual**: se os **Grupos de nível de acesso** do MM Universal BioBridge e os **Grupos de distribuição de usuários** do MorphoManager não forem iguais, você poderá realizar o mapeamento manualmente em **Mapeamentos de política de usuário**.

Outras configurações

Na maioria dos casos, as seguintes configurações podem ficar com os valores padrão:

Ativar política de usuário forçada	Quando selecionado, todos os usuários inscritos no cliente de inscrição do BioBridge receberão a política de usuário que estiver selecionada na lista adjacente.

	Se você marcar essa caixa de seleção, sempre use a política de usuário chamada `Per User`
Hora de início e hora de término de sincronização de usuários	O mecanismo de sincronização de usuários só poderá ser executado entre esses dois horários.
Atraso entre cada sincronização de usuários	O intervalo de tempo entre sincronizações de usuários. O aumento do atraso economizará recursos do sistema, mas aumentará o tempo de atualização de todos os usuários.
Permitir sincronização de usuários enquanto o cache de usuário é atualizado	Quando ativado, o mecanismo de sincronização de usuários será executado paralelamente à atualização do cache de usuário. É um processo que consome muitos recursos do sistema. É recomendado desativar essa configuração ao usar bancos de dados grandes.
Programação de atualização do cache de usuário	Dias e horas em que o cache de usuário pode ser atualizado. Para ter o maior nível de precisão, isso deve ser possível sempre. No entanto, para o desempenho de sistemas com bancos de dados grandes, algum comprometimento é necessário.

Mapeamentos de grupo de distribuição de usuários

– Na tabela de mapeamentos, verifique se todos os **Grupos** (**Classes de pessoal** definidas no ACS) são mapeados para **Grupos de distribuição de usuários** (definidos no MorphoManager).

21.3 Configuração do cliente de inscrição do BioBridge

Introdução

O cliente de inscrição do BioBridge é um computador em que é possível criar registros biométricos para usuários do sistema de controle de acesso. A configuração de um cliente de inscrição do BioBridge tem três partes:

– Adição de um operador de inscrição ao MorphoManager
– Configuração de computadores cliente do MorphoManager para tarefas de inscrição
– Teste do cliente de inscrição

Pré-requisitos

O MorphoManager BioBridge é instalado em cada estação de trabalho AMS da qual você realiza a inscrição biométrica de sistemas IDEMIA.

21.3.1 Adição de um operador de inscrição ao MorphoManager

Procedimento

Siga as instruções do guia de instalação do cliente do MorphoManager.

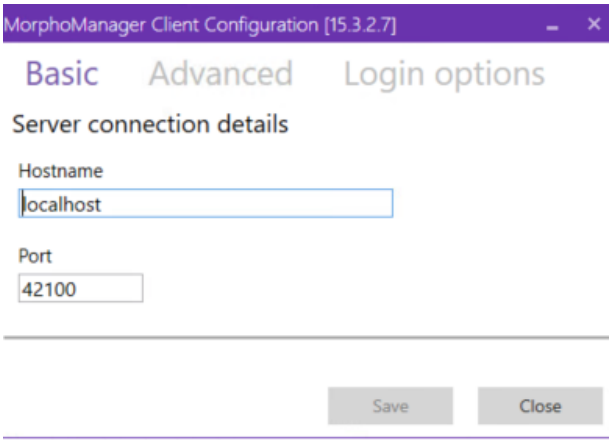
Observação: por motivos de segurança, as contas de usuário do Active Directory são recomendadas.

21.3.2 Configuração de computadores cliente do MorphoManager para tarefas de inscrição

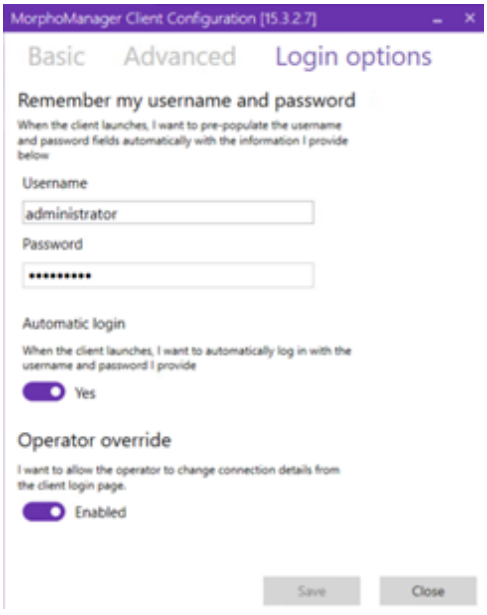
Realize esse procedimento em cada computador que deseja usar para inscrição biométrica.

Procedimento

1. No diretório de instalação do MorphoManager (padrão: `C:\Program,Files(x86)\Morpho\MorphoManager\Client\`) execute o arquivo `ID1.ECP4.MorphoManager.AdvancedClientConfig.exe` como administrador



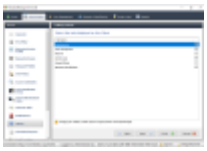
2. Na guia **Básico**, insira o nome do host do servidor do Morpho em **Nome do host**.
3. Para instalações seguras, use o Active Directory ou nome de usuário nativo e senha, de acordo com a documentação do Morpho.
4. Como alternativa [NÃO recomendado para instalações altamente seguras], na guia **Opções de login**



- Insira o nome de usuário e a senha inseridos para o operador de inscrição na seção anterior
- Defina a opção **Login automático** como `Yes`

1. No diretório de instalação do MorphoManager (padrão: `C:\Program Files(x86)\Morpho\MorphoManager\Client\`)
   execute o arquivo `Start ID1.ECP4.MorphoManager.Client.exe` como administrador
2. Navegue até **Administração** > **Clientes**
3. Selecione um computador cliente
4. Clique em **Editar**

5. Insira o nome do cliente de inscrição desejado e, opcionalmente, o local e uma descrição
6. Clique em **Next (Próximo)**



7. Marque as caixas de seleção das guias que deseja exibir no cliente de inscrição:

– **Administração,**
– **Gerenciamento de usuários,**
– **Relatórios,**
– **Logs de acesso,**
– **Identificação biométrica**

8. Clique em **Next (Próximo)**

9. Em **Câmera:**, selecione `No camera` na lista
10. Clique em **Next (Próximo)**

11. Em **Política de chave**, selecione `Default` na lista
12. Clique em **Next (Próximo)**

13. Selecione o leitor de inscrição biométrico que deseja usar na estação de trabalho de inscrição
14. Clique em **Concluir**
15. Feche o aplicativo MorphoManager

Consulte

– *Configuração do cliente de inscrição do BioBridge, página 172*

21.3.3 Teste do cliente de inscrição

1. No diretório de instalação do MorphoManager (padrão: `C:\Program,Files(x86)\Morpho\MorphoManager\Client\`)
   execute o arquivo `ID1.ECP4.MorphoManager.BioBridgeEnrollmentClient.exe`

1. Verifique se é possível acessar a tela de inscrição sem precisar inserir o nome de usuário e a senha do operador de inscrição.

21.4 Suporte para diferentes formatos e tecnologias de cartão

Para que o MAC interprete os cartões de acesso corretamente, verifique se os perfis de Wiegand definidos no MorphoManager incluem o formato desses cartões de acesso:

Card Family	HID Prox	HID Class	HID iClass Seos	MIFARE Classic	MIFARE DESFire EV0	MIFARE DESFire EV1
Card Variant	Prox	2k/2 16k/2 16k/16 32k(16k/2+16k/1) 32k(16k/16+16k/1)	Seos	1K 4-byte NUID 1k 7-byte UID 4k 4-byte NUID 4k 7byte UID	2k 4k 8k	2k 4k 8k
HID OMNIKEY 5427CK	✓	✓	✓	✓	✓	✓
HID OMNIKEY 5427G2	✓	✓	✓	✓	✓	✓

Figura 21.1: Cartões IDEMIA compatíveis

Procedimento geral

1. No MorphoManager, navegue até **Administração** > **Perfil de Wiegand**
2. Clique em **Adicionar** para criar um perfil de Wiegand personalizado
3. Nas caixas de diálogo relacionadas, insira as informações de formatação e a tecnologia de cartão que seu sistema usa
4. Para usar o perfil de Wiegand recém-definido no sistema, insira o nome dele no campo **Perfil de Wiegand** das seguintes caixas de diálogo do MorphoManager:

– **Administração > Perfil do dispositivo biométrico**
– **Administração > Política de usuário**

Mifare Classic CSN

1. Adicione o elemento Wiegand `User CSN Element` e insira os seguintes detalhes

– **Nome**: `CSN` (por exemplo)
– **Comprimento** `32`
– **Modo de transformação:** `Reversed`

2. **Em Administração > Perfil do dispositivo biométrico**, na página **Configurações do modo multifatorial**, marque a caixa de seleção **MIFARE Classic**

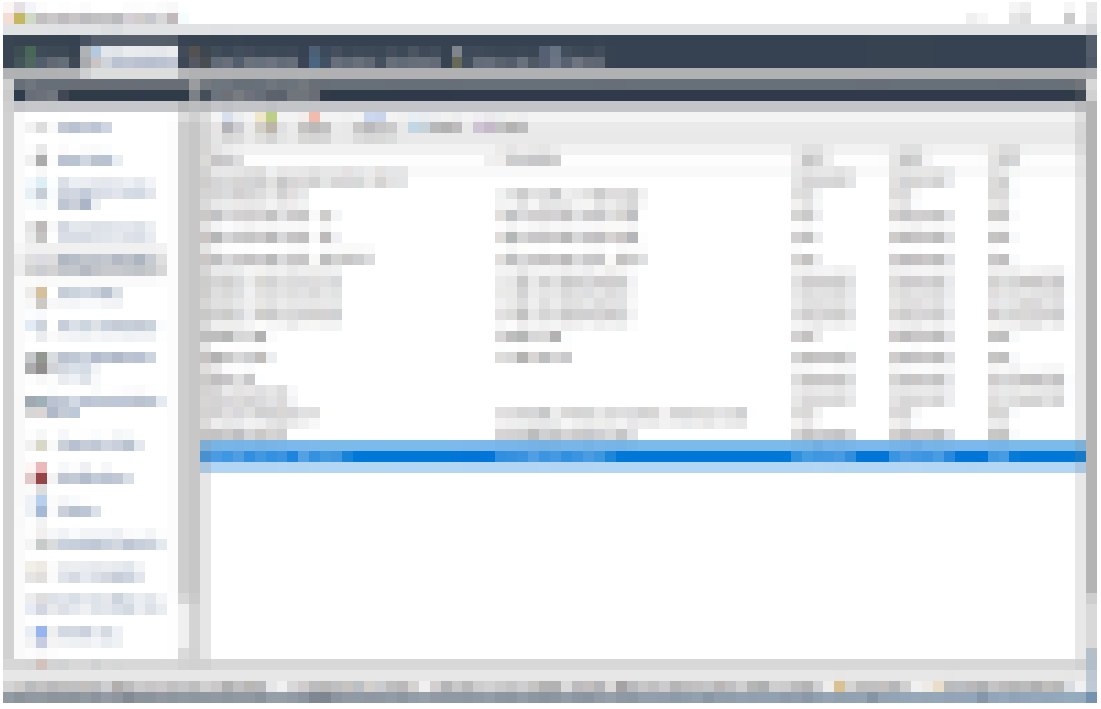
Mifare DESFire CSN

A configuração é idêntica ao Mifare Classic, exceto pelos seguintes detalhes:

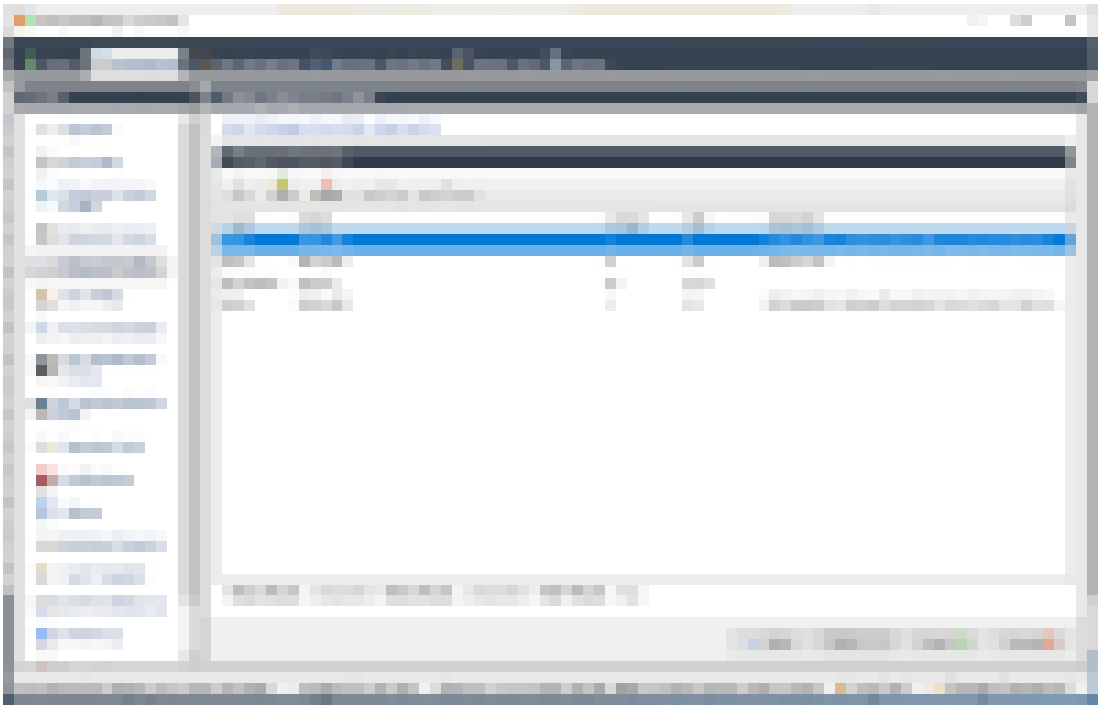
- **Comprimento:** `56`
- Adicione **Elemento CSN do usuário do elemento Wiegand**
  - Insira um nome em **Nome:**
  - Em **Comprimento**, insira 56
  - Em **Modo de transformação:**, insira `Reversed`
- **Em Administração > Perfil do dispositivo biométrico**, na página **Configurações do modo multifatorial**, marque a caixa de seleção **Mifare DESFire 3DES**

iClass 26 BIT

1. Selecione o perfil predefinido `Standard 26 bit-HID PACS`



2. Clique em **Editar**
3. Clique em **Next (Próximo)**



4. Clique em **Editar**
5. Exclua a linha `Fixed Facility Code`
6. Selecione a linha `HID iClass SEP User ID`
7. Clique em **Editar**
8. Altere o comprimento do ID de usuário de `1..16` para `1..24`
9. **Em Administração > Perfil do dispositivo biométrico**, na página Configurações do dispositivo biométrico, para Perfil de Wiegand, selecione `Standard 26 BIT-HID-PACS`
10. **Em Administração > Perfil do dispositivo biométrico**, na página **Configurações do modo multifatorial**, marque a caixa de seleção `HID iClass`
11. Clique em Próximo até chegar à página **Parâmetros personalizados**
12. Clique em **Adicionar**
13. Adicione o parâmetro personalizado (que diferencia maiúsculas de minúsculas) Wiegand.site_code_propagation
14. Defina o valor como `1`
15. Clique em **Concluir**.
16. Insira esse perfil de Wiegand concluído em **Administração > Política de usuário**

iClass 35 BIT

1. Selecione o perfil predefinido `HID Corporate 1000 35 BIT`
2. Clique em **Editar**
3. Clique em **Next (Próximo)**
4. Selecione e exclua a linha do elemento `Fixed Company ID`
5. Selecione e exclua a linha do elemento `User Card ID Number`
6. Adicione a linha do elemento `HID iClass/iClass SE PACS Data` e, nos detalhes do elemento, defina o seguinte:

– Nome: `Card ID Number`
– Comprimento: `32`
– **Em Administração > Perfil do dispositivo biométrico**, na página **Configurações do modo multifatorial**, marque a caixa de seleção `HID iClass`
– Clique em **Próximo** até chegar à página **Parâmetros personalizados**

- Clique em **Adicionar**
- Adicione o parâmetro personalizado (que diferencia maiúsculas de minúsculas) Wiegand.site_code_propagation
- Defina o valor como `1`
- Clique em **Concluir**.
- Insira esse perfil de Wiegand concluído em **Administração > Política de usuário**

iClass 37 BIT

- **Comprimento** `37`

1. Adicione o elemento Paridade:

- **Nome**: (por exemplo) `EvenParityBit 1`
- **Prioridade**: `1`
- **Comprimento**: `18`
- **Modo**: `Even`
- **Bits de base**: `1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18`

2. Adicione o elemento `User HID iClass/iClass`

- **Nome**: (por exemplo): `Parity Bits 2`
- **Prioridade**: `2`
- **Comprimento**: `19`
- **Modo**: `Odd`
- **Bits de base**: `19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37`
- **Em Administração > Perfil do dispositivo biométrico**, na página **Configurações do modo multifatorial**, marque a caixa de seleção `HID iClass`
- Clique em **Próximo** até chegar à página **Parâmetros personalizados**
- Clique em **Adicionar**
- Adicione o parâmetro personalizado (que diferencia maiúsculas de minúsculas) Wiegand.site_code_propagation
- Defina o valor como `1`
- Clique em **Concluir**.
- Insira esse perfil de Wiegand concluído em **Administração > Política de usuário**

iClass 48BIT

1. Selecione o perfil predefinido `HID Corporate 1000 48 BIT`
2. Clique em **Editar**
3. Clique em **Next (Próximo)**
4. Selecione e exclua a linha do elemento `Fixed Company ID`
5. Selecione e exclua a linha do elemento `User Card ID Number`
6. Adicione a linha do elemento `HID iClass/iClass SE PACS Data` e, nos detalhes do elemento, defina o seguinte:

- Nome: `User`
- Comprimento: `45`

7. **Em Administração > Perfil do dispositivo biométrico**, na página **Configurações do modo multifatorial**, marque a caixa de seleção `HID iClass`
8. Clique em **Próximo** até chegar à página **Parâmetros personalizados**
9. Clique em **Adicionar**
10. Adicione o parâmetro personalizado (que diferencia maiúsculas de minúsculas) `Wiegand.site_code_propagation`

- Defina o valor como `1`

11. Clique em **Concluir**.
12. Insira esse perfil de Wiegand concluído em **Administração** > **Política de usuário**

HID Prox

1. Selecione o perfil predefinido `Standard 26 BIT`
2. Clique em **Editar**
3. Clique em **Next (Próximo)**
4. Exclua a linha `Fixed Facility Code`
5. Clique em **Editar**
6. Altere o comprimento do ID de usuário de `1..16` para `1..24`
7. **Em Administração > Perfil do dispositivo biométrico**, na página Configurações do dispositivo biométrico, para Perfil de Wiegand, selecione `Standard 26 BIT`
8. **Em Administração > Perfil do dispositivo biométrico**, na página **Configurações do modo multifatorial**, marque as caixas de seleção:

– **Biometria**
– **Cartão de proximidade**

9. Clique em **Próximo** até chegar à página **Parâmetros personalizados**
10. Clique em **Adicionar**
11. Adicione o parâmetro personalizado (que diferencia maiúsculas de minúsculas) `Wiegand.site_code_propagation`

– Defina o valor como `1`

12. Clique em **Concluir**.
13. Insira esse perfil de Wiegand concluído em **Administração** > **Política de usuário**

21.5 Modos de identificação em dispositivos biométricos

Introdução

Os leitores biométricos podem identificar portadores de credenciais de diferentes maneiras. Essas formas são conhecidas como modos de identificação ou modos de autenticação.

– Por **Cartão OU biometria**, dependendo da credencial que o titular apresenta para o leitor
– Por **Cartão E biometria**. Nesse método, o usuário deve comprovar pelas credenciais biométricas que é o verdadeiro proprietário do cartão.
– Somente por **Biometria**

Esta seção descreve como configurar esses modos no MorphoManager.

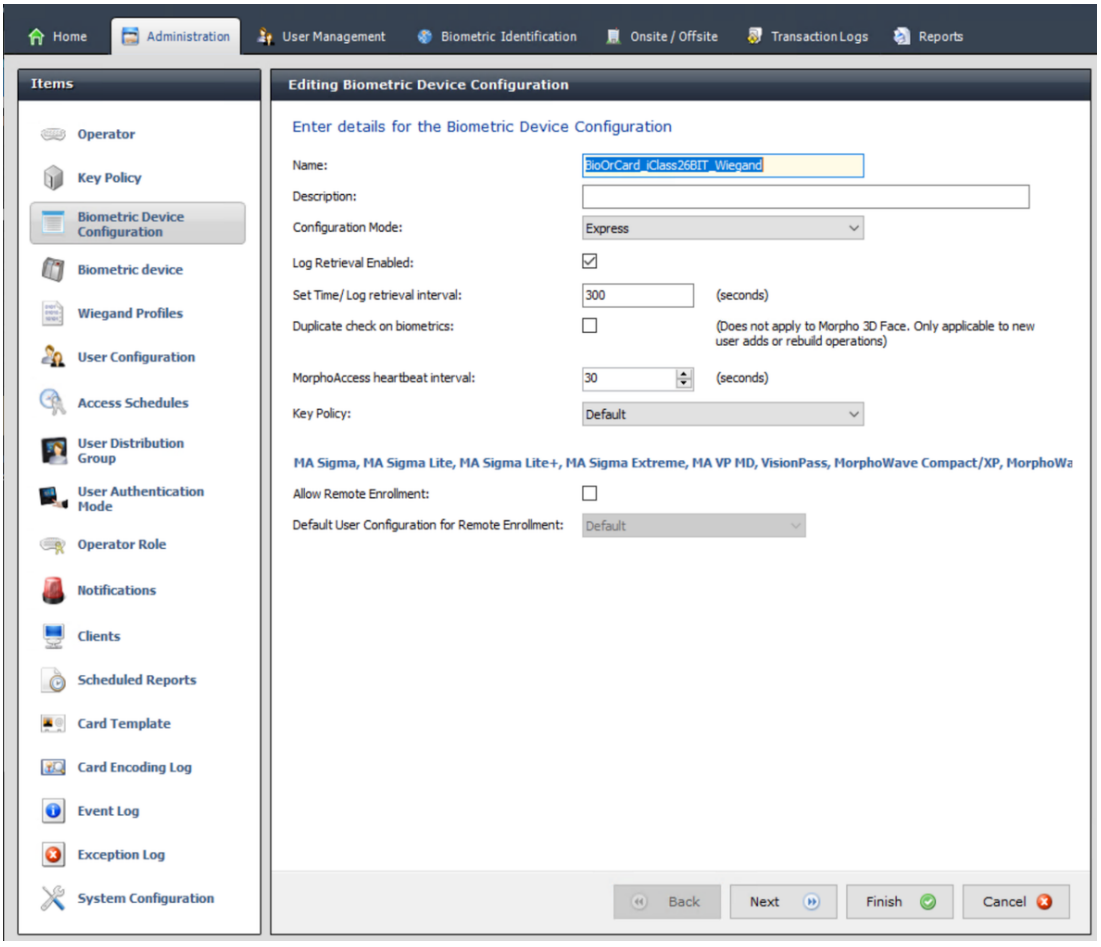
Caminho da caixa de diálogo

Na guia **Administração** do MorphoManager

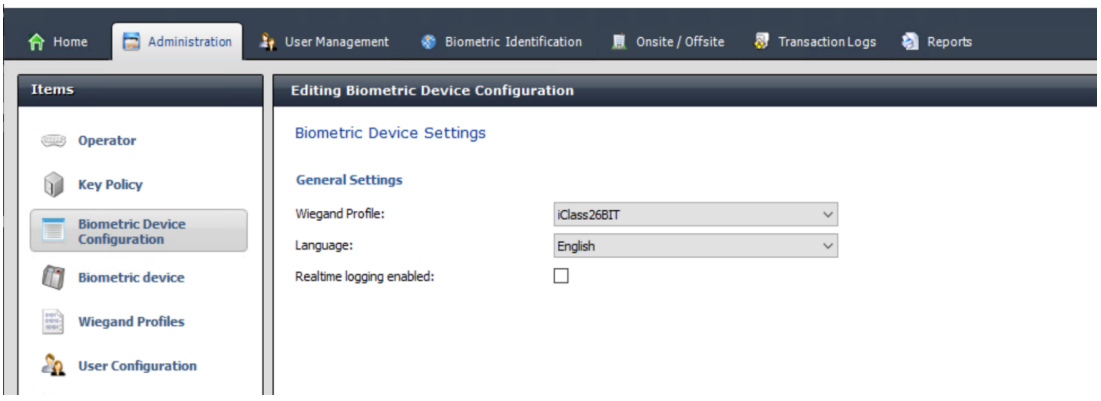
21.5.1 Cartão OU biometria

Crie este modo de autenticação personalizado se os usuários se identificarem por cartão OU por credenciais biométricas.

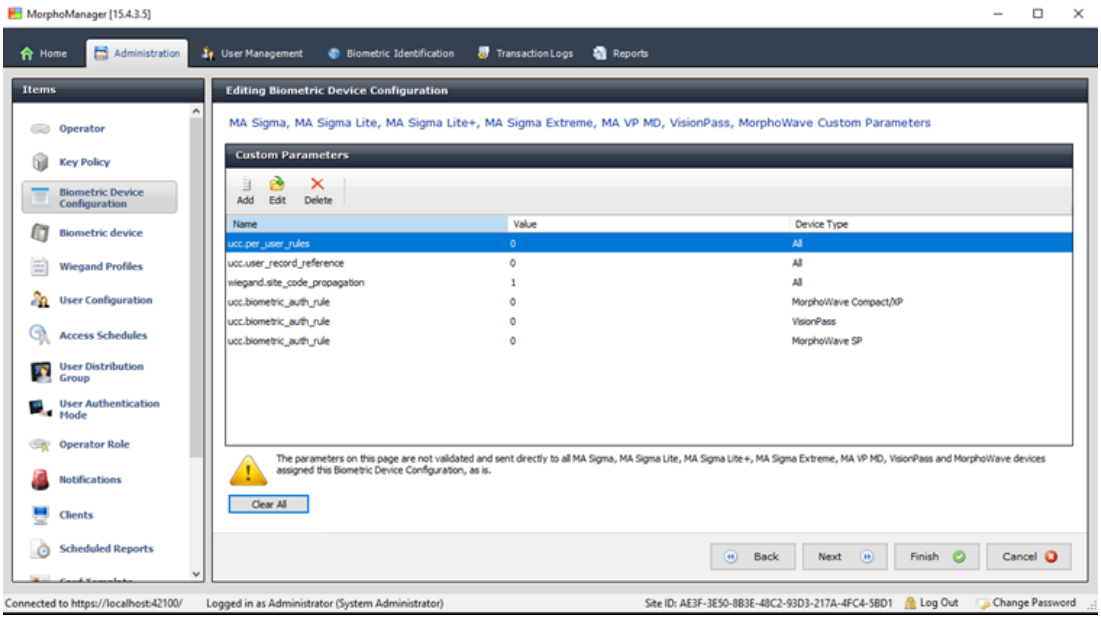
1. No MorphoManager, vá até **Administração** > **Configuração do dispositivo biométrico**
2. Insira um nome para essa configuração de dispositivo biométrico, por exemplo, `CardORBiometric`



3. Clique em **Próximo** até chegar à página **Configurações de dispositivo biométrico**



4. Em **Perfil de Wiegand**, selecione o mesmo perfil definido para os dispositivos biométricos ao configurar o BioBridge.
5. Clique em **Avançar** até chegar à caixa de diálogo **Configurações do limite biométrico**.
6. Defina os valores do **Limite biométrico** de acordo com as condições locais e a documentação do MorphoManager. O valor padrão é `Recommended`
7. Clique em **Avançar** até chegar à tela **Configurações do modo multifatorial**.
8. Marque a caixa de seleção **Biométrico**, além da caixa de seleção da tecnologia de cartão usada por sua instalação.
9. Clique em **Próximo** até chegar à tela **Parâmetros personalizados**



10. Para cada dispositivo que você usa:
    Clique em **Adicionar** para adicionar dois parâmetros personalizados.
    (Se esses dois parâmetros forem definidos, o leitor enviará os dados do cartão diretamente para o AMC. O usuário não precisa estar inscrito no leitor IDEMIA.)
- `ucc.per_user_rules`
- `ucc.user_record_reference`

11. Para leitores WAVE e VisionPass, adicione mais um parâmetro:
- `ucc.biometric_auth_rule=0`
- Neste caso, selecione `MorphoWave Compact/XP`, `MorphoWave SP` ou `VisionPass` em **Tipo de dispositivo**

12. Clique em **Concluir**

Atribua este modo de autenticação aos usuários

No ACS, você deve atribuir um cartão com uma definição de cartão válida para cada titular.

1. No MorphoManager, vá até **Administração** > **Modo de autenticação do usuário**
2. Defina os seguintes atributos**:**
- Defina **Modo** como `Enabled`
- Defina a lista **Local do modelo** como `Download to Device`
- Marque a caixa de seleção **Permitir início por biometria**
- Marque a caixa de seleção **Permitir início por cartão sem contato**
- Desative **Exigir correspondência de modelo**

3. Vá até **Administração** > **Configuração do usuário**
4. Clique em **Adicionar**
5. Para **Modo de autenticação do usuário**, selecione o nome do modo que você criou acima para Cartão OU Biometria.
6. Clique em **Concluir**

21.5.2 Cartão E biometria

Faça estas definições se os usuários precisarem usar um cartão E credenciais biométricas para comprovarem que são os proprietários do cartão.

1. No MorphoManager, vá até **Administração** > **Configuração do dispositivo biométrico**
2. Clique em **Próximo** até chegar à página **Configurações de dispositivo biométrico**

3. Em **Perfil de Wiegand**, selecione o mesmo perfil definido para os dispositivos biométricos ao configurar o BioBridge.
4. Clique em **Próximo** até chegar à página **Configurações do modo multifatorial**
5. Marque a caixa de seleção da tecnologia de cartão usada por sua instalação.
6. Clique em **Concluir**

Atribua este modo de autenticação aos usuários

No ACS, você deve atribuir um cartão com uma definição de cartão válida para cada titular.

1. No MorphoManager, vá até **Administração** > **Configuração do usuário**
2. Em **Modo de autenticação do usuário,** selecione `Contactless Card ID + Biometric` na lista.
3. Clique em **Concluir**.

21.5.3 Somente biometria

Faça estas definições se os usuários conseguirem se identificar somente por credenciais biométricas.

1. No MorphoManager, vá até **Administração** > **Configuração do dispositivo biométrico**
2. Clique em **Avançar** até chegar à página **Editar configuração do dispositivo biométrico**
3. Em **Perfil de Wiegand**, selecione o mesmo perfil definido para os dispositivos biométricos ao configurar o BioBridge
4. Clique em **Próximo** até chegar à página **Configurações do modo multifatorial**
5. Em **Modo multifatorial**, selecione `Biometric only` na lista
6. Clique em **Concluir**

Atribua este modo de autenticação aos usuários

No ACS, você deve atribuir um cartão com uma definição de cartão válida para cada titular.

1. No MorphoManager, vá até **Administração** > **Configuração do usuário**
2. Em **Modo de autenticação do usuário,** selecione `Biometric(1:many)` na lista.
3. Clique em **Concluir**.

21.6 Observações técnicas e limites

Sistemas operacionais Windows com suporte oficial

O IDEMIA é compatível com as mesmas versões do Windows 10 que o Bosch ACS.

Versão do Microsoft SQL Server com suporte oficial

A versão com suporte é SQL Server 2017

Um sistema IDEMIA por sistema de acesso

Um sistema de controle de acesso da Bosch pode oferecer suporte para apenas um sistema IDEMIA.

Um cartão IDEMIA por titular de cartão.

Os sistemas de controle de acesso da Bosch oferecem suporte para vários cartões por titular, mas o IDEMIA oferece suporte para apenas um. Portanto, depois da inscrição e ao sincronizar com o BIS, o primeiro cartão válido (isto é, com status = 1) do tipo “Acesso”, “Temporário” ou “Estacionamento” é atribuído ao IDEMIA. Se o cartão for bloqueado depois, seu número ainda será transmitido e registrado no log de eventos.

Número máximo de titulares de cartão IDEMIA
O BioBridge MorphoManager pode lidar com até 100.000 titulares de cartão.

