Access Management System

AMS configuration and operation

pt-BR Manual do software

Sumário

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

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 de computador deste computador. Entre em contato com o seu representante de vendas para obter instruções.
Caminho da caixa de diálogo: **Configuration (Configuração)** > **Licenses (Licenças)**

1. Faça login no AMS, o Access Management System.
   Observação: Se o AMS estiver instalado nas pastas de Arquivos de Programas do Windows, faça login com direitos de Administrador do Windows.
2. Navegue até **Configuration (Configuração)** > **Licenses (Licenças)**
3. Clique em **Start license manager (Iniciar o gerenciador de licenças)**
4. Na janela **License Manager (Gerenciador de licenças)**, marque a caixa de seleção do pacote base que você adquiriu.
5. Na janela pop-up **License Activation (Ativação de licença)**,
   – Cole a **Computer Signature (Assinatura do computador)** do computador do servidor do Gerenciador de acessos,
   – Cole a **License Activation Key (Chave de ativação da licença)** recebida para o pacote base,
   – Clique em **Activate... (Ativar...)**
6. Na janela **License Manager (Gerenciador de licenças)**, verifique se o pacote base que você acabou de licenciar agora apresenta o status **Activation valid (Ativação válida)**.
7. Na janela **License Manager (Gerenciador de licenças)**,
   – Clique em **Import Bundle Info (Importar informações do pacote)** para pesquisar e ativar qualquer pacote de licenças adquirido e recebido como arquivos.
   – Clique em **Import License (Importar licença)** para pesquisar e ativar qualquer licença individual adquirida e recebida como arquivos.
8. Clique em **Close (Fechar)** para fechar o **License Manager (Gerenciador de licenças)**.
9. De volta à caixa de diálogo principal **Licenses (Licenças)**, verifique se os recursos adquiridos estão listados com o número correto de unidades.

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.

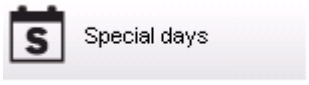
1. Faça login no Gerenciador de acesso
2. Navegue até **Configuration (Configuração)** > **Licenses (Licenças)**
3. Clique no botão **Activate Demo Mode (Ativar modo de demonstração)**
4. Verifique se os recursos estão listados na janela da caixa de diálogo **Licenses (Licenças)**.

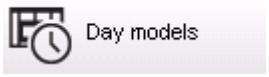
O modo de demonstração é ativado para 5 horas. Observe que o tempo de expiração é exibido próximo ao topo da caixa de diálogo **Licenses (Licenças)** e na barra de títulos da maioria das janelas de caixa de diálogo.

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.

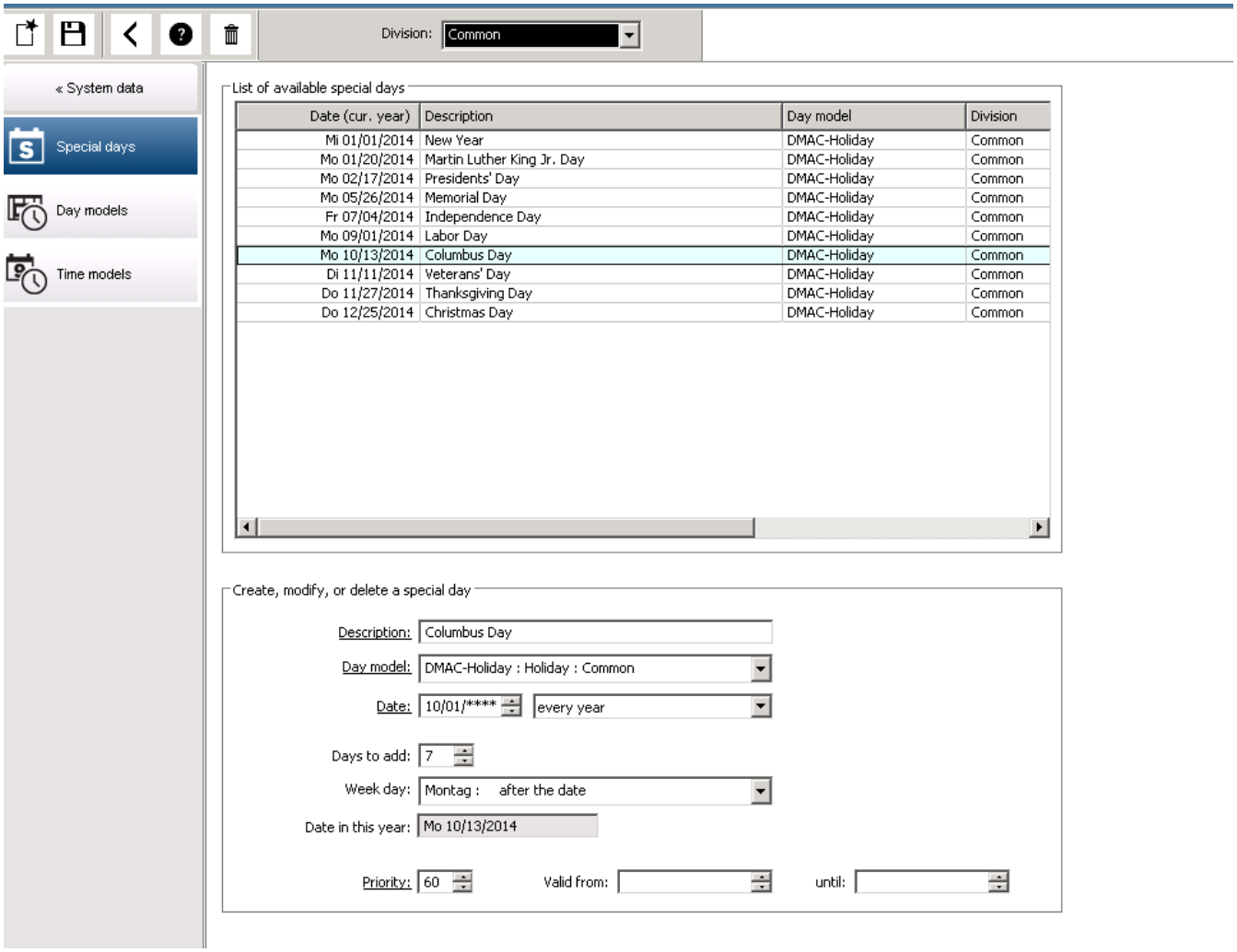
1. Defina os **dias especiais** do calendário que se aplicam à sua localização.
2. Defina **modelos de dia** que descrevem os períodos ativos e inativos de cada tipo de dia. Por exemplo, o modelo de dia para um feriado será diferente do modelo para um dia útil normal. O trabalho em turnos também afetará 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	**.**.****

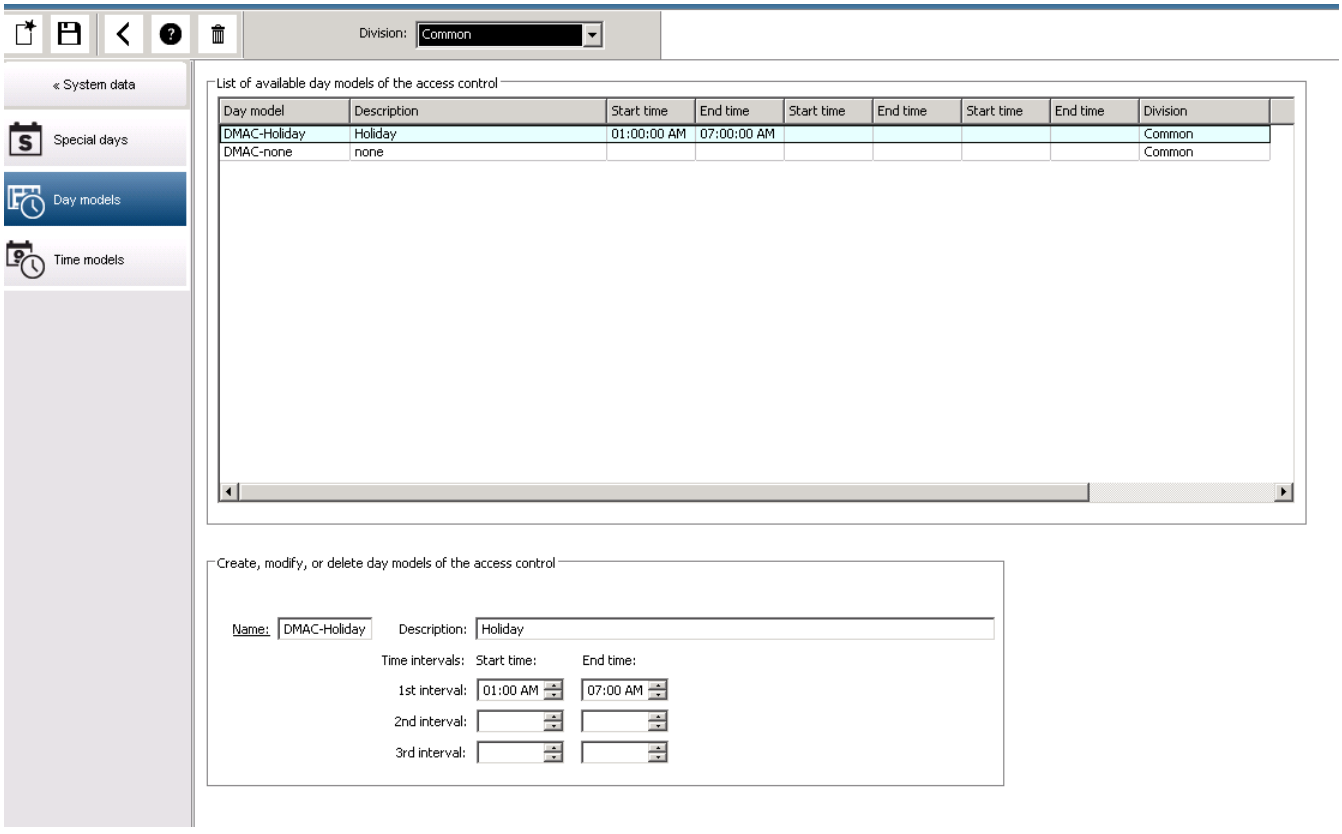
Os feriados que dependem da Páscoa não são especificados com sua data, mas com a diferença de dias desde o domingo de Páscoa. A data do domingo de Páscoa no ano em curso é indicada no campo **Date within this year (Data dentro deste ano),** e a variação desta data é digitada ou selecionada no campo **Days 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:

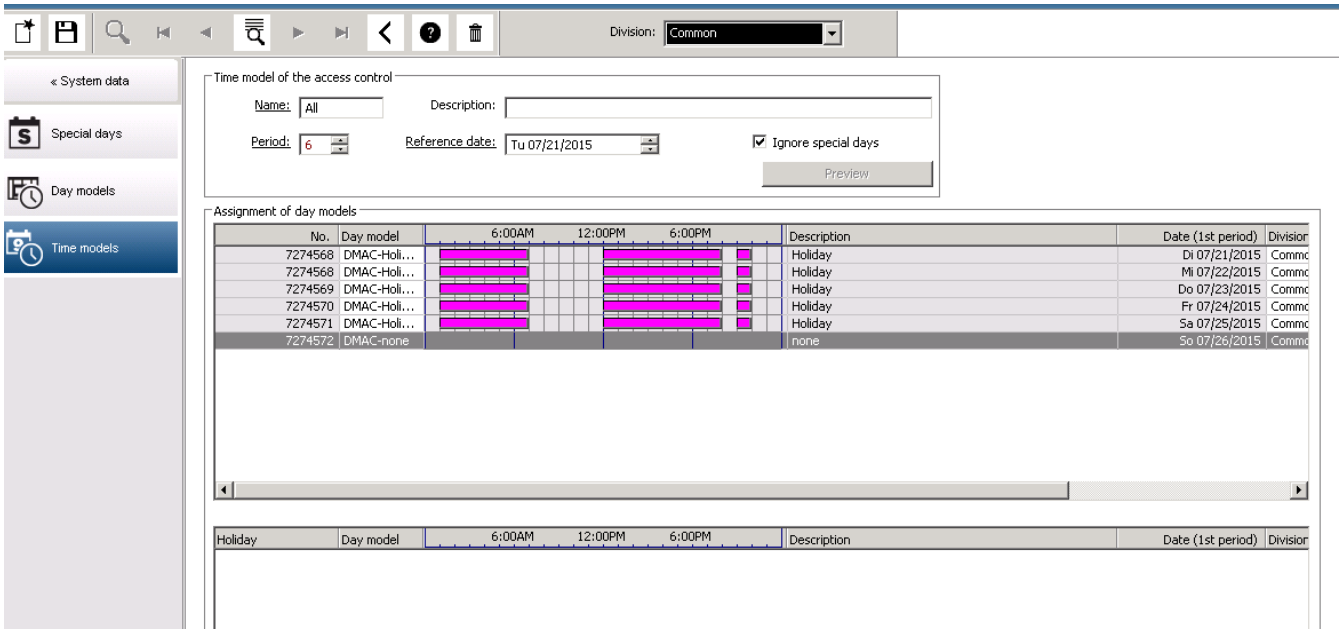
1º Intervalo	de:	...	até:	00:00
Intervalo seguinte	de:	00:00	até:	...

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.

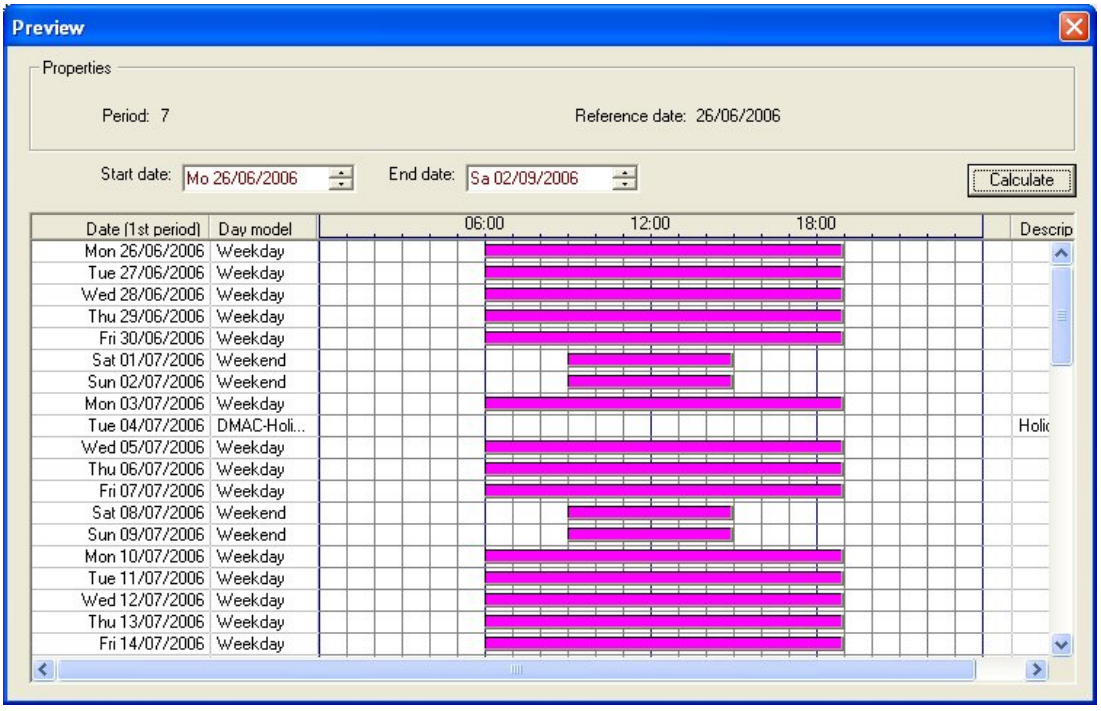
Se a máscara estiver vazia, o modelo de tempo pode ser criado do zero. Para tanto, você deve inserir um **nome** e o número de dias em **período** e selecionar uma data inicial ou **data de referência**. Quando esses dados são confirmados (**Enter**), uma lista é exibida no campo **Assignment of day 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.

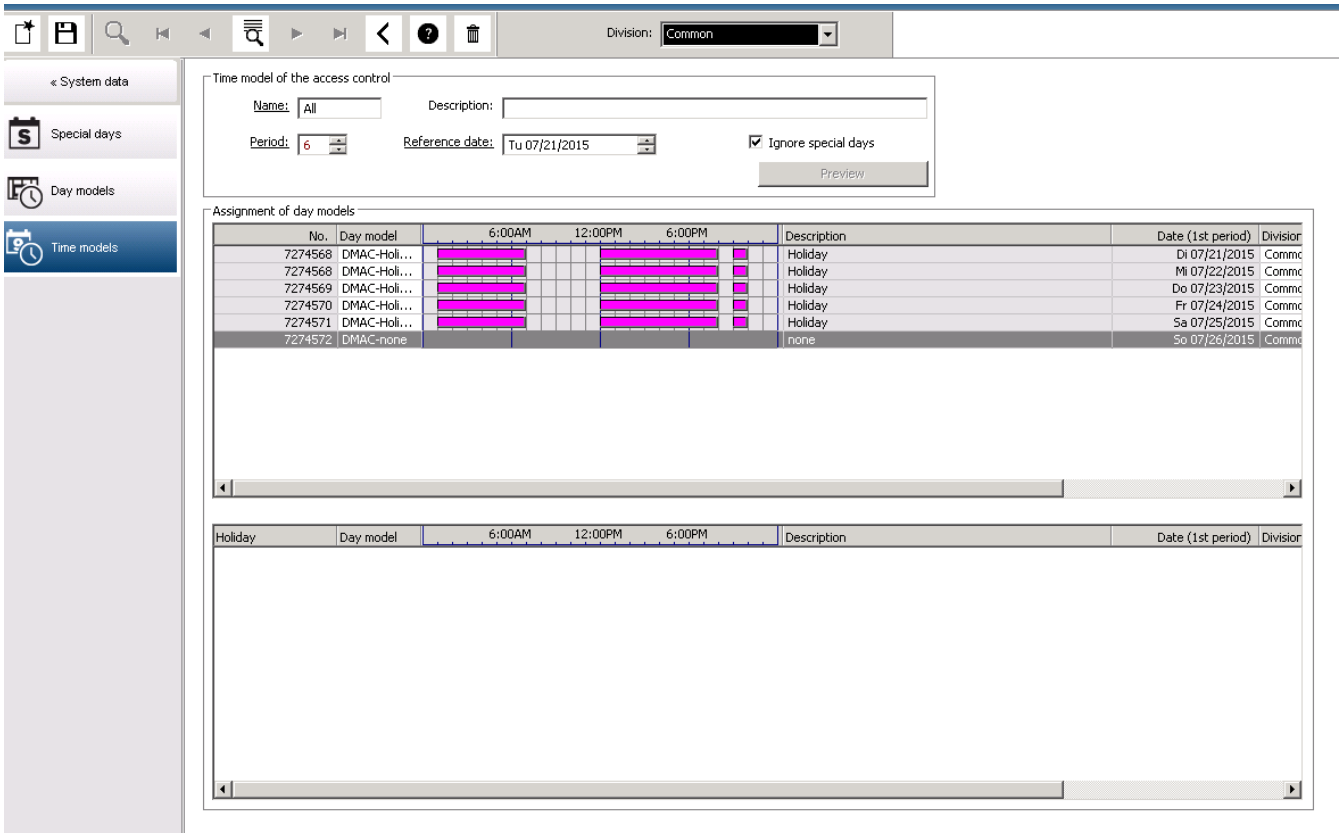
Ao clicar duas vezes na linha relevante da coluna **Day model (Modelo de dia)**, um campo de listagem é ativado para seleção. Um dos modelos de dia existentes pode ser selecionado nesta lista. Desse modo, um modelo de dia específico pode ser atribuído a cada dia do período. Quando o usuário passa para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

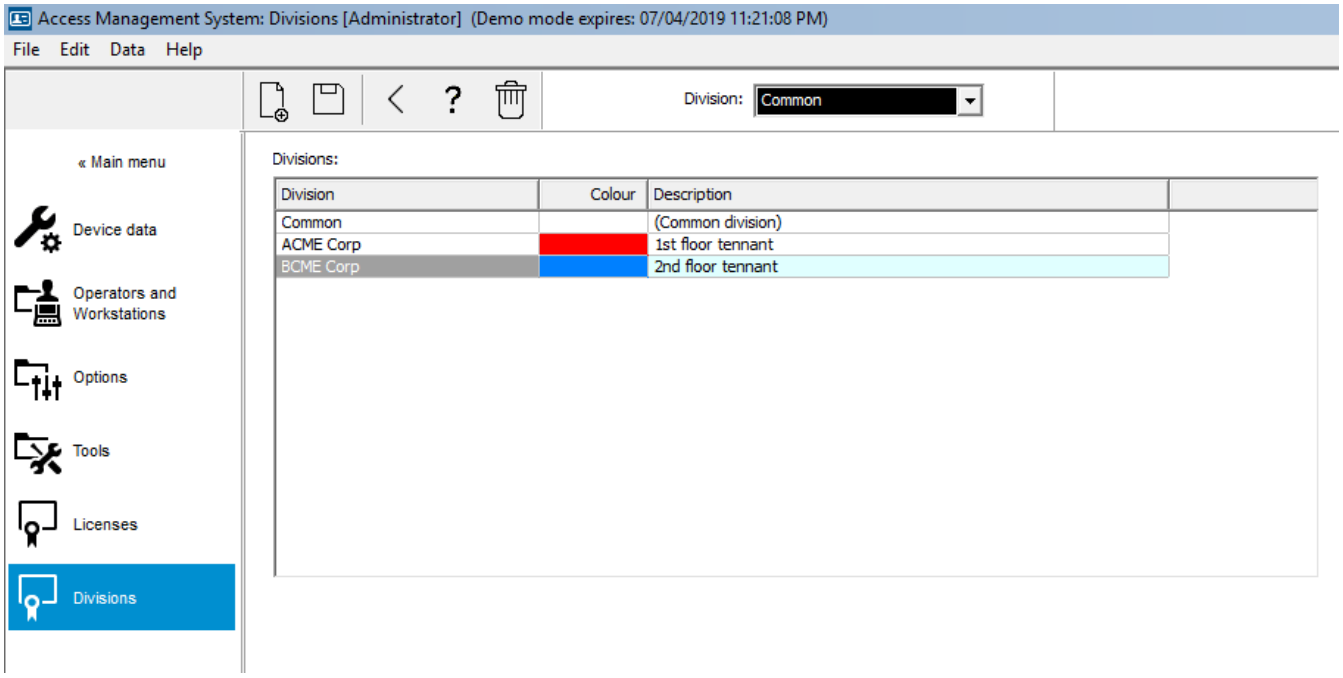
– O recurso Divisões deve estar licenciado para a instalação.

Caminho da caixa de diálogo

– Main menu (Menu principal) > **Configuration (Configuração)** > **Divisions (Divisões)**

Procedimento

1. Clique em  na barra de ferramentas.
   – Uma divisão é criada com um nome padrão.
2. Substitua o nome padrão e (opcional) insira uma descrição para o benefício de outros operadores.
3. Clique na coluna **Color (Cor)** para atribuir uma cor para ajudar a diferenciar os ativos da divisão na interface do usuário.
4. 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 Uso do editor de dispositivos

Introdução

O Editor de dispositivos, **DevEdit**, destina-se à adição e exclusão de pequenos números de entradas e dispositivos, ou para adição, modificação ou exclusão de parâmetros individuais. Para importação de configurações grandes existentes, use a função **Configuration Import/ Export (Importação/exportação de configuração)** em **Main menu (Menu principal)** > **Configuration (Configuração)** > **Tools (Ferramentas)**

O Editor de dispositivos oferece visualizações correspondentes às seguintes hierarquias editáveis:

- **Device configuration (Configuração do dispositivo)**: os dispositivos eletrônicos dentro do sistema de controle de acesso.
- **Workstations (Estações de trabalho)**: os computadores que cooperam com o sistema de controle de acesso.
- **Areas (Áreas)**: as áreas físicas nas quais o sistema de controle de acesso está 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)**

Uso da barra de ferramentas do DevEdit

Os botões da barra de ferramentas do DevEdit têm as seguintes funções, independentemente de qual visualização está ativa, por exemplo, **Devices (Dispositivos)**, **Workstations (Estações de trabalho)** ou **Areas (Áreas)**.

Botão	Atalho	Descrição
	Ctrl + N	Cria um novo item abaixo do nó selecionado. Como alternativa, clique com o botão direito no nó para invocar seu menu de contexto.
	Del	Exclui o item selecionado e tudo que estiver abaixo.
	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 ao carregá-los novamente do banco de dados. **Todas as alterações não salvas são descartadas.**

	Ctrl-S	Salva a configuração atual
	Ctrl-F	Abre uma janela de pesquisa
		Abre a árvore **Device configuration (Configuração do dispositivo)**
		Abre a árvore **Workstations (Estações de trabalho)**
		Abre a árvore **Areas (Áreas)**

Em todas as visualizações do DevEdit, inicie 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 invocá-lo). Para adicionar subitens à árvore, primeiro selecione o item em que os subitens devem aparecer.

Ao terminar de adicionar itens à árvore, clique em **Save (Salvar)**  para salvar a configuração.

Para fechar o DevEdit, clique em **File (Arquivo)** > **Exit (Sair)**.

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.

Procedimento para exclusão de áreas.

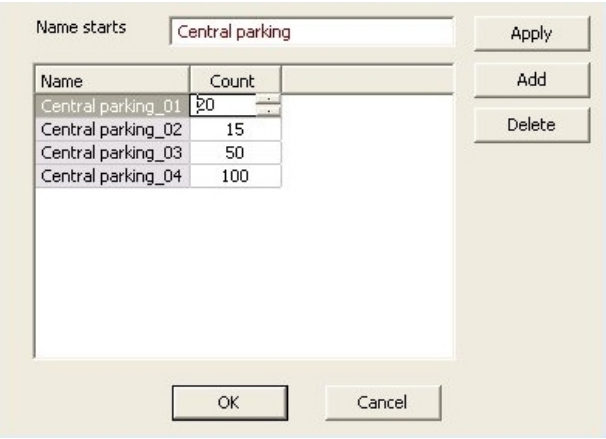
1. Clique em uma área na hierarquia para selecioná-la.
2. Clique em **Delete (Excluir)**  ou clique com o botão direito para excluir por meio do menu de contexto.