Número máximo de grupos de acesso
O IDEMIA oferece suporte para até 5.000 grupos de acesso (grupos de distribuição de usuários). Eles são mapeados para **Classes de pessoa** no sistema de controle de acesso da Bosch.

Desempenho de download de modelos
– Mil modelos para um dispositivo: o download leva menos de um minuto.
– Mil modelos para 100 dispositivos: o download é feito em alguns minutos.

O IDEMIA não oferece suporte para divisões
Quando um sistema IDEMIA está integrado, um sistema ACS não consegue examinar os titulares de cartão de uma divisão com confiança nos operadores de controle de acesso de outra divisão. Se for obrigatório ter privacidade absoluta entre divisões, não integre um sistema IDEMIA.

Cartões virtuais/acesso somente por código PIN.
O IDEMIA não oferece suporte para acesso somente por código PIN. Um cartão físico é necessário.

Função de dedo de coação do IDEMIA
A função de dedo de coação do IDEMIA não é compatível no momento com os controladores AMC.

Conjunto mínimo de critérios de identificação.
A inscrição no sistema IDEMIA requer pelo menos os seguintes critérios de identificação:
– First name (Nome)
– Last name (Sobrenome)
– Classe da pessoa
– Um cartão físico atribuído ao titular do cartão

Estados exibidos nos leitores
Nenhum estado de leitor (por exemplo, “Dispositivo bloqueado”) é exibido nos leitores Wiegand e OSDP.

Backup e restauração
Antes de restaurar um backup com IDEMIA, exclua e recrie o banco de dados IDEMIA usando a ferramenta do provedor IDEMIA DataBridge.
Na caixa de diálogo **Dispositivo biométrico**, verifique se todas as configurações foram enviadas corretamente aos leitores IDEMIA. Se uma das tarefas de sincronização falhar, recrie a configuração do leitor:
1. No MorphoManager, vá até **Dispositivo biométrico**.
2. Selecione o dispositivo afetado.
3. Clique em **Recriar**.

Compatibilidade das funcionalidades de cartão ACS com os modos de autenticação do IDEMIA:

Funcionalidade	Modo: Cartão E Bio	Modo: Cartão OU Bio
Cartões de acesso: inserir	OK	OK
Cartões de acesso: atualizar	OK	OK
Cartões de acesso: excluir	OK	OK
Cartões de acesso: vários cartões	Apenas o primeiro cartão	Primeiro cartão usado para biometria.
Cartão de substituição	OK	OK
Cartão temporário	OK	OK
Cartão temporário: somente período	OK	OK
Cartão temporário: desativar todos os cartões imediatamente no período	OK	OK
Cartão temporário: ativar cartões automaticamente após o período definido	OK	OK
Cartão temporário: desativar cartões e ativar automaticamente	OK	OK
Cartões de alarme	Não compatível	OK
Modo de escritório	Não compatível (*)	Não compatível (*)
Visitante	É possível que os dados biométricos do primeiro visitante permaneçam atribuídos ao cartão.	É possível que os dados biométricos do primeiro visitante permaneçam atribuídos ao cartão.
Vigilante	Não compatível	Não há biometria compatível. O cartão funciona.
Cartão de estacionamento	OK	OK
Código PIN	Não compatível (*)	Não compatível (*)
Validação de terceiros	Sem código PIN (*)	Sem código PIN (*)
(*) Leitor IDEMIA não utilizável como leitor de teclado		

22 Conformidade com a norma EN 60839

Introdução

EN 60839 é uma família de normas internacionais europeias para hardware e software do seguinte:

– alarme e sistemas eletrônicos de segurança
– sistemas eletrônicos de controle de acesso

Para garantir a conformidade do seu sistema de controle de acesso com essa norma, partes da configuração talvez precisem ser adaptadas. A lista a seguir contém as partes mais importantes. Para obter uma lista completa, consulte a norma como adotada em seu próprio país.

Requisitos para usar o AMS 4.0 como um sistema certificado pela norma EN 60839, grau 2

– O sistema satisfaz os requisitos para anti-passback global em termos de uso de uma zona por MAC.
– Os diferentes fusos horários usados pelo sistema AMS dependem do número de MACs. Um fuso horário separado pode ser usado para cada MAC.
– A fiação dos contatos das portas não deve impedir a abertura da porta para uma evacuação de emergência acionada por um sistema de prevenção de incêndio ou intrusão.
– Apenas os leitores OSDP usam criptografia na interface RS485.
– O acesso ao modo de configuração deve ser estritamente controlado. Isso pode ser alcançado, por exemplo, localizando os computadores em áreas seguras e por tempo limite em sessões de login, particularmente tempo limite para inatividade no nível de aplicativos e sistema operacional.
– A rede e o cabeamento elétrico devem ser colocados em uma área segura ou envoltos em tubos.
– Somente os leitores de cartões podem ser montados em áreas não seguras; todos os outros dispositivos devem estar em áreas seguras.
– O tempo mínimo de verificação de PINs para credenciais biométricas ou físicas deve ser definido como pelo menos `4`.
– O tempo mínimo de identificação dos PINs deve ser definido como pelo menos `8`.
– O computador do servidor principal, os servidores de conexão, os servidores MAC e os clientes devem ser sincronizados com um servidor de tempo de rede.
– O monitoramento de energia deve ser ativado em controladores de acesso locais (por exemplo, AMCs).
– O funcionamento offline dos controladores de acesso locais (por exemplo, AMCs) só é permitido durante falhas de rede. Por exemplo, o parâmetro do AMC **Tempo limite do host** não deve ser definido como `0`.

Regras para o nível de segurança da senha

– O comprimento mínimo da senha deve ser pelo menos `5` caracteres.

23 Definição de autorizações e perfis de acesso

23.1 Criação de autorizações de acesso

Caminho da caixa de diálogo

Main menu (Menu principal) > **System data (Dados do sistema)** > **Authorizations (Autorizações)**

Procedimento

1. Limpe os campos de entrada clicando em **New (Novo)**  da barra de ferramentas.

   Como alternativa, clique em **Copy (Copiar)**  para criar uma nova autorização com base em outra existente.
2. Digite um nome único para a autorização
3. (Opcional) Digite uma descrição
4. (Opcional) Selecione um modelo de tempo para governar essa autorização
5. (Opcional) Escolha um **Inactivity limit (Limite de inatividade)** na lista.
   Isso é um período programado entre 14 e 365 dias. Se um titular dessa autorização falhar ao usá-la durante o período definido, ela será perdida. Toda vez que o titular usar a autorização, o temporizador é reiniciado.
6. (Obrigatório) Atribua pelo menos uma **Entrance (Entrada)**.
   As entradas existentes são listadas em guias diferentes, dependendo dos modelos de porta.
   (Genérico) **Entrance (Entrada)**, **Time management (Gerenciamento de tempo)**, **Elevator (Elevador)**, **Parking lot (Estacionamento)**, **Arming Intrusion detection (Armar a detecção de intrusão)**.
   Selecione entradas individuais a partir das listas nas diversas guias, conforme descrito abaixo.
   Como alternativa, use os botões **Assign all (Atribuir todas)** e **Remove all (Remover todas)** em cada guia.
   - na guia **Entrance (Entrada)**, selecione uma entrada marcando uma ou ambas as caixas de seleção para **In (Entrada)** ou **Out (Saída)**
   - na guia **Time management (Gerenciamento de tempo)** (para leitores de frequência), marque uma ou ambas as caixas de seleção para **In (Entrada)** ou **Out (Saída)**
   - na guia **Elevator (Elevador)**, selecione os andares
   - na guia **Parking lot (Estacionamento)** selecionando um estacionamento e uma zona de estacionamento
   - na guia **Arming Intrusion detection (Armar detecção de intrusão)** selecionando **Armed (Armada)** ou **Disarmed (Desarmada)**.
7. Selecione o MAC adequado na lista
8. Clique em salvar  para salvar a autorização.

Aviso!
As alterações subsequentes em autorizações afetarão os titulares existentes, a menos que o perfil governante esteja bloqueado.
Exemplo: se um limite de inatividade de 60 dias for reduzido para 14 dias, a autorização será perdida para todas as pessoas que não usaram a autorização nos últimos 14 dias.
Exceção: se uma autorização fizer parte de um perfil de acesso que está **bloqueado** para uma Identificação do funcionário (tipo de pessoa), as pessoas deste tipo não são afetadas pelos limites de inatividade sobre a autorização. Os bloqueios de perfil podem ser definidos com a caixa de seleção a seguir.
Main menu (Menu principal) > **System data (Dados do sistema)** > **Person Types (Tipos de pessoa)** > tabela: **Predefined Employee IDs (Identificações de funcionários predefinidas)** > caixa de seleção: **Profile locked (Perfil bloqueado)**

23.2 Criação de perfis de acesso

Observação: Usar perfis de acesso para agrupar autorizações
Para fins de consistência e conveniência, autorizações de acesso não são atribuídas individualmente, mas sim geralmente agrupadas em **Perfis de acesso** e atribuídas como tal.
- ACE Client (Cliente do ACE): **System data (Dados do sistema)** > **Access profiles (Perfis de acesso)**
- Main menu (Menu principal): **> System data (Dados do sistema)** > **Access profiles (Perfis de acesso)**

Pré-requisitos
Autorizações de acesso já foram definidas no sistema.

Procedimento

1. Limpe os campos de entrada clicando em **New (Novo)** da barra de ferramentas.
   Como alternativa, clique em **Copy (Copiar)** para criar um novo perfil com base em outro existente.
2. Digite um nome único para o perfil
3. (Opcional) Digite uma descrição
4. (Opcional) Marque a caixa de seleção **Visitor profile (Perfil de visitante)** para limitar esse perfil para visitantes
5. (Opcional) Defina um valor para **Standard duration of validity (Duração padrão da validade)**.
   - Se nenhum valor for definido, o perfil permanecerá atribuído indefinidamente.
   - Se um valor for definido, ele será usado para calcular a data de validade de qualquer atribuição posterior do perfil.
6. (Obrigatório) Atribua pelo menos uma **Authorization (Autorização)**:
   As autorizações disponíveis para atribuição estão listadas à direita.
   As autorizações que já estão atribuídas estão listadas à esquerda.
   Selecione itens e clique nos botões entre as listas para movê-los de uma lista para a outra.
   - ≤ atribui o item selecionado.
   - ≥ cancela a atribuição do item selecionado.

7. Clique em salvar  para salvar o perfil.

24 Criação e gerenciamento de dados de funcionários

Caminho da caixa de diálogo

Main menu (Menu principal) > **Personnel data (Dados de funcionários)** > <subdiálogos>

Procedimento geral

1. No subdiálogo **Persons (Pessoas)** digite os dados de identificação do funcionário.
2. No subdiálogo **Cards (Cartões)**:
   - atribua perfis de acesso ou autorizações de acesso individuais.
   - atribua um modelo de tempo, se necessário.
   - atribua o cartão.
3. No subdiálogo **PIN-Code (Código PIN)**: atribua um código PIN, se necessário.
4. No subdiálogo **Print Badges (Imprimir crachás)**, imprima o cartão.

Para **Visitors (Visitantes)**, faça o seguinte:

- Insira os dados pessoais na caixa de diálogo **Visitors (Visitantes)** do menu **Visitors (Visitantes)** e atribua um acompanhante (atendente), se necessário.

Aviso!

Cartões de identificação e a autorização de acesso não precisam ser atribuídos ao mesmo tempo. Portanto, é possível atribuir cartões de identificação a pessoas sem atribuir autorizações de acesso, ou vice-versa. No entanto, em ambos os casos todo o acesso será negado a estas pessoas.

O processo de leitura de cartões.

Quando os cartões são lidos nos leitores, o leitor realiza algumas verificações:

- O cartão é válido e está registrado no sistema?
- O usuário do cartão está bloqueado (desabilitado no sistema)?
- O usuário do cartão tem autorização de acesso para entrar nesta direção?
- A autorização de acesso é uma autorização de área/hora? Em caso afirmativo, a hora da leitura está dentro dos intervalos definidos pelo modelo de tempo?
- A autorização de acesso está ativa, ou seja, não está **vencida** nem **bloqueada** (desabilitada)?
- O usuário do cartão está sujeito a um modelo de tempo? Em caso afirmativo, a hora da leitura está dentro dos intervalos definidos?
  Pré-requisito: as verificações do modelo de tempo devem estar ativadas no leitor em questão.
- O usuário do cartão está no local correto de acordo com Monitoramento da sequência de acesso?
  Pré-requisito: o Monitoramento da sequência de acesso deve estar ativado no leitor em questão.
- Foi definido um número máximo de pessoas para a área de destino desse leitor, e esse número já foi atingido?
- No caso de Monitoramento da sequência de acesso, incluindo anti-passback: este cartão está sendo escaneado em um leitor antes do término do tempo de bloqueio definido pelo anti-passback?
- Um código PIN adicional é necessário? **Pré-requisito**: o leitor deve ter um teclado.
- Se um nível de ameaça está em operação, o **Person security profile (Perfil de segurança de pessoas)** do usuário do cartão tem um **nível de segurança** que é pelo menos igual ao nível de segurança do leitor no nível de ameaça?

24.1 Pessoas

A tabela a seguir lista os dados que são exibidos por padrão nas caixas de diálogo **Pessoas**. As caixas de diálogo são extremamente personalizáveis. Consulte a seção **Campos personalizados para dados de pessoal**.
Quase todos os campos são opcionais. Os campos obrigatórios são claramente marcados com rótulos sublinhados na interface do usuário.

Guia	**Nome do campo**
Cabeçalho da caixa de diálogo	Name (Nome)
	First name (Nome)
	Birth name (Nome de nascimento) (chamado de nome de solteiro em algumas culturas)
	Personnel no. (Nº do funcionário)
	Date of birth (Data de nascimento)
	Employee ID (ID do funcionário) (também conhecido como tipo de pessoa)
	Gender (Gênero)
	Company (Empresa)
	Title (Cargo)
	ID card no. (Número do cartão de identificação)
	Car license no. (Número da carteira de habilitação)
Address (Endereço)	Zip code (CEP) (chamado de código postal em algumas culturas)
	Street, no. (Rua, número)
	Country, state (País, estado)
	Nationality (Nacionalidade)
Contact (Contato)	Phone other (Outro telefone)
	Company phone (Telefone da empresa)
	Company fax (Fax da empresa)
	Mobile phone (Telefone celular)
	Phone (Telefone)
	E-Mail
	Web page address (Endereço da página da Internet)
Additional Person Data (Dados pessoais adicionais)	Patronymic (Sobrenome) (um nome adicional usado em várias culturas)
	Birthplace (Local de nascimento)
	Marital status (Estado civil)

	Official identity card (Carteira de identidade oficial)
	Identity card no. (Número da carteira de identidade)
	Valid until (Válida até)
	Height (Altura)
Additional Company Data (Dados adicionais da empresa)	Department (Departamento)
	Location (Local)
	Cost center (Centro de custos)
	Job title (Cargo)
	Attendant (Escort) (Atendente [acompanhante])
	Reason for visit (Motivo da visita)
	Remarks (Observações)
Remarks (Observações)	(Fornece um campo de texto de forma livre para notas e observações sobre a pessoa.)
Extra Info (Informações adicionais)	10 campos definidos pelo usuário
Signature (Assinatura)	Capturar, regravar e excluir assinaturas
Fingerprints (Impressões digitais)	Capture, regrave, exclua e teste impressões digitais como credenciais biométricas. Designe determinadas impressões digitais para sinalizar coação.

Consulte

– *Campos personalizados para dados de funcionários, página 134*

24.1.1 Opções de controle do cartão ou do edifício

Visão geral

Use a guia **Controle do cartão** para permitir que os titulares de cartão ativem uma ou duas saídas genéricas do controlador de acesso com o cartão. Para atribuir a opção a um titular de cartão, marque a caixa de seleção **Controle do edifício** na caixa de diálogo **Pessoas**. As caixas de seleção **Controle do edifício** (ou **Controle do cartão**) são campos personalizados predefinidos que ficam visíveis na guia **Controle do cartão** de Pessoas por padrão, mas podem ser posicionados em qualquer lugar.

Existem duas tarefas principais para uma opção Controle do edifício. Elas são descritas abaixo:

– Configure a caixa de seleção: escolha um rótulo adequado e (se desejar) posicione-a em uma guia diferente da caixa de diálogo **Pessoas**.
– Atribua a função a uma saída em um controlador de acesso AMC e uma caixa de seleção.

Pré-requisitos

– A saída do controlador de acesso é conectada eletricamente ao dispositivo que deve ser ativado pelo cartão.

Caminho da caixa de diálogo

– Navegador de configuração do BIS > **Infraestrutura** > **Campos personalizados do ACE** > guia **Controle do cartão**
– Menu principal do AMS > **Configuração** > **Opções** > **Campos personalizados**> guia **Controle do cartão**

Configurando as caixas de seleção

1. Na página **Campos personalizados**, selecione a guia **Detalhes** no painel superior.
2. Localize a função **Controle do edifício**, 1 ou 2, que deseja usar.
3. Substitua um rótulo por um nome adequado (recomendado). Se desejar, posicione a caixa de seleção em uma guia diferente de **Controle do cartão**. Consulte a seção **Visualizando e editando campos personalizados** no link abaixo para obter instruções mais detalhadas.

Atribuindo a função a uma saída do controlador de acesso e uma caixa de seleção

Consulte a seção **Parâmetros e configurações do AMC** no link abaixo.

1. No **Editor de dispositivos**, na árvore de dispositivos, selecione o controlador de acesso AMC cujo sinal de saída você deseja usar.
2. Na guia **Saídas**, no painel superior, selecione a saída que deseja usar.
3. No painel do meio, **Dados de saída**, selecione o tipo **25, Controle do cartão**
4. Clique no botão **>** para adicionar a saída ao painel inferior.
5. No painel inferior, coluna **Param11**, selecione o rótulo da função Controle do edifício que selecionou no procedimento anterior **Configurando as caixas de seleção**.
6. Salve a árvore de dispositivos.

Consulte

– *Parâmetros e configurações do AMC, página 55*
– *Pré-visualização e edição de campos personalizados, página 134*

24.1.2 Informações adicionais: gravação de informações definidas pelo usuário

Use a guia **Extra info (Informações adicionais)** para definir campos adicionais que não são fornecidos em outras guias. Se nenhum campo adicional tiver sido definido, a guia permanecerá vazia.

24.1.3 Gravação de assinaturas

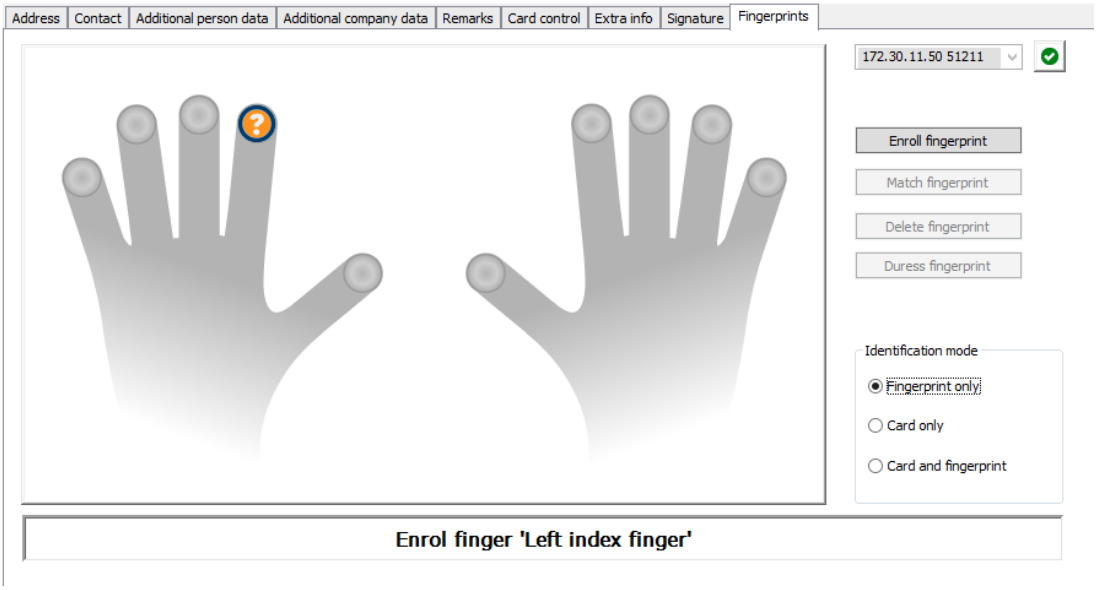
Um pad de captura de assinatura da empresa Signotec deve ser conectado e configurado no sistema para capturar assinaturas. Consulte seu gerente do sistema em caso de dúvidas.

1. Clique na guia **Signature (Assinatura)**
2. Clique no botão **Capture Signature (Capturar assinatura)** para gravar uma nova assinatura.
3. Assine diretamente no pad de captura usando o stylus especial.
4. Clique no botão de marca de seleção no pad de captura para confirma.
   A nova assinatura será agora exibida na tela (clique na assinatura para ampliá-la).

Procedimentos relacionados:

– Clique no botão **Capture Signature (Capturar assinatura)** para substituir uma assinatura existente.
– Clique no botão **Delete Signature (Excluir assinatura)** para excluir uma assinatura existente.

24.1.4 Cadastramento de dados de impressão digital



Pré-requisitos

- Um ou mais leitores de impressões digitais devem ser configurados nas entradas para realizar o controle de acesso biométrico.
- IMPORTANTE: periodicamente, esses leitores recebem e armazenam dados de cartões e impressão digital dos servidores. As configurações do leitor individual decidem, em última instância, quais credencias são aceitas. Elas substituem qualquer configuração feita aqui para a pessoa.
- Para usar impressões digitais como verificação para (ou como alternativa a) a autenticação baseada em cartão, todos os titulares de cartões devem digitalizar suas impressões digitais.
- O inscrito está na frente de um leitor de impressão digital que está conectado e configurado para sua estação de trabalho. Esse leitor de inscrição por impressão digital **não** deve ser um leitor de acesso.
- Como operador, você se comunica diretamente com o inscrito, ou seja, com a pessoa cujas impressões digitais devem ser registradas como credenciais biométricas para acesso.
- Você se familiarizou com o modo de apresentar o dedo várias vezes no leitor em questão usado para permitir a captura eficaz das impressões digitais.

Procedimento para cadastrar uma impressão digital para acesso

1. Navegue até a caixa de diálogo de impressões digitais: **Personnel data (Dados pessoais)** > **Persons (Pessoas)** > guia:**Fingerprints (Impressões digitais)** e crie ou ache a pessoa inscrita no banco de dados.
2. Pergunte à pessoa inscrita qual dedo ela deseja usar para acesso regular ao leitor de impressões digitais.
3. Selecione o dedo correspondente no diagrama de mãos.
   Resultado: a ponta do dedo é marcada com um ponto de interrogação.
4. Clique no botão **Enroll fingerprint (Cadastrar impressão digital)**.

5. Oriente a pessoa inscrita a posicionar seu dedo no leitor.
   Orientações de exemplo podem ser lidas no painel da caixa de diálogo abaixo do diagrama de mãos, mas cada tipo de leitor pode exigir um procedimento um pouco diferente.
6. Se a impressão digital for cadastrada de forma bem-sucedida, uma janela de confirmação será exibida.
7. Selecione um **Identification mode (Modo de identificação)**; isto determina quais credenciais um leitor de impressões digitais exigirá da pessoa inscrita quando ela solicitar acesso. Observe que o modo aqui estabelecido só terá efeito se o parâmetro do leitor **Person-dependent verification (Verificação dependente da pessoa)** tiver sido selecionado.
   As opções são:
   - **Fingerprint only (Somente impressão digital)** – apenas o scanner de impressões digitais do leitor é usado
   - **Card only (Somente cartão)** – apenas o scanner de cartões do leitor é usado
   - **Card and fingerprint (Cartão e impressão digital)** – ambos os scanners do leitor são usados. O inscrito deverá apresentar o cartão e o dedo escolhido no leitor para obter acesso.
8. Clique em **Accept (Aceitar)** para armazenar a impressão digital e o modo de identificação para o inscrito.
9. Clique em  (Salvar) para armazenar a impressão digital e o modo de identificação para o inscrito.

Aviso!
As configurações do leitor substituem as configurações da pessoa
Observe que o modo de identificação escolhido na caixa de diálogo das impressões digitais só funcionará se o próprio leitor de impressões digitais for configurado com a opção **Person-dependent verification (Verificação dependente da pessoa)** no editor de dispositivos. Se estiver em dúvida, consulte o seu administrador do sistema.

Procedimento de cadastro de impressão digital para sinalizar coação
Pré-requisitos:
- Os leitores de impressão digital só poderão enviar sinais de coação se estiverem configurados no **Editor de dispositivos** com a seguinte configuração
  guia **Rede e modos de operação** > **Modelos no servidor** > **Cartão e impressão digital**
- Pelo menos uma impressão digital do inscrito já foi inscrita e armazenada.
- O leitor de impressão digital está on-line. No modo off-line, o leitor obviamente não consegue enviar um sinal de coação para o sistema.

1. Peça à pessoa inscrita que escolha o dedo que deseja usar para sinalizar coação, isto é, caso seja forçada por uma pessoa não autorizada a usar o leitor de impressão digital.
2. Repita o procedimento de cadastro de impressão digital descrito acima para esse dedo.
3. Quando a segunda impressão digital for cadastrada com êxito, selecione-a no diagrama de mãos e clique no botão **Duress finger (Dedo de coação)**.
   O dedo de coação designado é identificado com uma marca de exclamação no diagrama de mãos.

Se, depois disso, a pessoa inscrita usar o dedo de coação no leitor de impressões digitais e o leitor não estiver offline, o sistema sinalizará coação ao operador por meio de uma janela pop-up.

Procedimento de teste das impressões digitais armazenadas

1. No diagrama de mãos, selecione a impressão digital que deseja testar.
2. Instrua o inscrito a colocar o dedo no leitor.
3. Clique no botão **Coincidir impressão digital**
   Resultado: uma janela pop-up confirmará se a impressão digital armazenada coincide com a colocada no leitor. Observe que talvez seja preciso repetir esse procedimento para reduzir a probabilidade de um alarme falso.

Procedimento de exclusão das impressões digitais armazenadas

1. No diagrama de mãos, selecione a impressão digital que deseja excluir.
2. Clique no botão **Excluir impressão digital**
3. Aguarde a confirmação da exclusão.

24.1.5 Registro dos dados de veias da palma da mão

Verificação biométrica

Verificação biométrica significa permitir que o usuário do cartão entre apenas após ter apresentado uma prova biométrica de que é o verdadeiro proprietário do cartão de identificação (ou credencial equivalente).

Pelo menos dois leitores biométricos devem ser configurados no sistema antes que a verificação de ID biométrica possa ser usada de maneira proveitosa:

- Um leitor conectado a uma estação de trabalho do operador para registro de dados biométricos.
- Um ou mais leitores nas entradas para verificar as identidades dos usuários de cartões.

Pré-requisitos:

- O leitor de veias da palma da mão deve estar licenciado e configurado no software do fabricante. Você definiu o seguinte:
  - O endereço IP do leitor
  - O ID do leitor (`1` ou `2`) para distinguir entre leitores no mesmo controlador biométrico.
- Você anotou cuidadosamente a senha do leitor, conforme fornecida pelo instalador do leitor.

Configuração do leitor de veias da palma da mão em uma estação de trabalho do operador
Caminho da caixa de diálogo

- Navegador de configuração do BIS > **Infrastructure (Infraestrutura)** > **ACE Card reader (Leitor de cartões do ACE)**

Procedimento

1. No painel **Workstations (Estações de trabalho)**, selecione a estação de trabalho à qual você deseja conectar o leitor de veias da palma da mão.
2. Clique no ícone verde com sinal de mais no painel **Workstations (Estações de trabalho)**.

3. Insira as seguintes informações no painel **Card reader (Leitor de cartões)**:
– **Type (Tipo)**: selecione **Palm vein sensor (Sensor de veias da palma da mão)** na lista suspensa.
– **IP address (Endereço IP)**: insira o endereço IP do controlador do leitor de veias da palma da mão.
– **Reader ID (ID do leitor)**: selecione o ID do leitor de veias da palma da mão na lista suspensa.
– **Password (Senha)**: insira a senha fornecida pelo instalador do leitor.
4. Clique em **Apply (Aplicar)** para aplicar as alterações e salvá-las ou clique em **Discard (Descartar)** para cancelar as alterações.

Criação de um controlador biométrico na árvore de dispositivos

Caminho da caixa de diálogo

– Navegador de navegação do BIS > **Connections (Conexões)**

Procedimento

1. Na guia **Device data (Dados do dispositivo)**, clique com o botão direito em um dispositivo MAC e selecione **New biometric controller (Novo controlador biométrico)** no menu de contexto.
2. Na caixa de diálogo do controlador do PCS, insira as informações necessárias:
– **Name (Nome)**: insira o nome do controlador.
– **Description (Descrição)**: insira uma descrição.
– **IP address (Endereço IP)**: insira o endereço IP do controlador do leitor de veias da palma da mão.
3. Clique em **Apply (Aplicar)** para aplicar as alterações e salvá-las ou clique em **Discard (Descartar)** para cancelar ou remover as alterações feitas.

Adição de um leitor de veias da palma a um controlador biométrico

1. Na guia **Device data (Dados do dispositivo)**, amplie a árvore de dispositivos, clique com o botão direito em **PCS controller device (Dispositivo do controlador do PCS)** e selecione **New palm vein reader (Novo leitor de veias da palma da mão)** no menu de contexto.
2. Na caixa de diálogo de veias da palma da mão do PCS, insira as informações necessárias:
– **Name (Nome)**: insira o nome do leitor de veias da palma da mão.
– **Description (Descrição)**: insira uma descrição (opcional).
– **Division (Divisão)**: selecione uma divisão.
– **Reader terminal / bus address (Endereço do terminal/barramento do leitor)**: insira o ID do leitor, 1 ou 2.
– **Number of retries (Número de tentativas)**: insira o número máximo de tentativas permitidas.
– **Password (Senha)**: insira a senha fornecida pelo instalador do leitor.
3. Clique em **Apply (Aplicar)** para aplicar as alterações e salvá-las ou clique em **Discard (Descartar)** para cancelar ou remover as alterações feitas.

Registro de um padrão de veias da palma para verificação de ID

Pré-requisitos:

– O leitor de veias da palma da mão deve estar configurado na estação de trabalho do operador.
– O leitor de veias da palma da mão deve estar ligado e conectado à rede.
O leitor de veias da palma da mão deve mostrar luzes azuis constantes.
– Você deve estar familiarizado com as instruções do fabricante para o processo de registro usando o leitor de veias da palma da mão.
– A pessoa já foi definida como usuário do cartão no sistema.

Procedimento

1. Inicie o cliente ACE (Dialog Manager) ou feche e reinicie se já estiver em execução.
2. Acesse **Personnel data (Dados de funcionários)** > **Persons (Pessoas)** > guia **Palm vein (Veias da palma da mão)**
– O ícone de verificação verde ao lado do botão **Enroll palm veins (Registrar veias da palma da mão)** indica que o leitor de veias está conectado.
3. Carregue o registro do usuário do cartão necessário na caixa de diálogo principal.
4. Pergunte à pessoa registrada qual palma deseja usar no leitor de veias da palma da mão.
5. Selecione a palma correspondente no diagrama de mãos.
A palma é marcada com um ponto de interrogação.
6. Oriente a pessoa a posicionar a palma no modelo do leitor de veias da palma da mão. (Dependendo da marca e do modelo, as etapas a seguir podem exigir algumas modificações.)
7. Clique no botão **Enroll palm veins (Registrar veias da palma da mão)**.
As luzes do leitor de veias da palma da mão mudam para indicar que o leitor está pronto para a leitura.
– Coloque a palma da mão no leitor de veias.
– Espere até as luzes do leitor piscarem
– Tire a palma do leitor por aproximadamente um segundo e posicione-a novamente.
– Se as luzes do leitor piscarem novamente, repita a etapa anterior até que o leitor mostre luzes verdes ou vermelhas sem piscar.
  – **Verde**: o padrão de veias da palma foi registrado com êxito.
  – **Vermelho**: o padrão de veias da palma não foi registrado com êxito. Verifique se a pessoa seguiu as instruções do fabricante e repita o procedimento.
8. Quando o padrão de veias da palma da mão é registrado com êxito, o ícone de ponto de interrogação no diagrama de mãos passa a ser um ícone de verificação verde.
9. Clique em  (Salvar) para armazenar o padrão de veias da palma registrado.

Teste de um padrão de veias da palma da mão armazenado

1. Acesse **Personnel data (Dados de funcionários)** > **Persons (Pessoas)** > guia **Palm vein (Veias da palma da mão)**
2. Carregue o registro do usuário do cartão necessário na caixa de diálogo principal.
3. No diagrama de mãos, selecione a mão que deseja testar.
4. Clique no botão **Compare palm veins (Comparar veias da palma da mão)**.
As luzes do leitor de veias da palma da mão mudam para indicar que o leitor está pronto para a leitura.
– Coloque a palma da mão no leitor de veias.
– Aguarde até que o leitor mostre luzes verdes ou vermelhas sem piscar.
  – **Verde**: o padrão de veias da palma corresponde ao padrão armazenado.

– **Vermelho**: o padrão de veias da palma não corresponde ao padrão armazenado Verifique se a pessoa registrada seguiu as instruções do fabricante e repita o procedimento, se necessário.

Remoção de um padrão de veias da palma da mão armazenado

1. Acesse **Personnel data (Dados de funcionários)** > **Persons (Pessoas)** > guia **Palm vein (Veias da palma da mão)**
2. Carregue o registro do usuário do cartão necessário na caixa de diálogo principal.
3. No diagrama de mãos, selecione a mão cujo padrão de veias da palma você deseja excluir.
4. Clique no botão **Delete palm veins (Excluir veias da palma da mão)**.
5. Aguarde uma caixa de diálogo confirmando a exclusão.

Sinais luminosos de LED

Note que os sinais luminosos variam de acordo com a marca e o modelo.

– **Azul (piscando)**: o dispositivo está ligado, mas não está conectado à rede.
– **Azul (sem piscar)**: o dispositivo está ligado e conectado à rede.
– **Azul e opaco (sem piscar)**: o dispositivo está pronto para ler um padrão de veias da palma.
– **Piscando sob a palma da mão da pessoa**: sinal para tirar a palma do leitor por aproximadamente um segundo e posicioná-la novamente.
– **Verde (sem piscar)**: o padrão de veias da palma foi reconhecido.
– **Vermelho (sem piscar)**: o padrão de veias da palma não foi reconhecido.

Uso de um leitor de veias da palma em uma entrada

Aviso!
Leitor offline
Se as luzes do leitor de veias da palma da mão estiverem piscando na cor azul, isso indicará que o leitor não está conectado à rede e, portanto, não funcionará. Informe a situação à equipe de segurança.

1. Apresente seu cartão no leitor de cartão.
   Se for necessária a verificação pelo padrão de veias da palma da mão, o leitor de veias agora indicará que está pronto para a leitura.
2. Mantenha a palma da mão sobre o leitor de veias da palma da mão até que ele mostre luzes verdes ou vermelhas.

– **Verde**: o padrão de veias da palma corresponde ao padrão armazenado. Acesso concedido.
– **Vermelho**: o padrão de veias da palma não corresponde ao padrão armazenado. Acesso negado.

24.2 Companies (Empresas)

- Essa caixa de diálogo pode ser usada para criar novas empresas e modificar ou excluir dados de empresas existentes.
- O nome da empresa e o nome abreviado devem ser inseridos. O nome abreviado deve ser único.
- Se a entrada de uma empresa for obrigatória na caixa de diálogo **Persons (Pessoas)**, crie a empresa nessa caixa de diálogo antes de tentar criar registros de funcionários para essa empresa.
- As empresas não podem ser excluídas do sistema se houver registros de funcionários atribuídos a elas.

24.3 Cartões: criação e atribuição de credenciais e permissões

A finalidade desta caixa de diálogo é atribuir **cartões**, **autorizações de acesso** ou pacotes de autorizações de acesso chamados **perfis de acesso** para registros de funcionários.
Autorizações e perfis de acesso são atribuídos a pessoas e não a cartões.
Novos cartões atribuídos a uma pessoa recebem as autorizações de acesso que já estão atribuídas a essa pessoa.

Observação: Usar perfis de acesso para agrupar autorizações
Para fins de consistência e conveniência, autorizações de acesso não são atribuídas individualmente, mas sim geralmente agrupadas em **Perfis de acesso** e atribuídas como tal.
- ACE Client (Cliente do ACE): **System data (Dados do sistema)** > **Access profiles (Perfis de acesso)**
- Main menu (Menu principal): **> System data (Dados do sistema)** > **Access profiles (Perfis de acesso)**

A lista de cartões
A lista de cartões de propriedade da pessoa selecionada é exibida na caixa de diálogo Cards (Cartões). Entre os atributos mostrados na lista estão:
- O tipo de uso do cartão.
- Um sinalizador que indica se o cartão pode ser usado em um sistema de bloqueio offline configurado.
- Se o cartão está bloqueado devido a um uso repetido de PINs inválidos. Este estado é realçado e fica em destaque.
- A data da criação do cartão
- Uma data de expiração (data de coleta) do cartão.
  Observação: Se um leitor de cartão motorizado estiver em uso, ele poderá reter fisicamente um cartão expirado. Caso contrário, o cartão será simplesmente invalidado.
- A data em que o cartão foi impresso pela última vez e o número de cartões impressos.
- Detalhes dos dados do código.

Opção **Administered globally (Administrados globalmente)**
Os dados das pessoas com a configuração **Administered globally (Administrados globalmente)** (caixa de seleção ao lado do quadro de foto) podem ser editados apenas por operadores com o direito adicional de **Administrador global**.
Os dados a seguir são somente leitura para operadores que não possuem esse direito:
- Todos os dados da caixa de diálogo **Persons (Pessoas)**, exceto as guias **Remarks, Extra info (Observações, Informações adicionais)** e os campos personalizados.

– Todos os dados da caixa de diálogo **Cards (Cartões)**.
– Todos os dados da caixa de diálogo **PIN Code (Código PIN)**.

Esse direito de **Administrador global** pode ser atribuído na seguinte caixa de seleção:
– Menu Navegador de configuração do BIS: **Adminstration (Administração)** > **Operators (Operadores)** > guia: **ACE operator settings (Configurações de operador do ACE)** > caixa de seleção: **Global Administrator (Administrador global)**.
– Main menu (Menu principal): **Configuration (Configuração)** > **Operators and workstations (Operadores e estações de trabalho)** > **User rights (Direitos de usuário)** > caixa de seleção: **Global Administrator (Administrador global)**.

24.3.1 Atribuição de cartões a pessoas

Introdução

Todas as pessoas sob controle de acesso precisam de um cartão ou outra credencial eletrônica, que é atribuída ao titular na caixa de diálogo **Cartões**.
Os números de cartão podem ser atribuídos manualmente ou por meio de um leitor de inscrições.

Caminho da caixa de diálogo

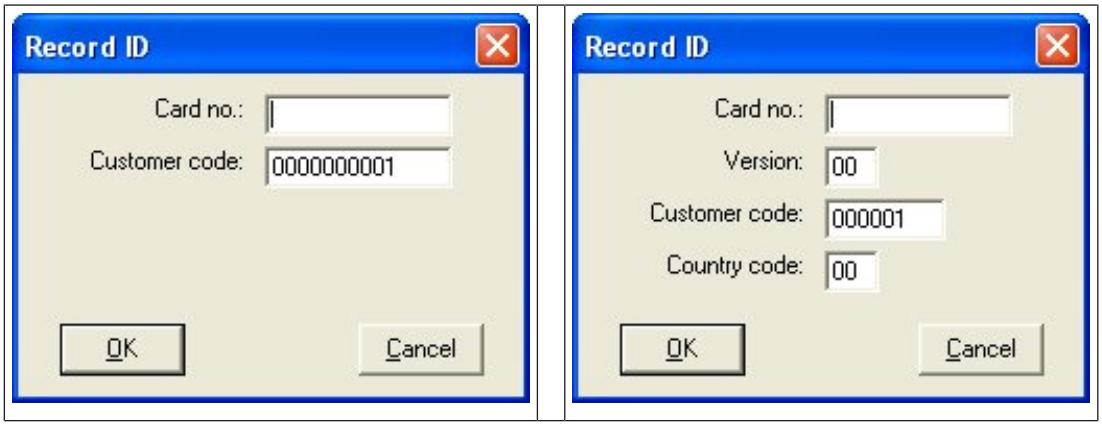
Main menu (Menu principal) > **Personnel data (Dados de funcionários)** > **Cards (Cartões)**

Pré-requisitos

– Você carregou o registro de pessoal que deve receber o cartão no cabeçalho da caixa de diálogo **Cartões**.

Inserção manual dos dados de cartão

Clique no botão **Record card (Registrar cartão)** para atribuir um cartão de identificação a uma pessoa. A máscara da caixa de diálogo **Record ID (Registrar identificação)** é exibida. Uma das duas caixas de diálogo de digitação será exibida, dependendo do tipo de cartão e dos controladores e leitores em uso.



Insira manualmente o número impresso no cartão de identificação – números de cartão são automaticamente preenchidos com zeros, para que possam sempre ser armazenados com 12 dígitos. Em alguns sistemas, nenhum novo número de cartão de identificação será atribuído se um cartão de identificação for perdido. Em vez disso, o mesmo número de cartão de

identificação é emitido com um número de versão superior. O código do país e o código do cliente são fornecidos pelo fabricante e devem ser introduzidos no arquivo de registro do sistema.
Se ainda não estiver sendo usado pelo sistema, o número de cartão é atribuído à pessoa. Uma atribuição bem-sucedida é confirmada por uma janela pop-up.

Usando um leitor de inscrições

Pré-requisito

– Um leitor de inscrições é configurado na sua estação de trabalho.

Procedimento para inscrição

1. Clique no botão ▸ no lado direito do botão **Registrar cartão** para selecionar um leitor de inscrições configurado.

– Para alterar a seleção do leitor de inscrições, é necessário fazer login no gerenciador de caixas de diálogo AMS como administrador.

2. Clique no botão **Registrar cartão** e siga as instruções na tela.
3. Dependendo do tipo de leitor, você pode inserir detalhes do cartão em uma caixa de diálogo ou ler dados do cartão apresentando-o para o leitor.

Procedimento para alterar cartões

1. Selecione um cartão na lista.
2. Clique no botão **Alterar cartão**
3. Na janela pop-up

– Selecione **Substituir cartão** se o original for permanentemente perdido ou danificado.
– Selecione **Cartão temporário** se o original tiver sido extraviado ou ficado em casa e somente uma substituição temporária for necessária.
  – Insira um período de validade para o cartão temporário.
  – Selecione se deseja desativar todos os outros cartões agora.
  – Selecione se os cartões originais devem ser reativados automaticamente quando o cartão temporário expirar.

4. Clique em **OK** para salvar.

Exclusão de cartões

1. Selecione um cartão na lista.
2. Clique no botão **Delete card (Excluir cartão)** para excluir a atribuição de uma pessoa a um cartão.

Observação: Se você excluir o último cartão de um titular, o status da pessoa mudará para **unregistered (não registrada)** (rótulo vermelho ao lado de **Registered (Registrada)** na barra de status). Essa pessoa não estará mais sujeita ao controle de acesso.

24.3.2 Impressão de crachás

Pré-requisitos

– O registro de funcionário para o novo titular do cartão já deve existir no sistema.
– Uma estação de trabalho com o seguinte hardware conectado, geralmente via USB:
  – Uma impressora de crachás
  – Uma câmera para capturar fotos de identificação.

Procedimento

Caminho da caixa de diálogo

Cliente do AMS: **Personnel data (Dados de funcionários)** > **Print badges (Imprimir crachás)**

1. Carregue o registro de pessoal para o qual o cartão deve ser impresso.

2. No menu suspenso **Layout**, selecione o layout de cartão desejado entre os layouts armazenados.
3. Obtenha uma foto de identificação usando um dos seguintes métodos:
   – Clique no botão **Capturar** e selecione a câmera desejada na lista de câmeras conectadas.
   – Clique no botão **Importar foto** e use o quadro de corte para selecionar a parte da foto a ser impressa no cartão.
4. Clique em **Visualizar** para garantir que os dados corretos apareçam no layout correto no crachá.
5. Clique em **Imprimir** para imprimir o crachá.

Câmeras compatíveis
Todos os dispositivos USB que o sistema operacional reconhece como uma câmera.

24.3.3 Guia de autorizações

Atribuição de autorizações agrupadas como Perfis de acesso
A maneira mais conveniente e flexível de atribuir autorizações para titulares de cartões é agrupá-las em Perfis de acesso e, em seguida, atribuir o perfil.
– Para criar Perfis de acesso, consulte a seção *Criação de perfis de acesso, página 187*
– Para atribuir um Perfil de acesso a esse titular, selecione um perfil definido na lista **Access profile: (Perfil de acesso:)**

Atribuição direta de autorizações de acesso
Na guia **Authorizations (Autorizações)**:
Todas as autorizações de acesso já atribuídas à pessoa são exibidas na lista à esquerda.
Todas as autorizações de acesso disponíveis para atribuição são exibidas na lista à direita.
Selecione os itens e clique nos botões entre as listas para mover os itens de uma lista para a outra.

 atribui o item selecionado.

 cancela a atribuição do item selecionado.

 atribui todos os itens disponíveis.

 cancela a atribuição de todos os itens atribuídos.

Opção: **Keep authorizations assigned (Manter autorizações atribuídas)**
O efeito de atribuir um perfil de acesso a uma pessoa depende da caixa de seleção **Keep authorizations assigned (Manter autorizações atribuídas)**:
– Se a caixa de seleção estiver desmarcada, qualquer seleção feita antes disso e quaisquer autorizações de acesso já atribuídas serão **substituídas** quando o perfil for atribuído.
– Se a caixa de seleção estiver marcada, as autorizações do perfil serão **adicionadas** às autorizações atribuídas.

Limite do intervalo de tempo das autorizações
Use os campos de data **Valid from: (Válido de:)** e **until: (até:)** para limitar as datas de início e término das autorizações e perfis. Se nenhum valor for definido, a autorização terá validade imediata e duração ilimitada.

Clique em  para abrir uma caixa de diálogo e definir durações para autorizações individuais.

Exibição das entradas de uma autorização
Clique com o botão direito em uma autorização em uma das listas para exibir uma lista das entradas que pertencem a ela.

24.3.4 Guia de outros dados: isenções e permissões especiais

Atribuindo um modelo de tempo:
Use a caixa de lista **Modelo de tempo** para especificar as horas diárias de acesso do titular do cartão, ou seja, os períodos em que as credenciais do titular concederão acesso.

Excluindo pessoas da revista aleatória
Marque a caixa de seleção **Excluído da revista aleatória** para impedir que sejam selecionadas aleatoriamente para inspeções em entradas e saídas.

Excluir pessoas de verificações do código PIN
Marque a caixa de seleção **Desativar verificação do código PIN** para que as pessoas não precisem inserir códigos PIN em leitores de código PIN fora do expediente normal.

Aviso!
A exclusão das verificações de código PIN afeta o sistema inteiro.
Por exemplo, como o código PIN dessas pessoas não é verificado, elas também não poderão armar ou desarmar alarmes em entradas no modelo de porta 10.

Estendendo o tempo de abertura da porta
Marque a caixa de seleção **Tempo de abertura da porta estendido** para que pessoas com deficiência tenham mais tempo (o padrão é 3x) para passar por uma entrada antes que o estado **Porta aberta muito tempo** seja gerada.
Observação: o fator de extensão padrão pode ser redefinido nas propriedades do MAC no Editor de dispositivos.
Selecione **Configurações de acesso globais** > **Fator de tempo para pessoas deficientes**

Monitoramento do tour
Um **Tour** ou **Rota** é uma sequência rígida de leitores que é definida no menu Cliente: **Monitoramento do tour** > caixa de diálogo **Definir rotas**.
Para atribuir um tour a um titular de cartão, marque a caixa de seleção **Monitoramento do tour** e selecione um tour definido na lista suspensa. Se nenhum tour tiver sido definido, a caixa de seleção ficará inativa.
Quando atribuído a um titular de cartão, um **Tour** é ativado assim que o titular passa o cartão no primeiro leitor da sequência. Depois disso, todos os leitores da sequência deverão ser usados em ordem, até o tour ser concluído. Os usos típicos são impor sequências rígidas de acesso em ambientes industriais limpos, higienicamente controlados, ou áreas de alta segurança.

Permissão para destravar portas
Marque a caixa de seleção para que o titular do cartão possa destravar portas por um período estendido (consulte **Modo de escritório**).

Consulte

– *Autorizar pessoas a ativarem o modo Escritório, página 204*

24.3.5 Autorizar pessoas a ativarem o modo Escritório

Introdução

O termo modo Escritório descreve a suspensão do controle de acesso em uma entrada durante o horário comercial. A entrada permanece destrancada durante essas horas, para permitir acesso público sem nenhum obstáculo. Fora do horário comercial, o modo Normal volta a valer, ou seja, o acesso é concedido somente a quem apresentar credenciais válidas ao leitor.

O modo Escritório é um requisito normal de lojas de varejo, instalações educacionais ou médicas.

Pré-requisitos

Para que o modo Escritório funcione, os seguintes requisitos devem ser satisfeitos:

Na configuração (árvore de dispositivos)

– Uma ou mais entradas devem ser configuradas para permitir períodos estendidos com a entrada destrancada.
– Pelo menos um leitor com teclado deve ser usado na entrada.

No cliente (caixas de diálogo de Persons (Pessoas))

– Um ou mais titulares de cartões devem ter autorização para colocar e tirar a entrada do modo Escritório.
– Seus cartões devem ser válidos e permitir o acesso à entrada fora do horário comercial.

Procedimentos para autorizar pessoas a ativarem o modo Escritório

Procedimento para titulares de cartões individuais

1. Navegue até: **Dados pessoais** > **Cartões** > guia:**Outros dados** e crie ou ache o titular do cartão designado no banco de dados.
2. Marque a caixa de seleção **Permissão para destravar portas**.
3. Clique no ícone de disquete  para salvar os dados do titular do cartão.

Procedimento para grupos de titulares de cartões

1. Navegue até: **Dados pessoais** > **Grupos de pessoas** e use os critérios de filtragem para criar uma lista de titulares de cartão na janela da lista.
2. A partir da lista suspensa **Campo a ser alterado,** selecione **Destravar portas**
3. Marque a caixa de seleção **Destravar portas**.
4. Clique no botão **Aplicar alterações** para salvar os dados do titular do cartão.

Instruir o titular do cartão sobre como iniciar e interromper o modo Escritório

Para iniciar ou interromper o modo Escritório na entrada, o titular do cartão pressiona o número 3 no teclado e, em seguida, apresenta ao leitor seu cartão com autorização especial. A entrada permanece destravada até que o titular do cartão autorizado pressione 3 e apresente o cartão novamente.

Observe que os guardas com cartões de vigilante podem interromper o modo Escritório da mesma maneira, sem permissão especial.

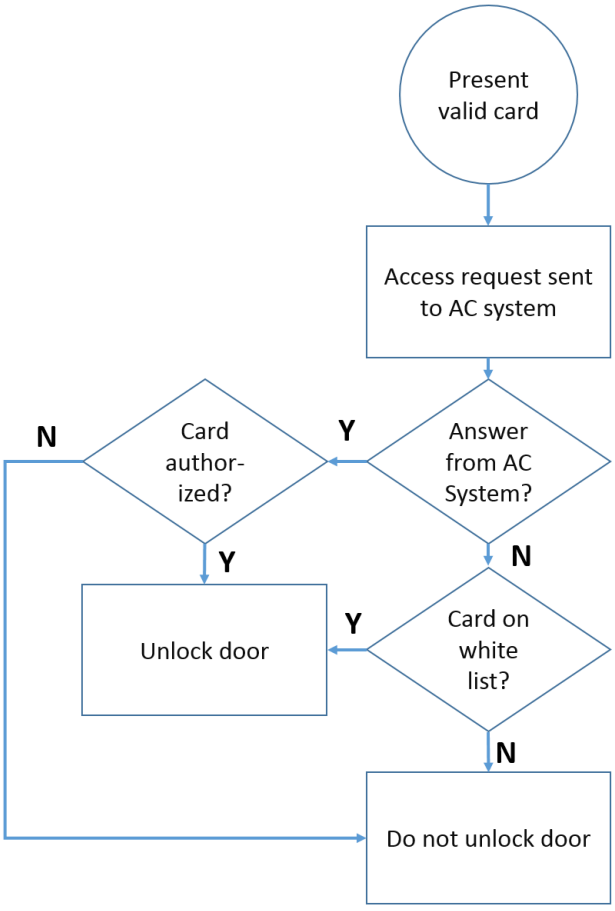
Aviso!
Modo de escritório e parâmetros do dispositivo para porta
O Modo de escritório substitui o parâmetro **Destravar porta** na guia **Opções** de uma porta no Editor de dispositivos, permitindo somente **0 Modo normal** e **1 Destravado**.

24.3.6 Guia SmartIntego

Sistemas de bloqueio SmartIntego

Introdução

O leitor de cartões SmartIntego tenta autorizar o acesso pelo sistema principal de controle de acesso (AC) primeiro. Se a conexão falhar, ele procura o número do cartão em sua lista de autorizações armazenada.



As autorizações de acesso para o sistema de bloqueio SmartIntego são atribuídas mais ou menos da mesma maneira que qualquer outra autorização de acesso.

Pré-requisitos

– Um sistema de bloqueio SimonsVoss SmartIntego foi configurado dentro do seu sistema de controle de acesso. Consulte o manual de configuração para mais instruções.

– Os titulares de cartões estão usando cartões MIFARE Classic ou MIFARE Desfire.
O SmartIntego usa o Número de Série do Cartão (CSN, na sigla em inglês).

O procedimento de atribuição

O seguinte procedimento descreve como adicionar um número de cartão a uma lista de autorizações do SmartIntego, além de quaisquer autorizações que já tenham sido atribuídas por meio do sistema de controle de acesso principal.
As listas de autorizações são armazenadas localmente nas portas do SmartIntego, para que um leitor possa dar acesso aos números de cartões da lista de autorizações mesmo quando a conexão com seu MAC não estiver funcionando.
As adições e exclusões das listas de autorizações são transmitidas aos leitores SmartIntego assim que os dados do titular do cartão são salvos e assim que uma conexão é disponibilizada.

1. No menu do cliente ACE, selecione **Personnel data (Dados de funcionários)** > **Cards (Cartões)**
2. No menu do cliente principal AMS, selecione **Personnel data (Dados de funcionários)** > **Cards (Cartões)**
3. Selecione a pessoa que receberá as autorizações do SmartIntego
4. Selecione a guia **SmartIntego.**
5. Faça as atribuições:
   – Todas as autorizações de acesso já atribuídas à pessoa são exibidas na lista à esquerda.
   – Todas as autorizações de acesso disponíveis para atribuição são exibidas na lista à direita.

Selecione os itens e clique nos botões entre as listas para mover os itens de uma lista para a outra.


atribui o item selecionado.


cancela a atribuição do item selecionado.


atribui todos os itens disponíveis.


cancela a atribuição de todos os itens atribuídos.

24.3.7 Criação de um cartão de alerta

Esta seção descreve como criar um cartão de alerta que pode ser usado para acionar um nível de ameaça

Introdução

Um cartão de alerta é um cartão que aciona um determinado nível de ameaça quando apresentado para um leitor. Um nível de ameaça não pode ser cancelado por um cartão de alerta, mas apenas pelo software de controle de acesso.

Pré-requisitos

– Um leitor de inscrições é configurado no seu sistema.
– Pelo menos um nível de ameaça foi definido no sistema.

Caminho da caixa de diálogo

Menu principal > **Dados de pessoal** > **Cartões** > **Cartão de alerta**

Procedimento

1. Carregue o registro da pessoa a quem o cartão de alerta será atribuído
2. Na guia Cartão de alerta, clique em Registrar cartão
   – Uma janela pop-up é exibida: **Selecionar nível de ameaça**
3. Na janela pop-up, selecione o nível de ameaça desejado e clique em **OK**
   – Uma janela pop-up é exibida: **Registrando ID do crachá**
4. Insira os dados do cartão normais que correspondem à instalação local e clique em **OK**
   – O cartão de alerta registrado aparece na lista na guia **Cartão de alerta**.

24.4 Cartões temporários

Um cartão temporário é um substituto temporário para um cartão que foi indevidamente alocado por um titular de cartão regular. É uma cópia que contém todas as autorizações e limitações do original, incluindo os direitos para portas offline.
Para evitar abusos, o sistema pode, opcionalmente, bloquear um ou todos os outros cartões do titular durante um período limitado, ou até que seja desbloqueado manualmente.
Cartões temporários são, portanto, **inadequados** para o uso como cartões de visitantes.

Pré-requisitos

– O operador tem acesso a um leitor de inscrições configurado na estação de trabalho.
– Um cartão físico adequado está disponível para inscrição no sistema como um cartão temporário.

Cliente do ACE: **Personnel data (Dados de funcionários)** > **Cards (Cartões)**
Main menu (Menu principal) > **Personnel data (Dados de funcionários)** > **Cards (Cartões)**

Procedimento: atribuição de cartões temporários

1. Carregue o registro de funcionário necessário na caixa de diálogo **Cards (Cartões)**
2. Na lista de cartões, selecione o cartão ou os cartões que exigem um substituto temporário
3. Clique em **Change card (Alterar cartão)**
4. Na janela pop-up **Change card (Alterar cartão)**, selecione **Temporary card (Cartão temporário)**
5. Na lista **Period (Período)**, selecione uma das opções:
   – **Today (Hoje)**
   – **Today and tomorrow (Hoje e amanhã)**
   – **Enter number of days (Inserir o número de dias)**
6. No caso da última opção, insira um inteiro para o número de dias na caixa.
   Observe que nos três casos, o **Period (Período)** sempre expira à meia-noite do dia relevante.
7. Se necessário, marque a caixa de seleção **Deactivate all cards now (Desativar todos os cartões agora)**.
   – Se marcada, todos os cartões pertencentes a esse titular serão bloqueados.
   – Se desmarcada, somente o cartão selecionado acima será bloqueado.
8. Se necessário, marque a caixa de seleção **Activate card(s) automatically after period (Ativar cartão(ões) automaticamente após o período)**.
   – Os cartões bloqueados serão desbloqueados automaticamente assim que o **Period (Período)** definido acima expirar.
9. Colocar o cartão temporário no leitor de cadastramento
10. Clique em **OK**
    A identificação do crachá será registrada pelo leitor de cadastramento.

- O cartão temporário aparece como ativo ✔ na lista de cartões, junto com o período de validade e os dados do código.
- Os outros cartões aparecem como bloqueado ✘, dependendo da definição feita acima: **Deactivate all cards now (Desativar todos os cartões agora)**.

11. (Opcional) Na lista de cartões, clique na coluna **Collecting date (Data de coleta)** para o cartão temporário e defina uma data recebê-lo de volta do titular.
    O valor padrão é **Never (Nunca)**.

Procedimento: exclusão de cartões temporários
Quando o cartão original alocado indevidamente for encontrado, exclua o cartão temporário da seguinte forma:

1. Carregue o registro de funcionário necessário na caixa de diálogo **Cards (Cartões)**.
2. Na lista de cartões, selecione o cartão temporário.
3. Clique em **Delete card (Excluir cartão)**
   O cartão temporário será excluído da lista e o cartão, ou cartões, substituídos serão desbloqueados imediatamente.

Procedimento: remoção de bloqueios temporários em cartões
Se o bloqueio do cartão original não for mais necessário, exclua o bloco da seguinte forma:

1. Navegue até a caixa de diálogo **Bloqueio**: **Dados de pessoal** > **Bloqueio**.
2. Na lista de cartões, selecione o cartão de pessoal marcado como bloqueado na coluna **Bloqueios**.
3. Clique em **Liberar bloqueio temporário**
   A remoção do **Bloqueio** não remove cartões temporários. Os cartões temporários expiram naturalmente depois dos períodos de validade. Se necessário, exclua-os manualmente.

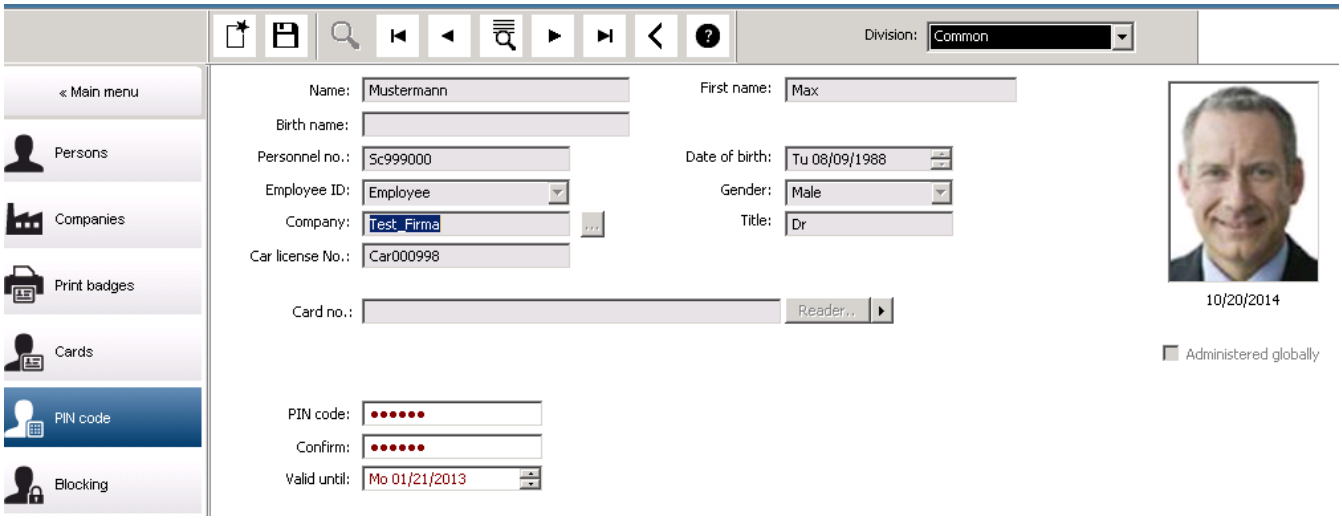
Observações sobre os cartões temporários

- O sistema não permite que os próprios cartões temporários sejam substituídos por outros cartões temporários.
- O sistema não permite que um cartão pessoal tenha mais de um cartão temporário.
- Para ver um resumo rápido de todos os cartões em posse de um titular, passe o mouse sobre o pequeno painel à extrema esquerda, rotulado **Registered (Registrada)**, na barra de status da janela de diálogo principal.

24.5 Códigos PIN para funcionários

Caixa de diálogo: PIN-Code (Código PIN)
Para acesso a zonas com requisitos de segurança mais altos, uma autorização de acesso pode não ser suficiente. Aqui um código PIN também deve ser digitado. Cada pessoa ou cartão de identificação pode ter um código PIN, que é válido para todas as áreas. O sistema impede a utilização de códigos muito simples (por exemplo, 123456 ou palíndromos como 127721). A validade pode ser restringida e é especificada para cada pessoa na caixa de diálogo.
Se o código PIN estiver bloqueado ou vencido o acesso à área que requer o código será negado, mesmo que o cartão de identificação ainda seja válido para todas as outras áreas.

Se um código incorreto for digitado três vezes consecutivas (configuração padrão – pode ser configurado entre 1 e 99), este cartão será bloqueado, ou seja, o acesso a todas as áreas será negado. Um cartão bloqueado dessa forma só pode ser desbloqueado através da caixa de diálogo Blocking (Bloqueio).



Insira um novo código PIN no campo **PIN-Code (Código PIN)** e confirme ao redigitá-lo. O comprimento do código PIN (entre 4 e 9 caracteres, o valor padrão é 6) é configurado pelo administrador do sistema.

Aviso!
A maneira como os usuários de cartões inserem PINs de identificação em leitores de cartão depende dos tipos de leitores configurados em seu sistema. Por exemplo:
Nos leitores RS485, os usuários de cartão inserem: **4 #** `<the PIN>`
No Wiegand e outros leitores de cartão, os usuários de cartão inserem: `<the PIN>` **#**
Certifique-se de informar aos usuários de cartões para inserirem seus PINs. Se estiver em dúvida, consulte seu administrador do sistema.