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 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)**

10.1 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
- **Automatic logout after (Logout automático depois de):** O número de segundos em que um login via leitor de cadastramento é encerrado automaticamente. Mantenha em 0 para tempo ilimitado.

10.2 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.

10.3 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.

10.4 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

10.5 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

10.6 Definição de senhas para os operadores

Como definir senhas seguras para si mesmo e para os outros.

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 a própria senha.

Pré-requisitos

Você está logado no gerenciador de caixas de diálogo.

Procedimento

1. No gerenciador de caixas de diálogo, selecione o menu: **File (Arquivo)** > **Change password (Alterar senha)**
2. Na janela pop-up, insira a senha atual, a nova senha e a nova senha novamente para confirmar.
3. Clique em **Change (Alterar)**.

Observe que este procedimento é a única forma de alterar a senha do Administrador.

Procedimento para alterar a senha 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.

Observe que coletores de datas **Valid from (Válido de)** e **Valid until (Válido até)**, abaixo do botão **Change password... (Alterar senha...)**, se referem 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/

XREF para criação de novos usuários

11 Configuração de 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)**
Inserir números na caixa de diálogo
Para evitar erros na codificação de cartões, todos os números podem ser inseridos nos formatos decimal ou hexadecimal. Selecione os botões de opções **Hexadecimal** ou **Decimal** de acordo com as instruções do fabricante de cartões. Quaisquer valores já inserido serão convertidos internamente de forma automática.
O painel da caixa de diálogo principal está dividido em dois grupos, descritos com mais detalhes abaixo:

- **Dados do código de cartão predefinidos**
- **Verificar apenas valores de associação**

Dados do código de cartão predefinidos
Use esses campos para definir valores para a **Version (Versão)**, **Country code (Código do país)** e **Facility code (Código da instalação)** que são atribuídos ao número do cartão quando o cartão for inscrito no sistema.
Se o cartão for inscrito manualmente em uma estação de trabalho do operador, uma caixa de diálogo aparece exibindo os valores padrão que podem ser personalizados para cada cartão.

Nº de código completo (padrão)	Somente o código da instalação está inserido (hex ou decimal).  **Inserindo dados de codificação:** O código da instalação é fornecido pelo fabricante como um valor decimal: 56720 Selecione o botão de opção **Decimal** e insira o código da instalação. Clique no botão Apply (Aplicar) para salvar os dados.
Nº de código dividido	Versão, Código do país e Código da instalação devem ser inseridos como valores **decimais**.  **Inserindo dados do código:** Os dados são fornecidos pelo fabricante como os seguintes valores decimais:

	Versão: 2 Código do país: 99 Código da instalação: 56720 Insira os dados nas caixas de texto apropriadas. Clique no botão Apply (Aplicar) para armazenar os dados.

Observações sobre a entrada de dados do 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.

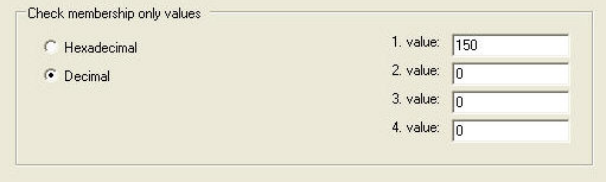
- Exemplo:
  - Entrada do número do cartão: 415
  - 10 dígitos: 0000000415
  - Convertido para hexadecimal: 0000019F

– Combinado com os dados de Código padrão (veja acima) e salvo como o número de código do crachá: 11D33E500000019F

Verificar apenas valores 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.

12 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

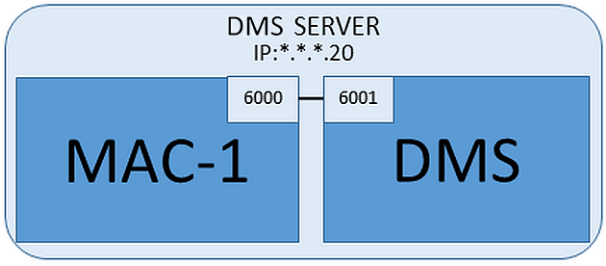
O uso básico do DevEdit está descrito na seção **Uso do editor de dispositivos** no link abaixo.

Consulte

– *Uso do editor de dispositivos, página 21*

12.1 Configuração de MACs e RMACs

12.1.1 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.

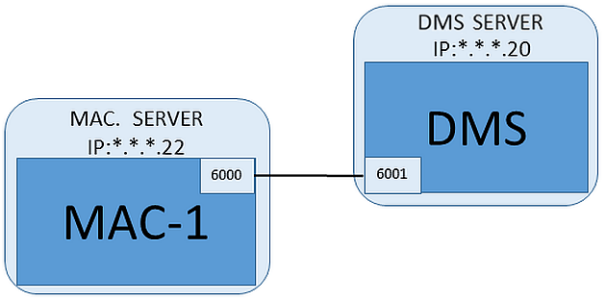
12.1.2 Preparação de computadores do servidor MAC para executar MACs e RMACs

Esta seção descreve como preparar computadores para se tornarem servidores MAC.
Por padrão, o primeiro MAC em um sistema Access Engine é executado no mesmo computador que o seu Sistema de gerenciamento de dados (DMS). No entanto, para alcançar mais resiliência, recomenda-se que o MAC seja executado em um computador separado, que pode assumir tarefas de controle de acesso caso o computador do DMS desligue.
Computadores separados onde residem MACs ou RMACs são conhecidos como servidores MAC, independente do fato de hospedarem um MAC ou um RMAC.
Para oferecer capacidade 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. Todos os servidores possuem a mesma versão do mesmo sistema operacional que o servidor DMS, com as últimas atualizações do Windows.
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: No Windows 7 isso é uma instalação. Nos sistemas operacionais Windows 10 e Windows Server já está habilitado como um recurso

6. Reinicialize o computador

12.1.3 Configuração de um MAC em seu próprio servidor MAC



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

1. No servidor DMS, desative o MAC desmarcando as caixas de seleção **Activate (Ativar)** e **Load devices (Carregar dispositivos)** para esse MAC no editor de dispositivos.
2. No servidor MAC, encerre o processo do MAC usando o programa do Windows `services.msc`.
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).
   –
4. Percorra as telas da ferramenta, fornecendo valores para os parâmetros a seguir.

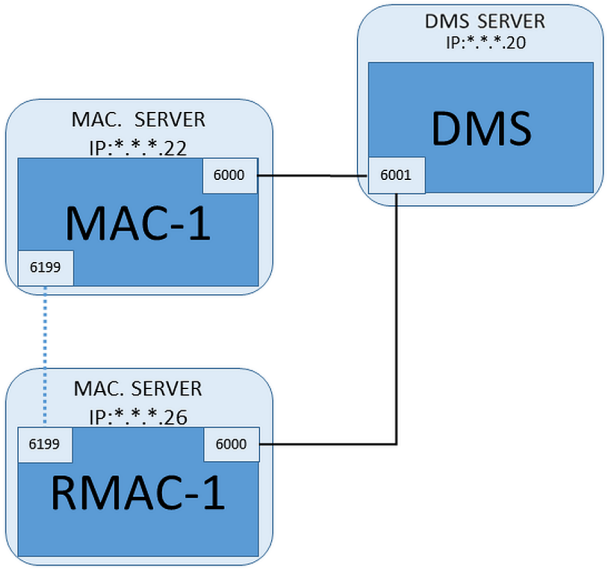
Nº da tela	Parâmetro	Descrição
1	**Destination Folder (Pasta de destino)**	O diretório local onde o MAC deve ser instalado. Escolha o padrão sempre que possível.
2	**Server (Servidor)**	O nome ou o endereço IP do servidor onde o DMS está em execução.
2	**Port (Porta) (porta para o DMS)**	A porta no servidor 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.
2	**Number (Número) (número do sistema MAC)**	Defina 1 para esse e todos os MACs (ao contrário dos RMACs)**.**
2	**Twin (Gêmeo) (nome ou endereço IP do MAC parceiro)**	Deixe esse campo em branco desde que esse MAC não venha a ter RMACs.
2	**Configure Only (Somente configuração)** (botão de opção)	Não selecione, pois você não está configurando um MAC no principal servidor de login DMS.
2	**Update Software (Atualizar software)** (botão de opção)	Selecione essa opção pois você está configurando um MAC no próprio computador (servidor MAC), não no servidor de login DMS principal.

5. Após finalizar a ferramenta, reinicie o servidor MAC ou, como alternativa, inicie o processo MAC no servidor MAC usando o programa do Windows `services.msc`.
6. No servidor DMS, selecione o MAC no Editor de dispositivos.
7. 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 ACE
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 seus AMCs subordinados.
Division (Divisão)	(Se aplicável) A divisão do ACE à qual o MAC pertence.

12.1.4 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 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 MAC

Para configurar novamente o MAC a fim de parear com o RMAC, faça o seguinte.

– No computador do servidor MAC preparado anteriormente, 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`
  – **Number (Número)**: `1` (todos os MACs têm número 1)
  – **Twin (Gêmeo)**: o endereço IP do computador onde o RMAC será executado.
  – **Update software (Software de atualização)**: selecione essa opção pois você está configurando um servidor MAC, e não o servidor DMS.

No servidor MAC para o RMAC

Para configurar o RMAC, faça o seguinte:

– No computador do servidor MAC preparado e próprio, 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.

– **Update software (Software de atualização)**: selecione essa opção pois você está configurando um servidor MAC, e não o servidor DMS.

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:

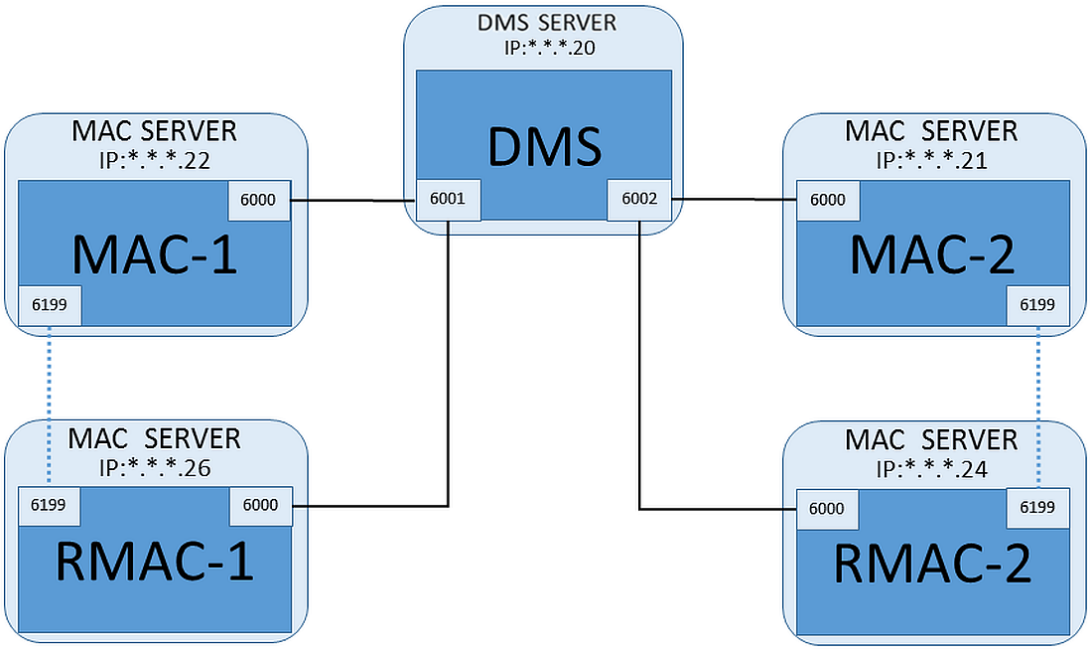
Parâmetro	Descrição
With RMAC (Com RMAC) (caixa de seleção)	**Selecionado** Uma nova guia rotulada **RMAC** aparece ao lado da guia **MAC**.
RMAC Port (Porta RMAC)	`6199` (o padrão estático) Todos os MACs e RMACs usam essa porta para verificar se os seus parceiros estão em execução e acessíveis**.**
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 deve ser chamado de RMAC-01
Descrição	Documentação opcional para operadores do ACE
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 parceiros estão em execução e acessíveis**.**

12.1.5 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.

12.1.6 Uso da ferramenta MACInstaller

`MACInstaller.exe` é a ferramenta padrão para configurar e reconfigurar 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 do BIS, no seguinte caminho:

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

Por meio de uma série de telas, ela coleta valores dos parâmetros abaixo.

Nº da tela	Parâmetro	Descrição
1	**Destination Folder (Pasta de destino)**	O diretório local onde o MAC deve ser instalado.
2	**Server (Servidor)**	O nome ou o endereço IP do servidor onde o DMS está em execução.
2	**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.**
2	**Number (Número) (número do sistema MAC)**	Defina 1 para todos os MACs originais. Defina 2 para todos os MACs de failover redundantes (RMACs).
2	**Twin (Gêmeo) (nome ou endereço IP do MAC parceiro)**	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.
2	**Configure Only (Somente configuração)** (botão de opção)	Selecione essa opção se estiver reconfigurando um MAC no servidor de login DMS principal. **Veja os detalhes abaixo**
2	**Update Software (Atualizar software)** (botão de opção)	Selecione essa opção se estiver instalando ou reconfigurando um MAC no próprio computador (servidor MAC), não no servidor de login DMS principal. **Veja os detalhes abaixo**

Os números de portas têm o seguinte esquema de numeração:

– Em um sistema sem hierarquia, onde existe apenas um servidor DMS, cada MAC e seu RMAC correspondente transmite a partir do mesmo número de porta, normalmente 6000. O DMS pode se comunicar com apenas um dos pares 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.

Aviso!
Porta de recebimento do DMS em sistemas hierárquicos
Observe que o esquema de numeração para portas de recebimento do DMS é diferente em sistemas hierárquicos. Para obter detalhes consulte

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

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)**.

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)**.

12.2 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

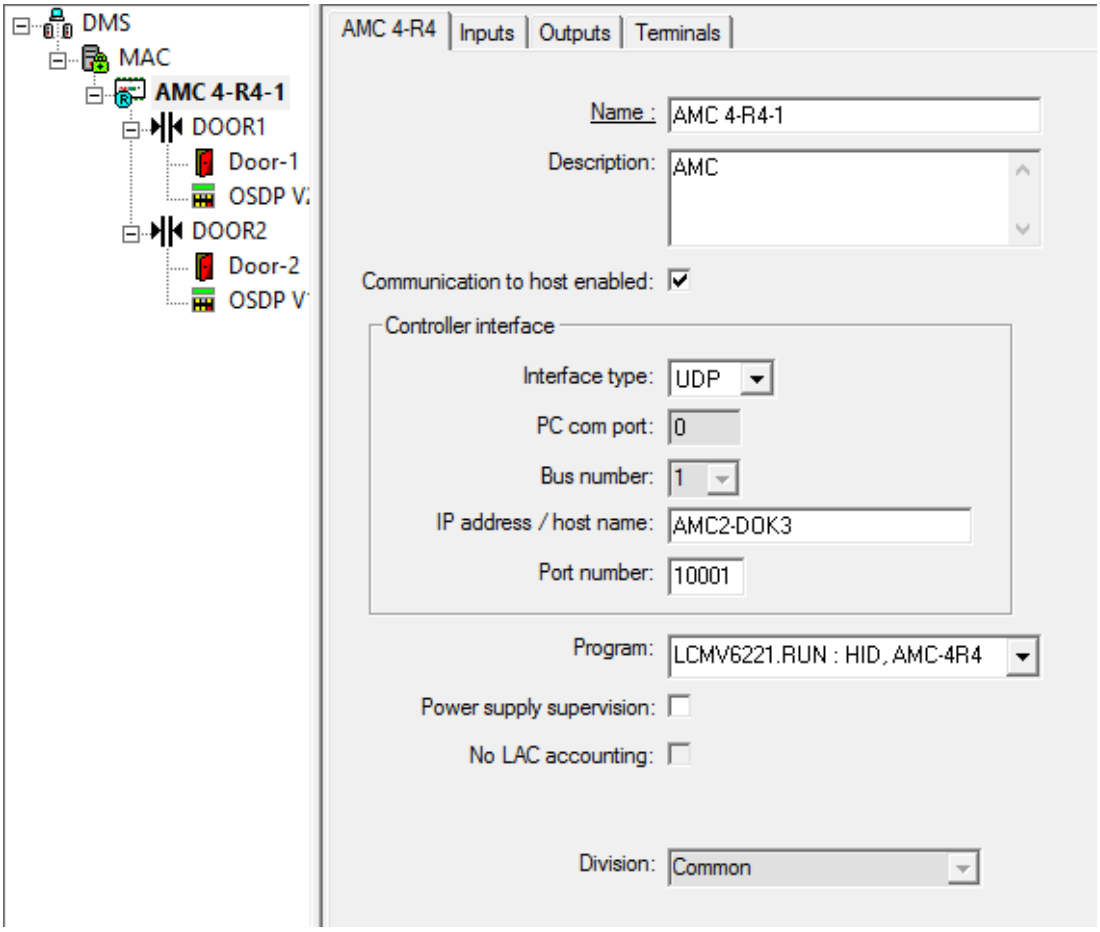
Os sistemas de controle de acesso normalmente são equipados com apenas um tipo de controlador e leitor.

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.

12.2.1 Parâmetros e configurações do AMC

Parâmetros gerais do AMC



Configuração de parâmetros do AMC

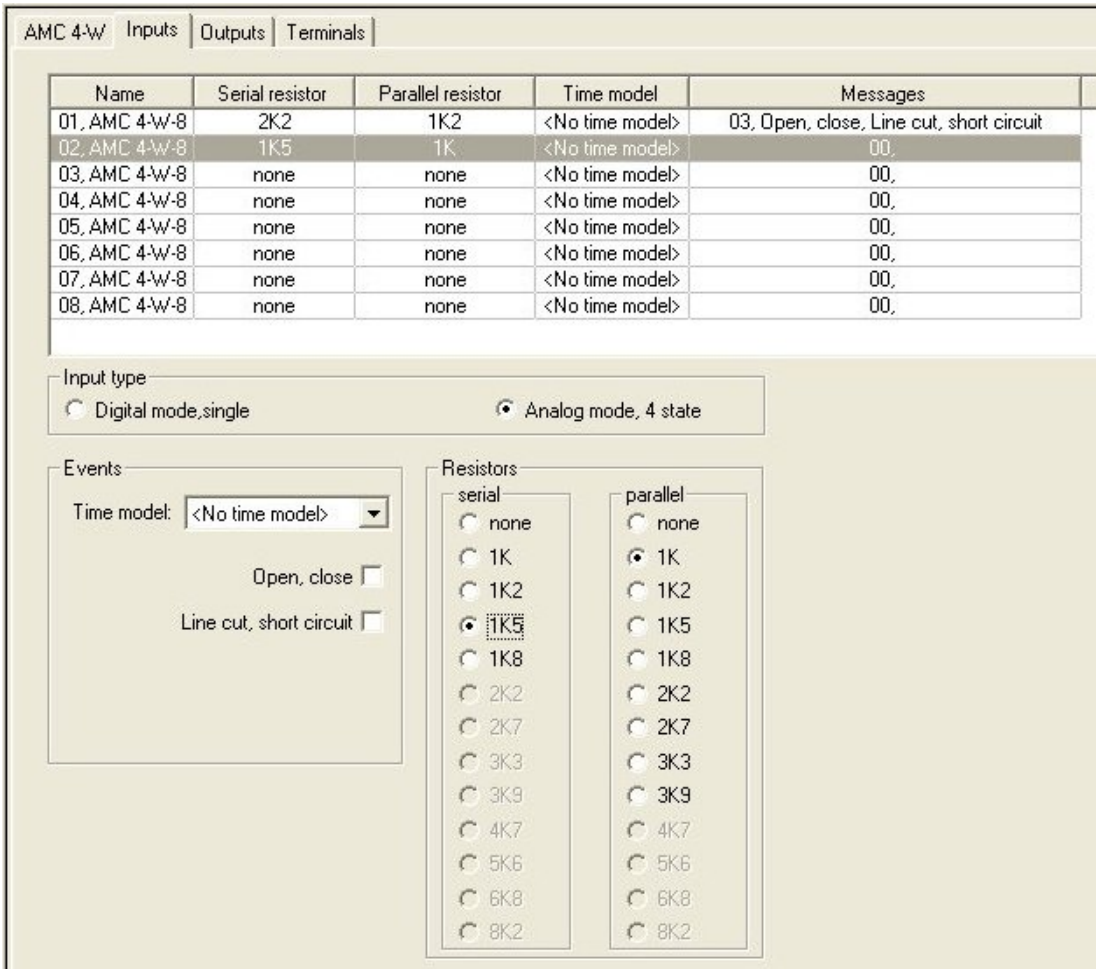
Parâmetro	Valores possíveis	Descrição
Controller name (Nome do controlador)	Alfanumérico restrito: 1 a 16 dígitos	A geração de ID (padrão) garante nomes únicos, mas eles podem ser substituídos individualmente. Em caso de substituição, é responsabilidade do usuário garantir que os IDs sejam únicos. Portanto, recomendamos que conexões da rede a servidores DHCP utilizem o nome da rede.
Controller description (Descrição do controlador)	alfanumérico: 0 a 255 dígitos	Esse texto é exibido na derivação OPC.
Communication to host enabled (Comunicação com host habilitada)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	Valor padrão = ativo A caixa de seleção exibe a configuração atual e também pode ser usada para alterá-la. O status da conexão de host é indicado pelos seguintes ícones no Explorer: Controller variant: (Variante do controlador:) ativo não ativo

		AMC2 4W   AMC2 4R4   A desativação oferece um meio de criação e parametrização de dispositivos a serem incluídos no sistema de controle de acesso posteriormente. Os dispositivos não devem ser ativados e, portanto, adicionados ao banco de dados do host, até que sejam colocados em operação. Isso também reduz o polling inútil dos dispositivos pelo host.  Por motivos de segurança, após uma atualização de software, todos os controladores são definidos como offline (caixa de seleção desmarcada). Isso garante que a instalação possa continuar em execução com o software antigo e possa, passo a passo, acelerar com o novo software. Inclui novos controladores na instalação gradualmente ao marcar suas respectivas caixas.
Controller Interface (Interface do controlador)		
Interface Type (Tipo de interface)	COM UDP	COM onde a conexão ao AMC ocorre por meio de umas das portas COM do MAC. UDP (User datagram protocol) onde a conexão ocorrer pela rede. No local em que esse tipo de conexão é selecionado, os parâmetros "nome do host" e "porta controlada remotamente" se tornam configuráveis.  Com o tipo de interface "UDP", o interruptor DIP "5" **deve** ser definido no AMC.

		Além disso, recomenda-se definir o interruptor "1" para LIGADO.
Porta COM do computador	numérico: com portas COM: 1 a 256 com portas UDP: 1 a 65535	Número das portas COM em que esse AMC está conectado ao MAC. Para conexões ethernet por meio dos conversores, as portas COM virtuais são geradas e mostradas aqui. Com o tipo "UDP", insira a porta através da qual o MAC receberá informações do AMC. Se essa porta for desconhecida, o campo pode ser deixado vazio e uma porta livre será selecionada automaticamente.
Bus number (Número do barramento)	numérico: 1 a 8	Usando o adaptador de interface AMC-MUX, até oito controladores podem ser configurados em uma porta COM. Nesses casos, insira o endereço exclusivo de cada AMC, conforme fornecido pelo interruptor DIP. **Observação:** O interruptor 5 pode ser ignorado pois somente os quatro primeiros interruptores são usados para endereçamento. Para conexões UDP, use a configuração padrão (= 0)
IP Address/ Hostname (Endereço IP/nome do host)	Nome da rede ou endereço IP do AMC	Essa caixa de entrada só será configurável se **UDP** for o tipo de porta selecionado. Se endereços IP forem alocados pelo DHCP, o nome da rede do AMC deve ser fornecido para que o AMC possa ser localizado após uma reinicialização, mesmo que o endereço IP tenha sido alterado. Para redes sem DHCP, o endereço IP deve ser fornecido.
UDP Port (Porta UDP)	numérico: 1 a 10001, com configuração padrão	Essa caixa de entrada só estará ativada se **UDP** for o tipo de porta selecionado. Essa é a porta do AMC que receberá as mensagens do MAC.
Parâmetros adicionais		
Program (Programa)	alfanumérico	Nome de arquivo do programa a ser carregado no AMC. Os programas disponíveis estão localizados no diretório BIN do MAC e podem ser selecionados a partir de uma lista. Por conveniência, o protocolo e a descrição também são mostrados.

		Esse parâmetro é definido automaticamente à medida que os programas são carregados, também automaticamente, dependendo de quais leitores estão conectados, e o parâmetro é substituído em caso de incompatibilidade entre o leitor e o programa.
Power supply supervision (Supervisão da fonte de alimentação)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	Supervisão da tensão de alimentação. Se a fonte de alimentação cair, uma mensagem informativa é gerada. A função de supervisão assume o pré-requisito de uma UPS (Fonte de alimentação ininterrupta) para que a mensagem possa ser gerada. 0 = sem supervisão 1 = supervisão ativada
No LAC accounting (Sem contabilidade LAC)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	Marque essa caixa de seleção para dispositivos do AMC que funcionam em conjunto para fornecer acesso aos estacionamentos, onde apenas o MAC pai mantém a contabilidade do número de unidades que entram e saem. **Observe** que, se esta opção for selecionada e o AMC estiver offline, o AMC não poderá impedir o acesso às áreas superlotadas, pois não terá acesso à contagem da população total.
Division (Divisão)	Valor padrão = "Comum"	Esse é um campo informacional somente leitura. "Divisões" são meios de dividir uma instalação de controle de acesso entre várias partes autônomas, criadas e mantidas no BIS Manager.

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.

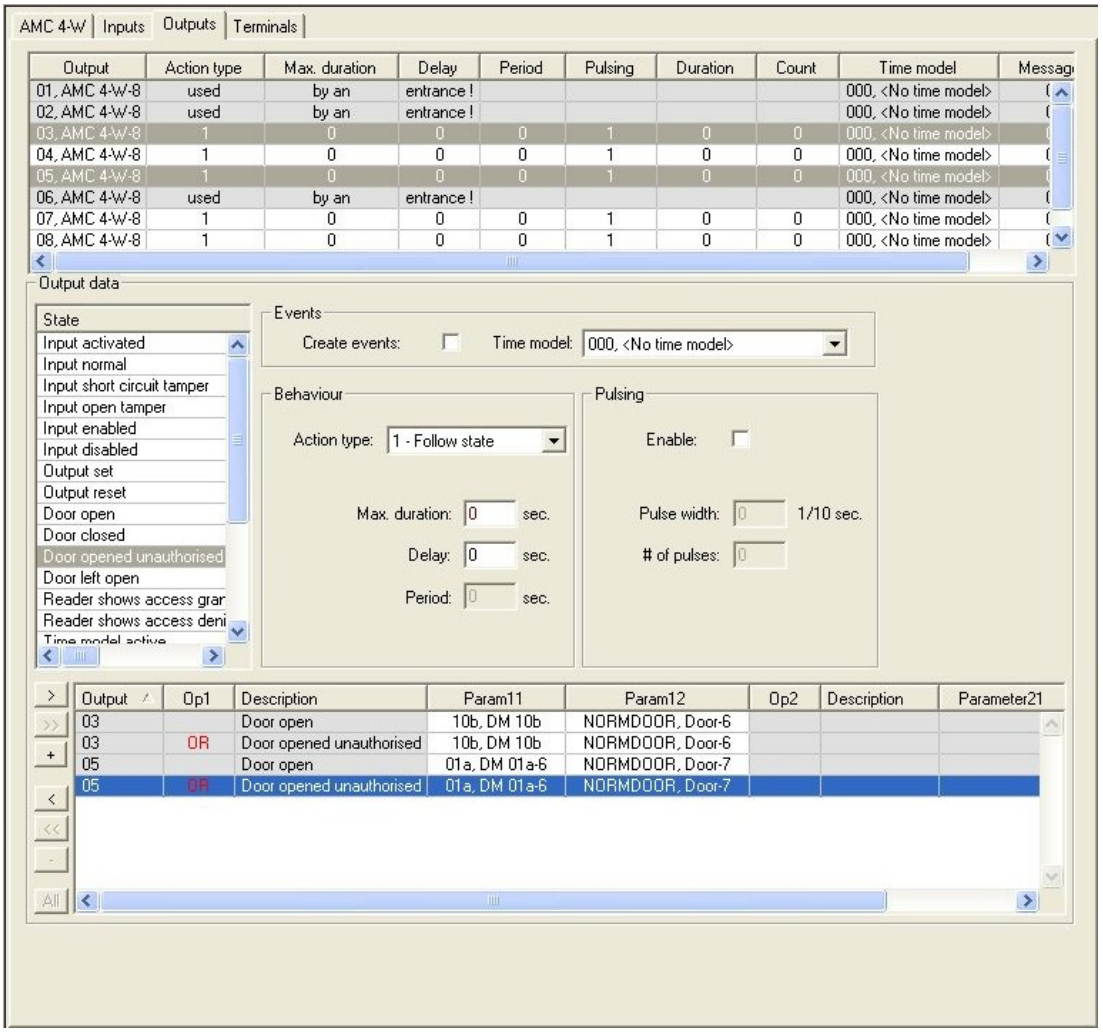
Série	**Intervalo**		**Paralelo**	**Intervalo**
"nenhum" ou "---"	1K até 8K2		"nenhum" ou "---"	1K até 8K2
1K	1K até 2K2		1K	1K até 1K8

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

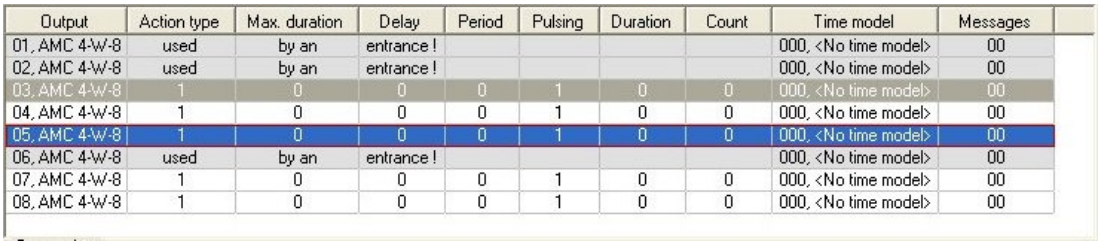
Essa página de caixa de diálogo fornece a configuração de cada saída em um AMC ou AMC-EXT, e contém três áreas principais:

– 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.

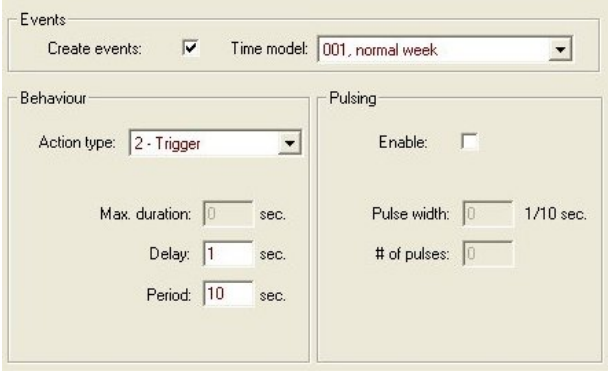
Parâmetros das saídas do AMC

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

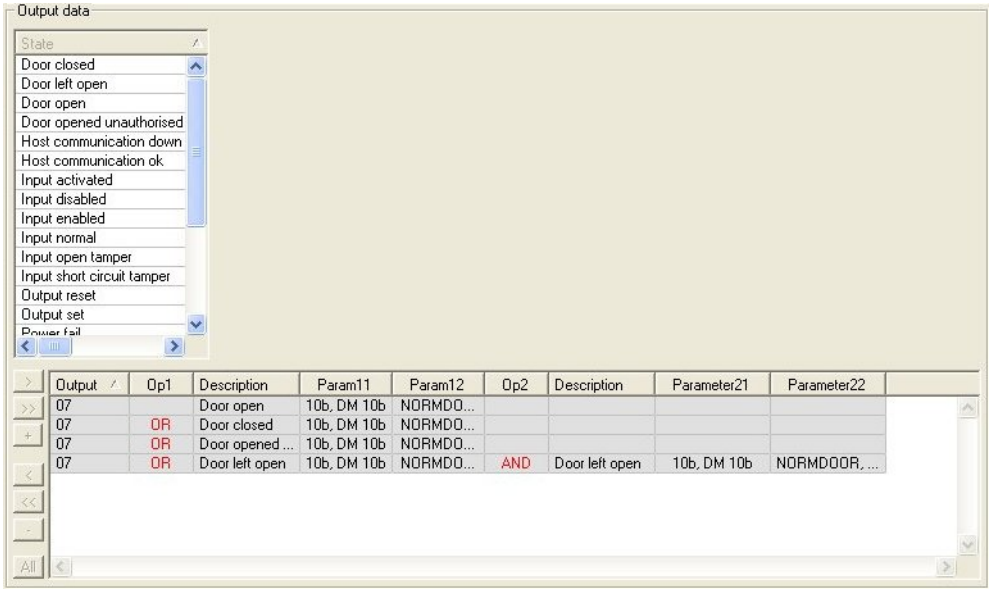
Todas as entradas da lista acima são geradas usando as caixas de seleção e campos de entrada nas áreas de caixa de diálogo **Events (Eventos)**, **Action (Ação)** e **Pulsing (Pulsação)**. Selecionar uma entrada da lista indica as configurações respectivas nessas áreas. Isso também vale para a seleção 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 acioná-las.



Configuração de estados para acionar saídas
Você pode configurar as saídas selecionadas acima para serem acionadas por estados individuais ou combinações lógicas de estados.
– Selecione uma ou várias saídas na caixa de listagem superior.
– Selecione um estado na lista **State (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 status) para criar, para cada saída selecionada, uma entrada do seu status 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 atalho 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 status já deve estar atribuído, ao qual outra condição é adicionada selecionando-a em uma coluna arbitrária.
– Em seguida, outro status 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 atalhos OR podem ser atribuídos a qualquer saída.
Para toda condição atribuída, **um** atalho AND pode ser criado.

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

As entradas da lista podem ser alteradas.
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 selecionados, seus números de tipo e descrições.

O campo da lista **State (Estado)** também contém esses parâmetros, eles são indicados ao rolar a lista para a direita.

Estado	Tipo	Descrição
Entrada ativada	1	Entrada local
Entrada normal	2	Entrada local
Violação de curto-circuito de entrada	3	Entrada local com resistor configurada
Violação de abertura de entrada	4	Entrada local com resistor configurada
Entrada habilitada	5	Entrada local ativada por modelo de tempo
Entrada desabilitada	6	Entrada local desativada por modelo de tempo
Definição de saída	7	Saída local, não saída atual
Redefinição da saída	8	Entrada local, não entrada atual
Porta aberta	9	GID da entrada, número da porta
Porta fechada	10	GID da entrada, número da porta
Abertura de porta não autorizada	11	GID da entrada, número da porta, substitui "Porta aberta" (9)
Porta deixada aberta	12	GID da entrada, número da porta
Leitor mostra acesso concedido	13	Endereço do leitor
Leitor mostra acesso negado	14	Endereço do leitor
Modelo de tempo ativo	15	Modelo de tempo configurado
Leitor de violação	16	Endereço do leitor
Violação da AMC	17	---
Placa E/S de violação	18	---
Falha de alimentação	19	somente para AMC alimentado por bateria
Alimentação ok	20	somente para AMC alimentado por bateria
Comunicação com o host ok	21	---

Sem comunicação com o host	22	---
Mensagens do leitor	23	(Os detalhes dependem da versão atual do software)
Mensagens de LAC	24	(Os detalhes dependem da versão atual do software)

Configuração de saídas

Além da atribuição do sinal com modelos de porta ou com atribuição individual, as condições podem ser definidas para saídas que ainda não estão alocadas. Se essas condições ocorrerem, a saída será ativada em correspondência com o parâmetro definido.

É necessário decidir o que será transferido para a saída. Em contraste com os sinais que podem ser associados a um modelo de porta específico, suas 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 e acústico ou uma mensagem ao UGM deve ser acionado pelos sinais de entrada **Violação de curto-circuito de entrada** e **Abertura de porta não autorizada**, essa entrada ou entradas que podem ser consideradas são atribuídas à saída de destino correspondente.

Exemplo em que apenas 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 os contatos selecionados:

Uma única entrada é criada para todos os contatos clicando em » ou removendo os contatos não necessários 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 diversas saídas se, por exemplo, além de um sinal óptico também for necessário um sinal acústico, uma mensagem deverá ser enviada ao UGM 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

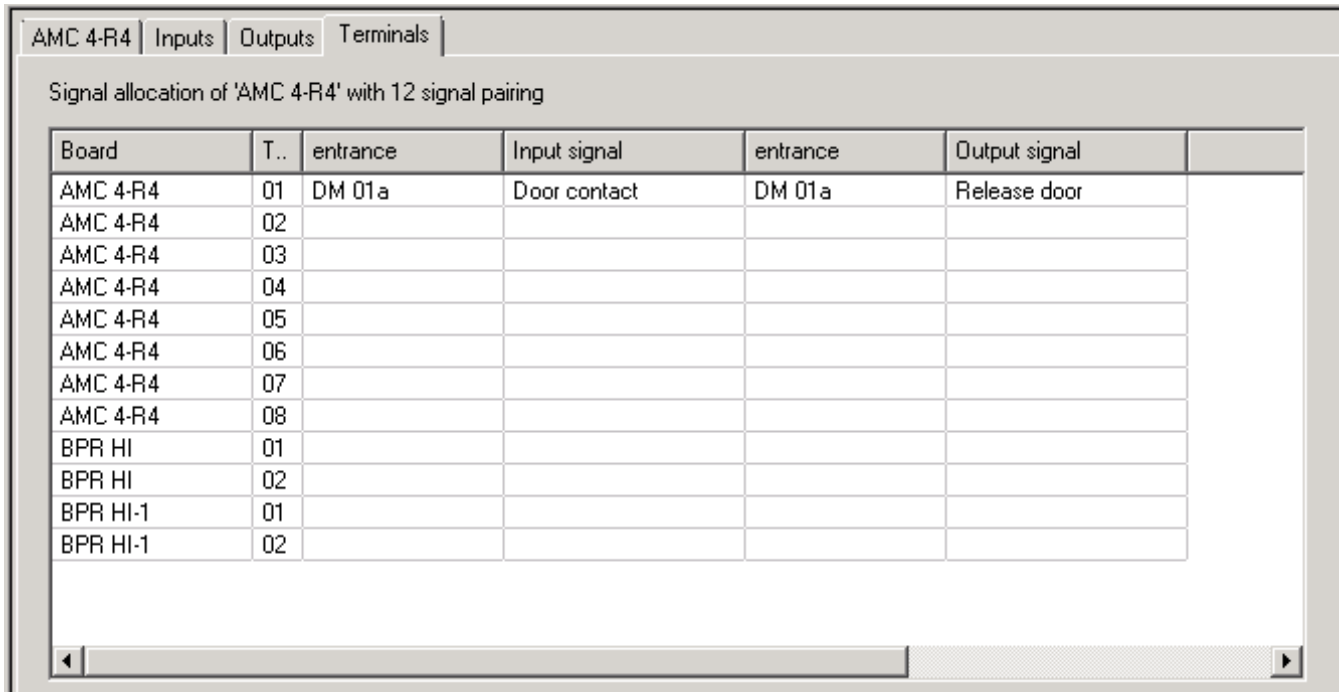
Lista de todos os estados existentes com os valores padrão para o Parameter11/21 e 12/22:

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				

13 Configuração de entradas

13.1 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.

13.2 Criação de entradas

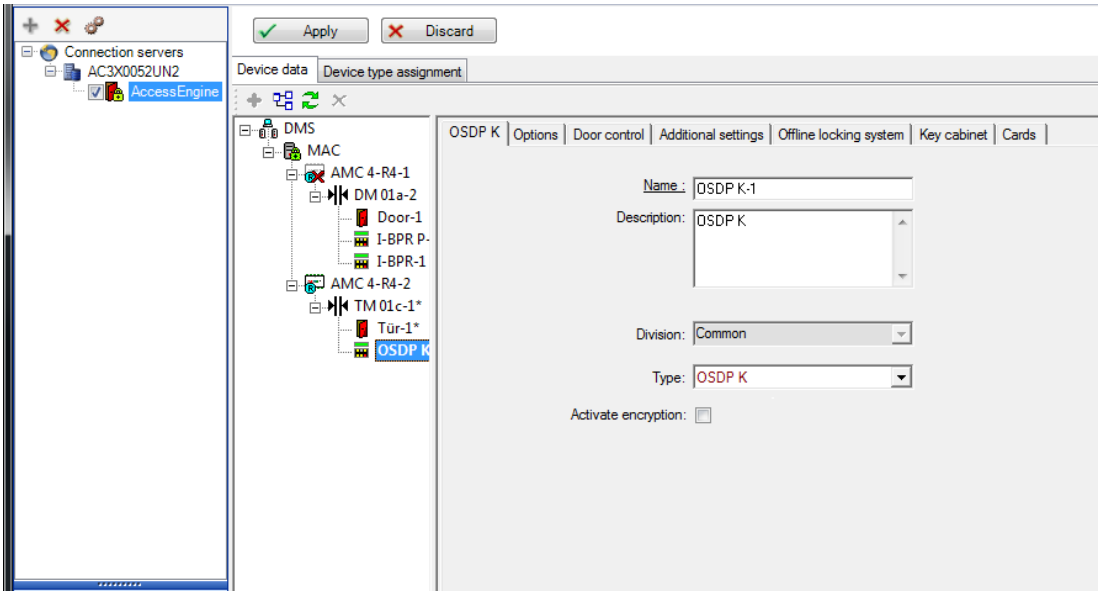
A lista de leitores apresentada para seleção se adequará ao tipo de controlador escolhido.

– 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	Wiegand-Protocol	Protocolo BPR	I-BPR-Protocol	HID-Protocol
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		
TB30 LE		X		
TB15 HI1		X		
INTUS 1600			X	
I-BPR			X	
I-BPR K (teclado)			X	
DT 7020			X	
OSDP				X
OSDP K (teclado)				X
OSDP KD (teclado + visor)				X
HADP				X
HADP K (teclado)				X
HADP KD (teclado + visor)				X
RKL 55 (teclado + LCD)				X

RK40 (teclado)				X
R40				X
R30				X
R15				X

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



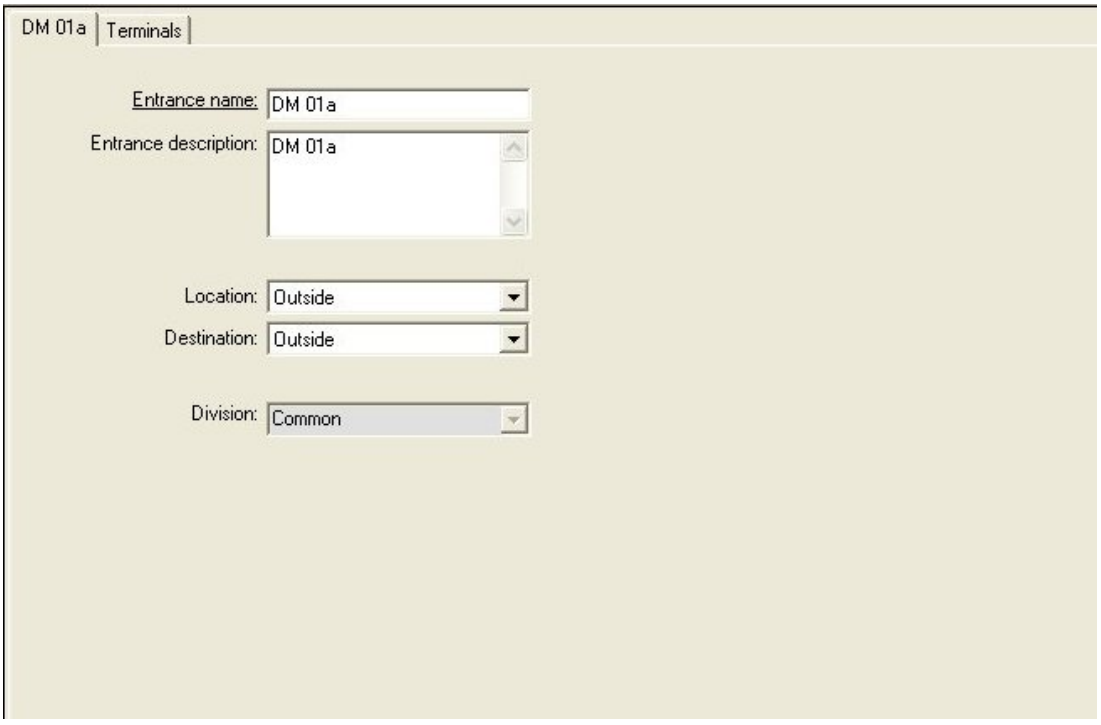
Os seguintes tipos de leitores OSDP estão disponíveis:

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.



Parâmetro	Valores possíveis	Descrição
Entrance name (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 desejado.
Entrance description (Descrição da entrada)	alfanumérico: 0 a 255 caracteres	Um texto descritivo arbitrário para exibição no sistema.
Location (Local)	Qualquer área definida (sem estacionamentos)	A área nomeada (conforme definido no sistema) onde o leitor está localizado. Essa informação é usada para o controle da sequência de acesso: se uma pessoa tentar usar esse leitor mas a localização atual dessa

		pessoa (conforme rastreada pelo sistema) for diferente daquela do leitor, ele negará o acesso à essa pessoa.
Destination (Destino)	Qualquer área definida (sem estacionamentos)	A área nomeada, conforme definido no sistema, á qual o leitor permite acesso. Essa informação é usada para o controle da sequência de acesso: se uma pessoa usar esse leitor, sua localização será atualizada para o valor do **Desintation (Destino)**.
Waiting time external access decision (Tempo de espera para decisão de acesso externa)	Quantidade de décimos de um segundo	O tempo que o controlador de acesso aguarda uma decisão do sistema de controle de acesso antes de tomar sua própria decisão.
Division (Divisão)	Um campo somente leitura	A divisão definida à qual o leitor pertence. A divisão padrão é **Common (Comum)**.
Latency alarm device (Dispositivo de alarme de latência) (somente para os modelos de entrada 10 e 14)	100 - 9999	O intervalo de tempo em que o mecanismo de abertura da porta pode permanecer ativado sem que um alarme seja ativado. Isso é um parâmetro do leitor que é definido e, em seguida, enviado aos leitores. A unidade desse parâmetro é um décimo (1/10) de segundo.
Arming Area (Área de arme) (somente para o modelo de entrada 14)	Uma letra: A até Z	As entradas de um grupo IDS serão ativadas juntas pela ativação dos leitores da área.

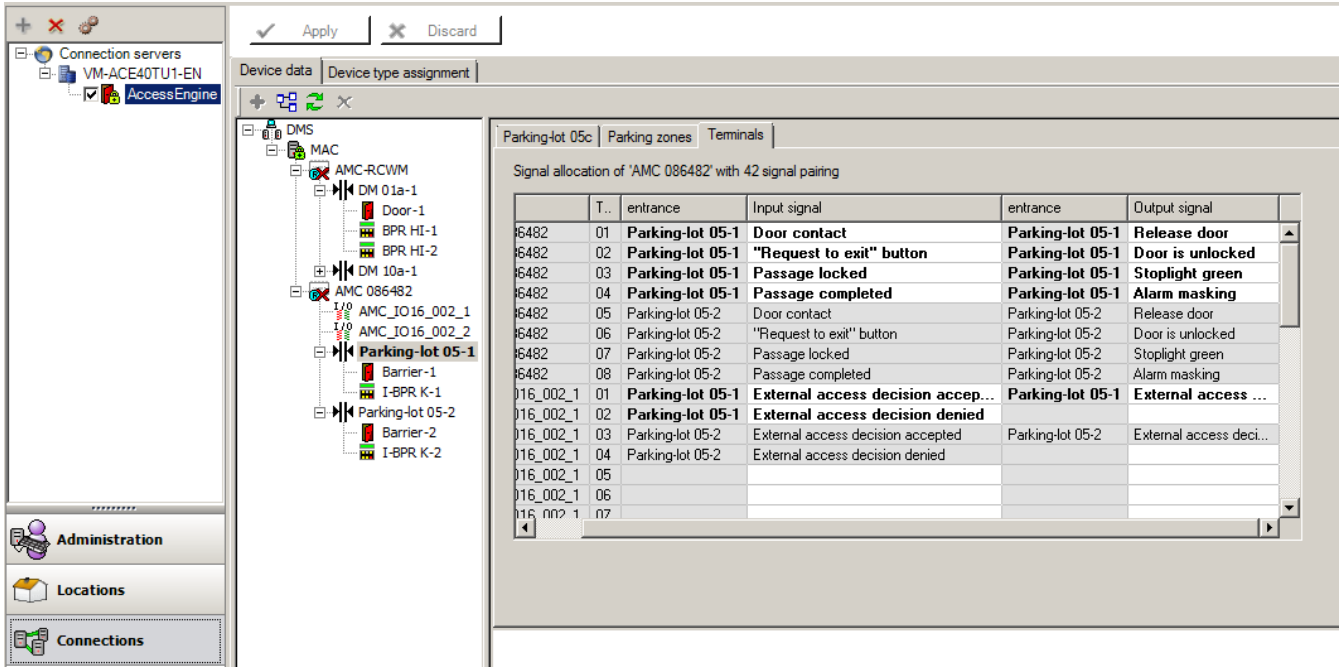
13.3 Verificações de E/S adicionais

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".

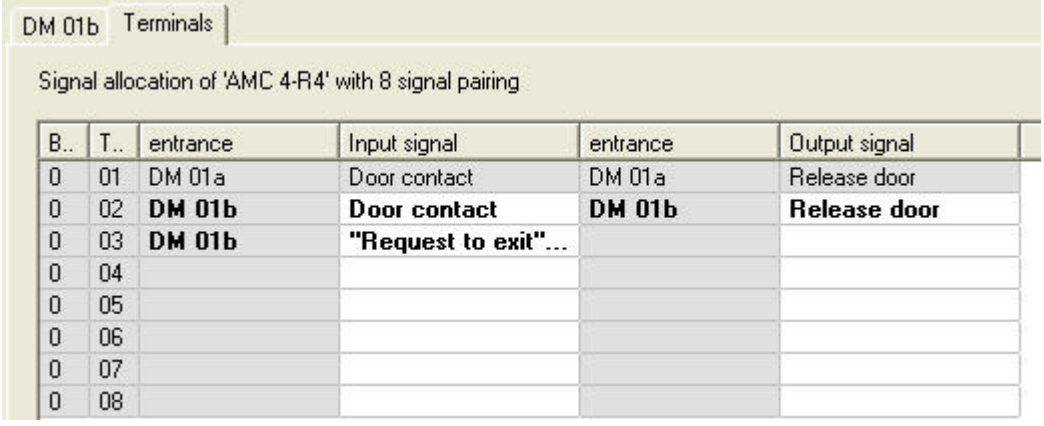


Status do cartão	Sinal = 1: autorizado por ANPR	Sinal = 0: não autorizado por ANPR
Cartão autorizado	Acesso	Evento de número de veículo inválido
Cartão na lista negra	Não autorizado – lista negra	Não autorizado – lista negra
Cartão expirou	Não autorizado – expirou	Não autorizado – expirou
Cartão não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

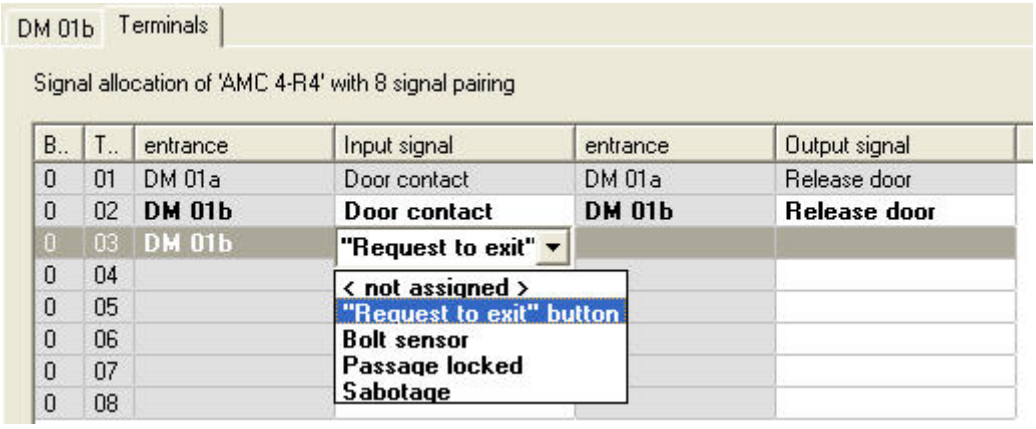
É possível abrir a barreira manualmente mesmo que o visitante não seja reconhecido.
Para essa funcionalidade, um interruptor é conectado aos contatos de E/S do AMC.
O AMC define um sinal de saída **Verificação adicional ativa** antes da análise do sinal de entrada.
Se um novo visitante for registrado, as informações da placa devem ser inseridas pelo operador no BIS (para relatórios) e no sistema ANPR (para varredura).
O ANPR reconhecerá um veículo registrado a partir do banco de dados.