Código PIN para armar sistemas de detecção de intrusão (IDS)
Um PIN de 4 a 8 dígitos deve ser inserido (padrão = 6 – o mesmo comprimento do PIN de verificação). Esse PIN será usado para armar um IDS.
A exibição desses campos pode ser parametrizada. O controle estará disponível somente se o controle **separate IDS PIN (PIN de IDS separado)** estiver ativado.

- Configuration Browser (Navegador de configuração) > **Infrastructure (Infraestrutura)** > **System configuration (Configuração do sistema)** > **ACE PIN-Codes (Códigos PIN do ACE)**
- Main menu (Menu principal) > **Configuration (Configuração)** > **Options (Opções)** > **PIN codes (Códigos PIN)**

Selecione uma data de validade, se necessário.
Se os campos para digitar o PIN de IDS não estiverem disponíveis, o PIN de verificação pode ser usado para armar e desarmar o IDS também. Mas se os campos de digitação forem exibidos nesta caixa de diálogo, o PIN de arme só poderá ser usado para o IDS.
Configuração padrão: os campos de digitação do código PIN de arme são invisíveis.

PINs de alarme (coação)

Pessoas sob coação podem acionar um alarme silencioso através de um código PIN especial. Como o alarme silencioso precisa permanecer oculto do agressor, o acesso será concedido, mas os operadores do sistema serão alertados sobre a coação.

Duas variantes estão disponíveis e são ativadas ao mesmo tempo. A pessoa ameaçada pode escolher entre:

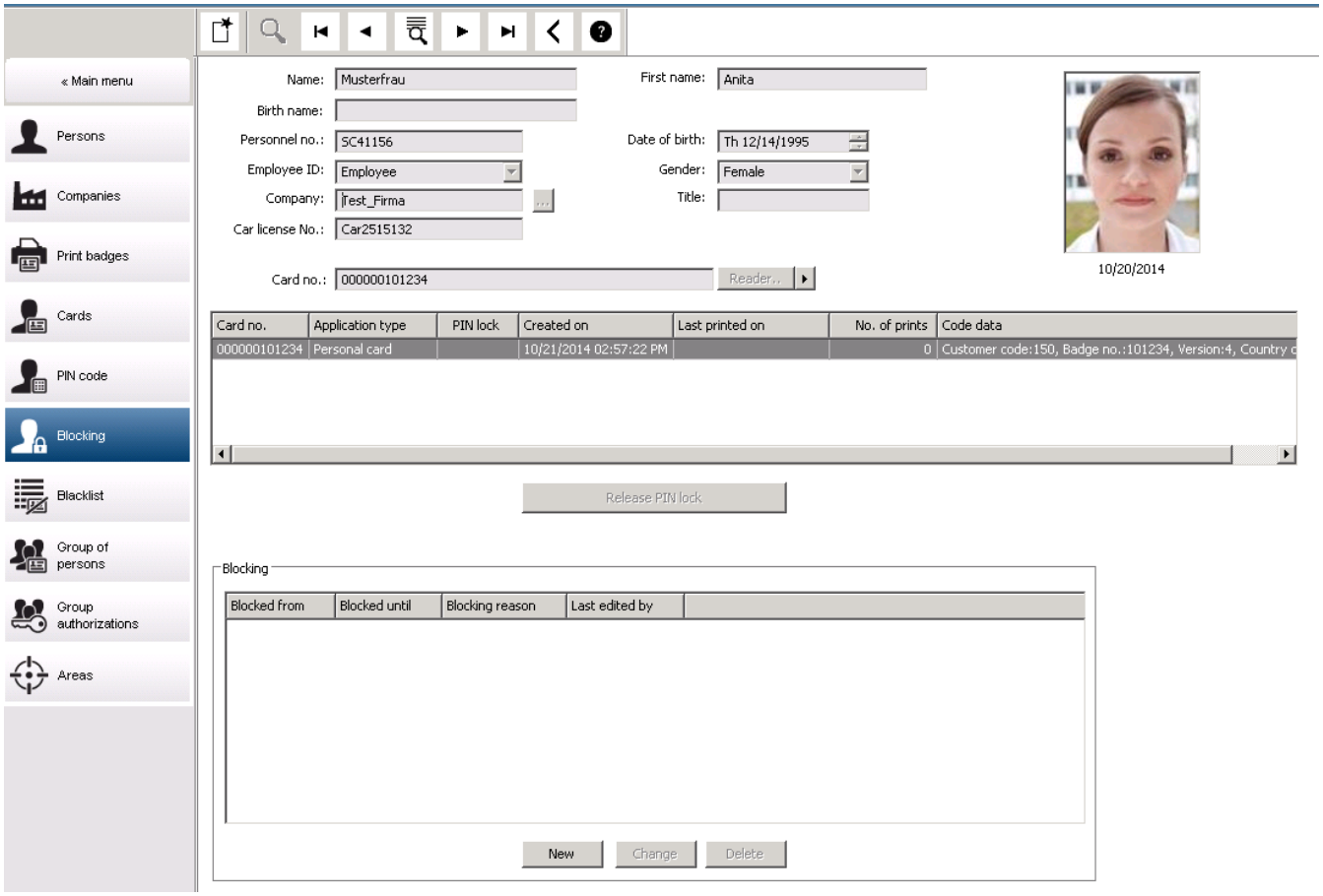
– Inserir o código PIN na ordem inversa (321321 em vez de 123123).
– Acrescentar 1 ao PIN (por exemplo: 123124 em vez de 123123). Observe que se o último dígito for 9, o PIN ainda será incrementado. Portanto, o PIN 123129 teria 123130 como PIN de coação.

24.6 Bloqueio do acesso para funcionários

Caixa de diálogo: Blocking (Bloqueio)

Em determinadas situações é necessário negar o acesso a uma Pessoa temporariamente ou remover um bloqueio imposto pelo MAC, por exemplo, devido a códigos PIN incorretos digitados três vezes ou à triagem aleatória.

O bloqueio significa que todo o acesso é negado para esta pessoa, independentemente da credencial usada.



1. Selecione a pessoa, como de costume.

2. No painel Bloqueio, clique em **New (Novo)** para criar um bloco para a pessoa selecionada no momento.
3. Insira informações adicionais na caixa de diálogo pop-up:
   – **Blocked from / until (Bloqueado de/até)**: (Se nenhuma data de término for especificada, a pessoa estará bloqueada até o bloqueio ser retirado manualmente.)
   – **Block type (Tipo de bloqueio):**
   – **Blocking reason (Motivo do bloqueio):** (Para o registro da pessoa, se o tipo de bloqueio for `Manual`)
4. Clique em **Save (Salvar)** no pop-up para salvar o bloqueio.

– Se necessário, selecione um bloco da lista e clique em **Change (Alterar)** ou **Delete (Excluir)** para alterar ou excluí-lo.

Se **Manual lock (Bloqueio manual)** for escolhido como tipo de bloco, insira um **Blocking reason (Motivo de bloqueio)** para o registro da pessoa.

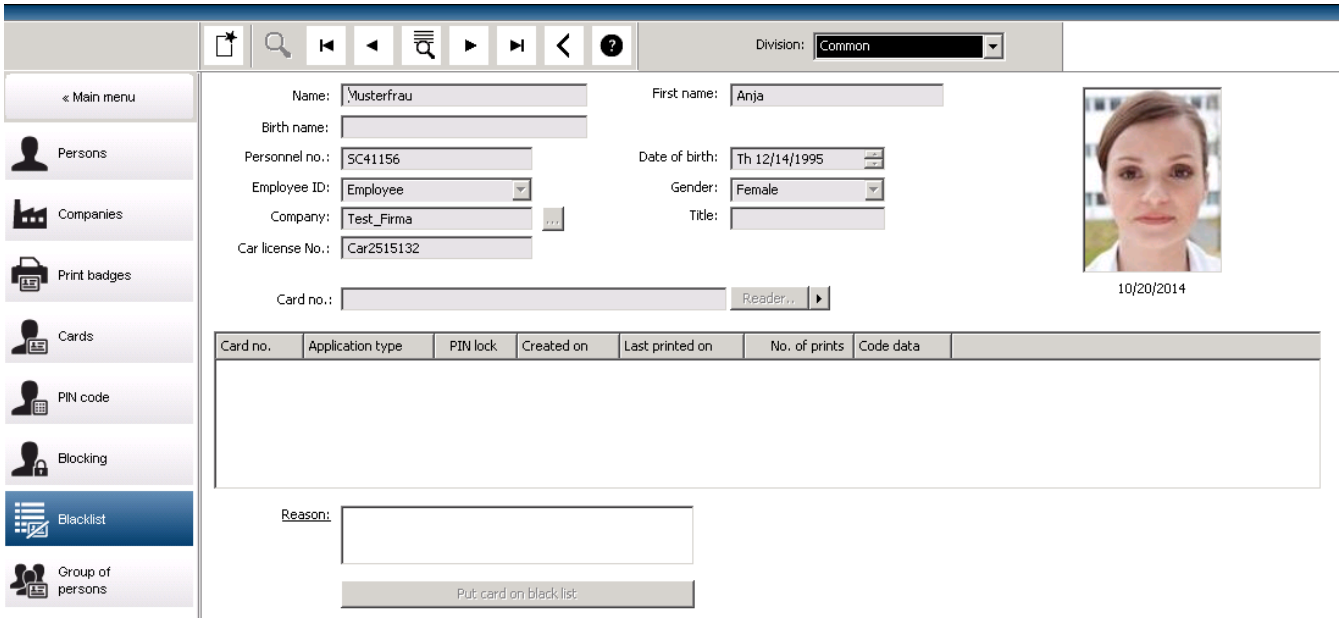
Aviso!
O bloqueio se aplica à pessoa, e não a uma credencial específica. Portanto, não é possível cancelar ou evitar o bloqueio através da atribuição de um novo cartão de identificação.

24.7 Cartões da lista negra

Caixa de diálogo: Blacklist (Lista negra)
Qualquer cartão que não deva nunca mais ser usado, por exemplo, que tenha sido roubado ou perdido, é inserido em uma lista negra.
Observe que a credencial incluída na lista negra, e não a pessoa.

Aviso!
O processo é irreversível. Os cartões na lista negra nunca poderão ser desbloqueados, mas devem ser substituídos.

Os cartões na lista negra não concedem acesso. Em vez disso, as tentativas de uso deles são registradas no arquivo de log, e um alarme é gerado.



Main menu (Menu principal) > **Personnel data (Dados de funcionários)** > **Blacklist (Lista negra)**

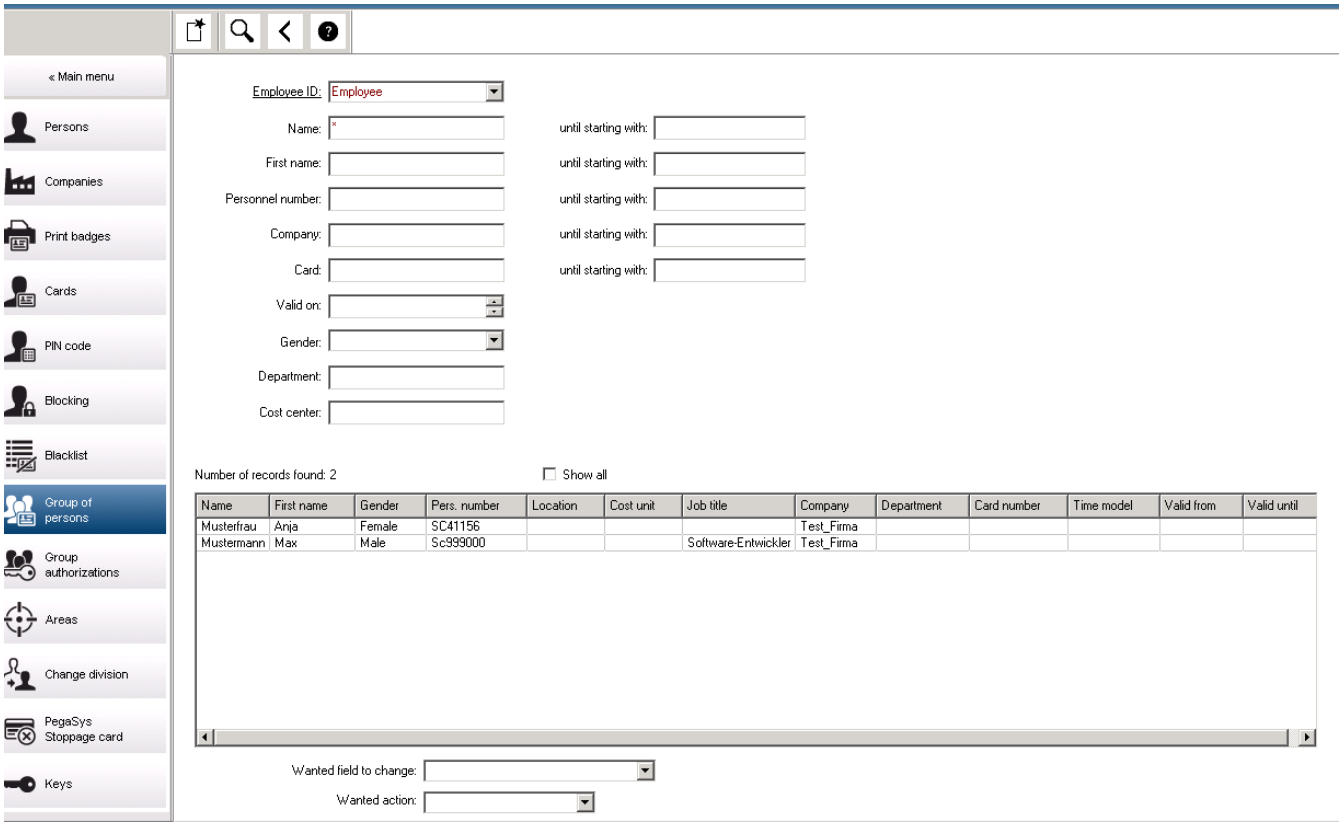
1. Selecione a pessoa cujo cartão de identificação deve ser inserido na lista negra.
2. Se mais de um cartão tiver sido atribuído a esse usuário, selecione o cartão na lista **ID card No (Número do cartão de identificação)**.
3. Insira o motivo para inserção do cartão na lista negra no campo de entrada **Reason (Motivo)**.
4. Clique no botão **Blacklist this card (Colocar este cartão na lista negra)**.
5. Confirme a inclusão na lista negra na janela pop-up.

O cartão é colocado na lista negra imediatamente.

Aviso!
A inclusão de cartões na lista negra afeta cartões, **não** os titulares de cartões.
Os cartões não incluídos na lista negra pertencentes ao mesmo titular do cartão não são bloqueados.

24.8 Edição de várias pessoas simultaneamente

Grupo de pessoas



Outra caixa de diálogo seleciona um grupo de pessoas para o qual as modificações podem ser definidas. Para manter controle sobre o grupo de pessoas selecionado, as primeiras dez pessoas são listadas com nomes e dados reais da base de dados (dados reais: se "ST-AC" for selecionado como departamento, então "ST-ACS" e "ST-ACX" serão exibidos, por exemplo). Além disso, o número de pessoas do grupo selecionado é exibido.
Depois que o grupo de pessoas for selecionado, os seguintes atributos podem ser selecionados:

- Employee ID (Identificação do funcionário)
- Name (Nome)
- First name (Nome)
- Personnel number (Número do funcionário)
- Company (Empresa)
- Card (Cartão)
- Valid on (Válido em)
- Gender (Gênero)
- Department (Departamento)
- Cost unit (Unidade de custo)
- Campos de reserva, se definidos

Em seguida, a opção de modificação pode ser selecionada:

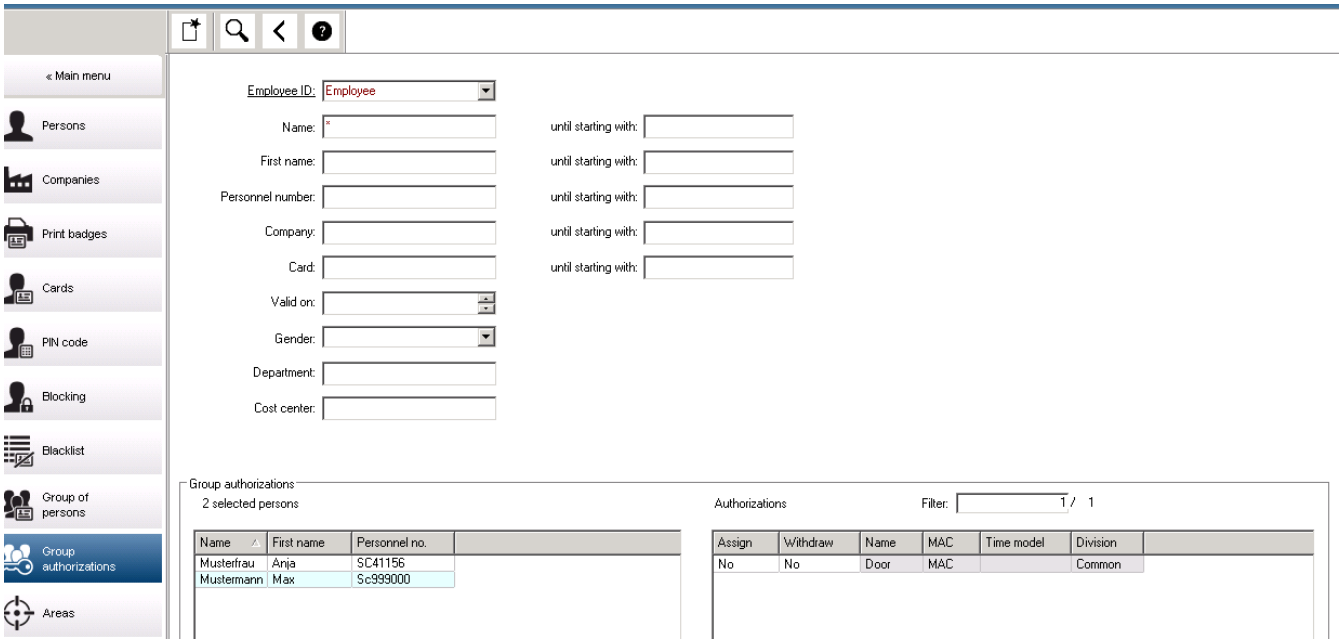
- Field to be changed (Campo a ser alterado)
- Desired action (Ação desejada)
- Old value (Valor antigo)

– New value (Novo valor).

Assim, os valores designados são digitados respectivamente no campo **Old value (Valor antigo)** ou **New value (Novo valor)**. Ao selecionar o botão **Apply changes (Aplicar alterações)** e confirmar a solicitação de segurança **apply changes for all selected persons? (aplicar alterações a todas as pessoas selecionadas?)** a ação será concluída, ou seja, a caixa de diálogo não poderá ser usada enquanto a ação estiver em curso. As ações disparadas pelos campos *1 a *4 provavelmente vão demorar mais tempo que as dos outros campos (sem asterisco), e nem todas as modificações serão permitidas. Assim, por exemplo, a **Desired action (Ação desejada)** não pode ser comparada com o **New value (Novo valor)**, uma vez que essas entradas não estão inclusas no produto padrão. Os campos **Old value (Valor antigo)** e **New value (Novo valor)** também podem variar, respectivamente.

24.8.1 Autorizações de grupo

Autorização em grupo



No item do menu **[Group Authorization] ([Autorização em grupo])** os seguintes critérios de pesquisa são compatíveis:

– Employee ID (Identificação do funcionário)
– Name (Nome)
– First name (Nome)
– Personnel number (Número do funcionário)
– Company (Empresa)
– Card (Cartão)
– Valid on (Válido em)
– Gender (Gênero)
– Department (Departamento)
– Cost unit (Unidade de custo)
– Campos de reserva, se definidos

Em seguida, a parte inferior da caixa de diálogo exibe uma lista com todas as pessoas selecionadas (com sobrenome, nome e número de funcionário). Todas as autorizações com descrição são listadas na parte inferior direita, com a descrição da autorização, o modelo de tempo e as colunas **[Assign] ([Atribuir])** e **[Withdraw] ([Retirar])**. Quando a lista de autorizações é aberta, as autorizações atuais não são mostradas e as colunas **[Assign] ([Atribuir])** e **[Withdraw] ([Retirar])** são predefinidas para "No" (Não). Agora as autorizações individuais podem ser atribuídas clicando duas vezes no campo de qualquer coluna, o que converte o "No" (Não) para um "Yes" (Sim) ou vice-versa. Ao clicar em Executar alterações, todas as autorizações marcadas com "Yes" (Sim) são adicionadas a todas as pessoas selecionadas – ou retiradas, respectivamente. Todas as outras autorizações das pessoas permanecem inalteradas, porque normalmente as pessoas selecionadas não têm autorizações completamente idênticas.

24.9 Alteração da divisão para pessoas

Introdução

Change division (Alterar divisão) é uma caixa de diálogo eficaz para alterar a divisão de um conjunto de registros de funcionários no sistema.

Aviso!
Use esse recurso com muito cuidado!
Uma mudança de divisão apresenta amplas consequências para os registros de funcionários alterados.

Pré-requisitos

O operador capaz de alterar a divisão de registros de funcionários deve ter autorizações para editar essas pessoas e ambas as divisões em questão.

Caminho da caixa de diálogo

Main menu (Menu principal) > **Personnel data (Dados de funcionários)** > **Change division (Alterar divisão)**

Procedimento

1. No painel **Filter persons (Filtrar pessoas)**, insira critérios de filtro em um ou mais dos seguintes campos:

Filter (Filtrar)	Remarks / Description (Observações / Descrição)
Last name (Sobrenome)	Use um asterisco simples para correspondência com todas as pessoas ou letras **sem** asteriscos
Personnel no. from/ to (Número de funcionário de/até)	Use ambos os campos para definir um intervalo de valores
Employee ID (Employee type) (Identificação do funcionário (tipo de funcionário))	Selecione na lista
Division (Divisão)	O botão Apply filter (Aplicar filtro) mostrará somente as pessoas dessa divisão

Company (Empresa)	Selecione entre as empresas disponíveis
Department (Departamento)	
Card no. (from/to) (Número do cartão (de/até))	Use ambos os campos para definir um intervalo de valores

2. Clique em **Apply filter (Aplicar filtro)**
   Todas as pessoas que corresponderem ao filtro serão exibidas na lista **Selected persons (Pessoas selecionadas).**
3. Para refinar ainda mais o conjunto de pessoas selecionadas, clique em uma ou mais linhas da lista **Selected persons (Pessoas selecionadas)** e clique no botão **Remove (Remover)**. Use as teclas Ctrl e Shift para selecionar vários registros de uma vez.
   – **IMPORTANTE:** Antes de prosseguir, verifique se a lista **Selected persons (Pessoas selecionadas)** contém somente as pessoas para as quais você deseja alterar a divisão.
4. Na lista **New division (Nova divisão)**, selecione a divisão de destino para as pessoas selecionadas.
5. Clique em **Change division of persons (Alterar divisão das pessoas)**
   TODAS as pessoas da lista **Selected persons (Pessoas selecionadas)** serão movidas para **New division (Nova divisão)**.

Efeitos da mudança de uma divisão para outra

Pessoas

– Autorizações de acesso e controle de caminho
– Os links para a divisão anterior são excluídos.
– Os links de dados da categoria Comum são mantidos.

Empresas

– Os links para empresas da divisão anterior são excluídos.

Efeitos da mudança de Comum para outra divisão

– Autorizações de acesso e controle de caminho
– Os links para Comum e para a nova divisão são mantidos.
– Os links para outras divisões são excluídos.

Efeitos da mudança de uma divisão para Comum

Todos os links são mantidos.

24.10 Definição da área para pessoas ou veículos

Introdução

Esta seção descreve como alterar a localização registrada de um titular de cartão ou de seu veículo de uma área definida para outra. Isso pode tornar-se necessário se o titular do cartão passar de uma área para outra sem realizar a leitura do cartão. Nessas circunstâncias, sistemas rígidos de antidupla entrada negarão os acessos subsequentes ao titular do cartão até que as localizações atual e registrada sejam iguais.

Pré-requisitos

– Áreas de acesso foram definidas no sistema e estão em uso. Para obter a documentação, consulte o link abaixo.
– Como operador, você tem autorização para modificar os dados do titular do cartão.

Procedimento para redefinir a localização de titulares de cartões e veículos individuais
Caminho da caixa de diálogo
Main menu (Menu principal) > **Personnel data (Dados de funcionários)** > **Areas (Áreas)**

1. Selecione o titular do cartão no banco de dados, como de costume
2. Na lista **Location (Localização)**, selecione uma nova localização
   ou
3. Na lista **Location of the vehicle (Localização do veículo)**, selecione uma nova localização para o veículo do titular do cartão
4. Clique em  para salvar

Consulte
– *Configuração de áreas de controle de acesso, página 24*

24.10.1 Procedimento para redefinir a localização de todos os titulares de cartões e veículos

Este procedimento poderá ser necessário, por exemplo, após um treinamento de evacuação. Todas as localizações são definidas como **UNKNOWN (Desconhecidas)** para que o monitoramento da sequência de acesso e a antidupla entrada sejam retomados.

Procedimento
Caminho da caixa de diálogo
Main menu (Menu principal) > **System data (Dados do sistema)** > **Reset areas unknown (Redefinir áreas desconhecidas)**

– Clique em **Set the areas of all persons present to UNKNOWN (Definir as áreas de todas as pessoas presentes como DESCONHECIDAS)**

ou

– Clique em **Set the areas of all parking vehicles to UNKNOWN (Definir as áreas de todos os veículos do estacionamento como DESCONHECIDAS)**

24.11 Personalizando e imprimindo formulários para dados de pessoal

Visão geral
Use **Formulários** para personalizar formulários para imprimir dados do titular do cartão do banco de dados. Essa função pode ser necessária de acordo com as leis locais de privacidade de dados.
Modelos de formulário são fornecidos. Esses modelos podem ser exportados como arquivos HTML, personalizados segundo seus requisitos e reimportados para uso no gerenciador de caixas de diálogo.
Instancie e imprima os formulários na caixa de diálogo **Dados de pessoal** > **Imprimir crachás**.

Caminho da caixa de diálogo
– Menu principal do AMS > **Configuração** > **Opções** > **Formulários**

Personalizando um formulário

1. Na caixa de diálogo **Formulários**, na lista **Formulários disponíveis**, selecione o modelo que deseja personalizar, normalmente `AllPersonalData_EN, `, que contém todos os campos de dados pessoais no banco de dados.
2. Clique em **Exportar** para salvar o formulário para um novo arquivo HTML no seu sistema
3. Use um editor de HTML para personalizar o arquivo HTML segundo seus requisitos
4. Na caixa de diálogo **Formulários**, clique em **Inserir** para importar o arquivo HTML personalizado para o gerenciador de caixas de diálogo.
   - (Opcional) Se o formulário for válido apenas para uma divisão específica, selecione uma divisão para o novo formulário na coluna **Divisão**.
   - (Opcional) Clique em **Visualizar** para ver o formulário não instanciado em um visualizador HTML.
   - (Opcional) Clique em **Excluir** para excluir um formulário da lista.

Instanciando e imprimindo um formulário

1. No gerenciador de caixas de diálogo, navegue até
– Menu principal do AMS > **Dados de pessoal** > **Imprimir crachás**
2. Carregue o registro de pessoal desejado no formulário
3. Selecione um formulário na lista **Formulário**.
4. Clique em **Imprimir formulário**
   - O formulário é instanciado com os dados do registro de pessoal selecionado e enviado para a impressora escolhida.

25 Gerenciamento de visitantes

Os visitantes têm um status especial no controle de acesso, e são mantidos separadamente dos outros dados de funcionários. Por esse motivo, os dados dos visitantes são criados e mantidos em caixas de diálogo separadas.

25.1 Dados do visitante

Introdução

O sistema oferece suporte à administração rápida e fácil de dados de visitantes. Os dados de visitantes que já são conhecidos podem então ser digitados e suas autorizações de acesso definidas antes do visitante chegar. Quando o visitante chega, somente o cartão deve ser atribuído. Ao final da visita, quando o cartão é devolvido, a relação entre o cartão de identificação e a pessoa é excluída novamente, e as autorizações são automaticamente retiradas.

Se os dados do visitante não forem excluídos pelo usuário, isso será feito pelo sistema ao final do período configurado (o valor padrão é 6 meses) após o cartão de identificação ter sido devolvido pela última vez.

Há duas caixas de diálogo para a administração de visitantes externos.

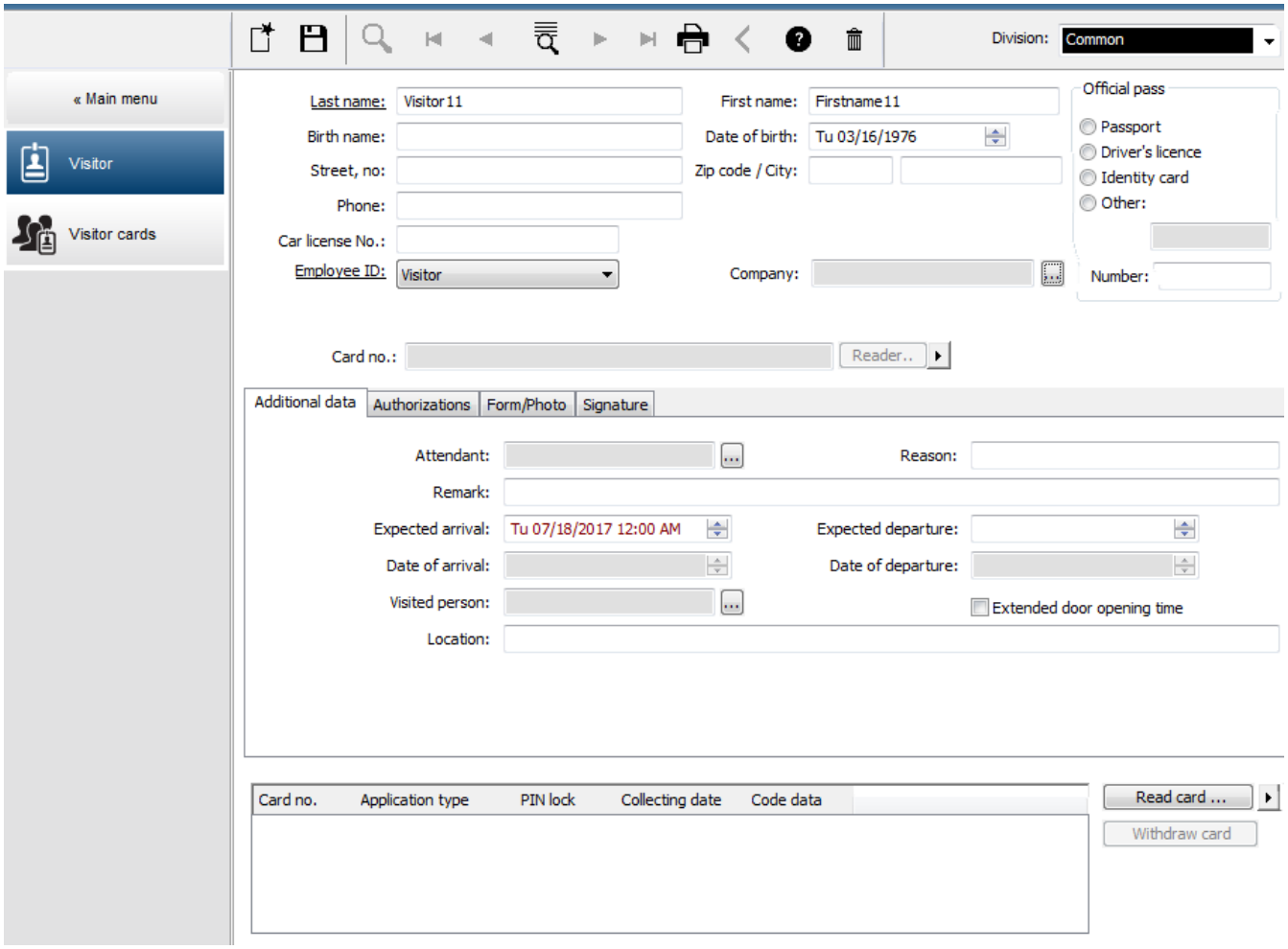
- A caixa de diálogo **Visitantes** é usada para a inserção de dados e autorizações de acesso de visitantes.
- A caixa de diálogo **Cartões de visitantes** regula o registro e o cancelamento dos cartões de visitante.