13.4 Configuração de terminais do AMC

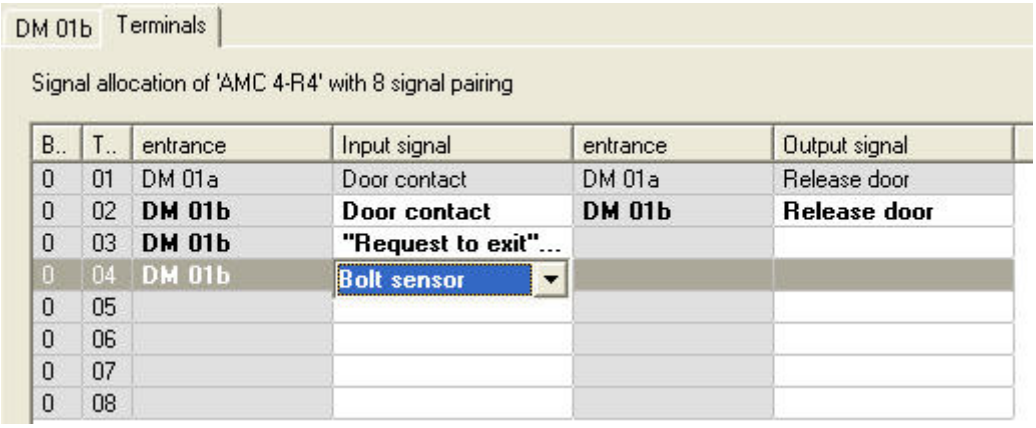
Quanto ao conteúdo e à estrutura, esta guia é idêntica à guia **Terminals (Terminais)** do AMC.



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:

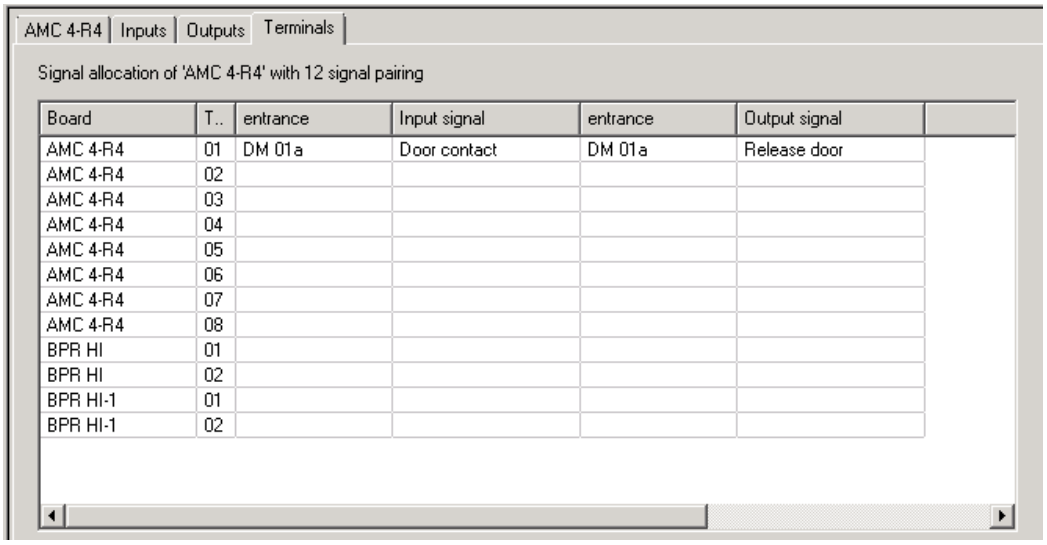


Atribuições de sinais inadequadas para a entrada em edição são somente leitura, com um fundo em cinza. Elas só podem ser editadas enquanto a entrada correspondente estiver selecionada.
Um fundo cinza semelhante e uma cor pálida de primeiro plano são aplicados a essas saídas que foram parametrizadas na 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
Sensor da porta	

Botão de solicitação de saída	Botão para abrir a porta.
Sensor da trava da fechadura	É usado somente para mensagens. Não há função de controle.
Entrada bloqueada	É usado para bloquear temporariamente a porta oposta em eclusas. Mas também pode ser usado para bloqueio permanente.
Sabotagem	Sinal de sabotagem de um controlador externo.
Catraca na posição normal	Catraca fechada.
Passagem concluída	Uma passagem foi concluída com sucesso. Este é o pulso de um controlador externo.
IDS: pronto para armar	Será configurado pelo IDS, se todos os detectores estiverem em repouso e se for possível armar o IDS.
IDS: está armado	O IDS está armado.
IDS: botão de solicitação para armar	Botão para armar o IDS.
Abertura local habilitada	Será usada se a configuração da porta abrir a porta sem envolver o AMC. O AMC envia uma mensagem de não intrusão, mas de "abertura local da porta".
Decisão de acesso externo aceita	O sinal é definido, se um sistema externo aceitar o acesso
Decisão de acesso externo negada	O sinal é definido, se um sistema externo aceitar o acesso

Tabela de sinais de saída

Sinais de saída	**Descrição**
Mecanismo de abertura da 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.
Indicador verde	Lâmpada indicadora – será controlada assim que a porta abrir.
Porta aberta durante muito tempo	Pulso de três segundos. Se a porta estiver aberta há muito tempo.
Ativação da câmera	A câmera será ativada no início de uma passagem.
Abrir a catraca para entrada	

Abrir a catraca para saída	
A porta está permanentemente aberta	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	- Sensor da porta - Botão "Solicitação de saída" - Sensor da trava da fechadura - Entrada bloqueada - Sabotagem - Abertura local habilitada - Decisão de acesso externo aceita - Decisão de acesso externo negada	- Mecanismo de abertura da porta - Eclusa: bloquear direção oposta - Supressão de alarme - Indicador verde - Ativação da câmera - Porta aberta durante muito tempo - 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 - Sabotagem - Decisão de acesso externo aceita - Decisão de acesso externo negada	- Eclusa: bloquear direção oposta - Abrir a catraca para entrada - Abrir a catraca para saída - Supressão de alarme - Ativação da câmera - Porta aberta durante muito tempo - 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	- Sensor da porta - Botão "Solicitação de saída" - Entrada bloqueada - Passagem concluída - Decisão de acesso externo aceita - Decisão de acesso externo negada	- Mecanismo de abertura da porta - Supressão de alarme - Indicador verde - Porta aberta durante muito tempo - A porta está permanentemente aberta - 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	- Sensor da porta - Botão "Solicitação de saída" - Entrada bloqueada - Passagem concluída - Decisão de acesso externo aceita - Decisão de acesso externo negada	- Mecanismo de abertura da porta - Supressão de alarme - Indicador verde - Porta aberta durante muito tempo - A porta está permanentemente aberta - 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	- Sensor da porta - Botão "Solicitação de saída" - IDS: pronto para armar - IDS: está armado - Sabotagem - IDS: solicitação para armar - Decisão de acesso externo aceita - Decisão de acesso externo negada	- Mecanismo de abertura da porta - Ativação da câmera - IDS: armar - IDS: desarmar - Porta aberta durante muito tempo - Decisão de acesso externo ativada
14	Porta simples com leitor de entrada e saída e arme/ desarme do IDS Leitores de frequência	- Sensor da porta - Botão "Solicitação de saída" - IDS: pronto para armar - IDS: está armado - Sabotagem - IDS: solicitação para armar	- Mecanismo de abertura da porta - Ativação da câmera - IDS: armar - Porta aberta durante muito tempo
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

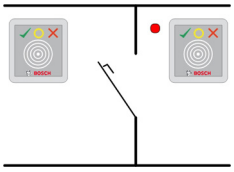
Quando uma entrada é criada, a guia **Terminals (Terminais)** da entrada correspondente mostra dois sinais de entrada e dois de saída para cada leitor abaixo do controlador. A coluna de Placa exibe o nome do leitor. Os sinais padrão da entrada são atribuídos, por padrão, aos primeiros sinais livres do 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.

13.5 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

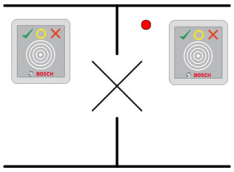
Sinais possíveis:

Sinais de entrada	**Sinais de saída**
Sensor da porta	Mecanismo de abertura da porta
Botão "Solicitação de saída"	Eclusa: bloquear direção oposta
Sabotagem	Indicador verde
Abertura local habilitada	Ativação da câmera
	Porta aberta durante muito tempo

Aviso!
A função onde apenas uma pessoa pode acessar por vez, especialmente o bloqueio do sentido oposto, pode ser parametrizada 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:

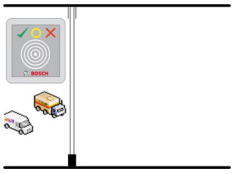
Sinal de entrada	**Sinais de saída**
Catraca na posição normal	Abrir a catraca para entrada
Botão "Solicitação de saída"	Abrir a catraca para saída
Sabotagem	Entrada bloqueada
	Ativação da câmera
	Porta aberta durante muito tempo
Sinais adicionais usando a opção de **eclusa**:	
Entrada bloqueada	Eclusa: 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**
Sensor da porta	Mecanismo de abertura da porta
Botão "Solicitação de saída"	A porta está permanentemente aberta
Entrada bloqueada	Indicador verde
Passagem concluída	Supressão de alarme
	Porta aberta durante muito tempo

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 do modelo

06a	Leitores de entrada **e** saída para frequência
06c	Leitores de entrada **ou** saída para frequência

Os leitores criados com esse modelo de porta não controlam o acesso, mas são usados exclusivamente para fins de frequência. Eles não controlam as portas, apenas transmitem os dados do cartão ao sistema de frequência.
Como consequência, nenhum sinal é definido. Esses leitores normalmente são instalados dentro de uma área já controlada.

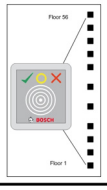
Aviso!
Para que pares de registro válidos (hora de entrada mais hora de saída) possam ser criados no sistema de frequência, é necessário parametrizar dois leitores separados com o modelo de porta 06: um para sincronia de entrada e outro para saída

Use a variante **a** quando entrada e saída não forem separadas. Use a variante **c** se a entrada e a saída forem espacialmente separadas 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.
Como qualquer entrada, é necessário criar e atribuir autorizações. Em Access Engine, a guia **Time Management (Gerenciamento de tempo)** nas caixas de diálogo **Access Authorizations (Autorizações de acesso)** e **Area/Time Authorizations (Autorizações de área/hora)** lista todos os leitores de frequência definidos. Ative pelo menos um leitor no sentido de entrada e um leitor no sentido de saída. Autorizações para leitores de frequência podem ser atribuídas junto com outras autorizações de acesso, ou como autorizações separadas.
Se existir mais de um leitor de frequência para um sentido, é possível atribuir determinados titulares de cartões a determinados leitores. Somente os horários de comparecimento de usuários atribuídos e autorizados serão registrados e armazenados 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.

Os horários de entrada e saída registrados são armazenados em um arquivo de texto no diretório: `C:\MgtS\AccessEngine\AC\TAExchange` com o nome `TAccExc_EXP.txt` e mantidos com exportação pendente para um sistema de frequência.
Os dados de registro são transmitidos no seguinte formato:
`ddMMyyyy;hhmm[s];Direction [0,1]; AbsenceReason; Personnel-Nr.`
d = dia, M = mês, y = ano, h = hora, m = minuto, s = horário de verão, 0 = saída, 1 = entrada
O arquivo de exportação não é classificado por pessoa, mas contém todos os registros em ordem cronológica, conforme recebido pelo módulo de administração. O separador de campos no arquivo é um ponto e vírgula.

Variantes do modelo de entrada 07:



Variantes do modelo:

07a	Elevador com, no máximo, 56 andares
07b	Elevador com, no máximo, 56 andares

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.

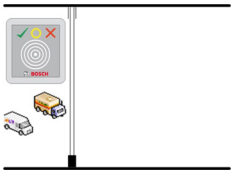
Ao chamar o elevador, o proprietário do cartão pode selecionar somente os andares para os quais seu cartão está autorizado.
Os modelos de porta de elevador não podem ser misturados com outros modelos de porta no mesmo controlador. Usando placas de extensão, até 56 andares podem ser definidos para cada 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

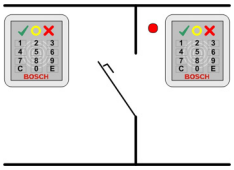


Sinais possíveis:

Sinais de entrada	**Sinais de saída**
Sensor da porta	Mecanismo de abertura da porta
Botão "Solicitação de saída"	Porta aberta por muito tempo
Entrada bloqueada	Semáforo verde
Passagem concluída	Supressão de alarme
	Porta aberta durante muito tempo

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**
Sensor da porta	Mecanismo de abertura da porta
IDS: está armado	IDS: armar
IDS: pronto para armar	IDS: desarme [somente DM 10e]
Botão "Solicitação de saída"	Ativação da câmera
Sensor da trava da fechadura	Porta aberta durante muito tempo
Sabotagem	
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.

Procedimentos diferentes são necessários dependendo de quais leitores estão instalados.
Leitores I-BPR: (por exemplo, DELTA 1010, INTUS 1600)
Arme 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 (#).

Leitor BPR: (incluindo Wiegand)
Arme pressionando 7, apresentando o cartão e inserindo o código PIN. Não é preciso 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.]

13.6 Entradas especiais

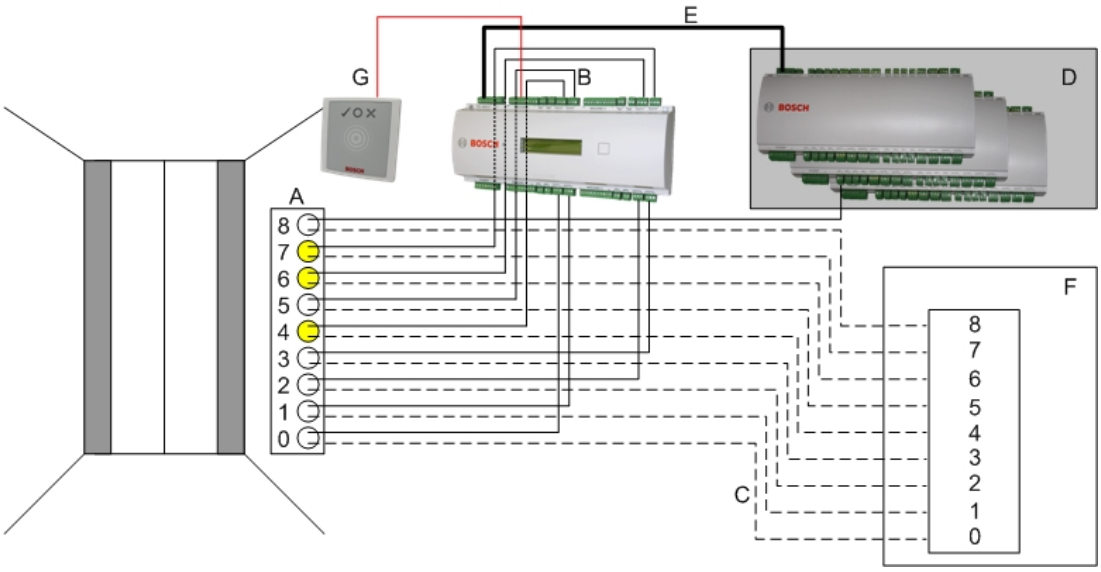
13.6.1 Elevadores (DM07)

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 do sistema Access Engine, você pode atribuir andares específicos à autorização de uma pessoa.
Se o elevador foi criado usando o modelo de entrada **07a**, um titular de cartão apresenta seu cartão de ID e os andares para os quais ele tem permissão se tornam disponíveis.
Com o modelo de entrada **07c**, o sistema verifica a autorização para o andar selecionar depois que a pessoa o seleciona. Os andares marcados como **públicos** estão disponíveis para todas as pessoas, independentemente da autorização. Junto com um modelo de tempo, a função pública pode ser restringida ao modelo de tempo especificado. Fora desse período, a autorização para o andar selecionado será verificada.

Esquema de fiação para elevadores:

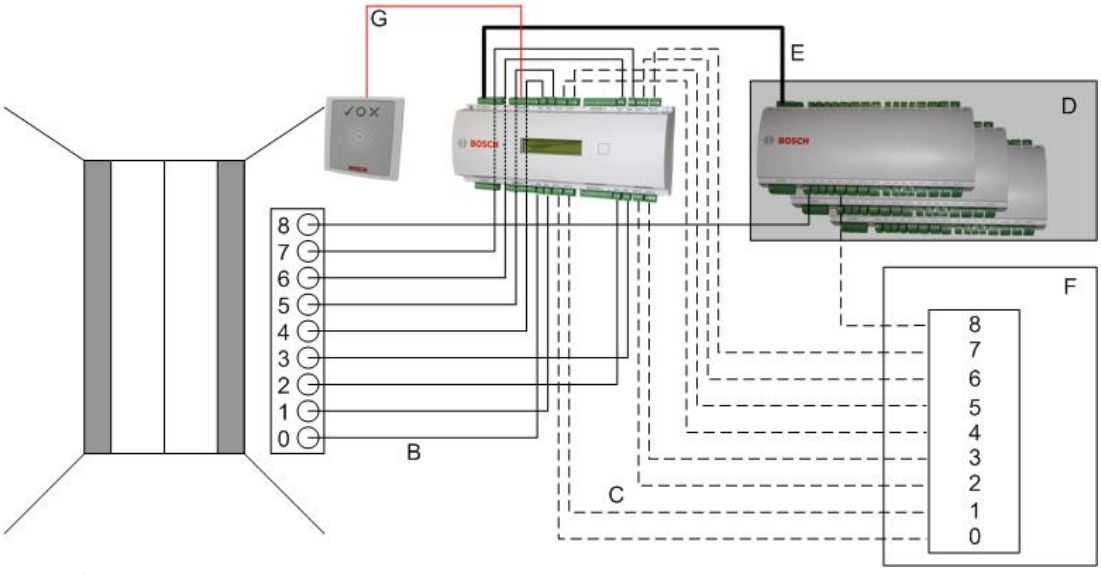
A figura a seguir mostra o esquema de conexão de um elevador usando o modelo de porta 07a.



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.



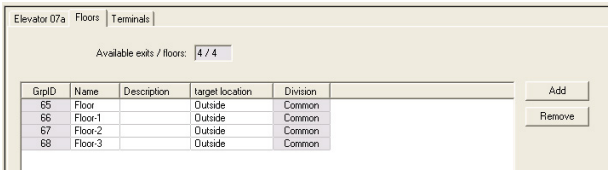
Legenda:

- 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

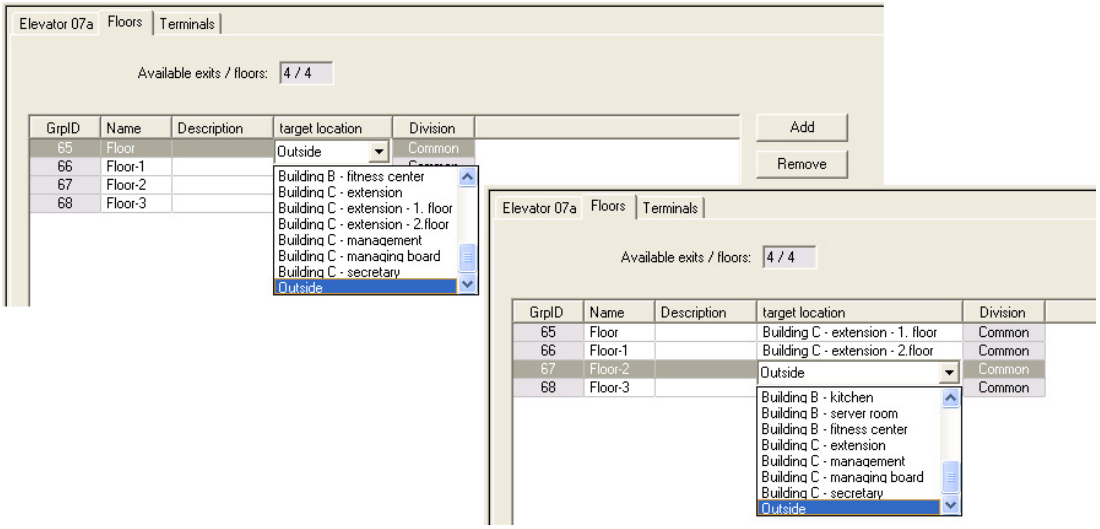
– G = leitor. Dois leitores podem ser configurados para cada elevador.

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.

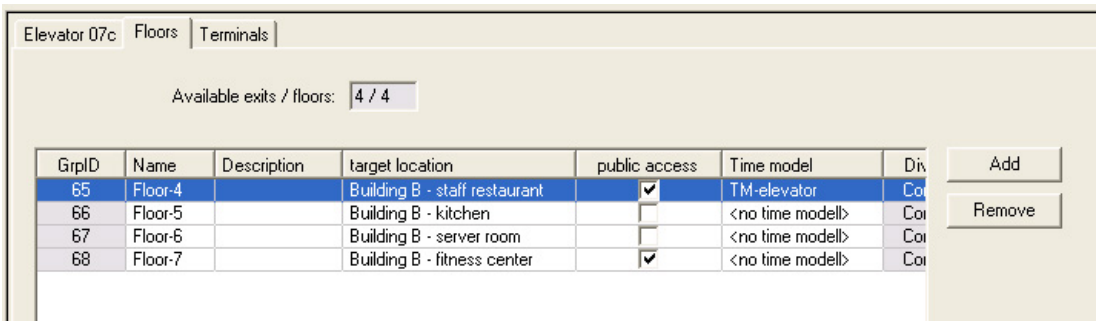
Andares para o modelo de entrada 07
Use a guia **Floors (Andares)** para adicionar e remover andares para o elevador, usando os botões **Add (Adicionar)** e **Remove (Remover)**.



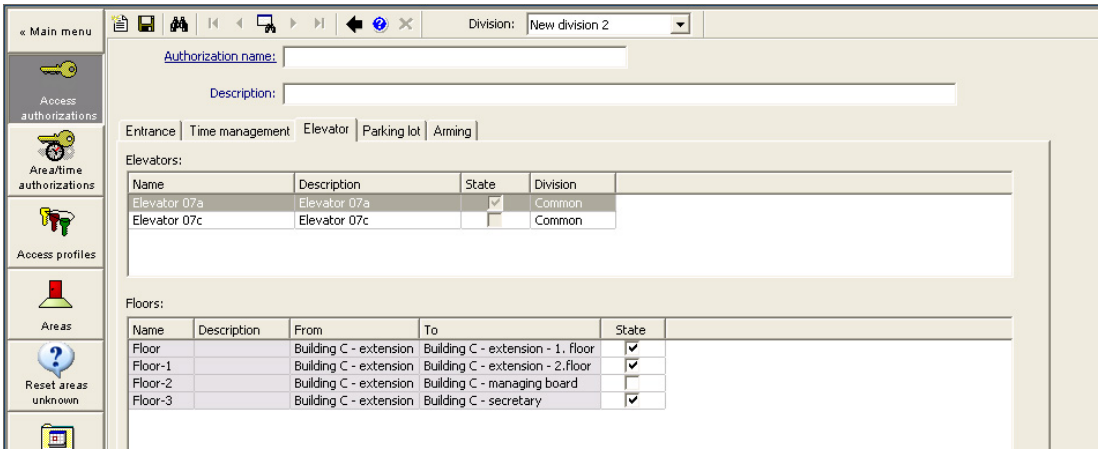
Os locais de destino para um andar podem ser qualquer **Área**, exceto estacionamentos e zonas de estacionamento.
Somente uma área pode ser atribuída a um andar específico. As opções de áreas oferecidas nas caixas de combinação são, portanto, reduzidas após cada atribuição, evitando atribuições duplas não intencionais.



Ao usar o modelo de entrada 07a, é possível tornar cada andar publicamente acessível marcando a caixa **Public access (Acesso público)**. Neste caso, não ocorrerá nenhuma verificação de autorização. Contudo, a atribuição adicional de um **Modelo de tempo** restringiria o acesso a períodos predefinidos.



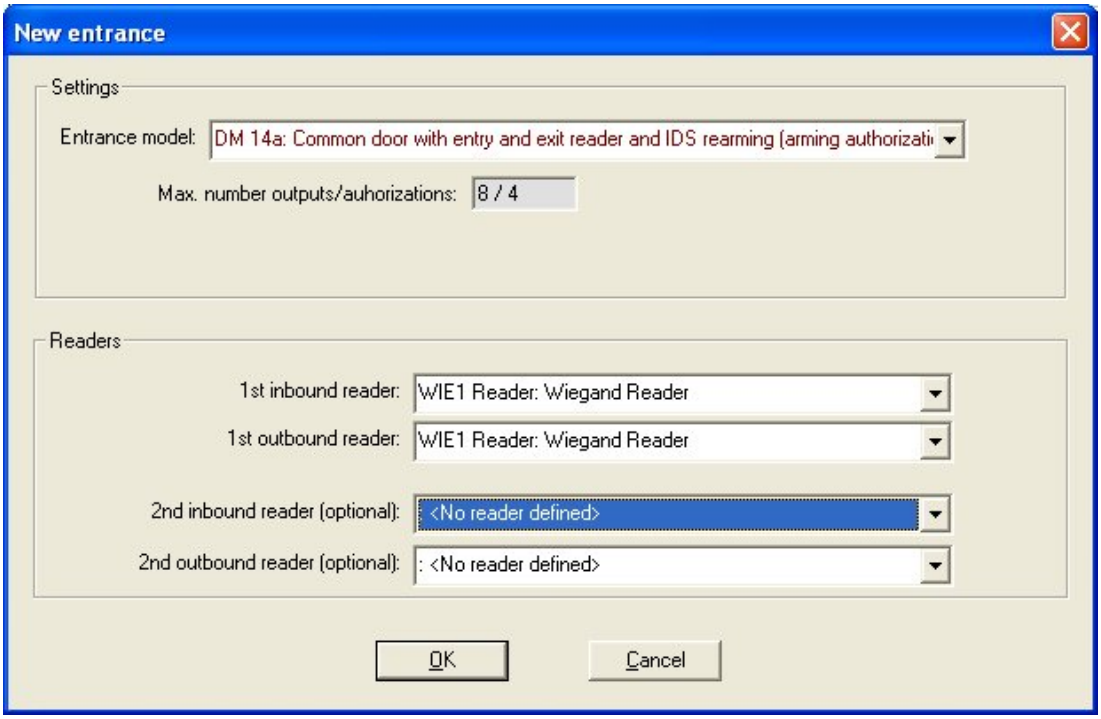
Na guia **Elevator (Elevador)** acima da caixa de listagem superior, nas caixas de diálogo **Access authorizations (Autorizações de acesso)** e **Area/time authorizations (Autorizações de área/horário)** do Access Engine, selecione primeiro o elevador necessário e, em seguida e abaixo, os andares aos quais o titular de cartão tem permissão para acessar.



13.6.2 Modelos de porta com alarmes de intrusão (DM14)

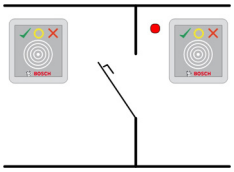
Arme e desarme de sistemas de detecção de intrusão – DM 14

Ao contrário do modelo de entrada 10, o DM 14 pode ser armado/desarmado.



Uma área de arme é designada por uma letra maiúscula na primeira página da entrada. Ao atribuir uma entrada a uma área de arme, o arme em um leitor será aplicado a todas as entradas dessa área.

Modelo de entrada 14



Variantes do modelo:

14a	Porta normal com leitor de entrada e saída e arme/desarme do IDS
14b	Porta normal com leitor de entrada, botão de destrave e arme/desarme do IDS

Sinais possíveis:

Sinais de entrada	**Sinais de saída**
Sensor da porta	Mecanismo de abertura da porta
IDS: está armado	IDS: armar
IDS: pronto para armar	Ativação da câmera
Botão "Solicitação de saída"	Porta aberta durante muito tempo
Sensor da trava da fechadura	
Sabotagem	
IDS: botão de solicitação para armar	

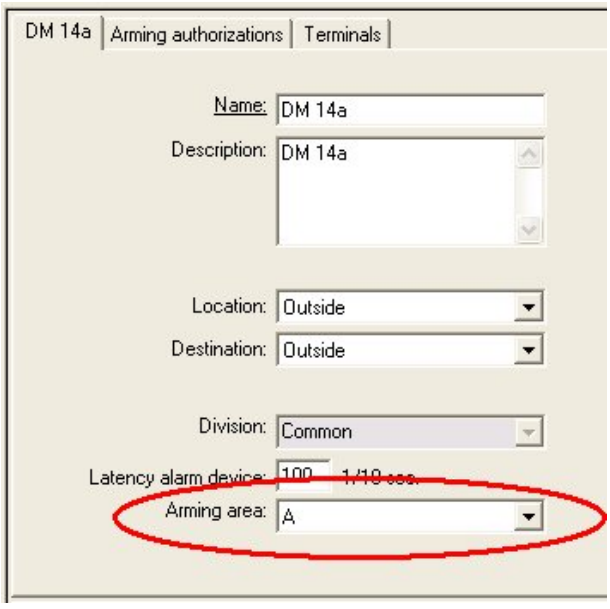
Com o modelo de porta 14 é possível formar áreas seguras onde o IDS (Sistema de detecção de intrusão) pode ser armado a partir de qualquer leitor da área. Nesse caso, os sinais **IDS armed (IDS armado)** e **IDS ready to arm (IDS pronto para armar)** precisam ser replicados em cada entrada.
Ao contrário do modelo de porta 10, o modelo de porta 14 pode utilizar leitores com ou sem teclado. Outra diferença é a atribuição de autorizações de arme/desarme. Somente titulares de cartões com as autorizações adequadas podem armar/desarmar.
No caso de leitores com teclado, o arme e o desarme são realizados do mesmo modo que o modelo de porta 10.
No caso de leitores sem teclado, o arme não acontece ao inserir o código PIN, mas sim usando um interruptor próximo do leitor, que possui a mesma função que a tecla 7 dos leitores com teclado. Após usar esse interruptor, o status do dispositivo de alarme é exibido pelos LEDs coloridos do leitor:

– Desarmado = luz verde e vermelha alternada
– Armado = luz vermelha constante

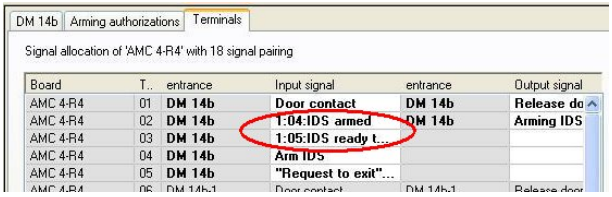
Arme apresentando um cartão devidamente autorizado.
Desarme usando o interruptor e apresentando um cartão devidamente autorizado.
A liberação da porta não é automática após o desarme, isso exige que o cartão seja apresentado novamente.

Autorizações para o arme do modelo de entrada 14

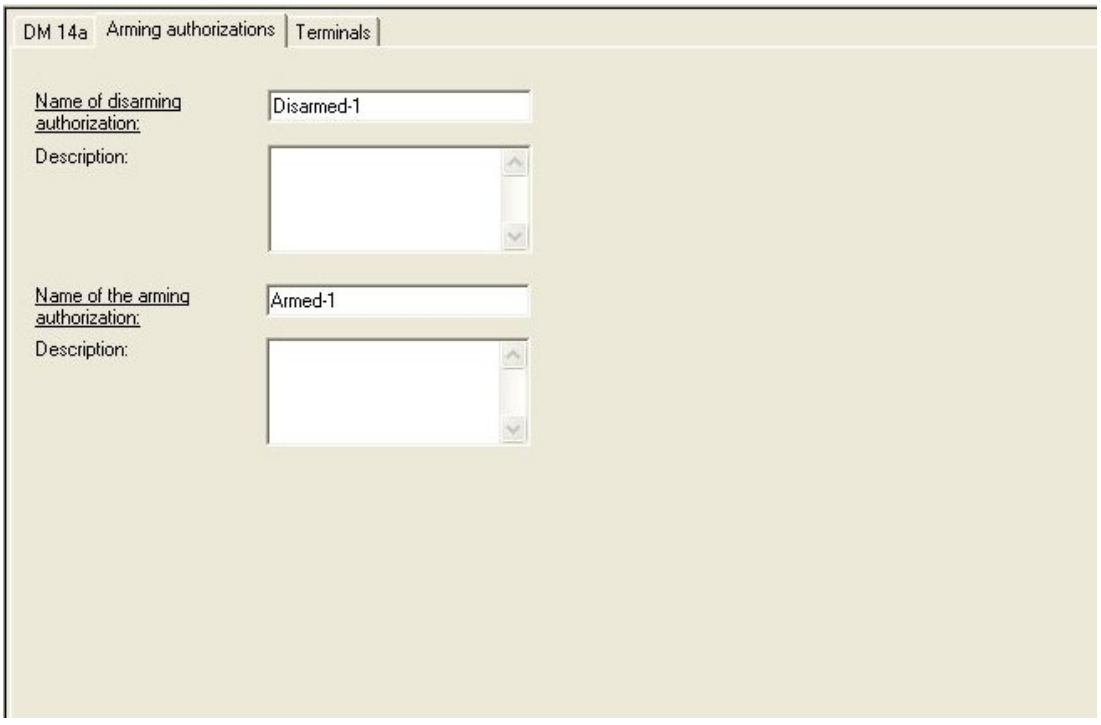
A primeira guia da caixa de diálogo da entrada 14 contém um parâmetro adicional para criação de "Áreas de arme". Várias entradas do modelo 14 podem fazer referência à mesma área de arma, para que qualquer leitor nessa área possa armar ou desarmar o IDS (Sistema de detecção de intrusão).



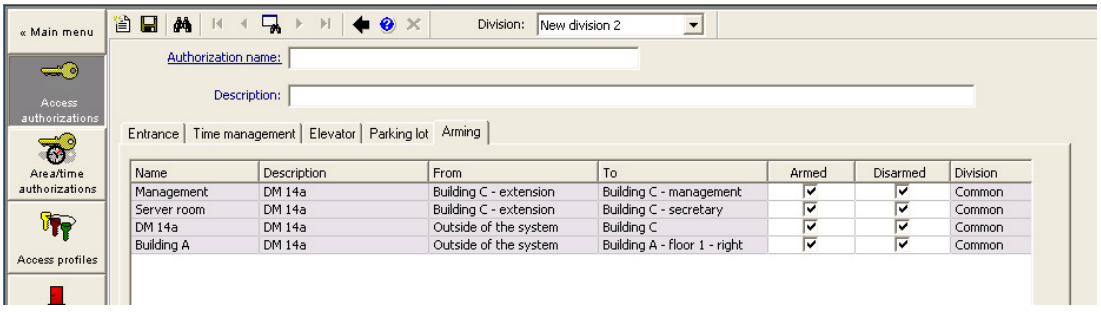
Nesse caso, os sinais **IDS armed (IDS armado)** e **IDS ready to arm (IDS pronto para armar)** precisam ser replicados nas entradas das outras aberturas. Quando um segundo modelo de entrada é criado para a mesma área de arme, o editor de dispositivos faz a replicação para você. A descrição do sinal da segunda porta será expandida pelo número do sinal correspondente do primeiro modelo de entrada, por exemplo, 1:04 [= o quarto sinal da placa 1]



Após a criação de uma instância do modelo de entrada 14, a guia adicional **Arming authorizations (Autorizações de arme)** lista as autorizações geradas pela criação. O usuário pode escolher nomes livremente para as autorizações de arme/desarme.



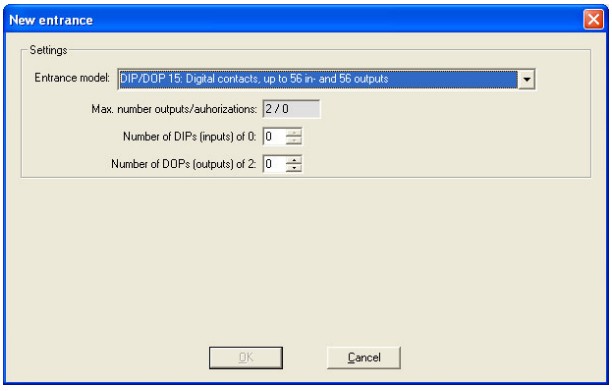
Ao reunir as autorizações, todas as instâncias do modelo de entrada 14 criadas são listadas na guia **Arming (Arme)** das caixas de diálogo **Access authorizations (Autorizações de acesso)** e **Area/Time Authorizations (Autorizações de área/hora)**. As autorizações de arme e desarme podem ser atribuídas separadamente.



13.6.3 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
Sinais possíveis: os nomes padrão podem ser substituídos.

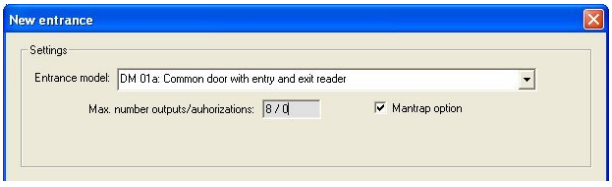
Sinal de entrada	Sinal de saída
DIP	DOP
DIP-1	DOP-1
...	...
DIP-63	DOP-63

Diferente dos outros modelos de porta, o modelo de entrada 15 gerencia essas entradas e saídas de um controlador que ainda estão livres e as coloca como entradas genéricas e saídas sem tensão à disposição do sistema.
Ao contrário dos contatos de saída de outros modelos de porta, os contatos do modelo de entrada 15 podem ser encontrados individualmente na interface gráfica do usuário do BIS.

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.

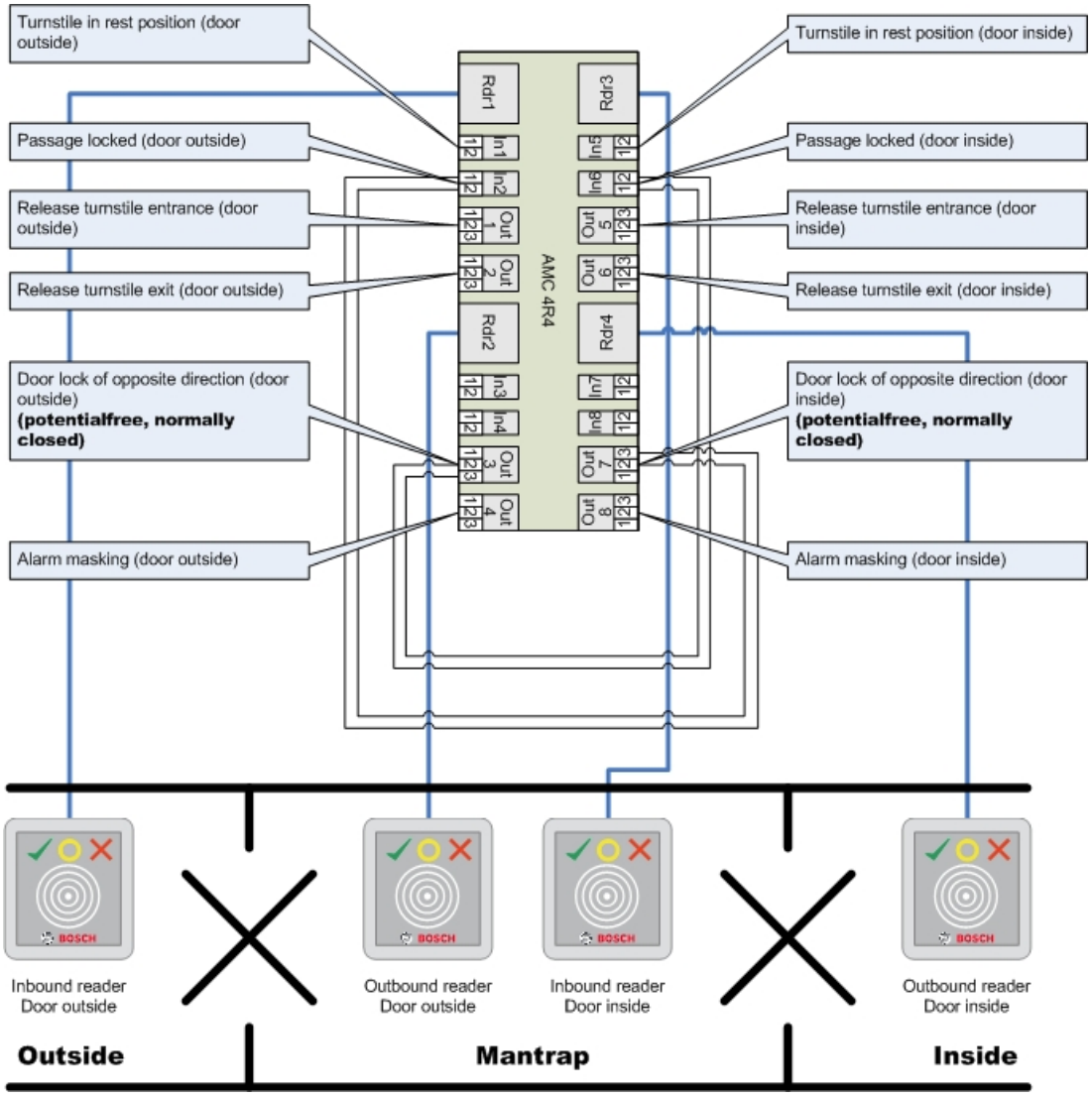
13.6.4 Modelos de porta de eclusa

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.

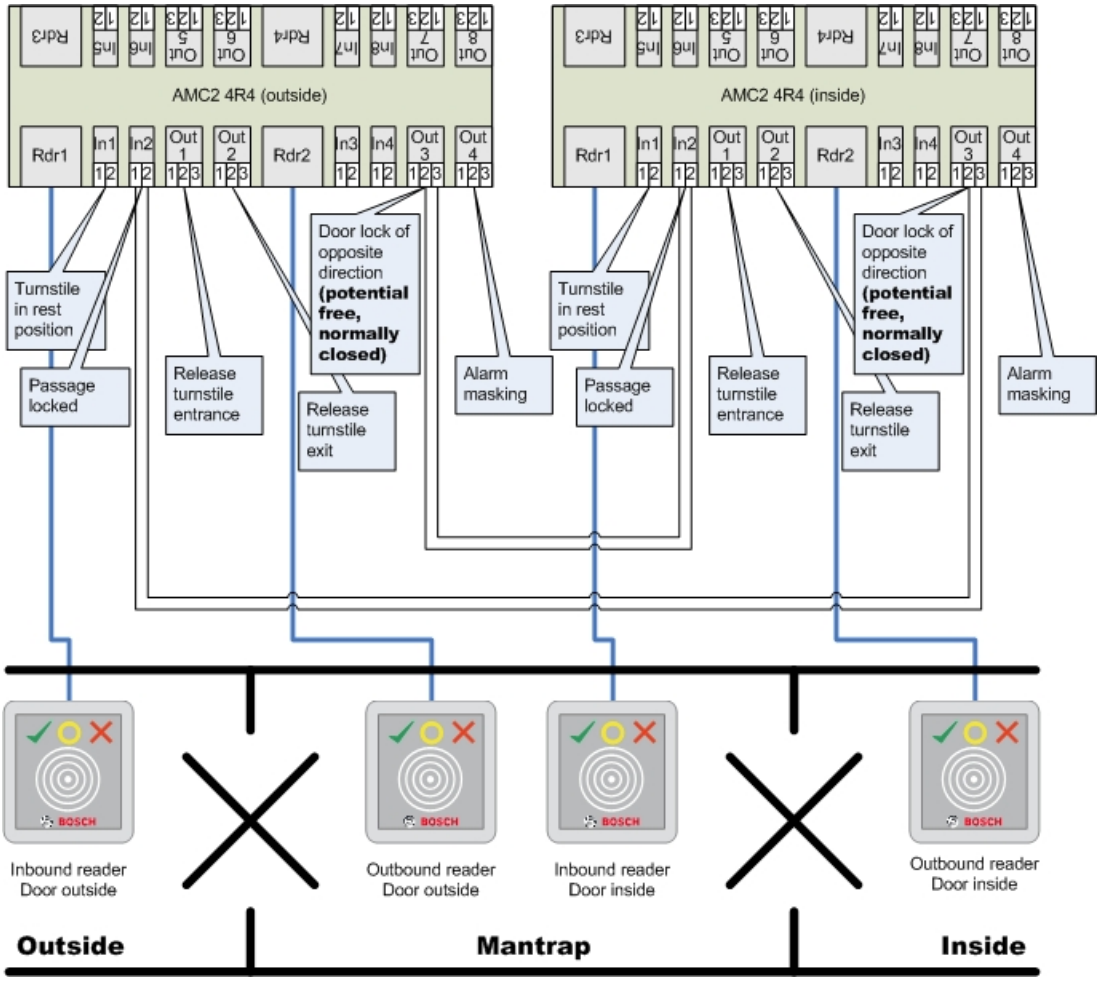
Exemplo: eclusa em um controlador
As catracas são os dispositivos mais comuns para permitir o acesso de um titular de cartão por vez. Assim, utilizamos nos seguintes exemplos o modelo de porta 3a (catraca com leitor de entrada e saída).
Configuração de eclusa com duas catracas (DM 03a):



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".

13.7 Portas

Configuração de uma porta: parâmetros gerais

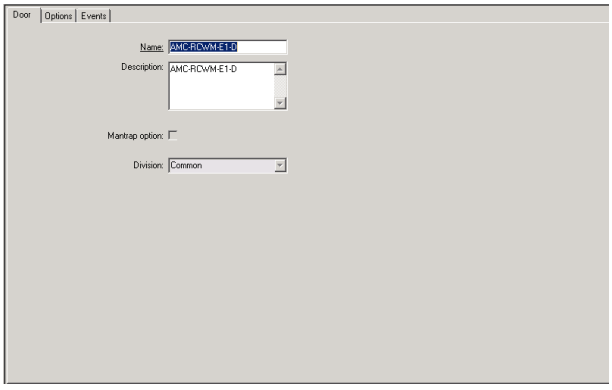
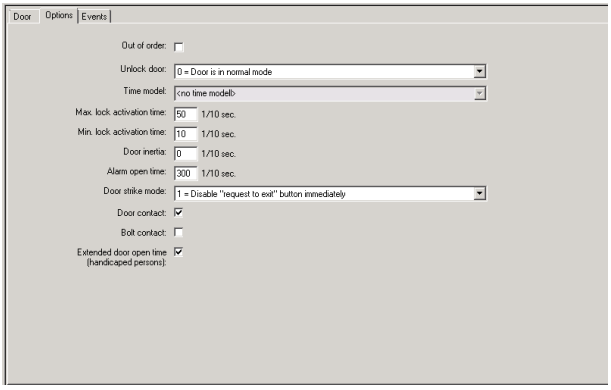


Figura 13.1:

Parâmetro	Valores possíveis	Descrição
Name (Nome)	Alfanumérico, até 16 caracteres	O valor padrão gerado pode, opcionalmente, ser substituído por um nome exclusivo.
Descrição	Alfanumérico, até 255 caracteres	
Division (Divisão)	A divisão padrão é "Comum"	Esse é um campo somente leitura. As atribuições para divisões são realizadas no editor de dispositivos DevEdit para cada porta na hierarquia de dispositivos
Somente para os modelos de porta 01 e 03 se uma eclusa estiver configurada:		
Mantrap option (Opção de eclusa)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	Uma eclusa existe onde duas portas combinadas usam o modelo de porta 01 ou 03. Ative a opção de eclusa para **ambas** as portas. As portas também exigirão fiação física especial.

Configuração de uma porta: opções

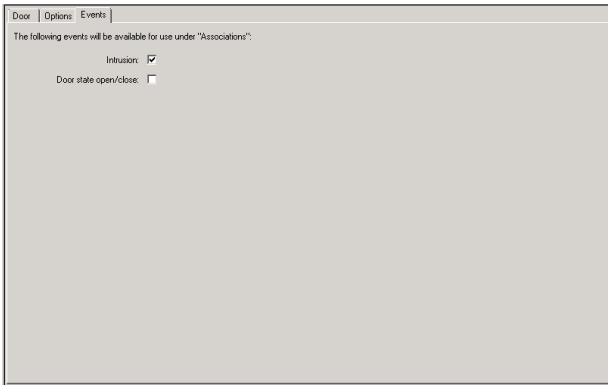


Parâmetro	Valores possíveis	Observações
Manual operation (Operação manual)	0 = caixa de seleção desmarcada 1 = caixa de seleção marcada.	0 = a porta está no modo normal (padrão, isto é, está sujeita ao controle de acesso realizado pelo sistema geral. 1 = a porta não faz parte do sistema de controle de 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.
Unlock door (Destravar porta)	0 = porta está no modo normal 1 = porta está destravada	0 = modo normal (padrão), a porta será trancada ou destrancada dependendo dos direitos de acesso das credenciais.

	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	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 até ser desbloqueada manualmente. 6 = travada a partir da ativação do modelo de tempo, não há controle da porta, ela não pode 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.
Max. lock activation time (Tempo máx. ativação fechadura)	0 - 9999	Intervalo de tempo para ativação do mecanismo de abertura da porta, em décimos de segundo – padrão: 50 para portas, 10 para portas giratórias (03) e 200 para barreiras (05c ou 09c).
Min. lock activation time (Tempo mín. ativação fechadura)	0 - 9999	Intervalo de tempo mínimo para a ativação do mecanismo de abertura da porta, em décimos de segundo. Fechaduras eletromagnéticas precisam de algum tempo para desmagnetizar – padrão: 10.
Door inertia (Inércia da porta)	0 - 9999	Assim que o tempo de ativação passar, a porta poderá ser aberta durante esse intervalo sem emissão de um alarme, em décimos de segundo. Porta hidráulicas precisam de algum tempo para acumular pressão – padrão: 0.
Alarm open time (Tempo de abertura do alarme)	0 - 9999	Se a porta permanecer aberta após esse intervalo de tempo, uma mensagem será emitida (porta aberta durante muito tempo), em décimos de segundo – padrão: 300. 0 = sem tempo limite, sem mensagem

Door strike mode (Modo de funcionamento porta)	List box entry (Entrada da caixa de listagem)	0 = botão REX (solicitação de saída) é desabilitado após o tempo de ativação 1 = botão REX (solicitação de saída) é habilitado imediatamente (= padrão)
Door contact (Contato de porta)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	0 = porta sem contato da estrutura 1 = porta tem um contato da estrutura. Um contato fechado normalmente significa que a porta está fechada. (= padrão)
Bolt contact (Contato da trava da fechadura)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	0 = porta sem contato da trava da fechadura (= padrão) 1 = porta tem um contato da trava da fechadura. Uma mensagem é emitida quando a porta é aberta ou fechada.
Extended door open time (Tempo estendido de abertura da porta) (pessoas com deficiência)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	0 = o tempo de ativação da fechadura é normal. 1 = o tempo de ativação da fechadura é estendido pelo fator definido no parâmetro EXTIMFAC em todo o sistema. Isso serve para oferecer mais tempo à passagem de pessoas com deficiência pela porta. (= padrão)

Configuração de uma porta: eventos

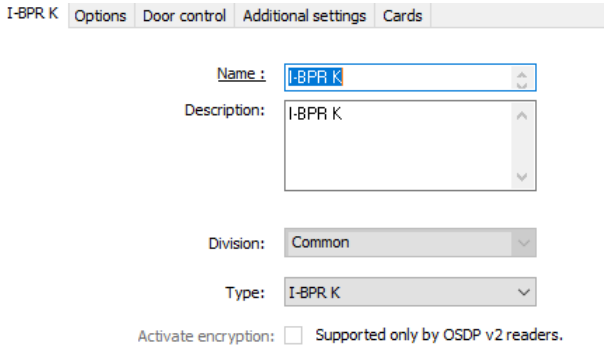


Parâmetro	Valores possíveis	Observações
Intrusion (Intrusão)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	0 = sem mensagem de intrusão. Isso é útil se uma porta puder ser aberta livremente pelo lado de dentro. 1 = uma mensagem é acionado após uma abertura não autorizada. Outra mensagem indicará o fechamento subsequente. (padrão)
Door state open/ closed (Estado de porta aberta/fechada)	0 = desativada (caixa de seleção desmarcada)	0 = nenhuma mensagem de "porta aberta" é enviada (padrão)

	1 = ativada (caixa de seleção marcada)	1 = uma mensagem é enviada após abertura ou fechamento.