Caixa de diálogo: Visitors (Visitantes)

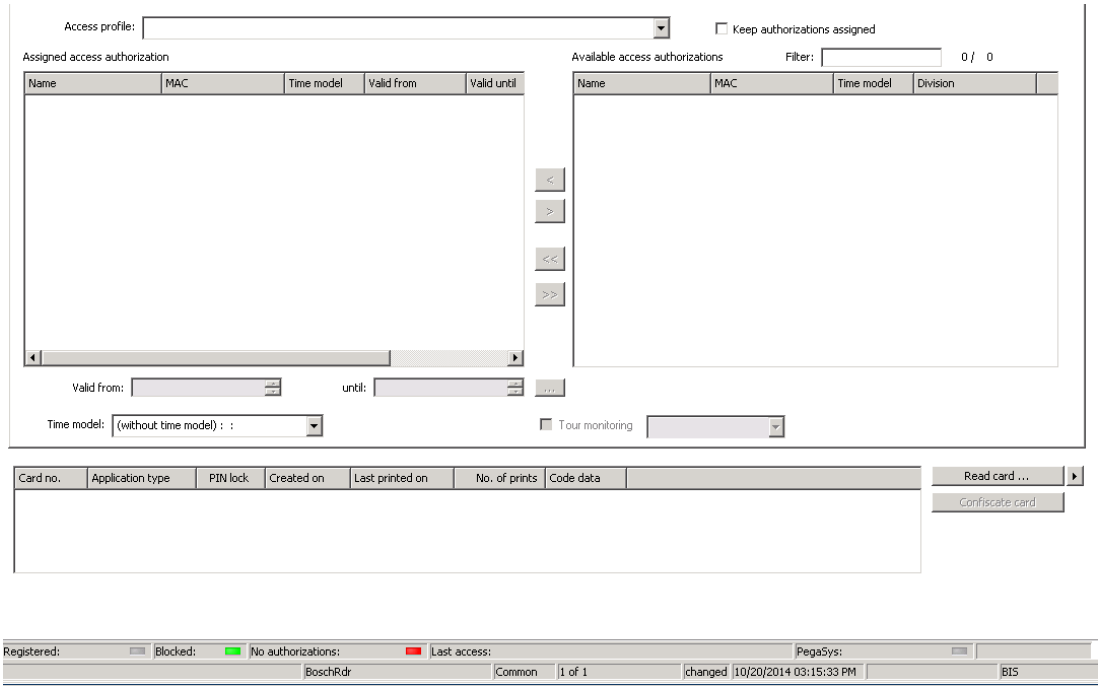
Os visitantes têm um status estritamente separado das outras pessoas e, portanto, são processados em uma caixa de diálogo separada. Pessoas com identificação de **visitante** não podem ser nem criadas na caixa de diálogo **Persons (Pessoas)**, nem ter cartões de identificação registrados para elas na caixa de diálogo usada para esta finalidade.

Entre outras coisas, não há nenhum campo de **Employee ID (Identificação do funcionário)** na caixa de diálogo **Visitors (Visitantes)**. Como há uma tabela de banco de dados separada para visitantes, as pessoas criadas na caixa de diálogo descrita aqui são automaticamente identificadas como visitantes. Portanto, isso significa que nenhuma pessoa além de um visitante pode ser criada aqui. Assim, as seleções são feitas apenas nesta caixa de diálogo, na tabela do banco de dados relevante. Em contrapartida, todas as pessoas cadastradas no sistema podem ser selecionadas nas outras caixas de diálogo de dados de funcionários, mas nem sempre estas podem ser usadas para visitantes (como a caixa de diálogo **Cards (Cartões)**).

Se conhecidos, os dados do visitante podem ser digitados total ou parcialmente no sistema antes da sua chegada. Isso minimiza o tempo de espera para os visitantes cujos dados já foram registrados.



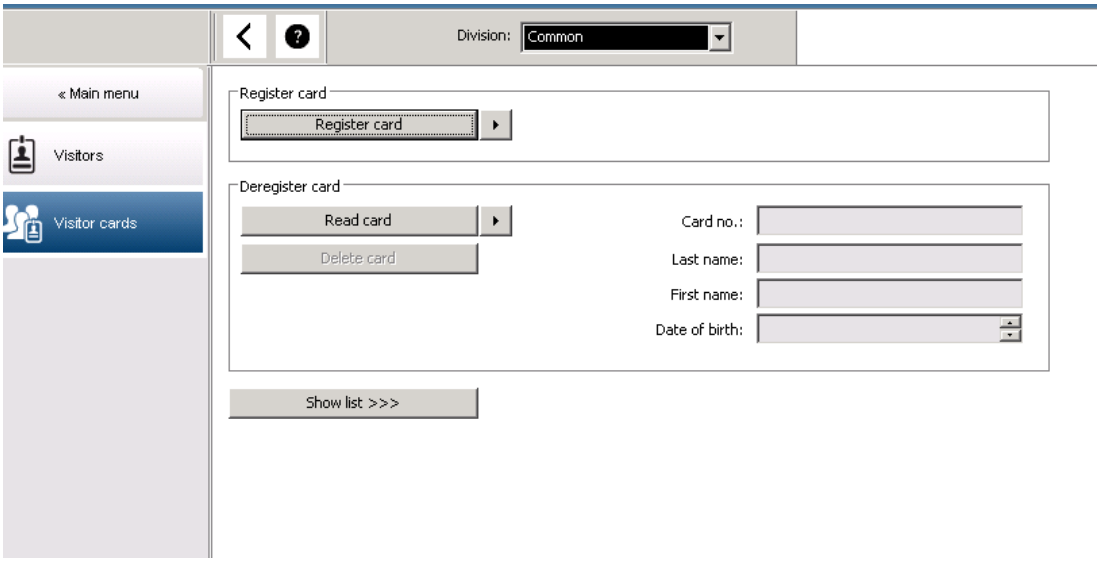
O **Reason (Motivo)** da visita, a **Location (Localização)** da visita do visitante e uma **Remark (Observação)** podem ser digitados nos campos abaixo.
Se você optar por digitar dados nos campos **expected arrival (chegada prevista)** e **expected departure (partida prevista)**, estas datas também serão exibidas nos campos **valid from (válido de)** e **until (até)**.
As datas relevantes são digitadas nos campos **Date of arrival (Data de chegada)** e **Date of departure (Data de partida)** pelo sistema quando os dados do visitante forem respectivamente atribuídos a, e separados do cartão de identificação do visitante.
Assim como na caixa de diálogo **Cards (Cartões)**, também há a possibilidade de atribuir a visitantes um "tempo maior de abertura das portas" para garantir um acesso mais fácil, para pessoas com deficiência, por exemplo.



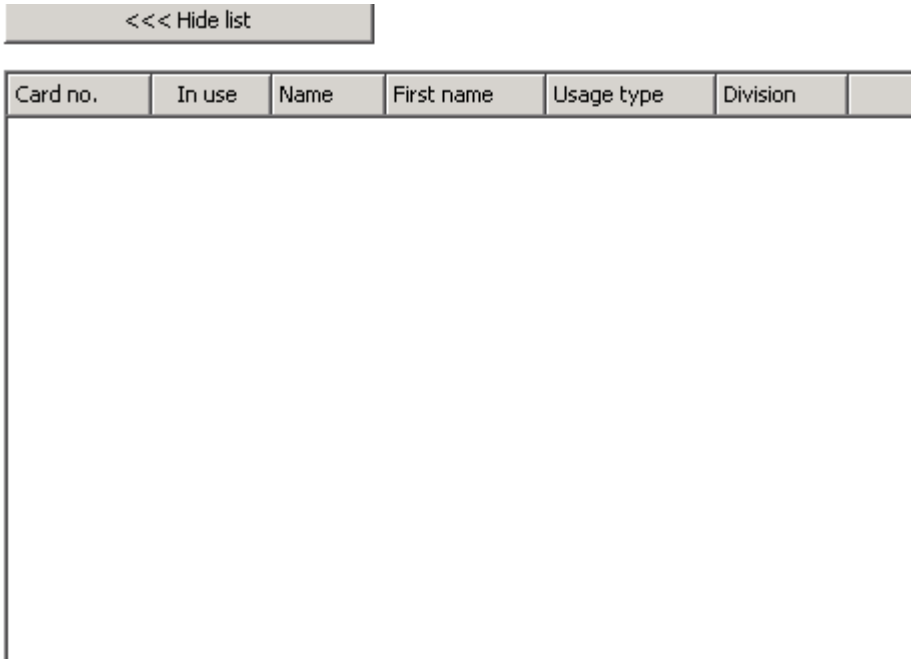
No campo da caixa de diálogo **Assign authorization (Atribuir autorização)**, um perfil de visitante existente pode ser selecionado na lista homônima, ou autorizações de acesso individuais da lista de **Available access authorization (Autorizações de acesso disponíveis)** podem ser selecionadas na lista de **Assigned access authorization (Autorizações de acesso atribuídas)** da esquerda, marcando-as e transferindo-as da lista da direita.
Apenas os perfis de acesso marcados como perfis de Visitantes podem ser selecionados nesta caixa de diálogo. Assim, deve-se evitar que visitantes tenham acesso a áreas especiais pela atribuição de autorizações gerais.
A validação das autorizações de acesso também pode ser definida para cada autorização individual.
Se a leitura do cartão resultar em erro, o número do cartão de identificação também pode ser digitado manualmente. Simultaneamente, a data atual é armazenada como a data de chegada.
Após a visita, o visitante devolve seu cartão de identificação. Enquanto este cartão de identificação é lido por um leitor de cartões ou o número do cartão de identificação é inserido manualmente, a pessoa associada é selecionada e seus dados são exibidos na tela.
O operador confirma a devolução do cartão. A associação entre o cartão de identificação e os dados pessoais do visitante é removida clicando no botão **Confiscate card (Confiscar cartão)**. A data e hora dessa ação são armazenadas como data de saída.

Caixa de diálogo: Visitor Cards (Cartões de visitantes)
Alguns cartões no sistema são reservados como cartões de visitante. Normalmente, um cartão de visitante é atribuído a um visitante na chegada e devolvido pelo visitante na saída. Em seguida, o cartão pode ser reutilizado. Esses cartões devem ser registrados como cartões de visitantes nessa caixa de diálogo para que possam ser atribuídos a visitantes:

Aviso!
Em geral, cartões de identificação de visitantes são criados sem nome ou foto para torná-los reutilizáveis.



Clique no botão **Register ID card (Registrar cartão de identificação)** para fazer o registro.
O procedimento de registro descrito anteriormente (seções **Pessoas** e **Cartões de identificação** no capítulo **Dados de funcionários**) é usado junto com o número do cartão para detectar o cartão de identificação. Isso permite ao sistema reconhecer o cartão de identificação como um cartão de identificação de visitante, e assim ele pode ser aplicado conforme as seguintes caixas de diálogo.

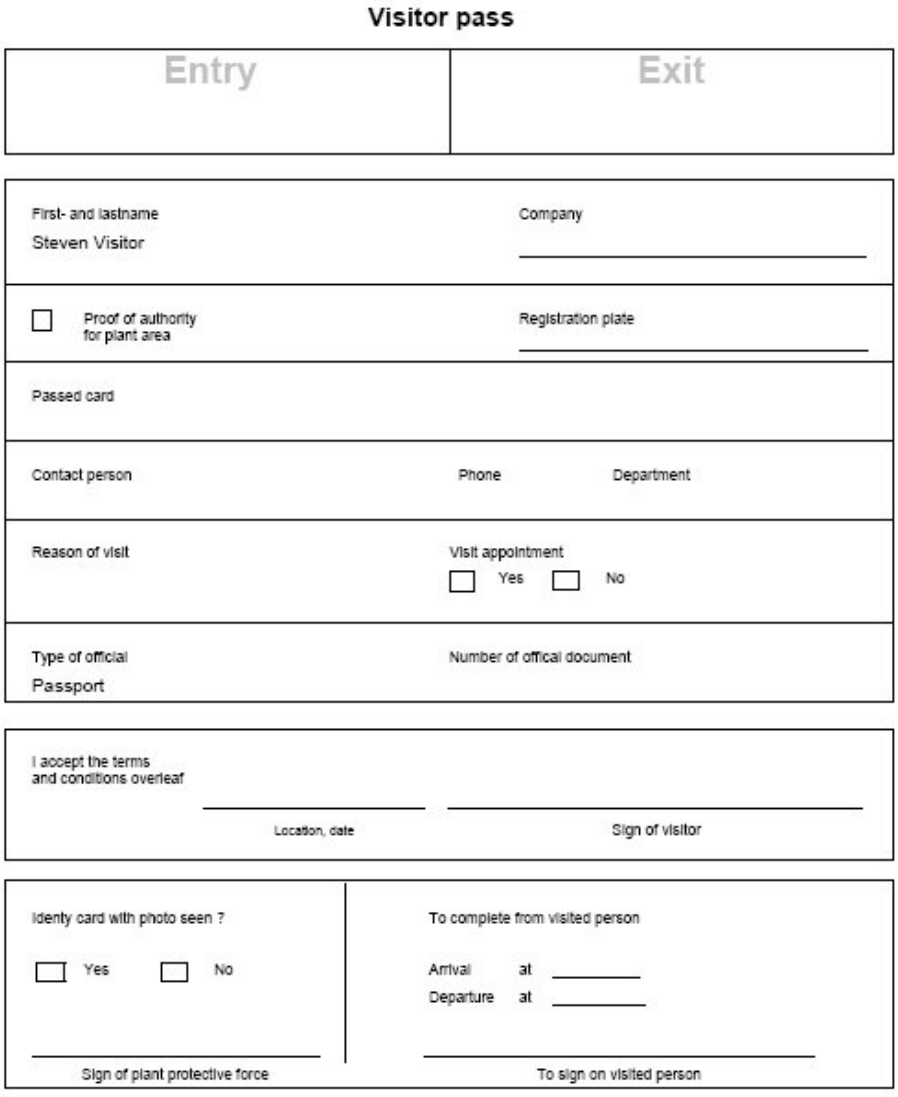


Para agilizar a atribuição de cartões de identificação de visitantes, é aconselhável digitalizar todos os cartões de identificação existentes, para que eles possam ser atribuídos aos respectivos visitantes na próxima caixa de diálogo.
Ao final da visita, o visitante devolve o cartão de identificação. Ao passar este cartão de identificação em um leitor ou digitar seu número na caixa de diálogo, a pessoa a quem é atribuído o cartão é selecionada, e seus dados pessoais são exibidos na tela. [Para digitar manualmente o número do cartão de identificação e alternar para o uso de leitores, consulte as descrições na **Caixa de diálogo: Cards (Cartões)** e **Caixa de diálogo: Visitors (Visitantes)**.]

O usuário confirma a devolução do cartão de identificação. A relação entre o cartão de identificação e os dados pessoais do visitante é removida utilizando-se o botão. A data atual é armazenada como a data da saída.

Impressão de um formulário de visitante

A barra de ferramentas da caixa de diálogo **Visitors (Visitantes)** contém um botão  adicional para imprimir um certificado de visitante. Entre outras coisas, a pessoa que recebe o visitante pode utilizar este certificado de visitante para confirmar se e quando o visitante chegou e saiu.



Visitor pass

Entry | Exit

First- and lastname
Steven Visitor

Company

☐ Proof of authority for plant area

Registration plate

Passed card

Contact person | Phone | Department

Reason of visit

Visit appointment ☐ Yes ☐ No

Type of official
Passport

Number of offical document

I accept the terms and conditions overleaf

Location, date

Sign of visitor

Identy card with photo seen ?

☐ Yes ☐ No

Sign of plant protective force

To complete from visited person

Arrival at _____
Departure at _____

To sign on visited person

25.2 Visitante atrasado

A visualização **Visitante muito atrasado** permite que o operador verifique a localização dos visitantes nas instalações e veja se eles estão muito atrasados com relação ao horário de saída programado.

– Para ver a página HTML, os operadores autorizados precisam ter o link configurado na tela inicial.

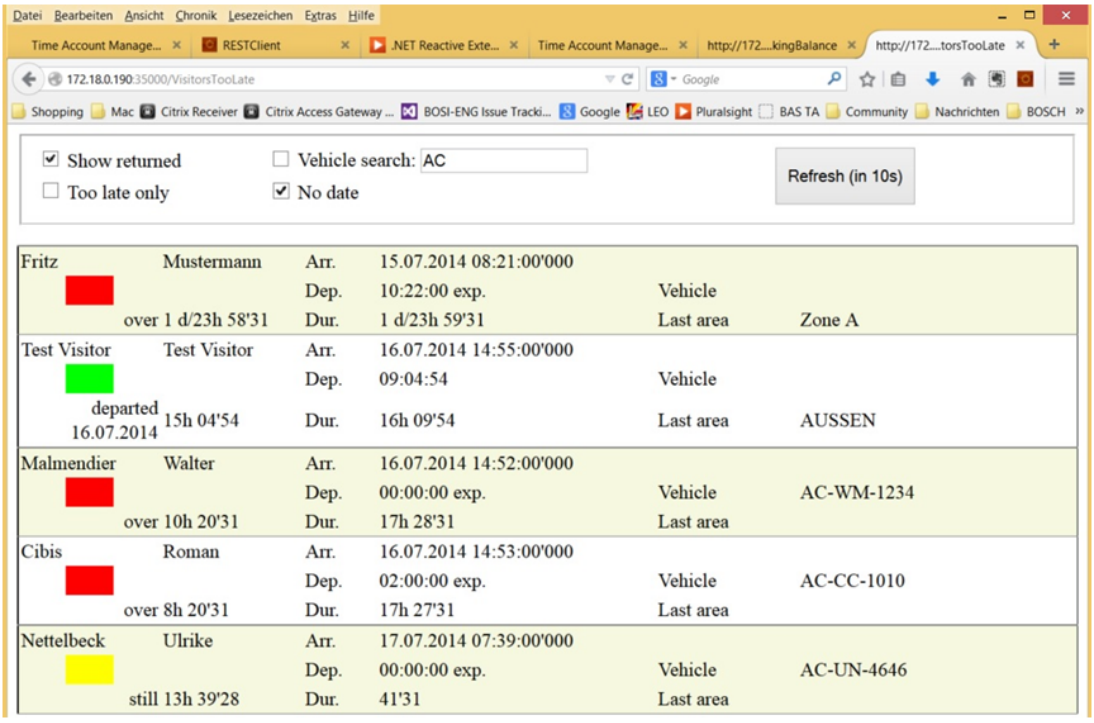
– É possível criar um acionamento de alarme no BIS para responder à mensagem **Visitante muito atrasado**. O acionamento pode abrir a página HTML com os dados do visitante.

Eventos que causam uma mensagem de Visitante atrasado:
Quando um cartão é atribuído a um visitante, o operador insere a hora esperada para sua saída. Ao término da visita, o visitante devolve o cartão na recepção, onde um operador cancela o cartão.
Opcionalmente, um leitor de cartões motorizado pode ser usado como leitor de saída e configurado para reter o cartão do visitante quando ele ou ela vai embora.
Se um visitante não devolver o cartão antes do horário de saída predefinido, independentemente de o visitante ainda estar ou não no local, uma mensagem **Visitor too late (Visitante atrasado)** é gerada pelo sistema.
Essa verificação de devoluções de cartões vencidas é executada em intervalos regulares (por exemplo, a cada minuto). Uma mensagem **Visitor too late (Visitante atrasado)** será gerada por cada verificação até o cartão ser devolvido. O intervalo de tempo pode ser configurado no registro do servidor em: `HKLM\Software\Micos\SPS\Default\VLDP\Interval`

Aviso!
A geração desta mensagem pode ser desativada no registro do servidor em:
`HKLM\Software\Micos\SPS\Default\VLDP\Active`

Esse recurso permite que o cliente detecte qualquer visitante que não encontre o funcionário designado, ou não se apresente na recepção ou portão de saída no prazo determinado após a reunião com o funcionário.
É verificado:
– Qual foi a última área utilizada pelo identificador de acesso ao edifício do visitante;
– Se o visitante devolveu o identificador de acesso ao edifício;
– Se o visitante devolveu o identificador do veículo, se aplicável.

Um relatório de **Visitante atrasado** e **Veículo atrasado** é gerado.
Se não for devolvido, a atual área do identificador pode ser impressa no relatório de 'visitante atrasado'.
O status de visitante é exibido no site com barras coloridas:
– **Verde**: o visitante devolveu todos os cartões de acesso.
– **Amarelo:** a visita ainda não acabou e o tempo ainda não se esgotou.
– **Vermelho:** a visita ainda não acabou e o tempo se esgotou, ou seja, **Visitor too late (Visitante atrasado)**.



A página faz uma atualização automática a cada 30 segundos. O tempo de atualização é configurado dentro da página Web. Além disso, a tela do operador pode ser ajustada usando os filtros **Show returned (Mostrar devolução)**, **Too late only (Atrasado apenas)** e **Vehicle search (Pesquisa de veículo)**.

26 Gerenciamento de estacionamentos

26.1 Estacionamento prolongado

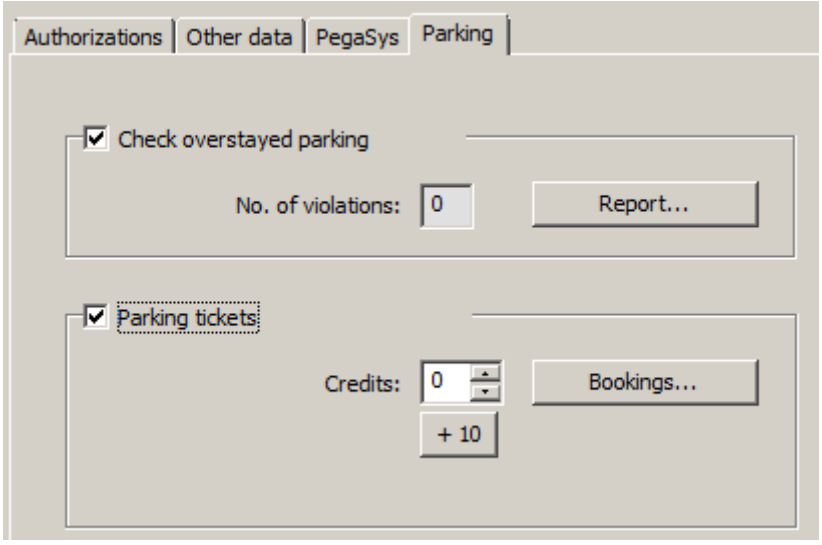
Esse recurso permite que o operador faça o seguinte:

- Detectar limites ultrapassados de permanência no estacionamento;
- Mostrar violações nos terminais de gerenciamento do estacionamento;
- Permitir a saída de uma pessoa com limite de permanência no estacionamento ultrapassado somente após o desbloqueio manual;
- Manter um registro das violações;
- Verificar limites de permanência no estacionamento ultrapassados em determinados leitores;
- Isentar certas pessoas das verificações de limite ultrapassado de permanência no estacionamento.

O recurso de gerenciamento do estacionamento pode detectar usuários que deixam seus veículos no estacionamento durante 24 horas ou mais.

Porém, se o período máximo for ultrapassado a barreira permanecerá fechada quando o cartão for apresentado, e a saída será negada. Uma mensagem aparece nas estações de trabalho do operador do estacionamento. Um operador deve aceitar a mensagem, que ativa automaticamente uma imagem de vídeo da saída em questão. O número de telefone da saída é exibido ao operador e ele pode entrar em contato com o motorista diretamente.

Após entrar em contato com o motorista e verificar sua situação, o operador pode liberar manualmente a barreira em sua interface, mas deve digitar um comentário. O incidente será registrado com o horário de entrada, o horário de saída e o comentário.



Detecção e tratamento do limite ultrapassado de permanência no estacionamento

O sistema registra os horários de entrada e saída de cada veículo, desde que o sistema completo esteja online. Se o LAC estiver offline, ele permitirá ou negará a entrada dependendo dos dados armazenados.

- Se o motorista estiver isento de verificações quanto ao limite ultrapassado de permanência no estacionamento, o MAC permite a saída pela barreira em qualquer caso.
- Se o motorista não estiver isento, o horário de saída é comparado com o último horário de entrada registrado para o veículo.
  - Se a permanência total for menor que o máximo permitido, a saída será permitida.
  - Se não, a barreira permanecerá fechada e o motorista precisará entrar em contato com o supervisor do estacionamento para abrir a barreira manualmente.

Estatísticas sobre o limite de permanência no estacionamento ultrapassado
Esta funcionalidade fornece uma visão geral de quantos veículos que ultrapassaram o limite de permanência estão no estacionamento.

26.2 Bilhetes de estacionamento

Este recurso permite que o cliente emita bilhetes de múltiplos estacionamentos para um número definido de procedimentos de estacionamento individuais (configurável).
O usuário autorizado recebe um bilhete de estacionamento que permite o acesso a um dos estacionamentos atribuídos.
Antes de conceder acesso a um estacionamento, o sistema verifica se ainda existe no mínimo um procedimento do estacionamento restante no bilhete.

- Nesse caso, o acesso será permitido e os créditos no bilhete são reduzidos em uma unidade.
- Caso contrário, o acesso será negado.

Ao entrar no estacionamento, é definido um intervalo de tempo durante o qual o proprietário do bilhete pode entrar e sair do estacionamento à vontade. Esse intervalo tem a mesma duração que o período máximo de permanência no estacionamento (padrão: 24 horas).
Possuir um bilhete de estacionamento significa ter permissão para utilizar qualquer uma das zonas de estacionamento permitidas durante um dia (24 horas). Dentro deste período de tempo, também é possível estacionar o carro em outra zona ou estacionamento

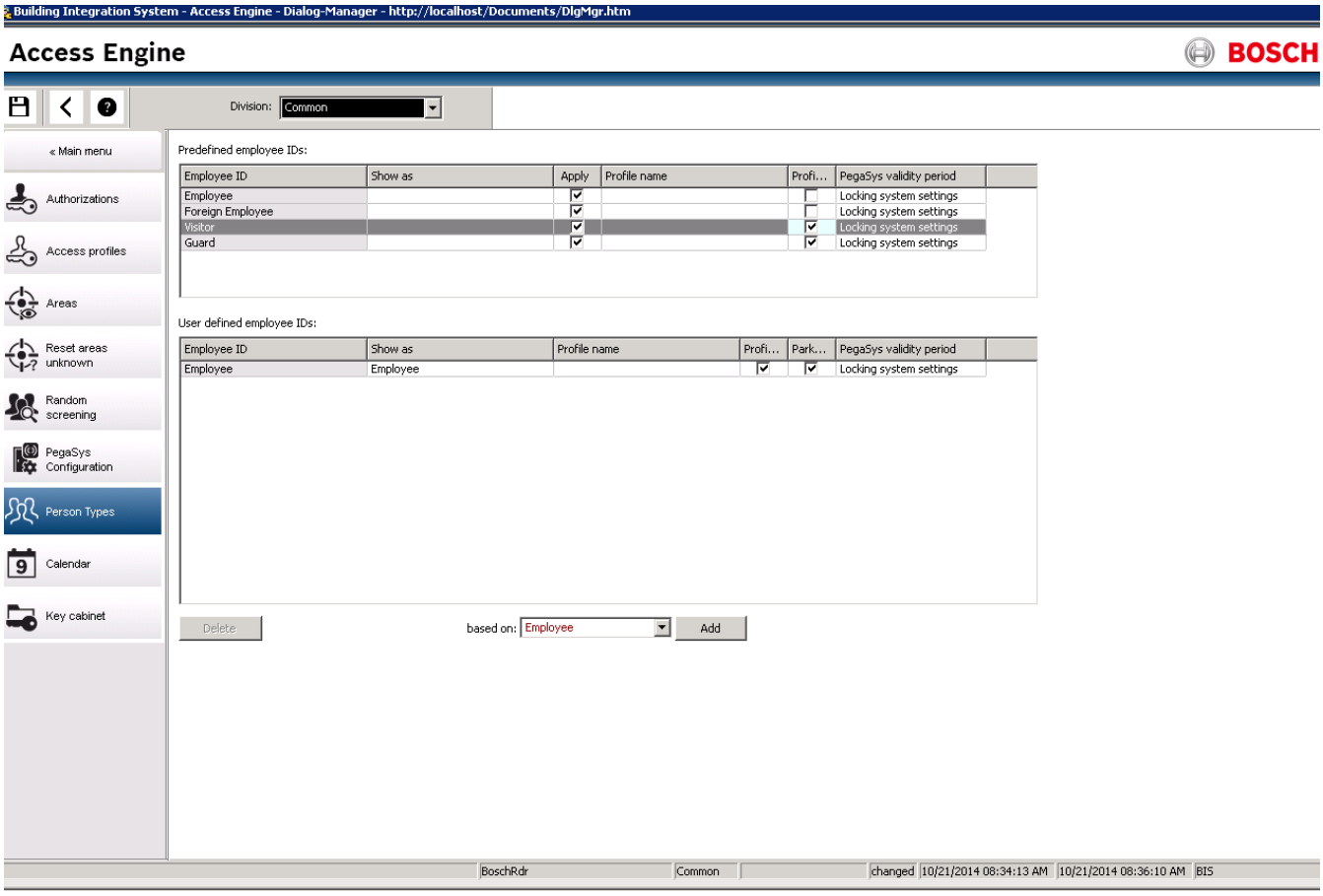
- Se o proprietário de um bilhete válido para múltiplos estacionamentos ultrapassar o período máximo de permanência, os créditos no bilhete serão reduzidos de maneira proporcional. Isso pode também resultar em créditos negativos! Nesse caso, aplica-se a mesma regra da permanência no estacionamento ultrapassado: a saída deve ser liberada manualmente e o incidente será registrado.
- Se o proprietário de um bilhete válido para múltiplos estacionamentos ultrapassar o intervalo de tempo inicial (por exemplo, entrando e saindo repetidamente) sem ultrapassar o período máximo de estacionamento, os créditos serão reduzidos em 1, e a saída será permitida.

Administração dos créditos do bilhete
Os créditos atuais de uma pessoa são salvos no banco de dados, no caso os proprietários queiram usar múltiplos tickets de estacionamentos. Um campo de registro **Créditos de estacionamento** na caixa de diálogo **Cartões** mostra o valor atual, que pode ser editado. As modificações neste campo são registradas e salvas no banco de dados.
Os créditos de estacionamento só podem ser editados se o operador tiver permissão especial para a caixa de diálogo de cartões (consulte **Permissão de caixas de diálogo** no Navegador de configuração).
A mesma permissão especial é necessária para usar a caixa de diálogo para conjuntos de dados para está finalidade.

Aviso!
É possível configurar vários cartões por portador de cartão. Os créditos de estacionamento são salvos com relação à pessoa, portanto uma troca de cartão não trará problemas de contagem de créditos.

Atribuição de bilhetes válidos para múltiplos estacionamentos
Para a atribuição de bilhetes válidos para múltiplos estacionamentos, o seguinte critério é aplicado:

– Somente pessoas em certas categorias especificadas de funcionários são autorizadas a ter um bilhete válido para múltiplos estacionamentos. Isso pode ser parametrizado na caixa de diálogo **Tipos de pessoa**.



– Se os créditos de um bilhete caírem abaixo de um valor ajustável (padrão = 4), o proprietário será informado automaticamente por e-mail.

O operador pode verificar os créditos de um proprietário de bilhete a qualquer momento e fazer as correções, se necessário. Todas as correções serão registradas e salvas no banco de dados.