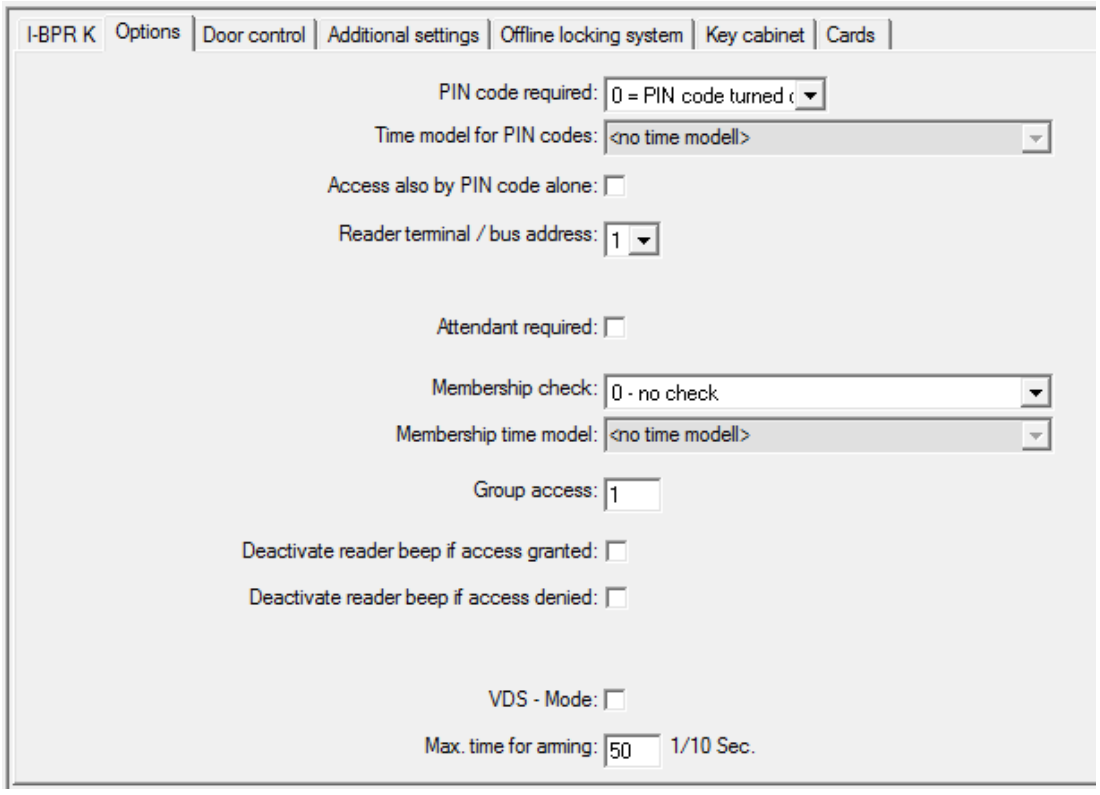
13.8 Leitores

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	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)	**Observe** que a verificação de associação funciona apenas com definições de cartão predefinidas no sistema (histórico cinza), não com definições personalizadas. **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 permanece 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.

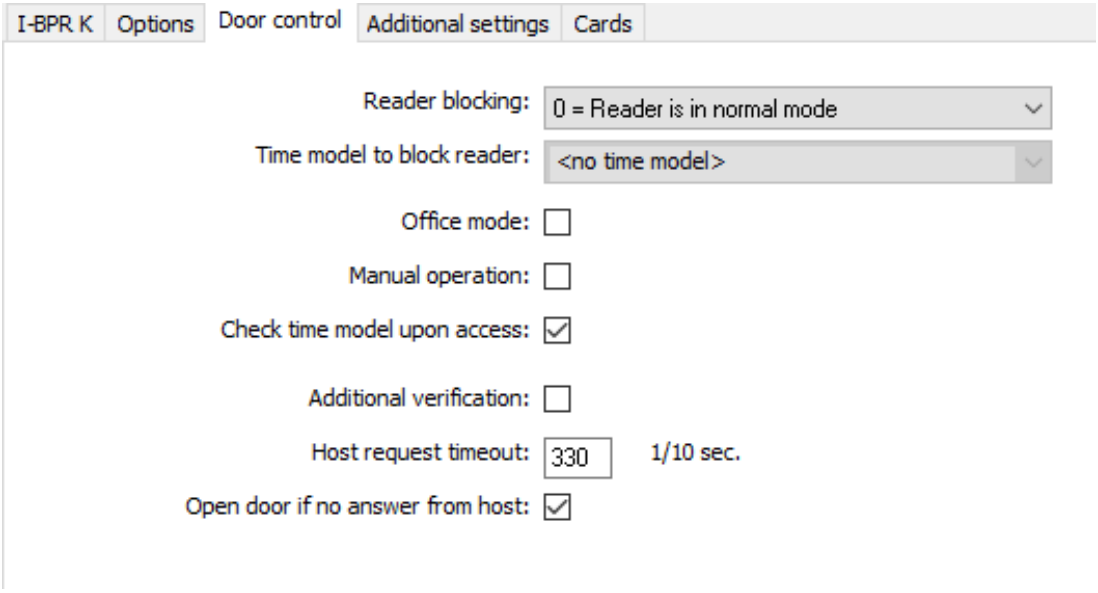
Os modelos podem ser armazenados em dispositivos acima do leitor na árvore de dispositivos e no próprio leitor. Os dados no leitor são atualizados periodicamente pelos dispositivos superiores.

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`

Parâmetro	Descrição
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) São 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

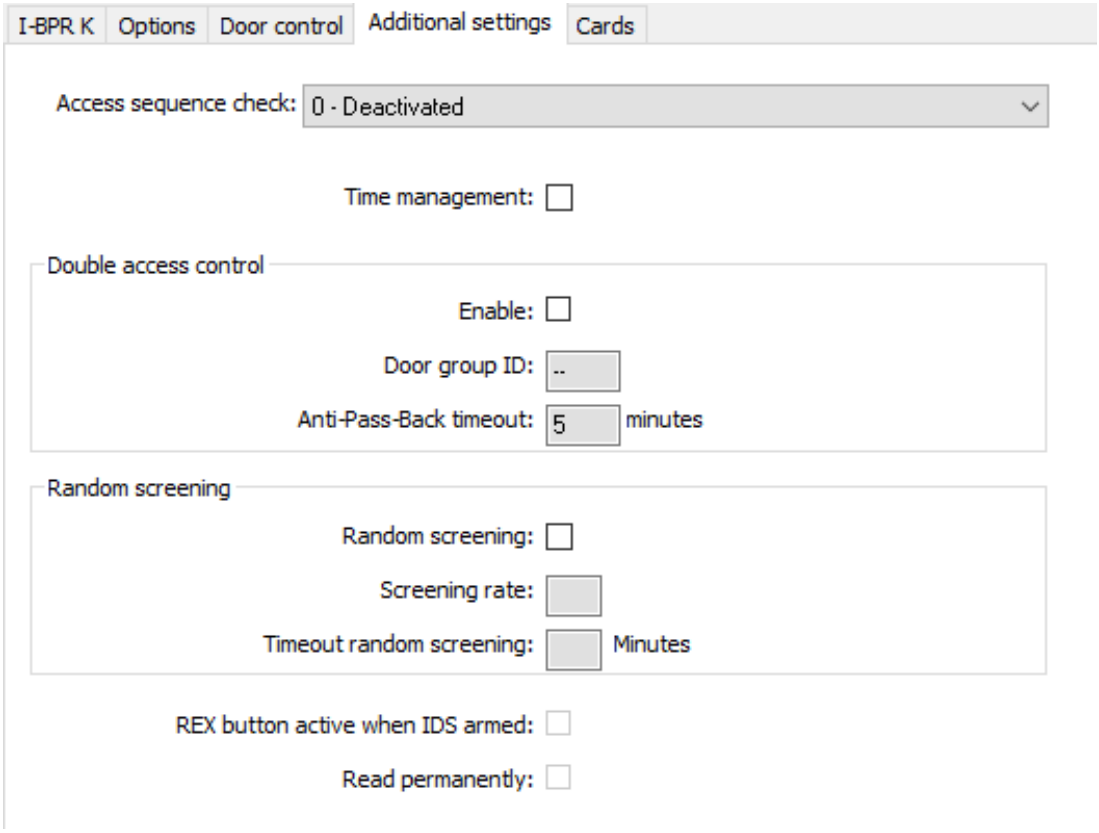


Parâmetro	Valores possíveis	Observações
Reader blocking (Bloqueio de leitor)	List box entry (Entrada da caixa de listagem)	0 = leitor está em modo normal – sem bloqueio (= padrão) 1 = leitor está permanentemente bloqueado – bloqueio permanente 2 = leitor está bloqueado dependendo do modelo de tempo – bloqueio de acordo com o modelo de tempo definido em *Time model to block reader (Modelo de tempo para bloquear leitor)*
Time model to block reader (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.
Office mode (Modo Escritório)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	Permite que esse leitor seja usado em Modo Escritório.
Manual operation (Operação manual)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	0 = leitor está em modo normal (= padrão) 1 = leitor está efetivamente removido do sistema de controle de acesso, isto é, "inoperante". Nenhum comando é recebido. Todos os outros parâmetros desse leitor estão desligados.

		O parâmetro deve ser definido de forma independente para o leitor e para a porta.
Check time models upon access (Verificar modelos de tempo no acesso)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	0 = modelos de tempo não serão verificados. Não há restrição de tempo para o acesso. 1 = se o titular de cartão tiver um modelo de tempo atribuído, diretamente ou como uma autorização de área/hora, o modelo de tempo será verificado. (= padrão)
Additional verification (Verificação adicional)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	0 = verificação do host não é obrigatória 1 = verificação do host é obrigatória (padrão) (**IMPORTANTE**: a ativação desta opção é obrigatória para verificação de vídeo adicional pelo operador de um sistema BVMS ou BIS)
Host request timeout (Tempo limite de solicitação de host)	0 = desativado	0 = o AMC funciona sem verificação do host (não funciona com *Area Change (Mudança de área)* ou *Person Countings (Contagens de pessoas)*). Esse controle só está ativo se a Host verification (Verificação do host) estiver desativada (0) e *Open door if no answer from host (Abrir porta se host não responder)* estiver ativada (1) 1 a 9999 = usar o leitor requer uma consulta do BIS. A consulta deve ser respondida dentro do intervalo de tempo especificado. Se o tempo expirar, o AMC verifica o parâmetro **Open door if no answer from host (Abrir porta se host não responder)** e toma uma decisão própria. Os valores são em décimos de segundo. (Padrão = 30)
Open door if no answer from host (Abrir porta se host não responder)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	Este controle só está ativo se o parâmetro **Host verification (Verificação do host)** estiver definido. 0 = não abre a porta se uma decisão do host for necessária mas não puder ser recuperada (operação offline). 1 = abre a porta após o tempo limite se puder ser liberada pelo AMC. (= padrão)
Check parking ticket credits (Verificar créditos de tíquete de estacionamento)	0 = desativada (caixa de seleção desmarcada)	Se ativada (1), os créditos de tíquete de estacionamento serão verificados.

	1 = ativada (caixa de seleção marcada)	
Check overstayed parking (Verificar estacionamento prolongado)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	Se ativada (1), é verificado se o período de estacionamento foi muito longo.

Configuração de um leitor: configurações adicionais

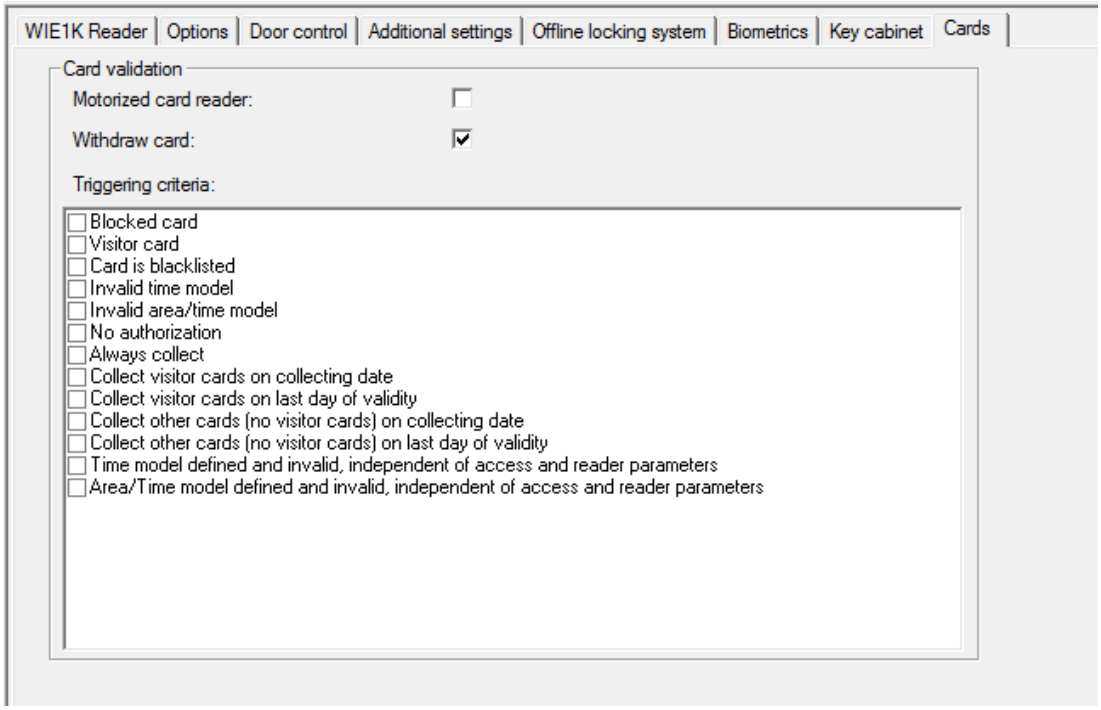


Parâmetro	**Valores possíveis**	**Observações**
Acess sequence check (Verificação da sequência de acesso)	0 – desativada 1 – ativada; desativada em caso de mau funcionamento de LAC 2 – ativada; permanece ativa em caso de mau funcionamento de LAC	0 = leitor não participa da verificação da sequência de acesso (= padrão) Uma verificação da sequência de acesso pode lidar com pessoas definidas como DESCONHECIDO das seguintes formas: 1 = a primeira leitura do cartão será realizada sem verificar a localização. Todos os controladores devem estar online. 2 = a primeira leitura do cartão será realizada sem verificar a localização.

	3 – ativada; usar verificação de sequência estrita mesmo em caso de mau funcionamento de LAC (observação: atualizar local da pessoa manualmente)	3 = a verificação da localização acontecerá para toda leitura de cartão durante mau funcionamento de LAC.
 Na plataforma do BIS, há um comando do MAC para ativar ou desativar todas as verificações da sequência de acesso de modo geral. Para desativar a verificação da sequência de acesso durante um período, é fornecido um valor em minutos com um máximo de 2880 (= 48 horas). Definir o valor "0" desativa a verificação da sequência de acesso completamente. **Observação:** Este comando pode modificar a verificação da sequência de acesso somente para leitores em que o parâmetro **Enable access sequence (Habilitar sequência de acesso)** estiver definido. Ele não desativa/ativa a verificação da sequência de acesso para *todos* os leitores.		
Time Management (Gerenciamento de tempo)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	Se ativado (1), o processo do Ace coleta dados para o sistema de frequência.
Double access control (anti-passback control) (Controle de acesso duplo (controle anti-passback))		
Habilitar	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	0 = sem controle de acesso duplo (= padrão) 1 = com controle de acesso duplo Durante o intervalo de tempo definido pelo parâmetro **Duration (Duração)**, esse leitor e outros leitores do grupo não podem ser usados com o mesmo cartão. Se esse parâmetro estiver ativado, um ID do grupo de portas deve 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 usando um ID do grupo de portas. Apresentar um cartão em um leitor bloqueará registros subsequentes em todos os leitores do grupo de portas (Padrão = **--**) até que o tempo limite acabe.

Anti-passback time out (Tempo limite de anti-passback)	1 - 120	O leitor pode ser usado com o mesmo cartão após o término desse intervalo de tempo. Assim que o cartão for usado em um leitor fora do grupo, o bloqueio é retirado imediatamente. Os valores estão em minutos – padrão = 5.
Random screening (Triagem aleatória)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	0 = sem triagem aleatória 1 = triagem aleatória de acordo com o fator terá a entrada proibida até que seja desbloqueada pela caixa de diálogo **Blocking (Bloqueio)**.
Screening rate (Taxa de triagem)	1 - 100	Porcentagem de triagem aleatória para uma verificação estendida. Disponível se a triagem aleatória estiver ativada.
Timeout random screening (Tempo limite da triagem aleatória)	1 - 120	Durante o tempo definido, o usuário estará sujeito à triagem aleatória. Os valores estão em minutos – padrão = 5.
REX button active when IDS armed (Botão REX ativo quando IDS armado)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	Somente para **DM10** e **DM14**: botões de destrave REX são exibidos por padrão quando o IDS estiver armado. Isso impossibilitaria a saída da área monitorada. Esse novo parâmetro do leitor habilita o botão REX mesmo quando o IDS estiver armado. Esse parâmetro também precisa ser definido onde um leitor for usado em vez de um botão de destrave.
Read permanently (Ler permanentemente)	0 = desativada (caixa de seleção desmarcada) 1 = ativada (caixa de seleção marcada)	O leitor lê permanentemente se tiver o firmware correspondente do fabricante.

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.

13.8.1 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.

13.9 Acesso apenas com código PIN

Contexto

Os leitores com teclado podem ser configurados para permitir acesso apenas com código PIN. Quando os leitores estão configurados assim, o operador do BIS pode atribuir códigos PIN individuais a funcionários selecionados. Na verdade, esses funcionários recebem um "cartão virtual" que consiste exclusivamente em um código PIN. Ele é chamado de PIN de identificação. Em contraste, um PIN de verificação é um código PIN usado em combinação com um cartão para aplicar um nível maior de segurança.

O operador pode inserir códigos PIN para funcionários manualmente ou atribuir-lhes códigos PIN gerados pelo sistema.
Observe que os mesmos funcionários podem continuar a acessar qualquer cartão físico que esteja também atribuído a eles.

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. Navegue até o Main menu (Menu principal) > **Configuration (Configuração)** > **Operators and workstations (Operadores e estações de trabalho)** > **User profiles (Perfis de usuário)**
2. 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.
3. 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.

4. No painel de Funções especiais, marque a caixa de seleção **Assign virtual cards (PIN) (Atribuir cartões virtuais (PIN))**
5. Clique em  ou **Apply (Aplicar)** para salvar as alterações

Definição do comprimento do PIN de identificação para todos os tipos de leitores
O comprimento de PINs inseridos manualmente ou gerados pelo sistema é governado pelo parâmetro definido na configuração do sistema.
– 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. Navegue até o Main menu (Menu principal) > **Configuration (Configuração)** > **Device data (Dados do dispositivo)** > árvore **Workstations (Estações de trabalho)** 
2. No painel **Workstation (Estação de trabalho)**, selecione a estação de trabalho à qual o leitor está fisicamente conectado.
3. 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)**.
4. 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)**.
5. Verifique se a lista suspensa **Card usage default (Utilização do cartão predefinida)** contém o valor padrão **Virtual card (Cartão virtual). Usar PIN como cartão**.
6. Clique em  ou **Apply (Aplicar)** para salvar as alterações
7. No editor de dispositivos DevEdit, navegue até a árvore **Device configuration (Configuração do dispositivo)** 
8. Selecione o leitor na entrada em que deseja configurar o acesso apenas com código PIN.
9. Na guia **Options (Opções)**, marque a caixa de seleção **Access also by PIN code alone (Acesso também só com código PIN)**.
10. Clique em  ou **Apply (Aplicar)** para salvar as alterações

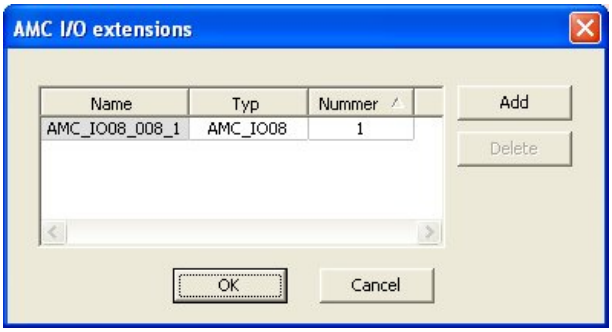
13.10 Placas de extensão do AMC

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.

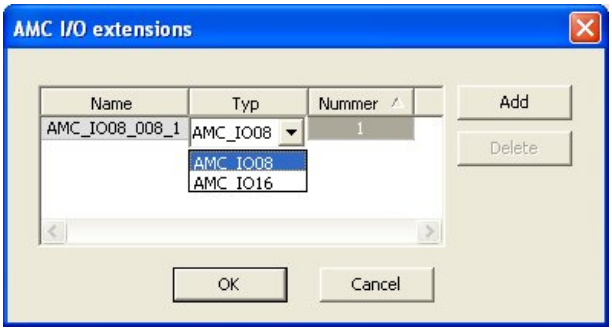
Uma caixa de diálogo de seleção para a criação das extensões aparece.



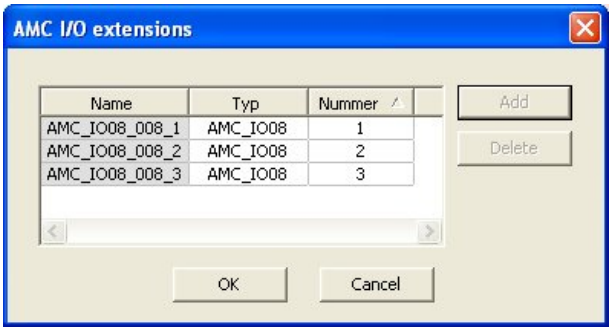
AMC-EXT está disponível em duas variantes:

- 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).

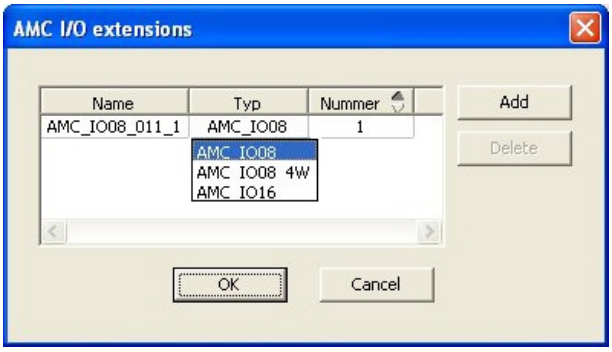
Criação de um AMC2 4W-EXT
É possível configurar placas de extensão especiais (AMC2 4W-EXT) para controladores com interfaces de leitor Wiegand (AMC2 4W). Esse módulos oferecem quatro conexões de leitor Wiegand adicionais, além de oito contatos de entrada e oito de saída cada. Logo, o número máximo de 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
Board name (Nome da placa)	Alfanumérico restrito: 1 a 16 dígitos	A identificação padrão garante um nome único, mas pode ser substituído manualmente. Certifique-se de que o ID seja único. As conexões de rede com servidores DHCP devem usar o nome da rede.
Board description (Descrição da placa)	alfanumérico: 0 a 255 dígitos	Esse texto é exibido na derivação OPC.
Board number (Número de placa)	1 - 3	Número da placa conectada ao AMC. Campo de exibição apenas.
Power supply (Fonte de alimentação)	0 = desativada (caixa de seleção marcada) 1 = ativada (caixa de seleção marcada)	Supervisão da tensão de alimentação. Em caso de interrupções da alimentação, uma mensagem é gerada ao final de um atraso. A função de supervisão assume o uso de um USV para que uma mensagem possa ser gerada. 0 = sem supervisão 1 = supervisão ativada
Division (Divisão)	Valor padrão = "Comum"	Este campo somente leitura só se aplica onde o recurso de divisões estiver licenciado e em uso.

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.

14 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 do ACE
- 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
- Qual tipo de dado eles contêm (texto, data e hora, inteiro etc.)
- Onde (em cada guia, em qual coluna e em qual linha) no cliente do ACE eles aparecerão
- Qual o tamanho de exibição
- 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.

14.1 Pré-visualização e edição de campos personalizados

Caminho da caixa de diálogo

- Main menu (Menu principal) > **Configuration (Configuração)** > **Options (Opções)** > **Custom fields (Campos personalizados)**

A janela principal é dividida em duas guias

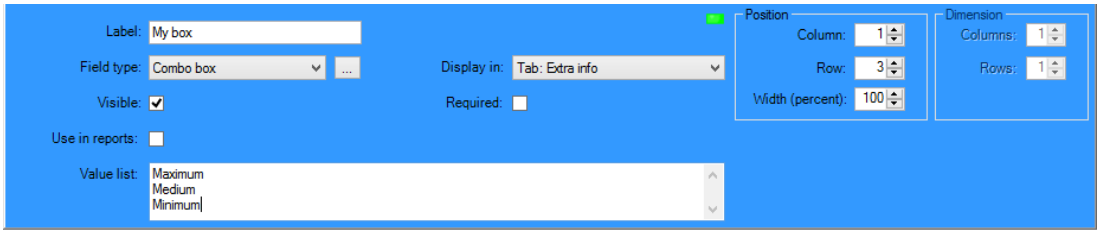
Overview (Visão Geral) Esta guia e suas subguias (**Address (Endereço), Contact (Contato), Additional person data (Dados pessoais adicionais), Additional Company data (Dados adicionais da empresa), Remarks (Observações), Card Control (Controle do cartão)** e **Extra Info (Informações adicionais)**) são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

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

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.