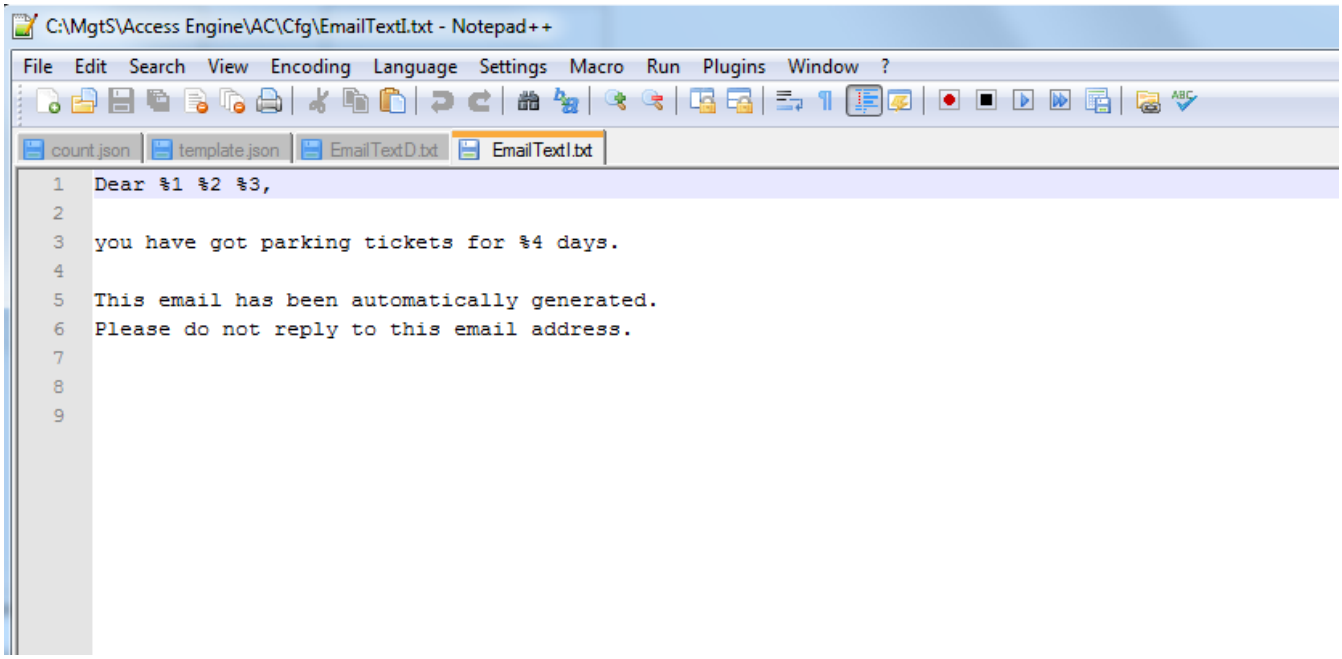
O sistema permite aumentar os créditos dos grupos inteiros de funcionários no valor de x. Os proprietários serão informados por e-mail.

Para configurar a mensagem de e-mail, vá até seu diretório de instalação do BIS ACE.

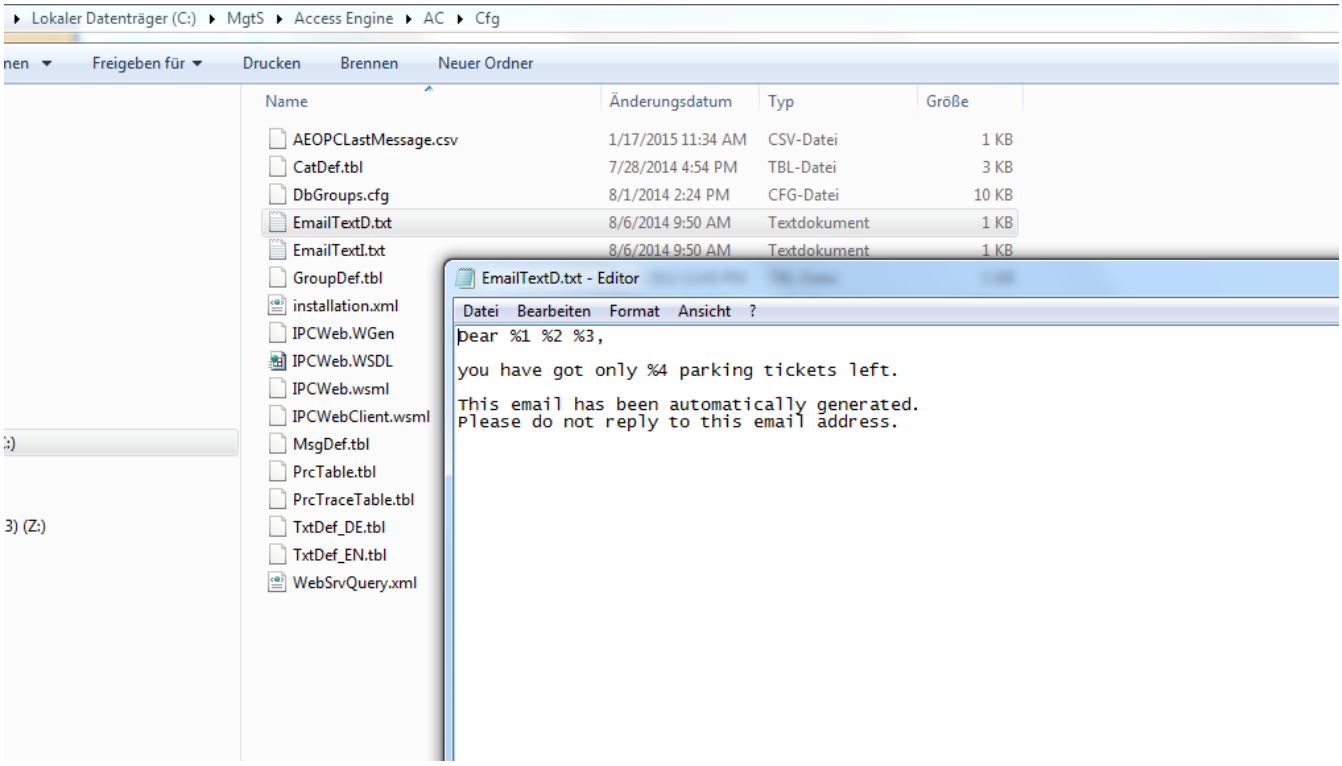
Selecione o diretório: **<Seu caminho até a instalação>\MgtS\AccessEngine\AC\Cfg.**

Nesse diretório você tem duas opções:

– Edite o arquivo **EmailTextI.txt** para criar uma mensagem de texto informando que a conta do bilhete foi aumentada:

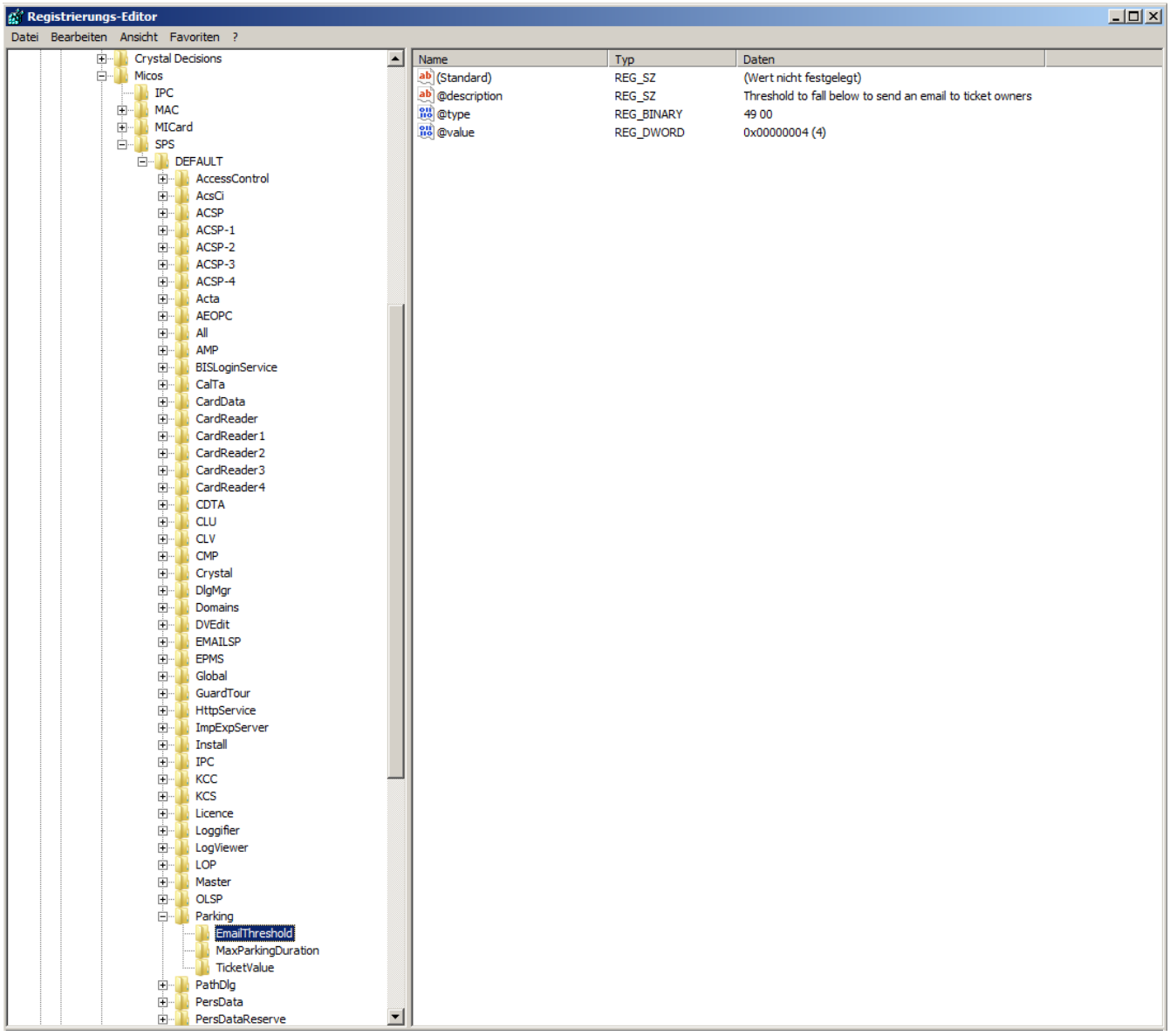


– Edite o arquivo **EmailTextD.txt** para criar uma mensagem de texto informando que o limite de e-mails configurado foi atingido (4 no exemplo):



Aviso!
Os caracteres universais %1, %2 e %3 na primeira linha das mensagens referem-se ao endereçamento do usuário, e serão preenchidos com o respectivo cartão, por ex. "Sr. Henry Average,".

O próprio valor limite pode ser definido no Registro do estacionamento em **Micos\SPS\DEFAULT\Parking\EmailThreshold:**



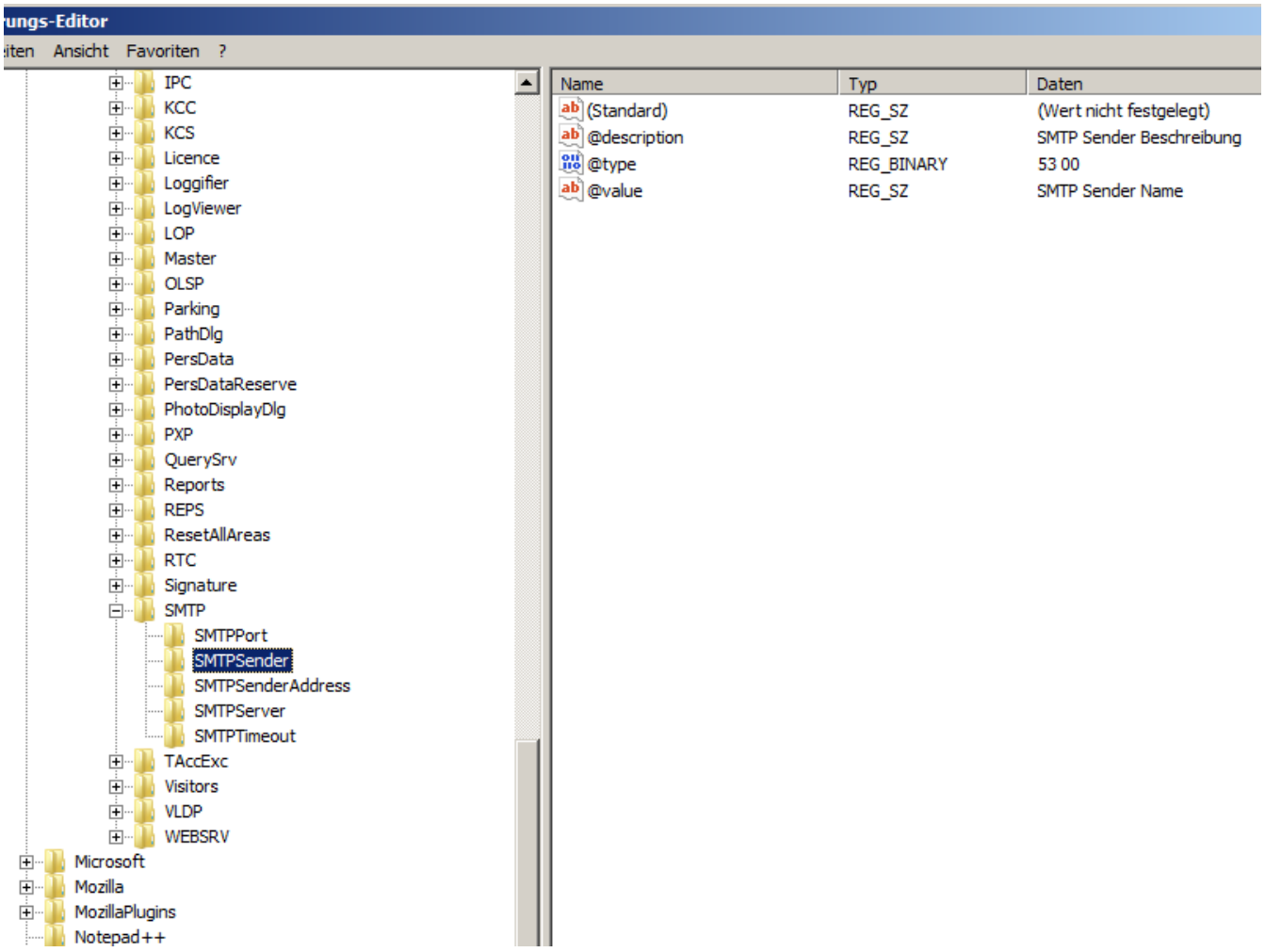
O exemplo mostra a configuração padrão de 4.

Da mesma maneira, pode-se definir os dois outros atributos da função **Estacionamento**:

- **Duração maxima no estacionamento**: A configuração padrão é 23:59 h
- **Valor do Ticket**: Configuração padrão 10 estacionamentos.

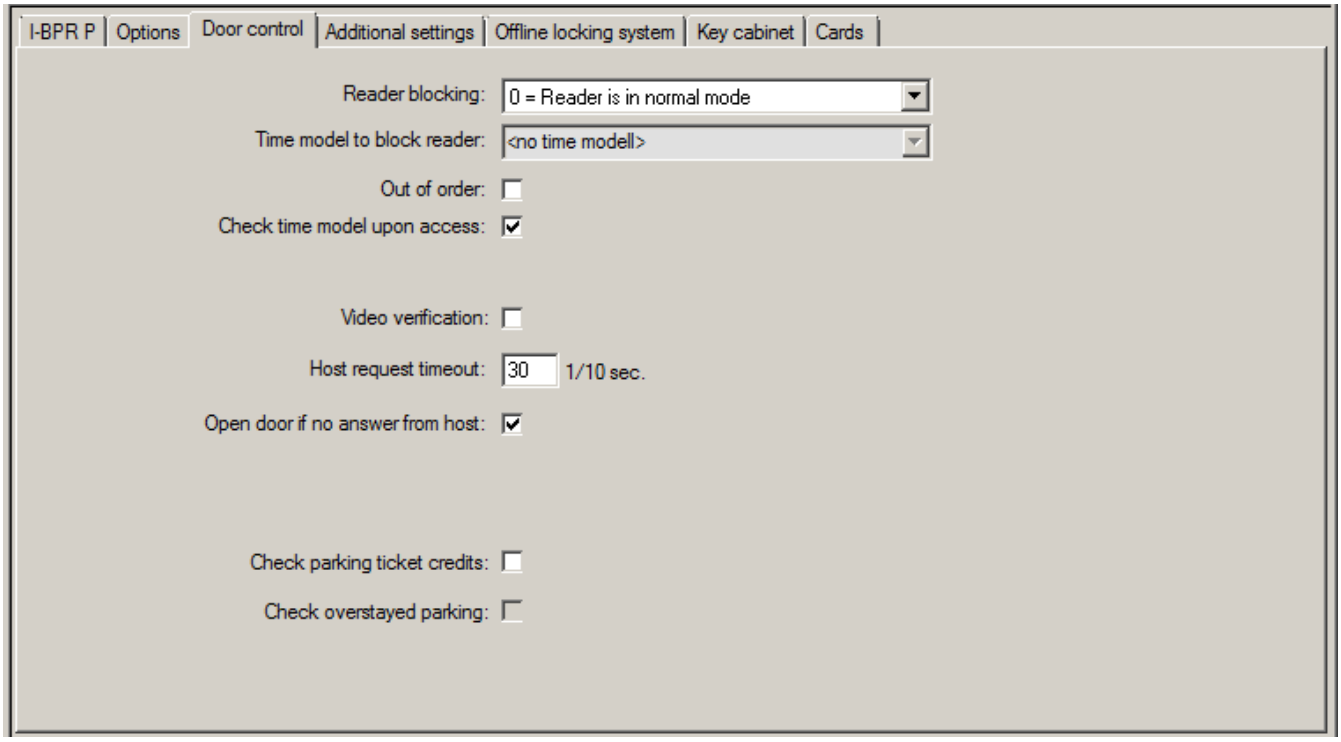
Configurações do SMTP

Use o editor do registro para definir suas **Configurações do SMTP**: para usar o e-mail no contexto de gerenciamento dos estacionamentos



Créditos são atualizados no acesso

No momento do acesso pelo proprietário de um bilhete válido para múltiplos estacionamentos, o sistema verifica o bilhete para a redução dos créditos. Se os créditos forem 0 ou menos, o acesso será negado.



- Para configurar a verificação do bilhete, ative a caixa de seleção **Check parking ticket credits (Verificar créditos do bilhete de estacionamento)**.
- **Para verificar se o limite de permanência no estacionamento foi ultrapassado, ative a caixa de seleção Check overstayed parking (Verificar limite de permanência no estacionamento ultrapassado).**

Antes de conceder acesso a um estacionamento, o sistema verifica se ainda existe no mínimo um procedimento de estacionamento restante no bilhete.

- Nesse caso, o acesso será permitido e os créditos no bilhete serão reduzidos em uma unidade, a menos que tenha havido uma mudança de zona de estacionamento dentro do período de tempo permitido (24 horas).
- Se esse não for o caso, o acesso será negado.

Aviso por e-mail se os créditos caírem abaixo do limite mínimo

Se os créditos de um bilhete caírem abaixo de um certo valor definido (por exemplo, 4), o proprietário do bilhete será informado automaticamente por e-mail.

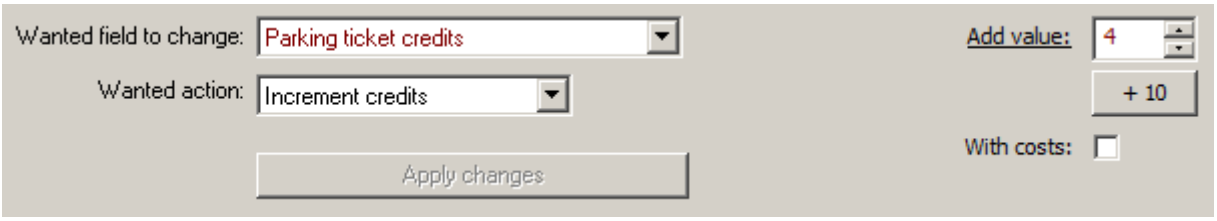
Se não for possível enviar o e-mail para o proprietário do bilhete, uma mensagem de erro será enviada para o BIS.

Crédito dos bilhetes

Os créditos do proprietário de um bilhete válido para múltiplos estacionamentos são exibidos em um campo na caixa de diálogo Dados mestre, em **Créditos do bilhete do estacionamento**. O operador pode editar o valor dos créditos do bilhete a qualquer momento. Qualquer modificação será registrada e salva no banco de dados.

O crédito dos bilhetes também podem ser modificados para grupos inteiros de pessoas. Para isto, o campo de digitação **Crédito do bilhete de estacionamento** está disponível na caixa de diálogo **Conjuntos de dados**. O grupo de pessoas é selecionado através das funções de filtragem na caixa de diálogo **Conjunto de dados**. Em seguida, um valor delta (por exemplo, "n") é digitado no campo **Crédito dos bilhetes de estacionamento**.

Isso aumenta os créditos de estacionamento pelo valor "n", e as pessoas envolvidas recebem um e-mail informando-os.



Se não for possível enviar o e-mail para os proprietários dos bilhetes, as mensagens de erro serão enviadas para o BIS.
Todas as modificações nos créditos de estacionamento serão coletadas no banco de dados do ACE e disponibilizadas como relatório na caixa de diálogo **Créditos do bilhete de estacionamento**.

26.3 Exportação dos números de utilização do estacionamento

Este recurso permite que o operador avalie estatisticamente a utilização de estacionamentos. O sistema de controle de acesso exporta figuras de utilização do estacionamento para um arquivo CSV conforme predefinido pelo operador.
A exportação para o arquivo CSV contém dados sobre a utilização de todos os estacionamentos pelas diversas categorias de proprietários de cartão – isto é, as categorias de funcionários. Os valores são coletados em intervalos periódicos e configuráveis, com uma duração máxima de 15 minutos.
Os dados para consulta no tempo são os seguintes:

- Data
- Hora
- Estacionamento
- Número de usuários, subdivididos por:
  - zonas de estacionamento
  - grupos de usuários (categorias de funcionários)

Aviso!
Se um titular do cartão individual mudar de categoria de funcionário, os dados do relatório do período anterior ainda mostrarão sua alocação anterior.

O caminho de exportação pode ser definido no editor de parâmetros do sistema em **Default\TAccExc\PB-Dir. Assim que um diretório válido for digitado, uma capacidade por estacionamento será exportada.**

26.4 Exportação do controle de validade de automóveis

Este recurso permite que o operador verifique as autorizações para estacionar de veículos no estacionamento.
Um arquivo CSV gerado a intervalos regulares contém todos os proprietários dos bilhetes, além de informações adicionais sobre as zonas de estacionamento. .
Para a configuração, selecione o editor de parâmetros do sistema em **Default\PXP\Task0001...** e explicitamente ative (ou desative, respectivamente) o caminho da exportação, o nome do arquivo e a exportação.

A exportação é realizada em intervalos configuráveis. Os dados exportados são:

- Validade do cartão (campo **válido até** em **AC Pessoas**)
- Nome da pessoa autorizada

- Número do registro do veículo
- Número de cartões registrados
- Número de telefone
- Status do cartão
- Nome do estacionamento ou na zona do estacionamento, se for o caso
- Campos de reserva (opcional, se configurado)

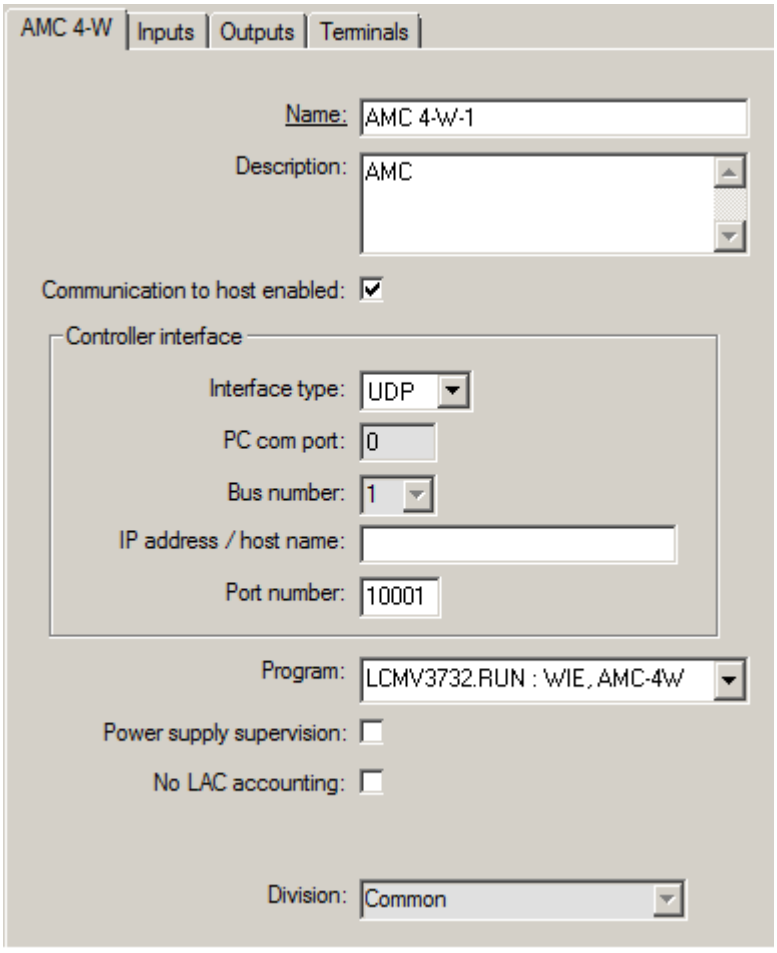
26.5 Autorizações para várias zonas de estacionamento

Alguns estacionamentos têm zonas para motoristas deficientes e não-deficientes. Neste caso, as seguintes regras se aplicam:

- Os proprietários dos bilhetes temporários só são autorizados a entrar desde que ainda haja vagas de estacionamento disponíveis para pessoas não-deficientes.
- As pessoas portadoras de deficiência são autorizadas a entrar desde que ainda haja vagas de estacionamento disponíveis para pessoas deficientes ou não-deficientes.

Aviso!
Isso pressupõe que os proprietários do bilhetes sigam as regras. Em especial, isso significa que:
Pessoas não-deficientes não devem estacionar em vagas de estacionamento para portadores de necessidades especiais
As pessoas portadoras de deficiência devem usar as vagas de estacionamento para deficientes desde que estejam disponíveis

Uma pessoa que tem várias autorizações pode acessar ambos, seja deficiente ou não. O AMC tenta reservar a pessoa de acordo com a ordem sequencial configurada de áreas de estacionamento. Caso uma área esteja cheia, a procura da próxima área livre e autorizada será feita.
Cálculo do contador no MAC e no AMC:
1) Um AMC controla todas as entradas e saídas de um estacionamento:
=> O AMC faz sua própria contagem e pode ser corrigido pelo MAC quando ficar on-line.
2) As entradas e saídas de um estacionamento são divididas em AMCs diferentes:
=> O MAC contabiliza o AMC em caso de operação on-line. Ao operar off-line, os AMCs permitem o acesso (se configurado corretamente), mas não são contabilizados.
Se vários AMCs controlarem um estacionamento, ativo a caixa de seleção **Sem contabilidade de LAC** na configuração do AMC



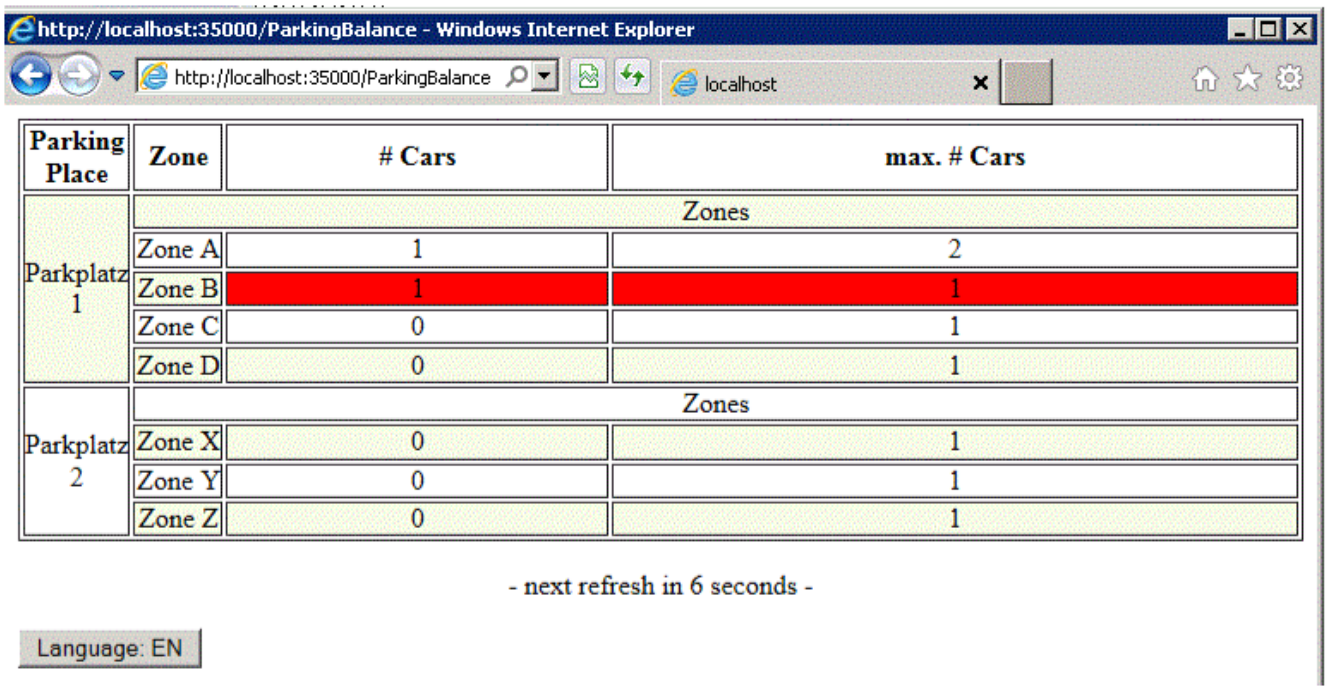
26.6 Relatório do estacionamento

Parking lot list

Date 08.11.2013 , 14:51:23
Page 1

Parking area	Zone	Vehicle count	State
Main Park		51	
	Zone A	30	full
	Zone B	9	--
	Zone C	12	--
Building A		39	
	Zone A	30	full
	Zone B	9	--
Building B		39	
	Zone A	30	full
	Zone B	9	--

Um segundo exemplo de **Vagas disponíveis** mostra o que é possível fazer com o servidor web. Todas as vagas do estacionamento são mostradas, incluindo os contadores atualizados da utilização de todas as zonas do estacionamento. Além disso, o exemplo contém um botão de seleção de idioma para mostrar como é fácil alternar entre alemão e inglês. A localização só é feita dentro da página web.



Parking Place	Zone	# Cars	max. # Cars
Parkplatz 1	Zones		
	Zone A	1	2
	Zone B	1	1
	Zone C	0	1
	Zone D	0	1
Parkplatz 2	Zones		
	Zone X	0	1
	Zone Y	0	1
	Zone Z	0	1

26.7 Gerenciamento do estacionamento ampliado

Introdução

O operador pode ajustar o número de vagas de estacionamento em uma área para compensar veículos de tamanhos não usuais, por exemplo:

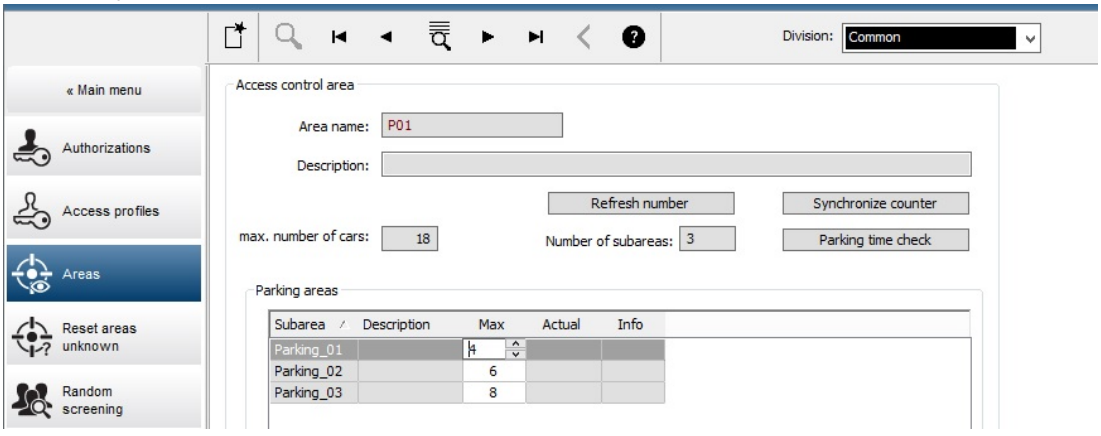
- Caminhões
- Acesso para deficientes
- Motocicletas

Caminho da caixa de diálogo

Menu principal > **Dados do sistema** > **Áreas**

Procedimento

1. Selecionar uma área de estacionamento
2. No painel **Áreas de estacionamento**, ajuste o valor na coluna **Max** para o novo número de espaços de estacionamento na área.



Observações:

- As configurações feitas na coluna **Max** substituem as configurações feitas em **Áreas**. Consulte **Configurando áreas para veículos** no link abaixo.

– Um zero 0 na coluna **Max** indica Ilimitado; a contagem de todos os veículos é desativada.

Consulte

– *Configuração de áreas para veículos, página 25*

27 Gerenciamento de rondas de segurança e patrulhas

Introdução a Rondas de segurança

Uma **Ronda de segurança** é uma rota ao redor das instalações, pontuada por leitores de cartão, onde funcionários do tipo **Guarda** devem apresentar um cartão de segurança especial para provar que visitaram fisicamente o leitor.

Cartões de segurança não abrem entradas, mas são usados exclusivamente para rastreamento. Para abrir entradas, o guarda necessita de um cartão de acesso adicional.

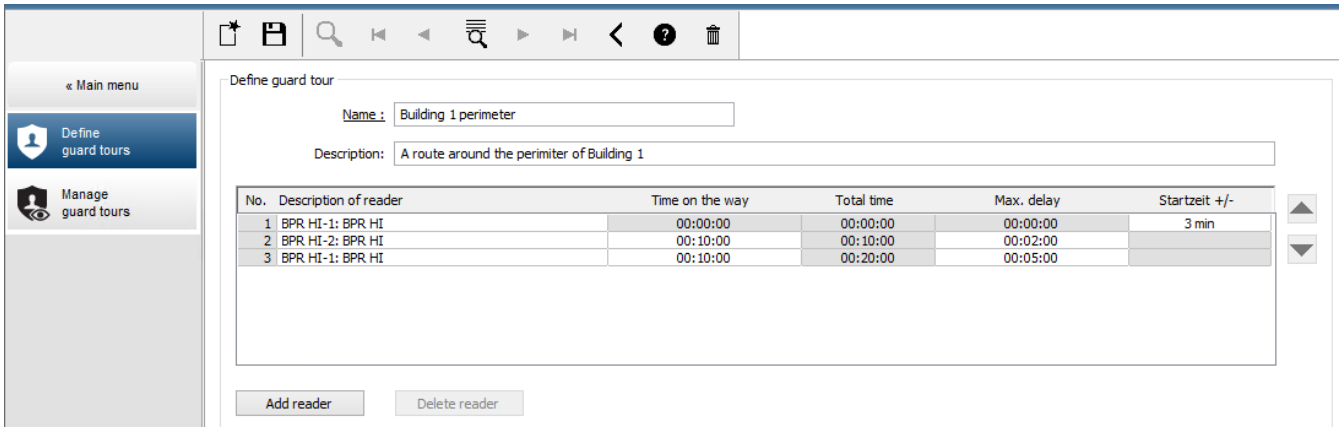
A Ronda de segurança consiste em uma série de leitores com tempos de caminhada aproximados entre eles. O atraso máximo tolerável entre leitores, e o desvio tolerável (+/-) desde a hora de início, também são atributos da Ronda de segurança. Desvios fora dessas tolerâncias definidas podem acionar alarmes e são gravados em **Patrulhas**.

Introdução a Patrulhas

Uma **Patrulha** é a passagem de uma Ronda de segurança em data e hora específicas. Cada patrulha é criada e gravada como uma entidade única no sistema, para fins forenses.

27.1 Definição de rondas de segurança

Selecione **Guard tours (Rondas de segurança)** > **Define guard tours (Definir rondas de segurança)**



- No campo de texto **Name (Nome)**, insira um nome para a Ronda de segurança
- No campo de texto **Description (Descrição)**, insira uma descrição mais detalhada da rota (opcional).

Adição de leitores à ronda de segurança:

1. Clique no botão **Add reader (Adicionar leitor)**.
   Uma linha é criada na tabela.
2. Na coluna **Description of reader (Descrição do leitor)**, selecione um leitor na lista suspensa.
3. Insira valores para desvios toleráveis:
   - Se este for o primeiro leitor na sequência, em **Start time +/- (Hora de início +/-)** , insira um número de minutos anterior ou posterior que ainda seria tolerável como hora de início para uma patrulha nesta ronda de segurança.

- Se este **não** for o primeiro leitor na sequência, em **Time on the way (Tempo decorrido)**, insira o tempo (hh:mm:ss) necessário para que o guarda se desloque entre o leitor anterior e este.
  O tempo total para a ronda, excluindo atrasos, é acumulado na coluna **Total time (Tempo total)**.

4. Em **Max. delay (Atraso máx.)**, insira o valor máximo do **Time on the way (Tempo de percurso)** adicional tolerável sem fazer com que a patrulha seja marcada como **Delayed (Atrasada)**.
5. Adicione quantos leitores forem necessários. Observe que o mesmo leitor pode ocorrer mais de uma vez se a ronda de segurança passar várias vezes, ou retornar a ele.

- Para excluir um leitor da sequência, selecione a linha e clique no botão **Delete reader (Excluir leitor)**.
- Para alterar a posição de um leitor na sequência, selecione a linha e clique nos botões para cima/para baixo  .

27.2 Gerenciamento de patrulhas

Selecione **Guard tours (Rondas de segurança)** > **Manage guard tours (Gerenciar rondas de segurança)**

Agendamento de uma nova patrulha

Para agendar uma patrulha ao longo de uma ronda de segurança específica, execute as seguintes etapas:

1. Certifique-se de que você tenha o cartão de segurança desejado para a patrulha, e acesso a um leitor de cartões de acesso configurado ou leitor de cadastramento diretamente conectado.
2. Na coluna **Guard tours (Rondas de segurança)**, selecione uma das rondas de segurança definidas.
3. Clique no botão **New patrol... (Nova patrulha...)**.
   Uma janela pop-up é exibida.
4. Na janela pop-up, altere a ronda de segurança na lista suspensa se desejar.
5. Se for necessário atribuir uma hora de início predefinida à patrulha, marque a caixa de seleção **Set start time: (Definir hora de início:)**
   - Insira a data e hora de início.
   - Se desejado, clique na caixa de rotação **Start time +/- (Hora de início +/-)** para ajustar a tolerância para inícios cedo ou tarde.
6. Clique na seta para a direita e selecione o leitor que deseja usar para registrar o cartão de segurança. Observe que o leitor já deve estar configurado no sistema antes que ele seja exibido aqui para seleção.
7. Clique no botão de adição verde para iniciar a leitura do cartão de segurança, apresente o cartão no leitor e siga as instruções pop-up.
   O cartão de segurança é registrado para uso na patrulha.
8. Repita a etapa anterior para registrar cartões de segurança alternativos para esta patrulha. Observe, no entanto, que o primeiro cartão a ser apresentado durante a patrulha deve ser usado em todos os leitores durante essa patrulha.
9. Clique em **OK**. A ronda de segurança selecionada será marcada na lista como **planned (planejada)**.

Rastreamento de uma patrulha

Todas as patrulhas planejadas e ativas são movidas para o topo da lista. Se várias patrulhas estiverem planejadas ou ativas, a patrulha selecionada será enquadrada em vermelho. Clique no quadro para obter mais informações.

Uma patrulha é iniciada quando o guarda apresenta seu cartão de segurança no primeiro leitor da ronda. Este cartão deve ser usado para o resto da patrulha, mesmo se cartões alternativos forem definidos para a patrulha.

O **State (Estado)** da patrulha é alterado para **Active (Ativo)**.

Cada leitor alcançado no cronograma recebe uma marca de seleção verde – ✔. Os tempos agendados e reais entre leitores na patrulha atualmente selecionada são exibidos na metade inferior da janela da caixa de diálogo.

Cada leitor alcançado após o tempo agendado mais **Max. delay (Atraso máx.)** recebe uma marca ⊘ vermelha. A patrulha é marcada como **Delayed (Atrasada)**.

Neste caso, o guarda chama o operador para confirmar que não há problema. Em seguida, o operador clica no botão **Resume patrol (Retomar patrulha)**. O leitor recebe uma marca de seleção verde com um "c" adicional – ✔c. O guarda pode agora continuar a patrulha no próximo leitor.

Se houver um atraso imprevisto, porém inofensivo, em uma patrulha ativa, o guarda pode chamar o operador para ajustar o cronograma. Insira os minutos de atraso na caixa de rotação **Delay (min) (Atraso (min))** e clique no botão **Apply (Aplicar)**.

Se a patrulha não puder ser concluída conforme o cronograma, o operador pode cancelá-la ao clicar no botão **Interrupt (Interromper)**. O **State (Estado)** da patrulha muda para **Aborted (Cancelada)** e cai abaixo das rondas de segurança planejada e ativa na lista.

27.3 Monitoramento de rondas (anteriormente controle de caminhos)

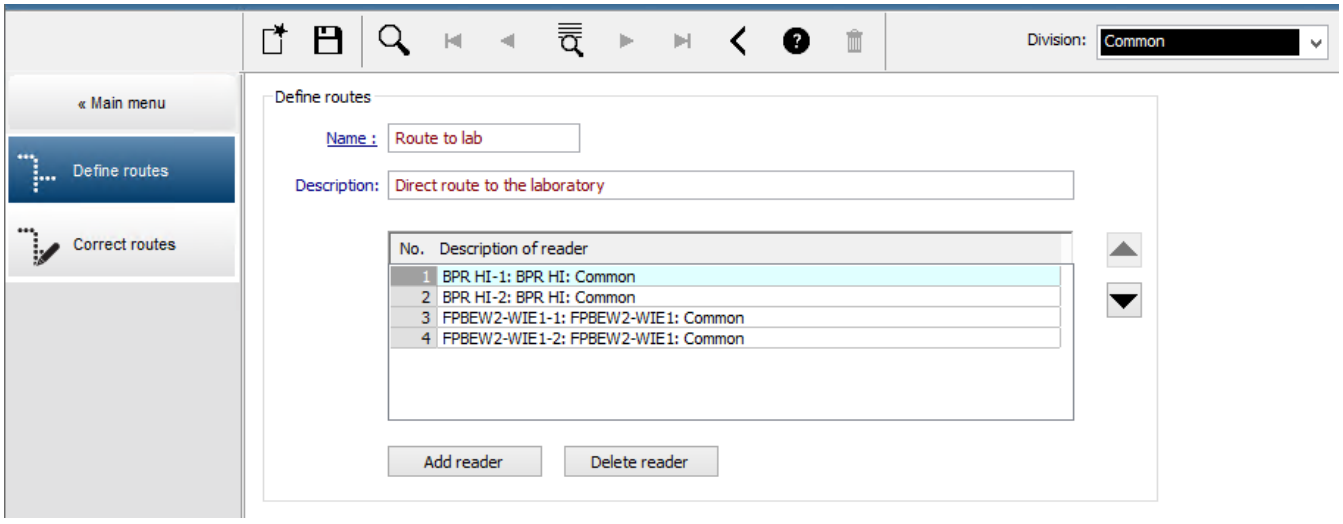
Introdução

Uma Rota (ou Ronda) é uma sequência predefinida de leitores no sistema de controle de acesso que pode ser imposta a Pessoas, para direcionar seus movimentos nas instalações, independentemente das autorizações da pessoa.

Usos típicos destinam-se a impor sequências de acesso restrito em ambientes de limpeza industrial, controlados higienicamente, ou áreas de alta segurança.

Definição de rotas

1. No Main menu (Menu principal), selecione **Tour monitoring (Monitoramento de rondas)** > **Define routes (Definir rotas)**
2. Insira um nome para a rota (até 16 caracteres)
3. Insira uma descrição mais detalhada (opcional)
4. Como em Rondas de segurança, clique no botão **Add reader (Adicionar leitor)** para criar uma sequência de leitores. Use os botões de seta para alterar a posição de um leitor na sequência e o botão **Delete reader (Excluir leitor)** para removê-lo.



Atribuição de uma rota a uma pessoa

Para atribuir uma rota a uma pessoa, execute as seguintes etapas:

1. No Main menu (Menu principal), clique em **Personnel data (Dados pessoais)** > **Cards (Cartões)**
2. Carregue o registro de funcionário da pessoa a ser atribuída
3. Na guia **Other data (Outros dados)**, marque a caixa de seleção **Tour monitoring (Monitoramento de rondas)**
4. Na lista suspensa ao lado dela, selecione uma rota definida (para definir uma rota, consulte a seção anterior).
5. Salve o registro do funcionário.

A rota é ativada quando a pessoa atribuída apresenta seu cartão no primeiro leitor da rota. Os outros leitores na rota devem agora ser usados em sequência, isto é, somente o próximo leitor na sequência concederá acesso. Após a rota ser completamente atravessada, a pessoa poderá se registrar em qualquer outro leitor em suas autorizações.

Correção e monitoramento de rotas

1. No menu principal, selecione **Tour monitoring (Monitoramento de rondas)** > **Correct routes (Corrigir rotas)**
2. Carregue o registro de funcionário da pessoa atribuída à rota.
3. Para localizar essa pessoa na rota, clique no botão **Determine location (Determinar localização)**.
4. Os leitores que já foram atravessados com êxito recebem uma marca de seleção verde ✔ na lista.
5. Para redefinir ou corrigir a localização de uma pessoa na rota, clique no botão **Set location (Definir localização)**.

28 Triagem aleatória de funcionários

O processo de revista aleatória

1. Um titular de cartão apresenta seu cartão para um leitor configurado para revista aleatória.

   Observação

   Somente pessoas autorizadas a passar pela entrada na direção definida podem ser selecionadas aleatoriamente. Conforme as autorizações são verificadas antes da revista aleatória, qualquer pessoa não autorizada é imediatamente barrada e não será incluída no processo de seleção.
2. Se o randomizador selecionar essa pessoa para revista, o cartão dela será bloqueado em todo o sistema.
   - O evento é registrado no log de eventos do sistema.
   - A caixa de diálogo **Bloqueio** recebe uma entrada de duração ilimitada chamada **Revista aleatória**. [Figura abaixo - número 1]
   - A barra de status das caixas de diálogos de dados de pessoal exibe os "LEDs" bloqueados (vermelhos) e com revista aleatória (roxo piscando).

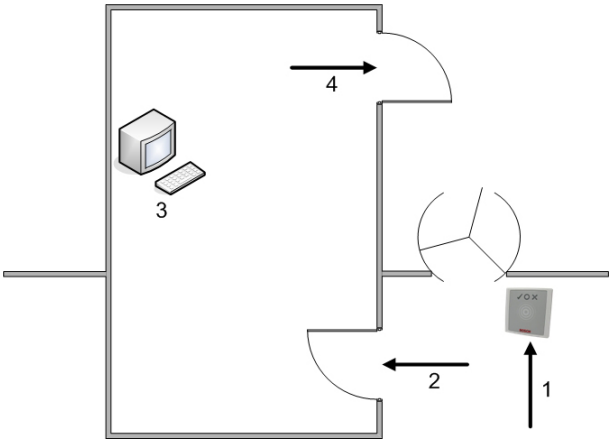
Aviso!

As pessoas cujo parâmetro **Excluído da revista aleatória** foi definido (na caixa de diálogo **Cartões**, guia **Outros dados**) não são incluídas no processo de revista.

3. A pessoa selecionada aleatoriamente é convidada para verificações adicionais em uma sala de segurança separada.
4. Depois de realizar essas verificações, o segurança redefine o bloqueio na caixa de diálogo **Bloqueio** da seguinte maneira:
   - Selecione o bloqueio apropriado na lista de controle **Bloqueio**.
   - Clique no botão **Excluir**.
   - Confirme a exclusão clicando em **Sim**.

A pessoa escolhida aleatoriamente agora pode usar seu cartão novamente em todos os leitores para os quais tem autorização.

Exemplo de layout da sala para triagem aleatória



1 = Apresentação do cartão - triagem - bloqueio no sistema inteiro
2 = Titular do cartão entra na cabine de segurança
3 = Titular do cartão é revistado e, em seguida, o bloqueio é retirado de seu cartão através da caixa de diálogo.

4 = Titular do cartão deixa o cabine de segurança sem apresentar o cartão ao leitor novamente.

Aviso!
A porcentagem de triagem é alcançada de forma cumulativa ao longo do tempo. Por exemplo, em uma triagem aleatória de 10% ainda existe a possibilidade (1 em 100, isto é, 1/10 x 1/10) de que duas pessoas consecutivas sejam selecionadas.

29 Usando o visualizador de eventos

Introdução

O Visualizador de eventos permite que operadores devidamente autorizados examinem eventos que foram registrados pelo sistema e gerem relatórios: virtuais, impressos ou como arquivos `.CSV`.

Para recuperar e exibir os registros desejados no banco de dados de log de eventos, defina os critérios de filtro e clique em **Atualizar**  . Esse processo pode levar alguns minutos, dependendo da quantidade de dados solicitada.

Os critérios de filtro podem ser definidos de maneiras diferentes:

Relativo	Para selecionar eventos relativos ao momento presente.
Intervalo	Para selecionar eventos dentro de um intervalo que pode ser definido livremente
Total	Para selecionar eventos independentemente da hora de ocorrência

Pré-requisitos

Você está logado no gerenciador de caixas de diálogo.

Caminho da caixa de diálogo

Menu principal do gerenciador de caixas de diálogo > **Reports (Relatórios)** > **Event viewer (Visualizador de eventos)**

29.1 Definição de critérios de filtragem para tempo relativo ao presente

1. Em **Time period (Período)**, selecione o botão de opção **Relative (Relativo)**
2. Na caixa **Search within the last (Buscar nos últimos)**, defina o número de unidades de tempo para a busca e escolha quais unidades usar, por exemplo, semanas, dias, horas, minutos, segundos.
3. No menu **Event types (Tipos de eventos)**, selecione a categoria de eventos para a busca e, em seguida, os tipos de eventos que te interessam.
4. No menu **Maximum number (Número máximo)**, limite o número de eventos que o visualizador de eventos tenta receber. Por motivos de desempenho, **não** é recomendado deixar o valor **(unlimited) (ilimitado)**.
5. Especifique outros critérios de filtragem que te interessam:
   - Last name (Sobrenome)
   - First name (Nome)
   - Personal number (Número pessoal)
   - Card number (Número do cartão)
   - User (Usuário) (isto é, operador do sistema)
   - Device name (Nome do dispositivo)
   - Area name (Nome da área).

- Clique em **Refresh (Atualizar)**  para começar a coletar os eventos e em **Cancel (Cancelar)** para encerrar.
- Clique em  para salvar os resultados ou em  para imprimi-los.
- Clique em  para limpar os resultados para outra busca.

29.2 Definição de critérios de filtragem para um intervalo de tempo

1. Em **Time period (Período)**, selecione o botão de opção **Interval (Intervalo)**
2. Nos coletores de data **Time from, Time until (Tempo a partir de, Tempo até)** defina o início e o término do período em que deseja buscar eventos.
3. No menu **Event types (Tipos de eventos)**, selecione a categoria de eventos para a busca e, em seguida, os tipos de eventos que te interessam.
4. No menu **Maximum number (Número máximo)**, limite o número de eventos que o visualizador de eventos tenta receber. Por motivos de desempenho, **não** é recomendado deixar o valor **(unlimited) (ilimitado)**.
5. Especifique outros critérios de filtragem que te interessam:
   - Last name (Sobrenome)
   - First name (Nome)
   - Personal number (Número pessoal)
   - Card number (Número do cartão)
   - User (Usuário) (isto é, operador do sistema)
   - Device name (Nome do dispositivo)
   - Area name (Nome da área).

- Clique em **Refresh (Atualizar)**  para começar a coletar os eventos e em **Cancel (Cancelar)** para encerrar.
- Clique em  para salvar os resultados ou em  para imprimi-los.
- Clique em  para limpar os resultados para outra busca.

29.3 Definição de critérios de filtragem independentes do tempo

1. Em **Time period (Período)**, selecione o botão de opção **Total**
2. No menu **Event types (Tipos de eventos)**, selecione a categoria de eventos para a busca e, em seguida, os tipos de eventos que te interessam.
3. No menu **Maximum number (Número máximo)**, limite o número de eventos que o visualizador de eventos tenta receber. Por motivos de desempenho, **não** é recomendado deixar o valor **(unlimited) (ilimitado)**.
4. Especifique outros critérios de filtragem que te interessam:
   - Last name (Sobrenome)
   - First name (Nome)
   - Personal number (Número pessoal)
   - Card number (Número do cartão)
   - User (Usuário) (isto é, operador do sistema)
   - Device name (Nome do dispositivo)
   - Area name (Nome da área).

- Clique em **Refresh (Atualizar)**  para começar a coletar os eventos e em **Cancel (Cancelar)** para encerrar.

– Clique em  para salvar os resultados ou em  para imprimi-los.

– Clique em  para limpar os resultados para outra busca.

30 Uso de relatórios

Esta seção descreve um conjunto de funções de relatório que podem ser usadas para filtrar dados do sistema e do log de eventos, e para apresentá-los em formatos claros.

Caminho da caixa de diálogo

Menu principal > **Reports (Relatórios)**.

Uso da barra de ferramentas de relatórios

Clique em  para exibir uma visualização antes de imprimir.

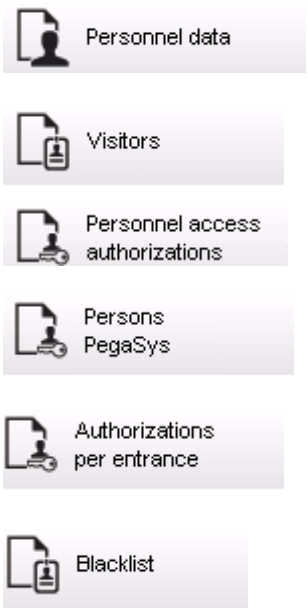
A visualização tem sua própria barra de ferramentas:

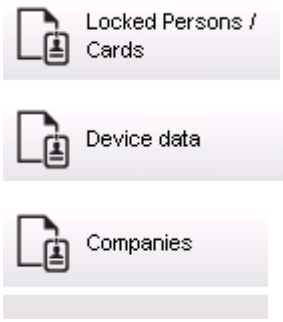
- Clique em ✕ para sair da visualização sem imprimir.
- Use as teclas de seta |◀ ◀ 2 of 17 ▶ ▶| na barra de ferramentas da visualização para navegar ou selecione páginas específicas pelo número de página.
- Clique em  para imprimir imediatamente usando a impressora padrão
- Clique em  para imprimir por meio de uma caixa de diálogo Print Setup (Configuração de impressão), que possibilita opções adicionais de impressão.
- Clique em  para exportar o relatório em diversos formatos de arquivo, incluindo PDF, RTF e Excel.
- Os números à direita da barra de ferramentas representam:
  - O número total de entradas existentes no banco de dados que correspondem aos critérios de filtragem.
  - A porcentagem dessas entradas do banco de dados que são exibidas na visualização.

30.1 Relatórios: Dados mestre

Visão geral dos relatórios – Dados mestre

Os relatórios de Dados mestre incluem todos os relatórios relacionados a pessoas, visitantes, cartões e suas autorizações de acesso. Além disso, os dados do dispositivo e da empresa podem ser exibidos.





Relatório: Dados de funcionários
Dois filtros podem ser aplicados na criação dos relatórios.
Filtro de pessoas: aqui o operador filtra com base nos campos usuais de dados de funcionários.
Filtro de cartões de acesso: aqui o operador pode filtrar com base nos números de cartão, intervalos de números, status e status de bloqueio.

Relatório: Visitantes
Semelhante aos dados de funcionários, os relatórios de visitantes podem ser criados aqui. Ao fazê-lo, ainda é possível ter acesso a todos os dados de visitantes criados, ou seja, até mesmo os visitantes que ainda não chegaram, mas que já foram registrados, podem ser selecionados.

Relatório: Autorizações de acesso de funcionários
Este relatório dá uma visão geral das autorizações de acesso registradas no sistema, e também mostra as pessoas a quem estas autorizações foram atribuídas.
Em termos de filtros, dados pessoais e a seleção de certas autorizações podem ser utilizados:
- Dados de funcionários: sobrenome, nome, número de funcionário
- Validação de todas as autorizações.
- O nome da autorização de entrada é incluído.
- O nome do modelo de tempo, se houver.
- O sentido de entrada.
- A validação da autorização especial.

Relatório: Lista negra
Nesta caixa de diálogo pode ser impressa uma lista detalhando a totalidade ou uma seleção desejada de cartões de identificação colocados na lista negra por vários motivos.

Relatório: Pessoas/cartões bloqueados
Esta caixa de diálogo pode ser usada para criar relatórios com dados sobre todas as pessoas bloqueadas.
Utilize datas para encontrar bloqueios durante períodos especificados.

Relatório: Dados de dispositivos
A caixa de diálogo pode ser usada para criar relatórios com base nos dados de dispositivos, por exemplo, nome do dispositivo ou tipo do dispositivo.

Relatório: Empresas

A caixa de diálogo do relatório de Empresas é usada para reunir os dados da empresa em uma lista.

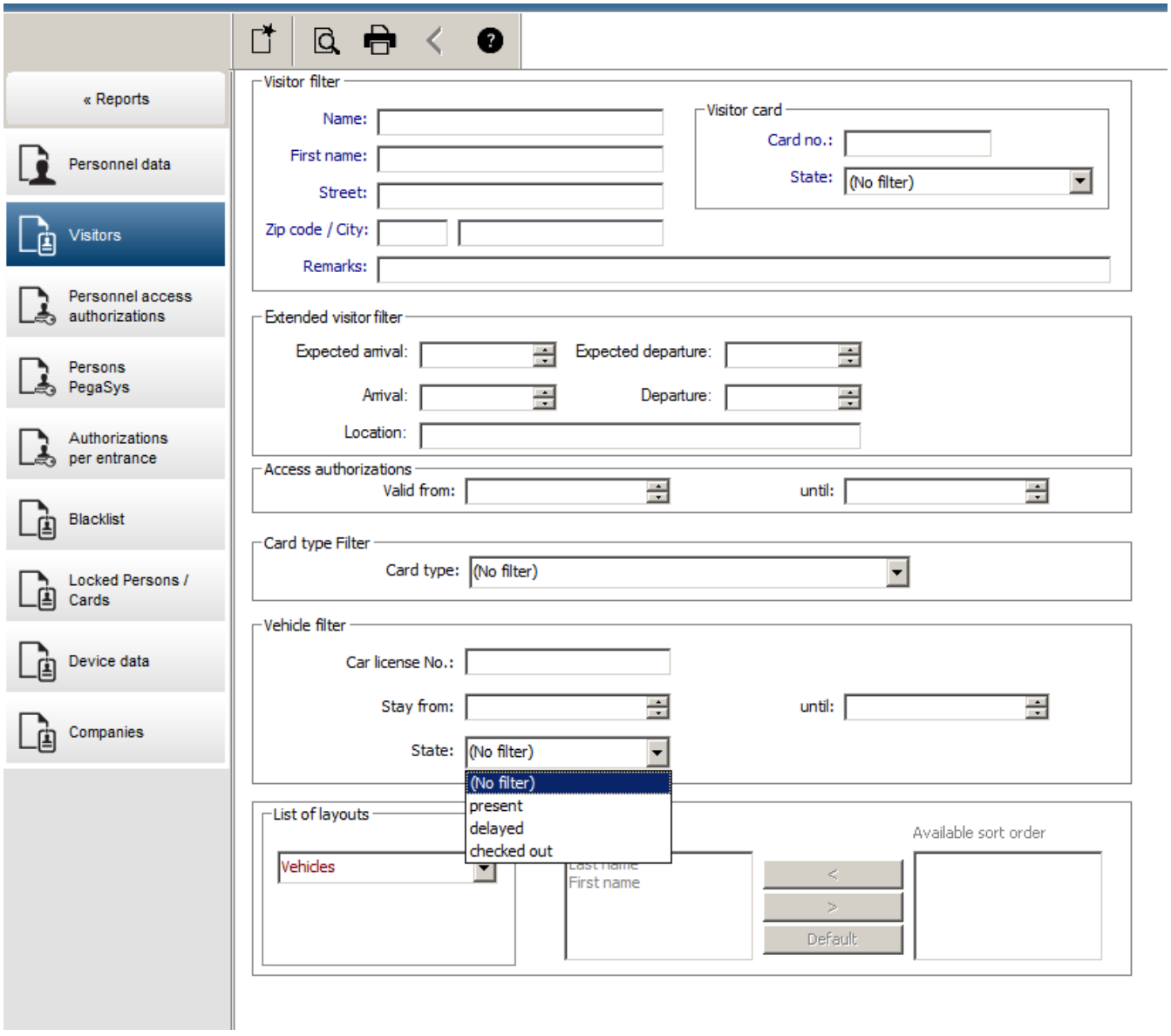
Utilize asteriscos, por exemplo, para encontrar empresas que começam com uma letra específica.

30.1.1 Relatório sobre veículos

Na caixa de diálogo **Relatórios > Visitantes** é possível selecionar **Veículos** na lista. Quando **Veículos** é selecionado a área da caixa de diálogo **Filtrar veículo** é ativada, e pode ser usada pelo operador para filtrar os veículos e seu estado.

O estado é exibido da seguinte forma:

- Presente: Visita ainda não é terminada e o tempo ainda não é esgotado.
- Atrasada: Visita ainda não é terminada, mas tempo já está esgotado.
- Saída registrada: O visitante devolveu todos os cartões de acesso.



O **Relatório de veículos** só está disponível para visitantes porque a data prevista de chegada, a data prevista de partida, a data de chegada e a data de partida só estão disponíveis para visitantes na tabela do banco de dados **Visitantes**.

O relatório lista apenas os números de veículo que estão armazenados na tabela do banco de dados **Pessoas**. Então, quando o número de um veículo é alterado, o relatório vai listar outros resultados.
A duração será calculada da seguinte forma:

- Se o visitante já tiver registrado sua partida, será exibida a diferença, em minutos, entre a chegada e a partida.
- Se o visitante ainda não tiver registrado sua partida, será exibido o tempo, em minutos, desde a chegada até agora.

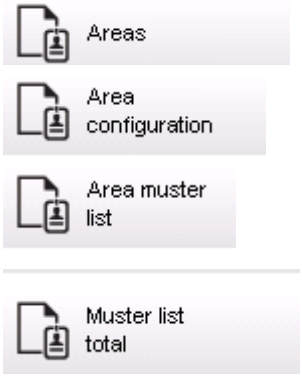
Access Engine

Vehicle Datum 02.07.2014 , 14:26:14
Seite 1

Lastname	Firstname Status	Arrival Departure Duration	Vehicle Last area	Person Last area
Neuer Besucher mit Langem Namen	**Vorname** present	02.07.2014 14:21 02.07.2014 14:30 0h 5'	AC BB 5678 parkplatz_01	ASB
Test	**Visitor** too late	01.07.2014 09:10 02.07.2014 12:00 29h 16'	AC AA 1234 parkplatz_01	ISB
Testbesucher mit sehr lagem Namen	**Besucher mit gaaaaaanz langem namen** departed	01.07.2014 07:30 01.07.2014 12:00 4h 30'	AC AA 2345 AUSSEN	AUSSEN

30.2 Relatórios: Dados do sistema

Relatórios – Dados do sistema
Ao contrário dos dados mestre, os dados do sistema são as informações atribuídas ao sistema, e não relacionadas a pessoas, cartões de identificação ou empresas. Esses relatórios são explicados em mais detalhes abaixo.



Relatório: Áreas
Esta caixa de diálogo pode ser usada para agrupar locais em um relatório. A caixa de diálogo contém apenas um filtro de área, que oferece os diversos edifícios e outras zonas para seleção.

A área em questão é selecionada através de um clique com o botão esquerdo do mouse. O usuário pode exibir o relatório na tela usando o botão **Preview (Visualizar)** antes de começar o processo de impressão com a função **Print (Imprimir)**.
Existem dois layouts disponíveis.

	Standard (Padrão)	Pessoas presentes no local – sem estacionamentos
	Parking lot occupancy (Ocupação do estacionamento)	Pessoas presentes no local – somente estacionamentos

Para confirmar que os conjuntos de dados exibidos estão atualizados, os últimos registros de cartões destas áreas também são listados.
Informações confiáveis sobre a localização de pessoas podem, portanto, ser obtidas para vários eventos.

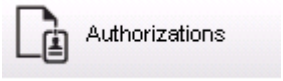
Relatório: Configuração de áreas
As áreas definidas e suas subáreas com um marcador que representa estacionamentos e o número máximo de pessoas ou carros.