Texto do rótulo	Descrição

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 rejeitar o conteúdo de campo de dados que não for único. Por exemplo, os números de funcionários devem ser únicos para cada funcionário.
	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.

Texto do rótulo	Descrição
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 texto. 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)**.

14.2 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.

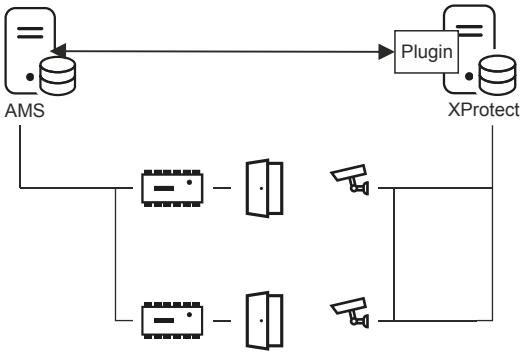
Aviso!
Recomendações urgentes antes do uso produtivo
Concorde e finalize os tipos de campo e seus usos antes de usá-los para armazenas dados pessoais:
Cada campo de entrada de dados é atribuído a um campo específico do banco de dados, para que os dados possam ser localizados manualmente e por geradores 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.

15 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.

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.

16 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.

16.1 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. Portas direcionais (por exemplo, catracas e eclusas) permitem apenas a saída.
- 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 são protegidas.
  - **Parents' evening (Jantar dos pais)**: 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 atributos que podem ser atribuídos 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.

16.2 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.

16.3 Etapas de configuração no Editor de dispositivos

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

16.3.1 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)**

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.

16.3.2 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)**

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 da porta)**
   – 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 atribuir o perfil corretamente.
5. Se for necessário atribuir o perfil a portas do tipo direcional (por exemplo, uma catraca ou eclusa), marque a caixa de seleção **Turnstile (Catraca)**.
   – Isso fornecerá mais opções para o estado de destino da porta em diferentes níveis de ameaça. 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

16.3.3 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)**

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 atribuir 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.

16.3.4 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)**

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.

✓ 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.

16.3.5 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)**

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.

16.4 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**.

16.4.1 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)**

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)

16.4.2 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

16.5 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 122*
- *Criação e gerenciamento de dados de funcionários, página 124*

17 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?

17.1 Pessoas

Os dados das pessoas para as quais a caixa de seleção **Administrados globalmente** foi marcada somente podem ser editados por operadores com o direito adicional de **Administrador global**. Esse direito é definido na caixa de diálogo do operador no Navegador de configuração do BIS.
Os dados protegidos são:

- Todos os dados da caixa de diálogo **Pessoas**, exceto a guia **Observações** e campos de informações adicionais especialmente definidos na guia **Informações adicionais**.
- Todos os dados da caixa de diálogo **Cartões**.
- Todos os dados da caixa de diálogo **Código PIN**.

Todos os outros dados dessas pessoas podem ser editados por qualquer operador.

A tabela a seguir lista os principais tipos de dados que podem ser gravados. Praticamente todos os campos são opcionais. Os campos obrigatórios estão 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.

17.1.1 Opções de controle de cartão/controle de edifício

17.1.2 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.

17.1.3 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.

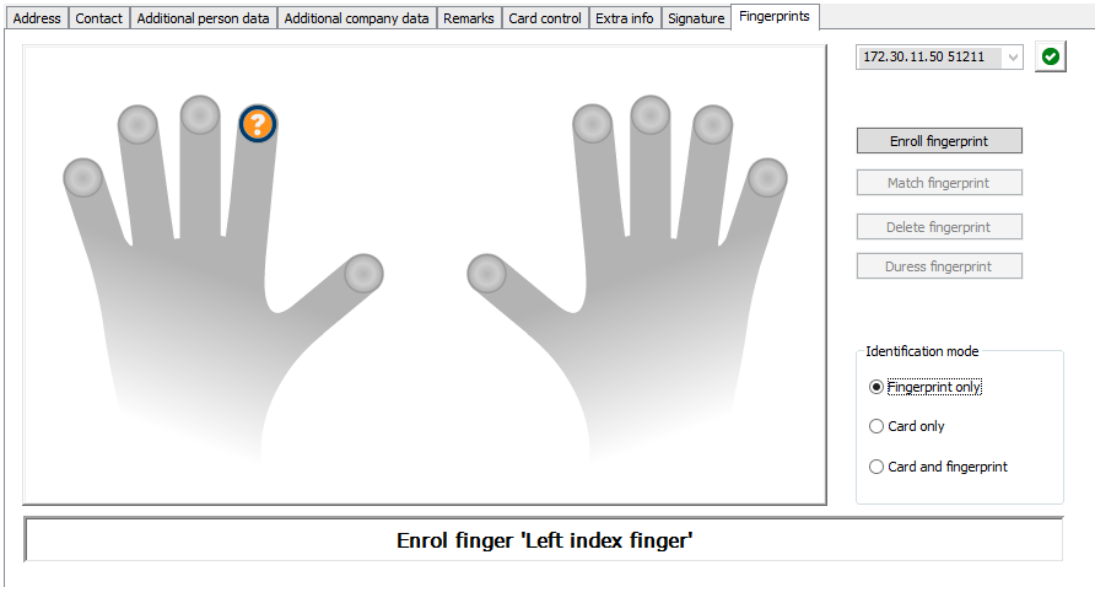
1. Clique na guia **Signature (Assinatura)**
2. Clique no botão **Capture Signature (Capturar assinatura)** para gravar uma nova assinatura.
3. Assine diretamente no pad de captura usando o stylus especial.

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.

17.1.4 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 impressões digitais conectado a, e configurado para, a estação de trabalho.
- Como o operador, você está se comunicando diretamente com o inscrito, isto é, com a pessoa cujas impressões digitais devem ser registradas como credenciais biométricas para acesso.
- Você se familiarizou sobre como apresentar seu dedo repetidamente no leitor específico utilizado, para permitir que ele capture impressões digitais de forma eficiente.

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  (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:
- Pelo menos uma impressão digital da pessoa inscrita já foi cadastrada e armazenada com êxito.
- O leitor de impressões digitais está on-line. Se estiver no modo off-line, o leitor não poderá enviar um sinal de coação ao 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.

17.2 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.

17.3 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.

– 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:
- 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)**.

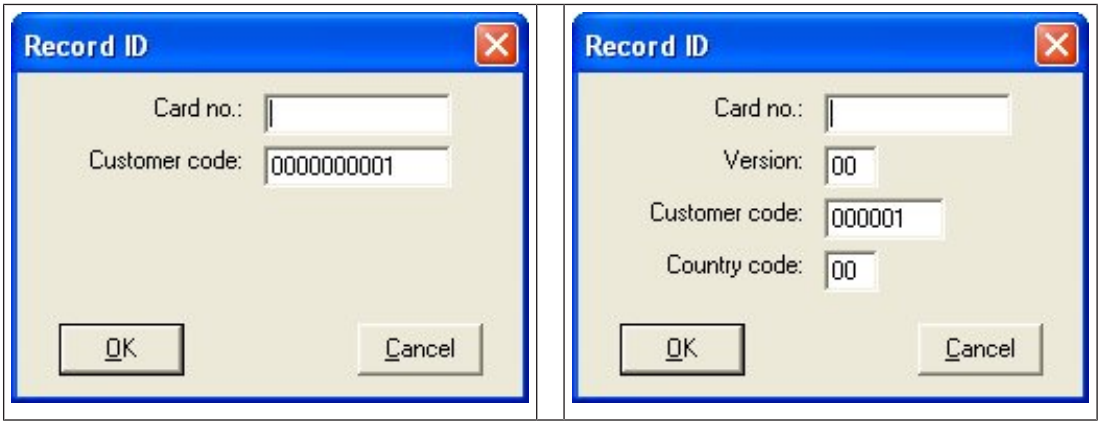
17.3.1 Atribuição de cartões a pessoas

Introdução
Uma pessoa sob controle de acesso requer um cartão ou outra credencial eletrônica, que é atribuída ao seu titular na caixa de diálogo Cartões.
Os números de cartões podem ser atribuídos manual ou automaticamente por meio de um leitor de cadastramento.

Caminho da caixa de diálogo
Main menu (Menu principal) > **Personnel data (Dados de funcionários)** > **Cards (Cartões)**

Pré-requisito
Você carregou o registro de funcionário que deve receber o cartão no cabeçalho da caixa de diálogo **Cards (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.

Uso de um leitor de cadastramento

Pré-requisito

Um leitor de cadastramento foi conectado à estação de trabalho em que você está trabalhando.

Procedimento de cadastramento

1. Clique no botão à direita do botão **Record card (Registrar cartão)** para selecionar um leitor de cadastramento configurado.
2. Clique no botão **Record card (Registrar cartão)** e siga as instruções na tela.
3. Dependendo do tipo de leitor, você poderá inserir detalhes do cartão em uma caixa de diálogo ou ler dados do cartão ao apresentá-lo ao leitor.

Procedimento para alteração de cartões

1. Selecione um cartão na lista.
2. Clique no botão **Change card (Alterar cartão)**
3. Edite os dados do cartão na janela pop-up e 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.

17.3.2 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 146*
– 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.

17.3.3 Guia de outros dados: isenções e permissões especiais

Atribuição de um modelo de tempo:

Use a caixa de listagem **Time model (Modelo de tempo)** para especificar as horas diárias de acesso do titular do cartão, isto é, os períodos nos quais as credenciais do usuário concederão acesso.

Exclusão de pessoas da triagem aleatória

Marque a caixa de seleção **Excluded from random screening (Excluído da triagem aleatória)** para isentá-las de serem selecionadas aleatoriamente para inspeções nas entradas e saídas.

Excluir pessoas das verificações de código PIN
Marque a caixa de seleção **Disable PIN code check (Desabilitar verificação do código PIN)** para isentá-las de inserir seus códigos PIN nos leitores fora das horas úteis normais.

Aviso!
A exclusão de verificações de código PIN afeta todo o sistema.
Por exemplo, como os códigos PIN dessas pessoas não são verificados, elas também não serão capazes de armar ou desarmar alarmes nas entradas no modelo de porta 10.

Extensão do tempo de abertura da porta
Marque a caixa de seleção **Extended door opening time (Tempo estendido de abertura da porta)** para fornecer a pessoas com deficiência o triplo do tempo para passar pela entrada antes que o estado **Door open too long (Porta aberta durante muito tempo)** seja gerado.
Monitoramento de rondas
Uma **Ronda** ou **Rota** é uma sequência estrita de leitores definida no menu do Cliente: **Tour monitoring (Monitoramento de rondas)** > caixa de diálogo **Define routes (Definir rotas)**.
Para atribuir uma rota a um titular de cartão, marque a caixa de seleção **Tour monitoring (Monitoramento de rondas)** e selecione uma rota definida na lista suspensa. Se nenhuma rota tiver sido definida, a caixa de seleção estará inativa.
Quando atribuída a um titular de cartão, uma **Rota** se tornará ativa assim que o usuário ler o seu cartão no primeiro leitor da sequência. Depois disso, todos os leitores na sequência deverão ser usados em ordem, até que a rota esteja concluída. Usos típicos destinam-se a impor sequências de acesso restrito em ambientes de limpeza industrial, controlados higienicamente, ou áreas de alta segurança.
Permissão para destravar portas
Marque a caixa de seleção para permitir que o usuário do cartão destrave portas durante um período estendido. Consulte **modo escritório**.

17.3.4 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.

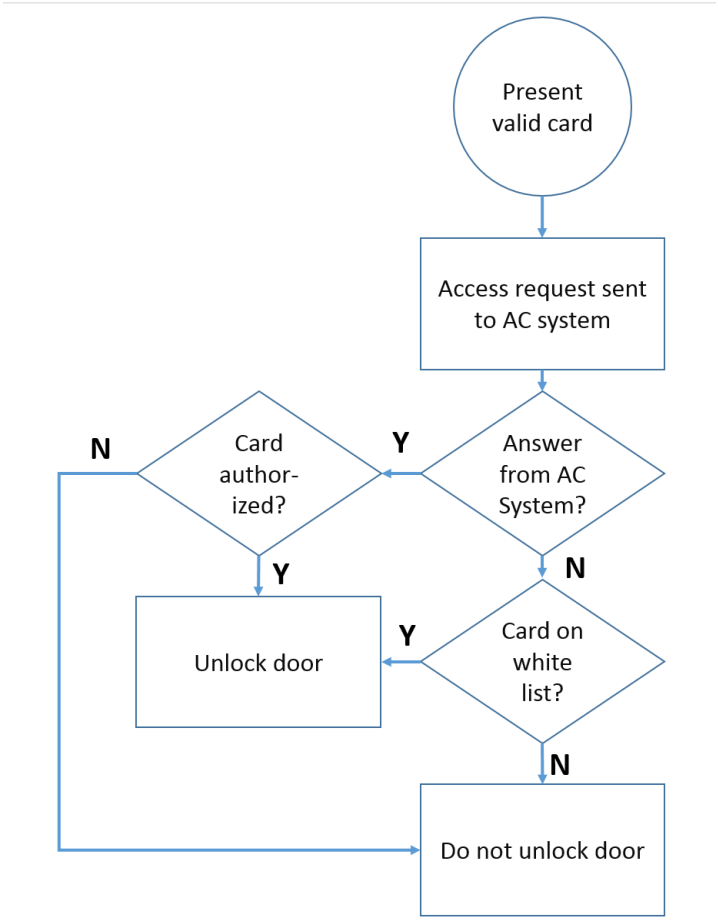
Observe que os guardas com cartões de vigilante podem interromper o modo Escritório da mesma maneira, sem permissão especial.

17.3.5 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 principal AMS, selecione **Personnel data (Dados de funcionários)** > **Cards (Cartões)**
2. Selecione a pessoa que receberá as autorizações do SmartIntego
3. Selecione a guia **SmartIntego.**
4. 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.

17.3.6 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 usado em um leitor. Um nível de ameaça não pode ser cancelado por um cartão de alerta, mas somente por meio do software de controle de acesso.

Pré-requisitos

- Um leitor de diálogos está instalado no seu sistema para gravar dados no cartão.
- Pelo menos um nível de ameaça foi definido no sistema.

Caminho da caixa de diálogo

Main menu (Menu principal) > **Personnel data (Dados de funcionários)** > **Cards (Cartões)** > **Alert card (Cartão de alerta)**

Procedimento

1. Carregar o registro de pessoa da pessoa a quem o cartão de alerta será atribuído
2. Na guia Alert card (Cartão de alerta), clique em Record card (Registrar cartão).
   - Uma janela pop-up é exibida: **Select threat level (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: **Recording badge ID (Registrando ID do crachá)**
4. Insira os dados habituais do cartão correspondentes à instalação do local e clique em **OK**
   - O cartão de alerta que você registrou é exibido na lista na guia **Alert card (Cartão de alerta)**.

17.4 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 cadastramento configurado em sua estação de trabalho.
– Um cartão físico adequado está disponível para cadastramento no sistema como um cartão temporário.
– O destinatário do cartão temporário tem pelo menos mais um cartão.

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 **Blocking (Bloqueio)**: **Personnel data (Dados de funcionários)** > **Blocking (Bloqueio)**.
2. Na lista de cartões, selecione o cartão pessoal marcado como bloqueado na coluna **Lock(s) (Bloqueio(s))**.
3. Clique em **Release temporary lock (Liberar bloqueio temporário)**
   Observe que o registro permanece na lista **Blocking (Bloqueio)**. A lista contém apenas um histórico de todos os bloqueios do registro de funcionário atual, antigos e atuais.

Observações sobre os cartões temporários

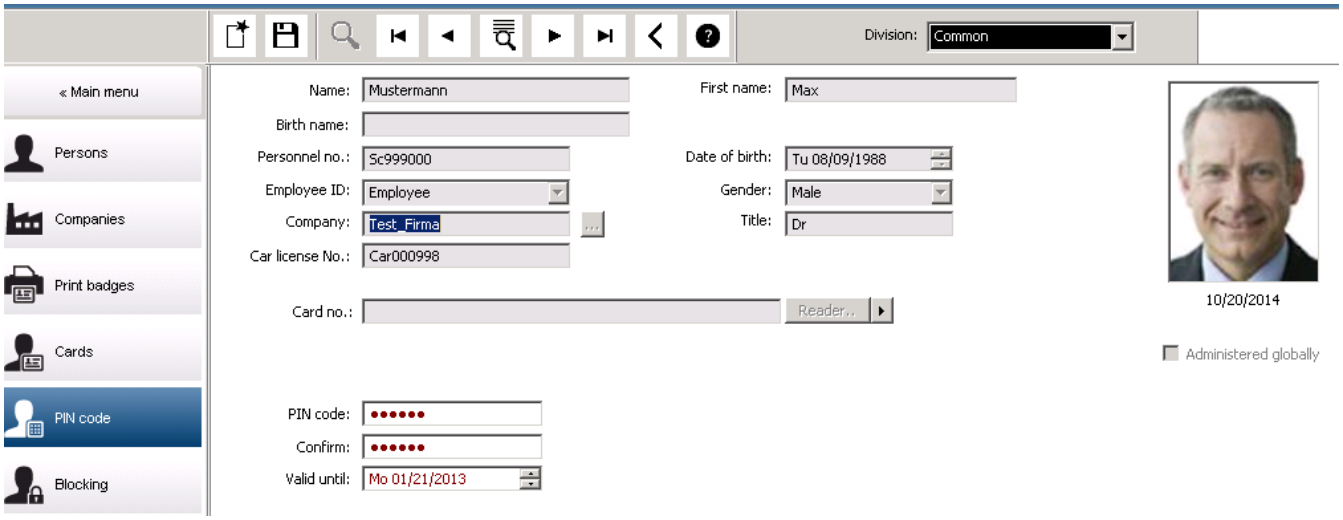
- O sistema não permite que os próprios cartões temporários sejam substituídos por outros cartões temporários.
- O sistema não permite que um cartão pessoal tenha mais de um cartão temporário.
- Para ver um resumo rápido de todos os cartões em posse de um titular, passe o mouse sobre o pequeno painel à extrema esquerda, rotulado **Registered (Registrada)**, na barra de status da janela de diálogo principal.

17.5 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.

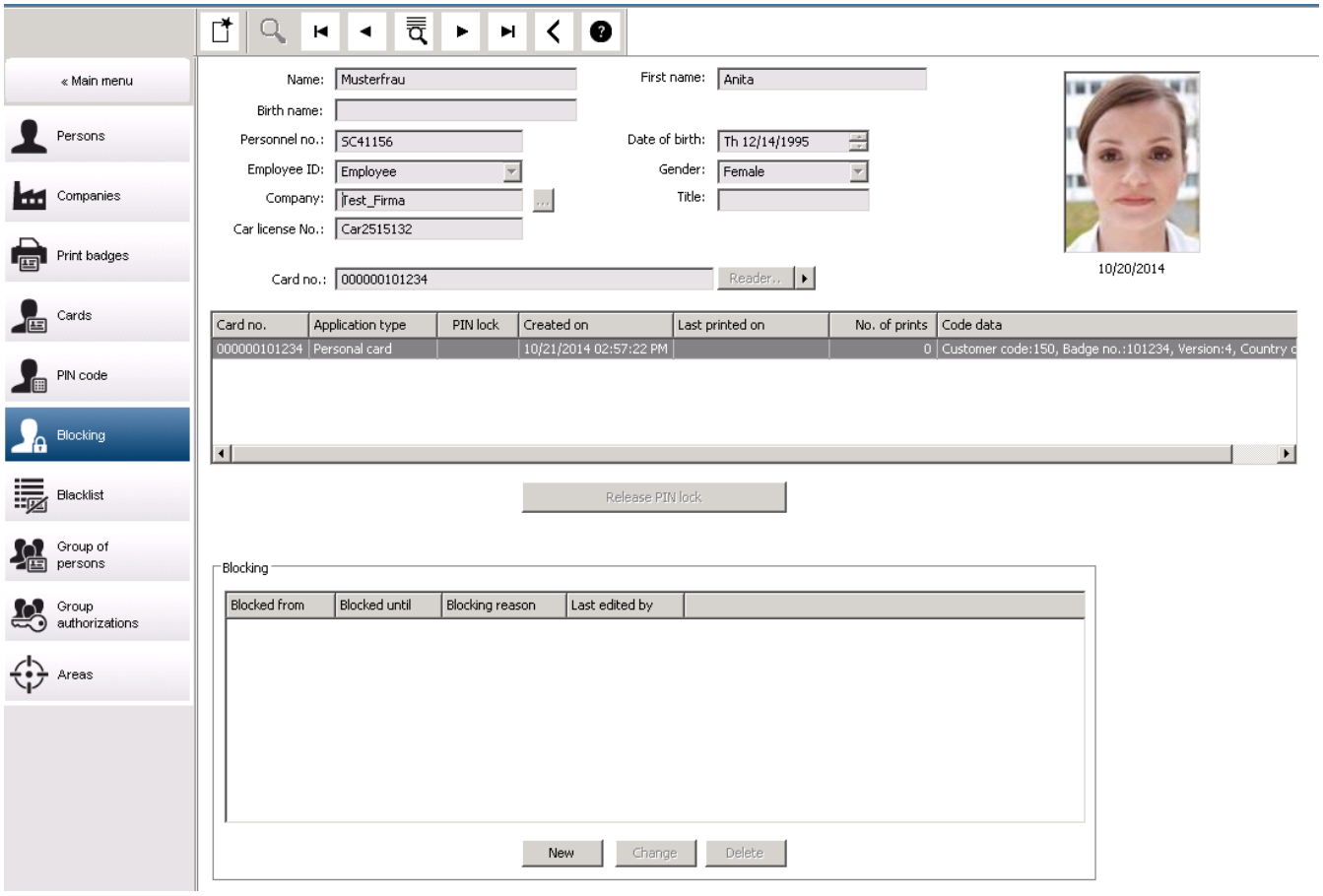
Código PIN para armar sistemas de detecção de intrusão (IDS)
Um PIN de 4 a 8 dígitos deve ser inserido (padrão = 6 – o mesmo comprimento do PIN de verificação). Esse PIN será usado para armar um IDS.
A exibição desses campos pode ser parametrizada. O controle estará disponível somente se o controle **separate IDS PIN (PIN de IDS separado)** estiver ativado.
– 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.

17.6 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.

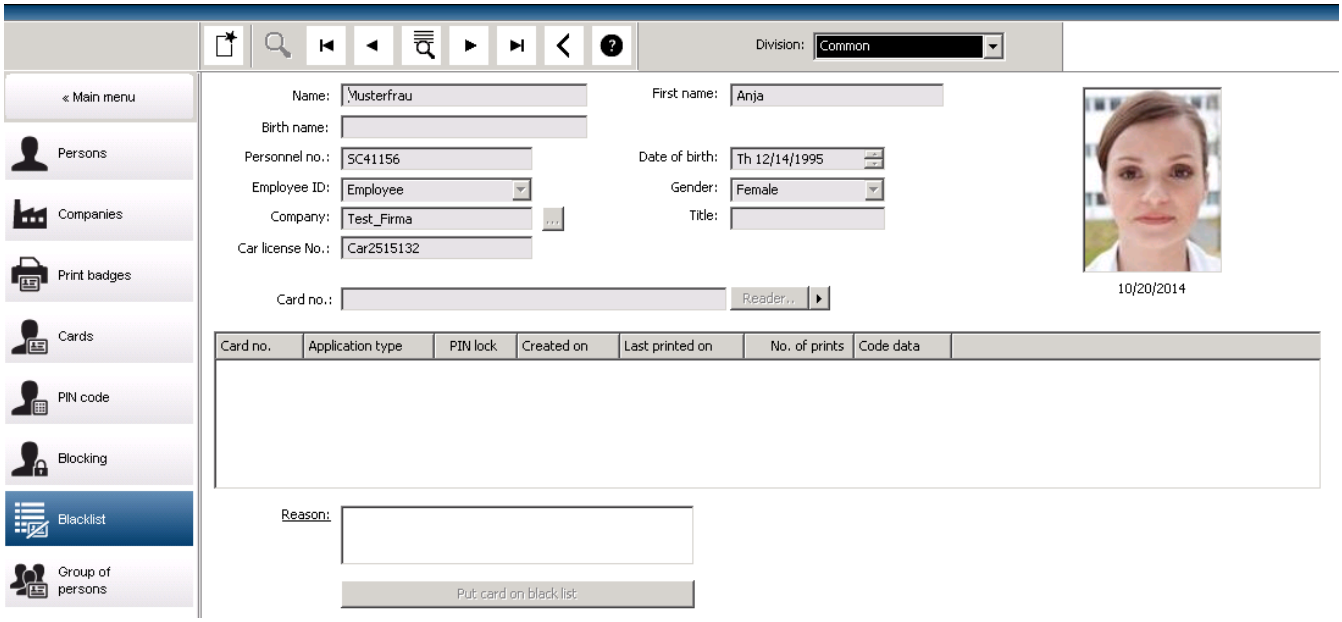
Aviso!
O bloqueio se aplica à pessoa, e não a uma credencial específica. Portanto, não é possível cancelar ou evitar o bloqueio através da atribuição de um novo cartão de identificação.