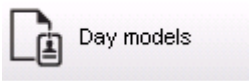
Relatório: Lista de convocação da área
Além de serem listadas de acordo com dados puramente numéricos, as pessoas de uma área também podem ser listadas por nome.
Com os tempos de leitura das áreas individuais, estes relatórios também contêm os tempos de cada pessoa individual.

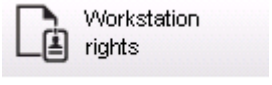
Relatório: Lista de convocação total
A princípio, as listas de convocação correspondem à caixa de diálogo do relatório **Áreas**. No entanto, elas disponibilizam listas de zonas específicas, que fornecem informações sobre o número de pessoas atualmente nesta área de acordo com o controle de acesso.

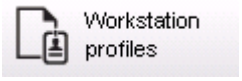
30.3 Relatórios: Autorizações

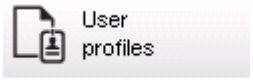
Overview (Visão geral)
Neste item do menu é fornecido um resumo das diversas autorizações concedidas nas caixas de diálogo correspondentes:











Relatório: Autorizações
Esta caixa de diálogo pode ser usada para exibir as autorizações de acesso definidas no sistema. As entradas relativas às autorizações de acesso individuais são listadas. O nome do modelo de tempo selecionado é exibido. Além disso, esse relatório mostra o número de pessoas a quem a autorização é atribuída.

Relatório: Modelos de tempo
Este relatório pode ser usado para exibir os modelos de tempo definidos no sistema, conforme selecionado. Esse relatório mostra todos os dados associados ao modelo, bem como o número de pessoas às quais o modelo se aplica.

Relatório: Modelos de dia
Este relatório exibe todos os modelos de dia definidos junto com seus nomes, descrições e os intervalos que contêm.

Relatório: Direitos de estação de trabalho
Esta caixa de diálogo pode ser utilizada para exibir os direitos atribuídos às estações de trabalho definidas no sistema.

Relatório: Perfis de estação de trabalho
Esta caixa de diálogo pode ser utilizada para exibir os perfis das estações de trabalho definidas no sistema, permitindo que as operações do sistema executadas nas estações de trabalho individuais sejam exibidas em um formato claro.

Relatório: Direitos de usuário
Esta caixa de diálogo pode ser usada para exibir os perfis de usuário atribuídos aos usuários definidos no sistema.

Relatório: Perfis de usuário
Esta caixa de diálogo pode ser usada para exibir as caixas de diálogo e direitos atribuídos aos perfis de usuário definidos no sistema.

31 Operação do gerenciamento do nível de ameaça

Esta seção descreve as várias maneiras de acionar um nível de ameaça e cancelá-lo. Para obter mais informações, consulte a seção *Configuração do gerenciamento de nível de ameaça, página 138*

Introdução

Um nível de ameaça é ativado por um alerta de ameaça. Um alerta de ameaça pode ser acionado de uma das seguintes formas:

- Por um comando na interface do usuário do software
- Por um sinal de entrada definido em um controlador de acesso local, por exemplo, um botão de destrave.
- Ao passar um cartão de alerta em um leitor

Lembre-se de que os alertas de ameaça podem ser cancelados pelo comando da interface do usuário ou pelo sinal de hardware, mas não pelo cartão de alerta.

Consulte

- *Configuração do gerenciamento de nível de ameaça, página 138*

31.1 Acionamento e cancelamento de um alerta de ameaça por meio de um comando da interface do usuário

Esta seção descreve como acionar um alerta de ameaça no AMS Map View.

Caminho da caixa de diálogo

- AMS Map View >  (Árvore de dispositivos)

Pré-requisitos

- Pelo menos um nível de ameaça deve ter sido definido
- Pelo menos um nível de ameaça foi marcado com Ativo no Editor de dispositivos.
- Você, como Operador do AMS e Map View, tem as permissões necessárias:
  - para operar os níveis de ameaça
  - para visualizar o MAC ou MACs na Divisão em que o alerta de ameaça deve ser acionado.

Procedimento para acionar um alerta de ameaça

1. Na árvore de dispositivos no AMS Map View, clique com o botão direito do mouse no dispositivo MAC em que o alerta de ameaça deve ser acionado.
   - Um menu de contexto será exibido. Ele contém os comandos que você tem autorização para executar no MAC em questão
   - Se nenhum nível de ameaça ainda estiver em operação, o menu incluirá um ou mais itens **Activate Threat level (Ativar nível de ameaça)** "`<name>`", que é o nome do nível de ameaça definido no Editor de dispositivos.
2. Selecione o nível de ameaça que você deseja acionar.
   - O nível de ameaça entra em operação.

Procedimento para cancelar um alerta de ameaça

Pré-requisito: um nível de ameaça já deve estar em operação.

1. Na árvore de dispositivos no AMS Map View, clique com o botão direito do mouse no dispositivo MAC em que o alerta de ameaça deve ser cancelado.

- Um menu de contexto será exibido. Ele contém os comandos que você tem autorização para executar no MAC em questão

2. Selecione **Deactivate Threat level (Desativar nível de ameaça)**. No menu de contexto.
   - O nível de ameaça atual está desativado.

31.2 Acionamento de um alerta de ameaça por sinal de hardware

Esta seção descreve como enviar um sinal de entrada de hardware para acionar um alerta de ameaça.

Pré-requisitos

- Pelo menos um nível de ameaça deve ter sido definido
- Pelo menos uma entrada deve ter sido configurada na árvore de dispositivos.
- Sinais de hardware devem ter sido definidos em um AMC, e um dispositivo deve ter sido conectado ao terminal correto nesse AMC, que enviará um sinal para ele. Se necessário, clique no link no final desta seção para obter instruções sobre como configurar o sinal de entrada ou entre em contato com o administrador do sistema.

Procedimento

Ative o dispositivo (normalmente um botão de destrave ou um switch de hardware) que está conectado ao AMC.
Para cancelar o alerta de ameaça, ative o dispositivo que envia o sinal de entrada definido como **Threat level: Deactivate (Nível de ameaça: desativar)**.

Consulte

- *Atribuição de um nível de ameaça a um sinal de hardware, página 143*

31.3 Acionamento de um alerta de ameaça por cartão de alerta

Esta seção descreve como acionar um alerta de ameaça por meio de um cartão de alerta.

Pré-requisitos

- Pelo menos um nível de ameaça deve ter sido definido
- Pelo menos uma entrada deve ter sido configurada na árvore de dispositivos.
- Um cartão de alerta foi criado para um usuário de cartão específico. Se necessário, clique no link no final desta seção para obter instruções sobre como criar um cartão de alerta ou entre em contato com o administrador do sistema.

Procedimento

1. O usuário mostra o cartão de alerta especial em qualquer leitor que **não usa impressão digital** no local.
   - O nível de ameaça definido para esse cartão é ativado.
2. Após o término da ameaça, cancele o nível de ameaça por meio do comando da interface do usuário ou do switch de hardware. Por padrão, não é possível cancelar um nível de ameaça usando um cartão de alerta.

Consulte

- *Criação de um cartão de alerta, página 206*

32 Operação do Swipe ticker

Introdução

Swipe ticker é uma ferramenta que ajuda os operadores do Map View a monitorar, em tempo real, quem está entrando ou saindo das instalações.

Visão geral

Swipe ticker é um aplicativo no AMS Map View que exibe os últimos 10 minutos de eventos de acesso em uma lista de rolagem dinâmica. Até 50 eventos de acesso são exibidos, e os eventos registrados há mais de 10 minutos são descartados automaticamente da lista. O operador pode monitorar todos os leitores no sistema ou selecionar um subconjunto.
Cada registro na lista contém informações do evento e a credencial usada, por exemplo:

- O nome do usuário do cartão e a foto armazenada, para confirmação visual da identidade.
- Um registro de data e hora.
- O nome da empresa e/ou do departamento, se armazenado.
- A entrada e o leitor em que a credencial foi usada.
- Uma categoria de evento com uma etiqueta colorida:
  - Verde: acesso concluído com uma credencial válida
  - Amarelo: acesso incompleto com uma credencial válida, por exemplo, o usuário do cartão girou a fechadura, mas não abriu a porta
  - Vermelho: tentativa falha de acesso com uma credencial inválida. O tipo de invalidez é mostrado, por exemplo, a credencial está na lista negra, é desconhecida ou expirou

O Swipe ticker não retém os próprios arquivos — ele extrai e exibe eventos de acesso do banco de dados do sistema. A rolagem dinâmica pode ser pausada para um estudo mais detalhado ou aberta em outra janela para uso paralelo com outros aplicativos do Map View.

Aviso!
Latência após edições
As alterações nas fotos de identificação no AMS geralmente levam alguns minutos para aparecerem no Swipe ticker.

Pré-requisitos

O perfil de usuário do operador exige autorização especial para executar o Swipe ticker.

1. No aplicativo principal do AMS, acesse o menu: **Configuration (Configuração)** > **User profiles (Perfis de usuário)**
2. Carregamento do nome do perfil do operador desejado
3. Na tabela, selecione **Access Manager Maps (Mapas do gerenciador de acesso)** > **Special functions (Funções especiais)** > Swipe ticker

Inicialização do Swipe ticker

- No Map View, clique em  para iniciar a ferramenta.

Seleção dos leitores a serem monitorados

Se os leitores ainda não tiverem sido selecionados ou se você desejar alterar a seleção:

1. Na janela Swipe ticker, clique em  (configurações).
   A janela **Filter devices (Filtrar dispositivos)** será aberta.
2. Na árvore de dispositivos, marque as caixas de seleção das entradas ou dos leitores que você deseja monitorar. As caixas de seleção têm este comportamento:
   Se você selecionar uma entrada, todos os dispositivos subordinados serão selecionados por padrão.
   As caixas de seleção de dispositivos subordinados individuais poderão ser desmarcadas se não forem necessários.
   Se **todos** os filhos de um dispositivo pai forem selecionados, a caixa de seleção do pai ficará branca. Se somente **alguns** forem selecionados, a caixa de seleção do pai ficará cinza.
3. Clique em **OK** para terminar a seleção dos leitores e feche a janela **Filter devices (Filtrar dispositivos)**.

Exibição dos leitores selecionados no mapa

- ▸ Clique duas vezes em um registro no Swipe ticker.

P O Swipe ticker é pausado automaticamente.

P O Map View exibe na janela principal a primeira cena de mapa relevante em sua hierarquia de mapas e destaca o leitor em que você clicou duas vezes.

Pausa do Swipe ticker

- ▸ Na janela Swipe ticker, clique em  ou clique duas vezes em um registro na lista para pausar a exibição dinâmica

P A exibição dinâmica congela. Os registros de eventos recebidos são armazenados em buffer, mas não são exibidos.

P Um aviso informando que o fluxo de eventos foi pausado é colocado no topo da lista.

Retomada de um Swipe ticker pausado

- ▸ Na janela Swipe ticker, clique em  para retomar a exibição dinâmica

P A lista dinâmica exibe em ordem cronológica (mais recente primeiro) todos os eventos de acesso que ocorreram nos leitores selecionados nos últimos 10 minutos, até o máximo de 50.

P Os eventos de acesso mais antigos que os 50 mais recentes ou mais antigos que 10 minutos são removidos da lista.

P Novos eventos de acesso são exibidos novamente em tempo real conforme ocorrem.

Duplicação do Swipe ticker em outra janela

Note que apenas uma janela Swipe ticker duplicada pode ser aberta de cada vez.

1. Na janela Swipe ticker, clique em  (janela adicional).

A janela separada é duplicada e **não** é independente do ticker na janela principal. Ela obedece às mesmas configurações.
Outros aplicativos do Map View, como a lista de alarmes, agora podem ser operados paralelamente na janela principal.

2. Após terminar de usar a janela separada, use a barra de título para fechá-la.

32.1 Casos especiais

Swipe ticker da Map View e portas do B901

Para fornecer informações corretas ao aplicativo **Swipe ticker** na Map View do AMS, os IDs das portas do B901 devem corresponder aos IDs dos pontos de porta. Ou seja, a Porta 1 deve ser atribuída ao Ponto de porta 1, Porta 2 ao Ponto de porta 2 etc.

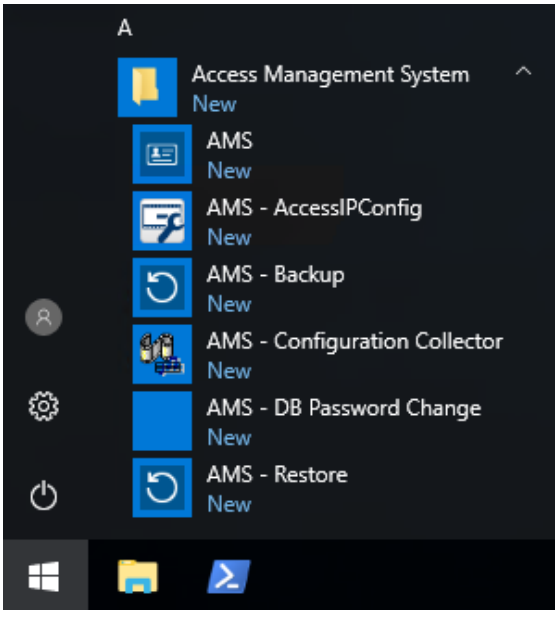
Doors 1 - 4	Door 1	Door 2	Door 3	Door 4
Door Name Text	Door 1	Door 2	Door 3	Door 4
Door Name Text (Second Language)				
Door Source	SDI2 (B901)	SDI2 (B901)	SDI2 (B901)	SDI2 (B901)
Entry Area	1	1	1	1
Associated Keypad #	Keypad 1	Keypad 1	Keypad 1	Keypad 1
Custom Function	Disabled	Disabled	Disabled	Disabled
Door Point	1	2	3	4
Door Point Debounce	600ms	600ms	600ms	600ms

Faça essas atribuições ao controlador de porta B901 na ferramenta RPS que configura painéis de intrusão e controladores.

33 Backup e restauração

A função **Backup & Restore (Backup e restauração)** permite que você transfira o sistema com os respectivos dados para uma nova versão do AMS ou para um novo computador.
Backup and Restore (Backup e restauração) só pode ser executada em uma máquina em que o servidor do AMS estiver instalado. Estão disponíveis dois atalhos no menu Iniciar do Windows:

– **AMS - Backup** para criação de um backup
– **AMS - Restore (Restauração)** para restauração de um backup:

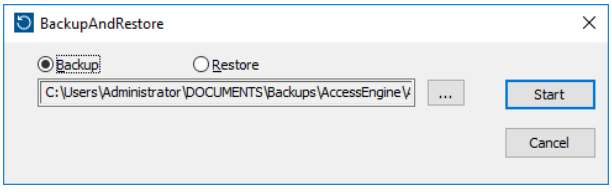


33.1 Backup do sistema

Esta seção descreve como criar um backup para o aplicativo AMS e localizar os arquivos de backup do SQL Server.

Criar um backup do aplicativo AMS

1. No menu Iniciar do Windows, clique com o botão direito em **AMS - Backup** e selecione **Executar como administrador**.
   – A ferramenta **Backup e restauração** é iniciada com a opção **Backup** pré-selecionada.



2. Insira um caminho para salvar o arquivo `.GZ`.
3. Clique em **Iniciar** para iniciar o backup.
   – A ferramenta **Backup e restauração** cria um único arquivo `.GZ` e exibe seu progresso em uma janela pop-up.
4. Copie esse arquivo para o armazenamento seguro em outro computador. Para segurança dos dados, **não** deixe a única cópia no servidor DMS.

Localize e copie os arquivos de backup do SQL Server.

1. Usando um explorador de arquivos no computador do servidor do AMS, navegue até o diretório em que o SQL Server mantém os arquivos `.BAK`.

- O diretório é o seguinte, em que `<version>` e `<instance name>` são variáveis que dependem do seu sistema:
  `C:\Program files\Microsoft SQL Server\MSSQL<version>.<instance name>\MSSQL\Backup\`
- Os nomes de arquivos estão no formato:
  `acedb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak`
  `Bosch.AlarmDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak`
  `Bosch.EventDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak`
  `Bosch.MapDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak`
  `Bosch.MapViewDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak`
  `Bosch.StatesDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak`

2. Copie **todos** os arquivos `.BAK` para um armazenamento seguro em outro computador. Para a segurança dos dados, **não** deixe as únicas cópias no servidor do DMS.

Aviso!
O diretório padrão para o log de eventos do AMS é:
`C:\Program Files (x86)\Access Management System\Access Engine\AC\LgfLog\`

33.2 Restauração de um backup

Pré-requisitos

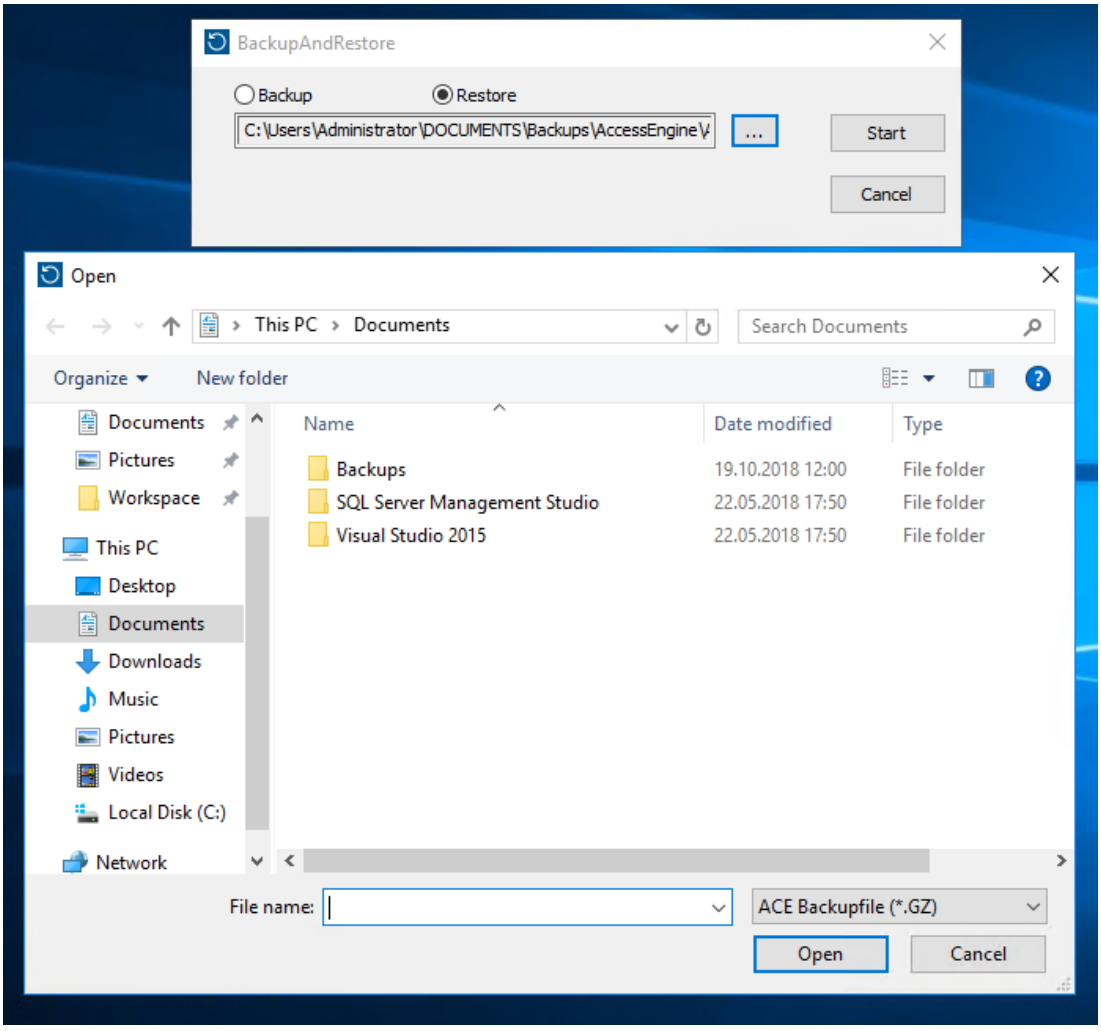
- O arquivo `GZ` que foi criado pela ferramenta **Backup e restauração**
- Os arquivos `.BAK` criados pelo SQL Server salvos durante o procedimento de backup.
- Uma conta do SQL com direitos **sysadmin**, como `sa`.
- Um computador de destino devidamente preparado com relação a **licenças** e **certificados**:
  - **Licenças**: o computador de destino (onde o backup é restaurado) requer pelo menos licenças equivalentes àquelas no computador em que o backup foi feito.
  - **Certificados**: todos os clientes do computador de destino precisarão dos novos certificados gerados pela instalação no computador de destino, não daqueles gerados pela instalação no computador original.
    Consulte o **Guia de instalação do AMS** para saber como gerar e instalar certificados clientes.

Procedimento

1. No programa AMS, clique em **Arquivo** > **Sair** para interromper o aplicativo AMS.
2. Quando o programa for encerrado, execute o aplicativo Windows **Services** e verifique se todos os serviços `Access Engine` e `Access Management System` foram interrompidos. Caso contrário, interrompa-os aqui.
3. **Se você estiver** executando um RMAC (MAC de failover redundante) com o 1. MAC ou principal, pule para o próximo subcapítulo e realize o procedimento descrito lá antes de voltar para esta etapa.
4. Copie os arquivos MSSQL `.BAK` salvos no computador original exatamente para o mesmo caminho no novo computador.

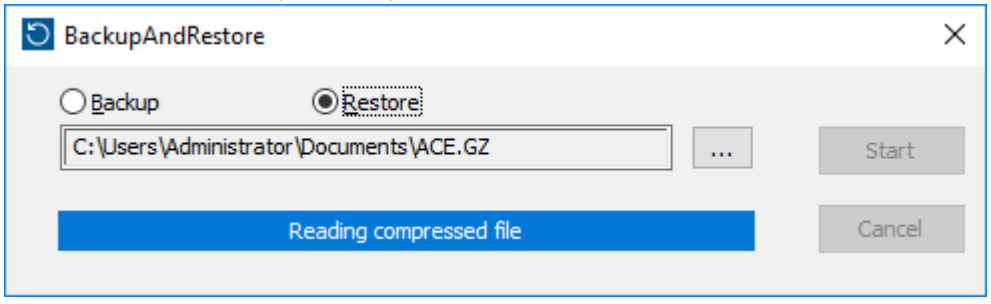
– O diretório é o seguinte, em que `<version>` e `<instance name>` são variáveis que dependem do seu sistema:
`C:\Program files\Microsoft SQL Server\MSSQL<version>.<instance name>\MSSQL\Backup\`

5. No menu Iniciar do Windows, clique com o botão direito em **AMS - Restaurar** e selecione **Executar como administrador**
   – A ferramenta **Backup e restauração** é iniciada com a opção **Restauração** pré-selecionada.
6. Clique no botão **[...]** para localizar o arquivo de backup `GZ` no sistema de arquivos e clique em **Abrir** para selecioná-lo.



7. Clique em **Iniciar** para iniciar o processo de restauração.
8. Quando as credenciais de servidor forem solicitadas, insira as credenciais de um sysadmin MSSQL como `sa`, não as credenciais de login do computador do servidor.

– O processo de restauração começa



9. Quando o processo de restauração terminar, execute o aplicativo Windows **Services** e reinicie todos os serviços `Access Engine` e `Access Management System` manualmente.
10. Execute o programa `AMS Server Setup.exe` de configuração do servidor como administrador para sincronizar novamente os dados do backup com os dados atuais do sistema.

Consulte

– *Backup do sistema, página 259*

33.2.1 Restauração de RMACs em uma nova instalação

Observação: Este procedimento só é relevante para os casos em que a restauração do backup de um sistema com MACs e RMACs é feita em hardwares diferentes.

Introdução

Se você restaurar um backup em novos computadores, será necessário configurar novamente os endereços IP do MAC e RMAC que foram armazenados no arquivo de backup para os endereços IP do novo hardware. Para realizar essa configuração, execute a ferramenta MACInstaller no novo hardware.

A ferramenta MACInstaller pode ser encontrada na mídia de instalação em `\AddOns\MultiMAC\MACInstaller.exe`

O uso da ferramenta MACInstaller está descrito em detalhes no capítulo *Uso da ferramenta MACInstaller, página 52*

Procedimento

1. Execute a ferramenta MACInstaller no computador em que o 1.MAC está em execução. Esse computador pode ser o servidor do DMS ou um servidor dedicado para 1.MAC.
   – Na ferramenta, defina os novos endereços IP do MAC primário (este computador) e RMAC.
2. Execute a ferramenta MACInstaller no computador em que o RMAC está em execução.
   – Na ferramenta, defina os novos endereços IP do MAC primário e RMAC (este computador).
3. Volte para a etapa em que interrompeu o procedimento de **Restauração**.

Consulte

– *Uso da ferramenta MACInstaller, página 52*

Glossário

1. MAC (primeiro MAC)

O MAC (Controlador de acesso mestre) primário em um Access Engine (ACE) do BIS ou sistema Gerenciador de acesso (AMS). Ele pode residir no mesmo computador que o DMS, mas também pode residir em um computador separado conhecido como servidor MAC, igual a um MAC subsidiário.

a reboque

Driblar o controle de acesso ao seguir de perto um titular de cartão autorizado através de uma entrada sem apresentar suas próprias credenciais.

ACS

termo genérico para um sistema de controle de acesso da Bosch, por exemplo, AMS (Access Management System) ou ACE (BIS Access Engine).

Alerta de ameaça

um alarme que aciona um nível de ameaça. Pessoas devidamente autorizadas podem acionar um alerta de ameaça com uma ação momentânea, por exemplo, pela interface do usuário do operador, por um sinal de hardware (por exemplo, botão de destrave) ou pela apresentação de um cartão de alarme especial em qualquer leitor.

anti-passback

Uma forma simples de Monitoramento da sequência de acesso em que o titular do cartão é impedido de entrar em uma Área duas vezes durante um período definido, a menos que o cartão tenha sido lido para sair da Área enquanto isso. O anti-passback impede que uma pessoa passe as credenciais novamente em uma entrada para o uso de uma segunda pessoa não autorizada.

Área (Armação)

Um agrupamento de entradas do modelo 14 em um sistema de controle de acesso. A armação ou o desarme do sistema de intrusão em uma dessas entradas simultaneamente tem o mesmo efeito em todas as entradas em que o parâmetro Arming area (Área de armação) tiver a mesma designação de uma letra.

Chave de hardware do AMC

Um código de autenticação interno que o AMC gera a partir de determinados parâmetros de hardware. Não fica visível para o usuário.

Chave de LCD aleatória

Um código alfanumérico temporário que o AMC gera sempre que é iniciado. A chave pode ser exibida no visor de cristal líquido (LCD) do AMC e pode ser solicitada por ferramentas de software para autenticar a comunicação de rede.

Chave mestre

Um código que o sistema gera a partir da DCP (Senha de comunicação de dispositivo) e usa para proteger os dispositivos de controle de acesso. A chave mestre nunca fica visível para nenhum usuário.

Controlador de acesso local (LAC)

Um dispositivo de hardware que envia comandos de acesso ao hardware de controle de acesso periférico, como leitores e travas, e processa solicitações desse hardware para o sistema de controle de acesso geral. O LAC mais comum é um Controlador modular de acesso ou AMC.

Data Management System (DMS)

Um processo de nível superior para gerenciar dados de controle de acesso no sistema. O DMS fornece dados para controladores de acesso principal (MAC) que, por sua vez, fornecem dados para controladores de acesso local (geralmente AMC).

DCP

uma senha a partir da qual o sistema de controle de acesso gera uma chave mestre que é usada para criptografar a comunicação de rede para todos os controladores de acesso local subordinados, normalmente dispositivos AMC.

DSN

Nome da fonte de dados. O nome da fonte de dados em Open Database Connectivity (ODBC).

DTLS

Datagram Transport Layer Security é um protocolo de comunicação segura que protege contra espionagem e falsificação.

Entrada

O termo Entrada denota em sua totalidade o mecanismo de controle de acesso em um ponto de entrada: inclui os leitores, alguma forma de barreira bloqueável e um procedimento de acesso, conforme definido pelas sequências de sinais eletrônicos enviados entre os elementos de hardware.

entropia de senha

uma medida de intensidade da senha calculada a partir de fatores como aleatoriedade, número de símbolos disponíveis e o número real de símbolos usados.

espera

para suspender um alarme em circunstâncias especialmente definidas.

Ferramenta IPConfig

Um programa auxiliar separado para configurar a rede e as configurações de segurança de rede dos dispositivos de hardware dentro do sistema de controle de acesso.

grupo de elevadores

Um grupo de elevadores que atendem aos mesmos andares do edifício. Cada grupo de elevadores é governado por um Servidor de entrada de destino (DES).

IDS

Sistema de detecção de intrusão, também conhecido como um sistema de alarmes contra roubo.

Lista de autorizações (SmartIntego)

Uma lista de autorizações é uma lista de números de cartões armazenada localmente nos leitores de cartões de um sistema de bloqueio SmartIntego. Se o MAC do leitor estiver off-line, o leitor concederá acesso aos cartões cujos números estiverem contidos em sua lista de autorizações local.

MAC (Master Access Controller)

Em sistemas de controle de acesso, um programa do servidor que coordena e controla os Controladores de acesso locais, geralmente AMCs (Controlador modular de acesso)

Modelo de porta

Um modelo de software armazenado de um tipo específico de entrada. Modelos de porta facilitam a definição de entradas em sistemas de controle de acesso.

Modo de configuração

o estado padrão dos dispositivos de controle de acesso no editor de dispositivos. As alterações entram em vigor e são propagadas para os dispositivos subordinados imediatamente.

Modo de operação

o estado de um dispositivo de controle de acesso no editor de dispositivos ao responder a comandos dados fora do editor de dispositivos. As alterações de configuração entram em vigor somente depois que o modo de operação termina e o modo de configuração é restaurado.

Modo Escritório

Suspensão do controle de acesso em uma entrada durante o horário comercial.

Modo Normal

Ao contrário do modo Escritório, o modo Normal concede acesso apenas a pessoas que apresentarem credenciais válidas ao leitor.

Monitoramento da sequência de acesso

O rastreamento de uma pessoa ou veículo de uma Área definida para outra ao registrar cada leitura do cartão de identificação e concessão de acesso somente das Áreas onde o cartão já foi lido.

PIN de identificação

Um número de identificação pessoal (PIN) que é a credencial exclusiva necessária para acesso.

PIN de verificação

Um número de identificação pessoal (PIN) usado em combinação com uma credencial física para aplicar um nível maior de segurança.

Ponto

Um sensor para detectar intrusão em uma área com controle de intrusão. Em alguns contextos, os pontos poderão ser chamados de zonas ou sensores.

Ponto de encontro

um local designado onde as pessoas são instruídas a aguardar após a evacuação de um edifício.

Reconhecimento de número da placa automatizado (ANPR)

O uso de tecnologia de vídeo para ler e processar números de placas, geralmente de automóveis.

Redirecionador de entrada de destino (DER)

Um computador no mesmo nível do Servidor de entrada de destino (DES) em um sistema Otis CompassPlus. Conecta-se a todos os grupos de elevadores e seu trabalho é aumentar a eficiência dos dispositivos DES.

REX

“Solicitação de saída”. Um sinal para solicitar que a porta seja destrancada por dentro para permitir a saída. O sinal normalmente é acionado por um botão ou barra no interior de uma entrada; às vezes por um detector de movimento.

RMAC

Um controlador de acesso principal (MAC) redundante que é um gêmeo sincronizado de um MAC existente e assume o gerenciamento dos dados se o primeiro MAC falhar ou for desconectado.

RPS

Remote Programming Software. Um programa que gerencia painéis de controle de intrusão ou incêndio em uma rede.

Servidor de entrada de destino (DES)

Um computador que governa um banco de elevadores para otimizar os tempos de deslocamento.

Servidor MAC

Hardware: um computador (diferente do servidor do DMS) em um Access Engine (ACE) ou Access Management System (AMS), em que um MAC ou RMAC é executado.

Sistema de despacho de destino (DDS)

também conhecido como Sistema de gerenciamento de destinos, mas use somente a abreviação DDS. O Otis CompassPlus é um tipo de DDS.

SmartIntego

Sistema de bloqueio digital da SimonsVoss Technologies. O SmartIntego já vem integrado em alguns sistemas de controle de acesso da Bosch.

Terminal de entrada de destino (DET)

Um dispositivo onde os passageiros do elevador podem inserir solicitações de destino para um grupo de elevadores.

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

Building solutions for a better life.

202209021612