17.7 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)**

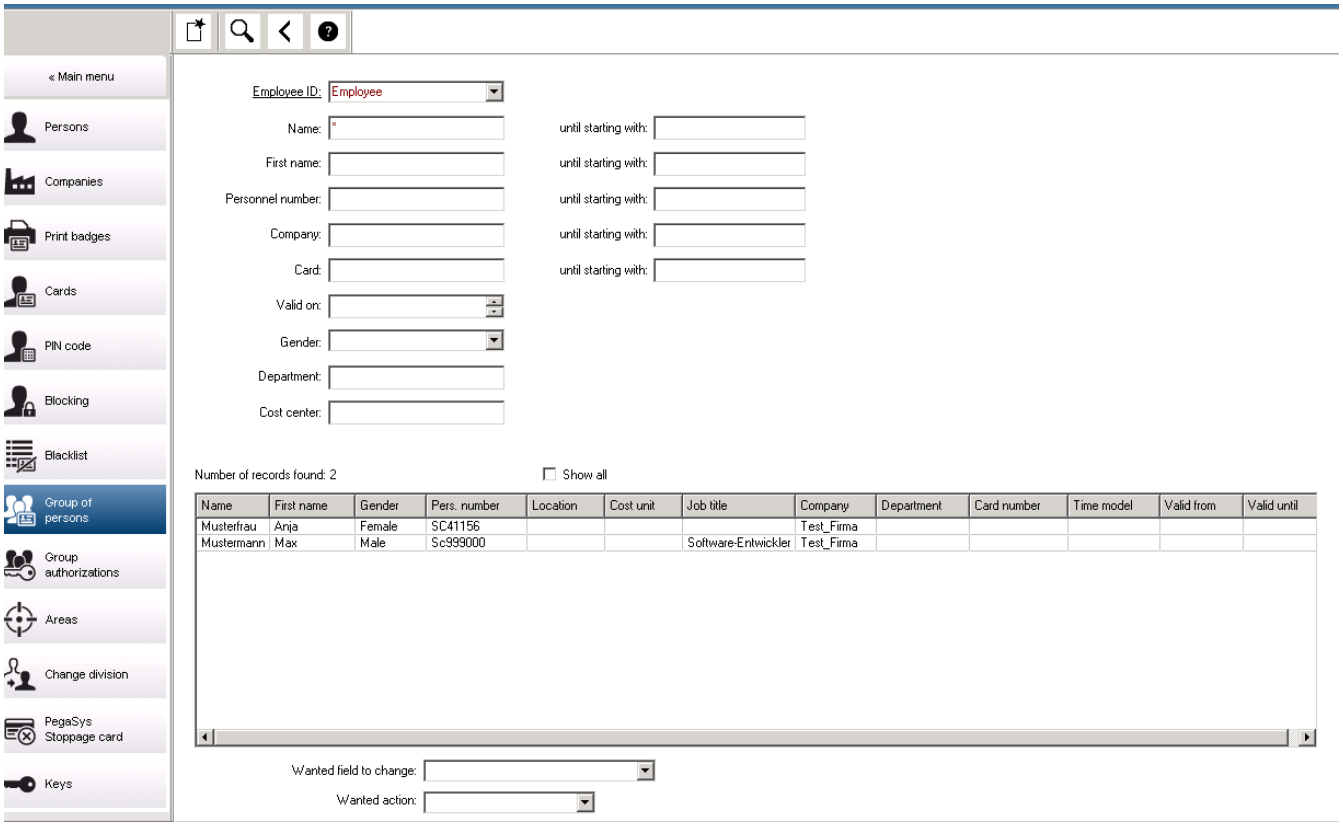
1. Selecione a pessoa cujo cartão de identificação deve ser inserido na lista negra.
2. Se mais de um cartão tiver sido atribuído a esse usuário, selecione o cartão na lista **ID card No (Número do cartão de identificação)**.
3. Insira o motivo para inserção do cartão na lista negra no campo de entrada **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.

17.8 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

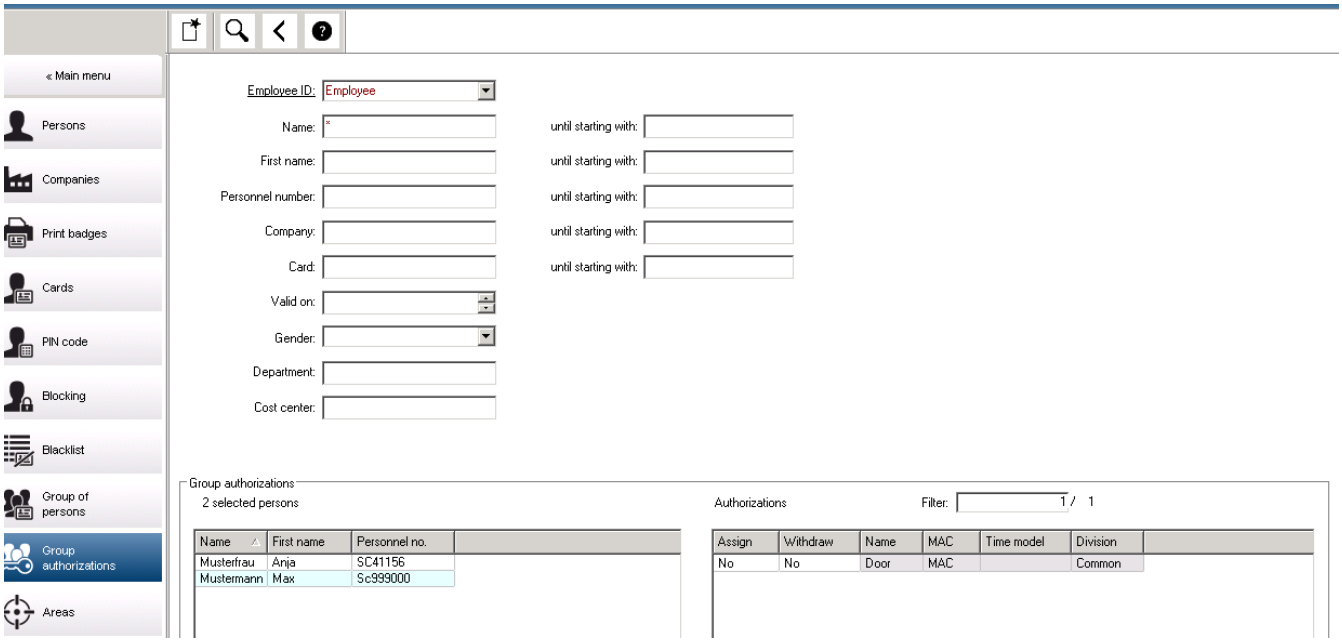
Em seguida, a opção de modificação pode ser selecionada:

- 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.

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.

18 Definição de autorizações e perfis de acesso

18.1 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)**

18.2 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.
– 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.

19 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.

19.1 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.

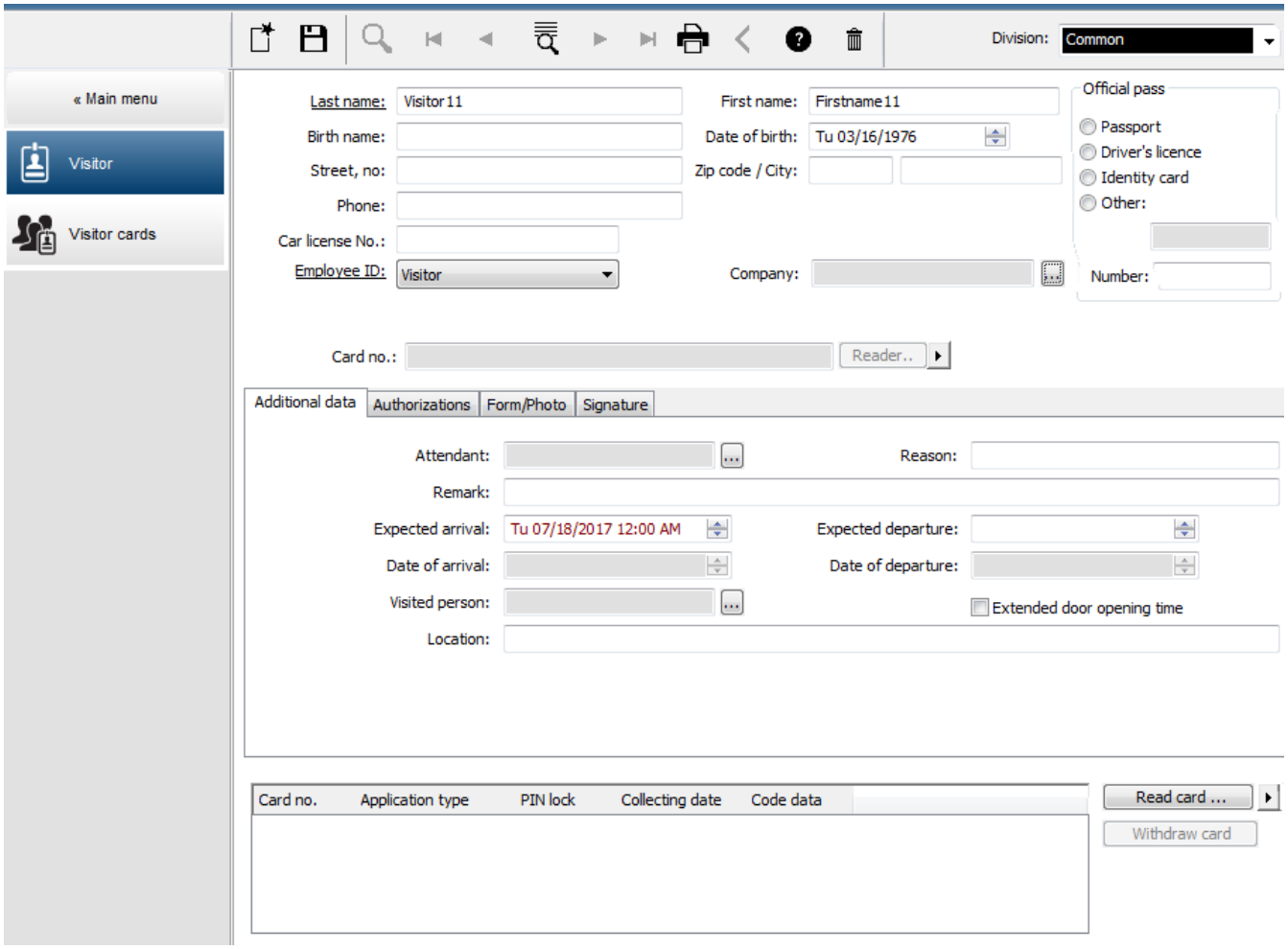
- A caixa de diálogo **Visitantes** é usada para a inserção de dados e autorizações de acesso de visitantes.
- A caixa de diálogo **Cartões de visitantes** regula o registro e o cancelamento dos cartões de visitante.

Caixa de diálogo: Visitors (Visitantes)

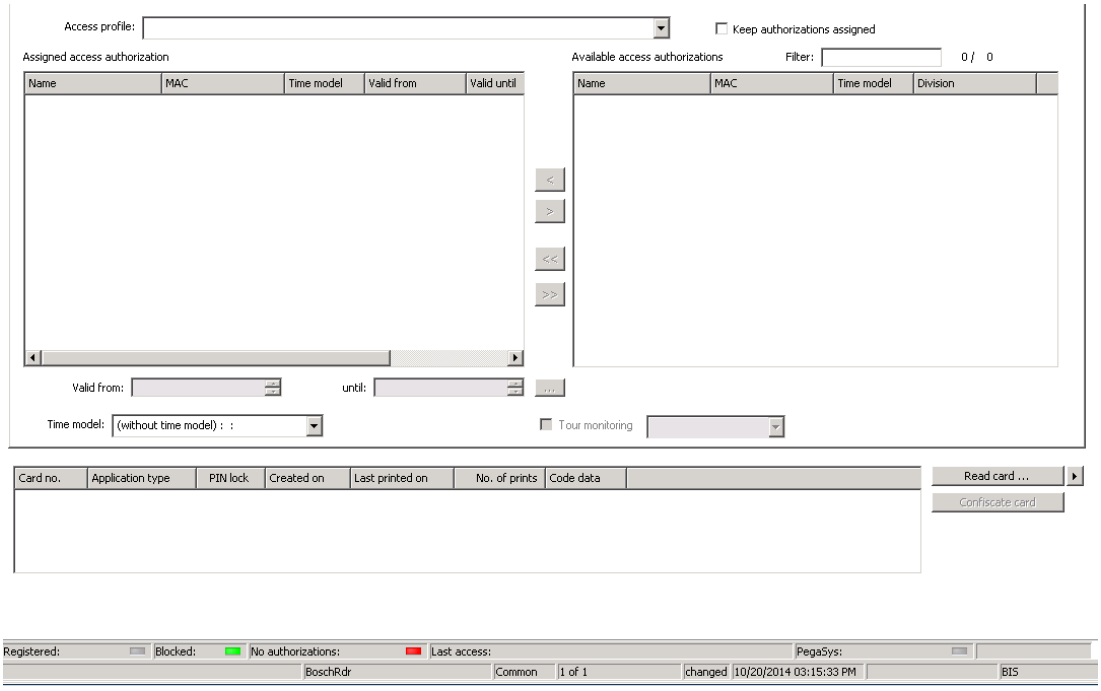
Os visitantes têm um status estritamente separado das outras pessoas e, portanto, são processados em uma caixa de diálogo separada. Pessoas com identificação de **visitante** não podem ser nem criadas na caixa de diálogo **Persons (Pessoas)**, nem ter cartões de identificação registrados para elas na 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.



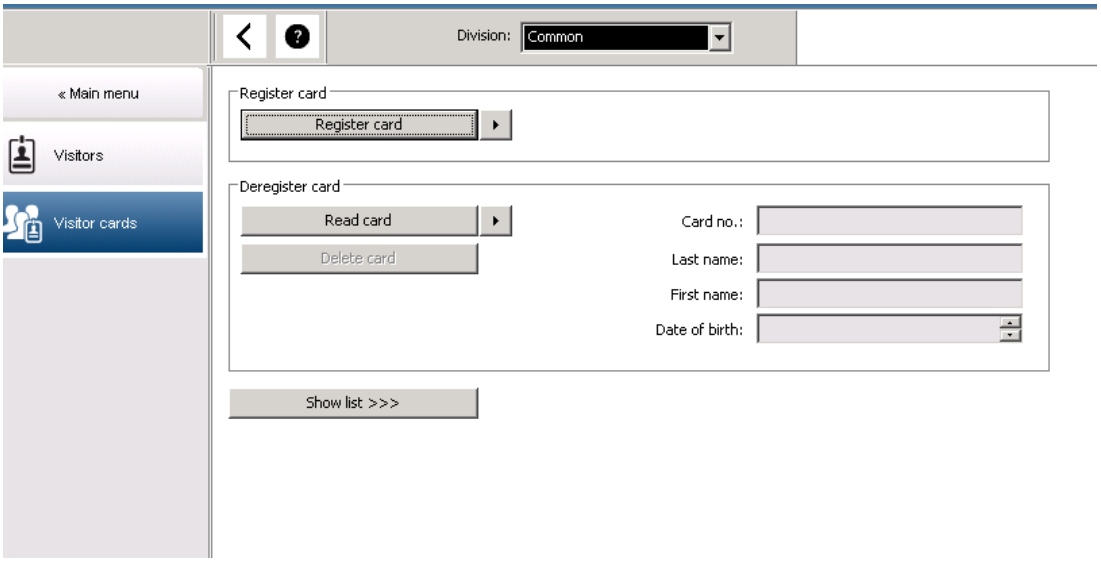
O **Reason (Motivo)** da visita, a **Location (Localização)** da visita do visitante e uma **Remark (Observação)** podem ser digitados nos campos abaixo.
Se você optar por digitar dados nos campos **expected arrival (chegada prevista)** e **expected departure (partida prevista)**, estas datas também 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.



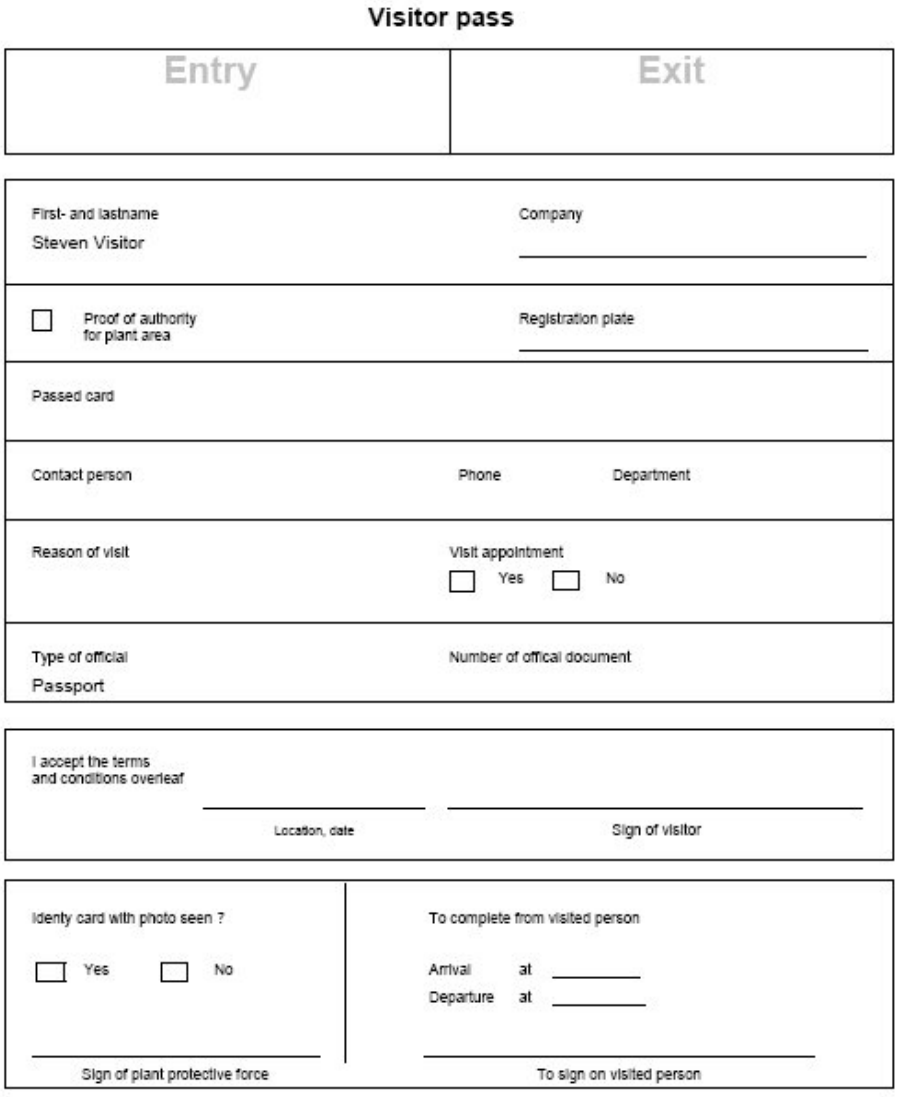
Clique no botão **Register ID card (Registrar cartão de identificação)** para fazer o registro.
O procedimento de registro descrito anteriormente (seções **Pessoas** e **Cartões de identificação** no capítulo **Dados de funcionários**) é usado junto com o número do cartão para detectar o cartão de identificação. 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

19.2 Visitante atrasado

A tela **Visitante atrasado** permite ao cliente verificar onde os visitantes permanecem dentro das instalações, e se eles possivelmente ultrapassaram a hora da saída prevista.
Os usuários autorizados do BIS precisam ter um link configurado em sua tela inicial para poderem visualizar este site.

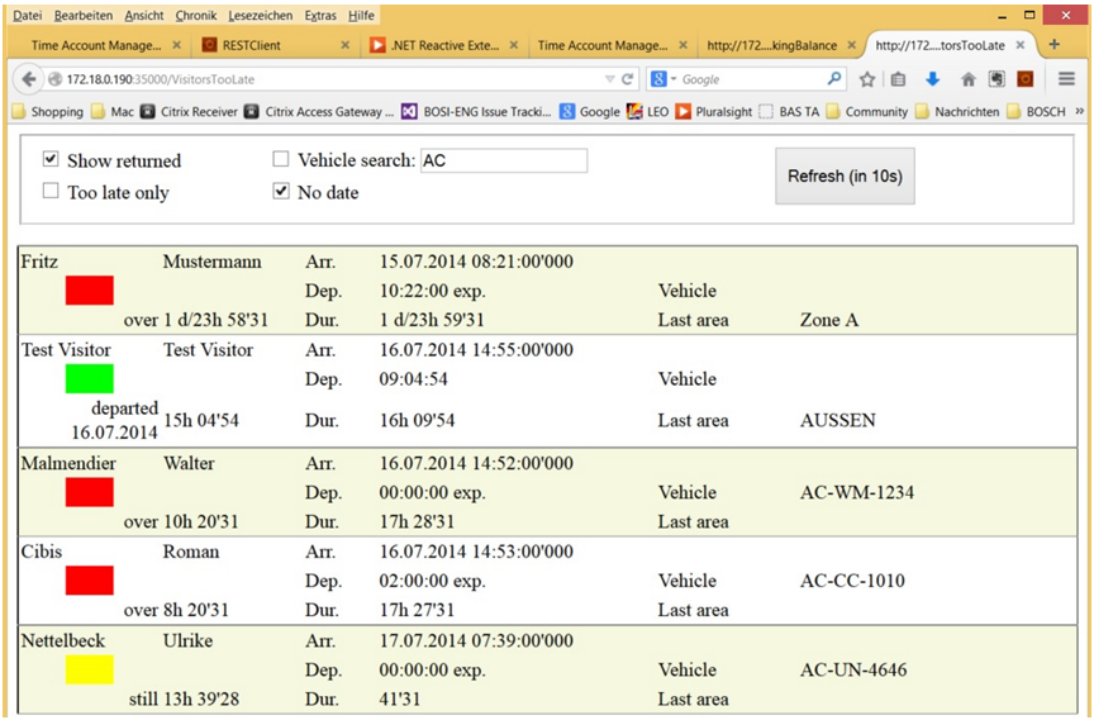
Além disso, é possível configurar um gatilho no BIS para o dispositivo de DMS, de modo que um alarme seja ativado caso uma mensagem de Visitante atrasado seja emitida, o que por sua vez abre uma tela no site com a última localização conhecida da respectiva pessoa.
[ver tela do site]

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)**.

20 Gerenciamento de estacionamentos

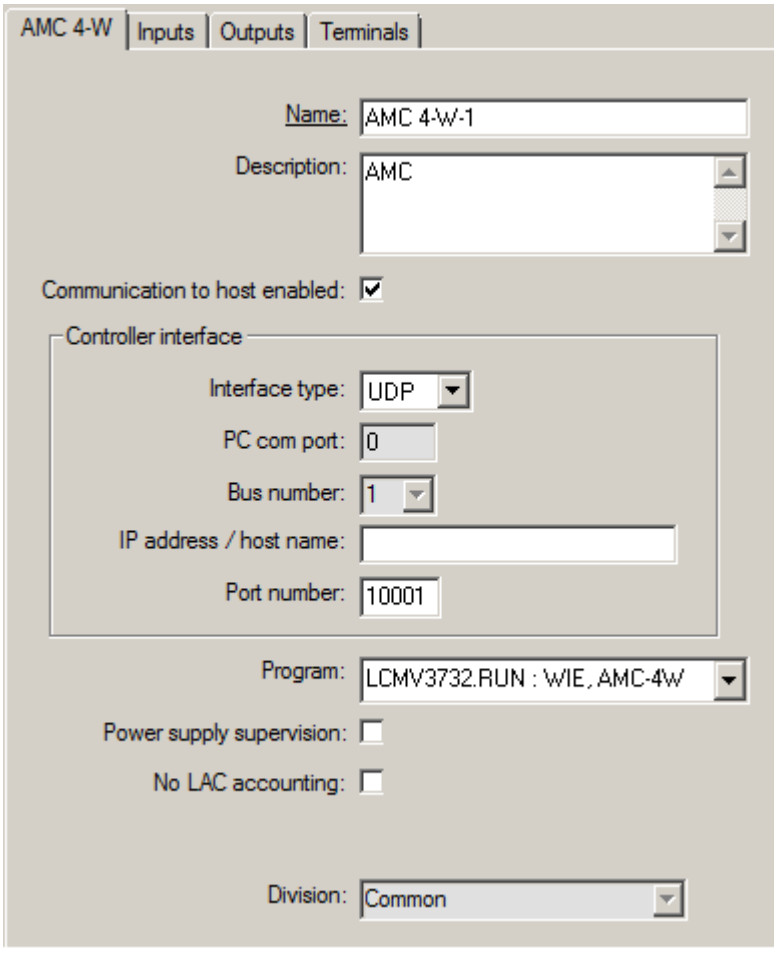
20.1 Autorizações para várias zonas de estacionamento

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 tiver várias autorizações pode acessar ambos os tipos de vaga, seja deficiente ou não O AMC tenta alocar a pessoa de acordo com a ordem sequencial configurada das zonas de estacionamento. Caso uma zona esteja cheia, a pesquisa continua com a próxima zona autorizada e livre.
Cálculo do contador no MAC e 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 entra online.
2) As entradas e saídas de um estacionamento são divididas entre diferentes AMCs:
=> O MAC faz a contagem para o AMC no caso de uma operação online. Ao operar offline, os AMCs permitem o acesso (se assim configurado), mas não fazem a contagem.
Se vários AMCs controlarem um estacionamento, ative a caixa de seleção **Sem contagem do AMC** na configuração do AMC



20.2 Visão geral do estacionamento de veículos

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	--

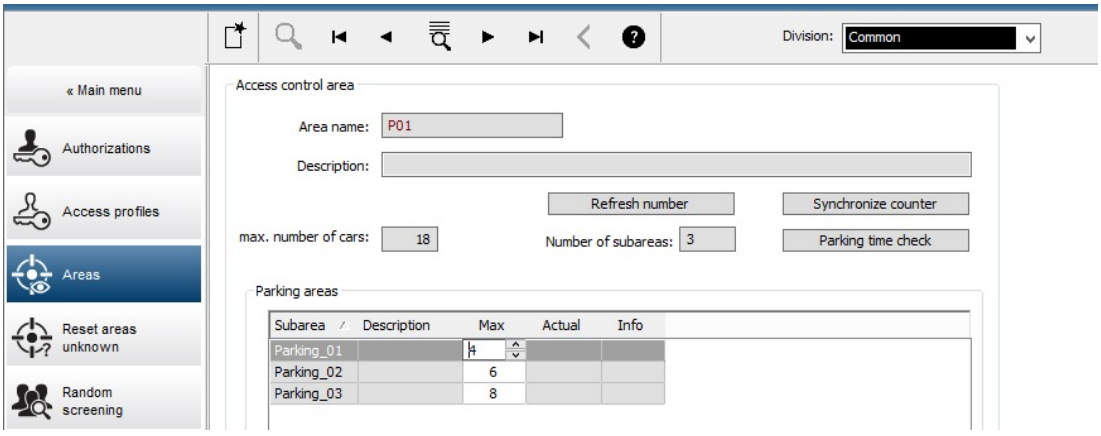
20.3 Gerenciamento do estacionamento ampliado

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

1. Selecionar uma área de estacionamento
2. No painel **Áreas de estacionamento**, ajuste o valor na coluna **Máx.** para o novo número de vagas de estacionamento para a área.



Menu principal > **Dados do sistema** > **Áreas**

21 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.

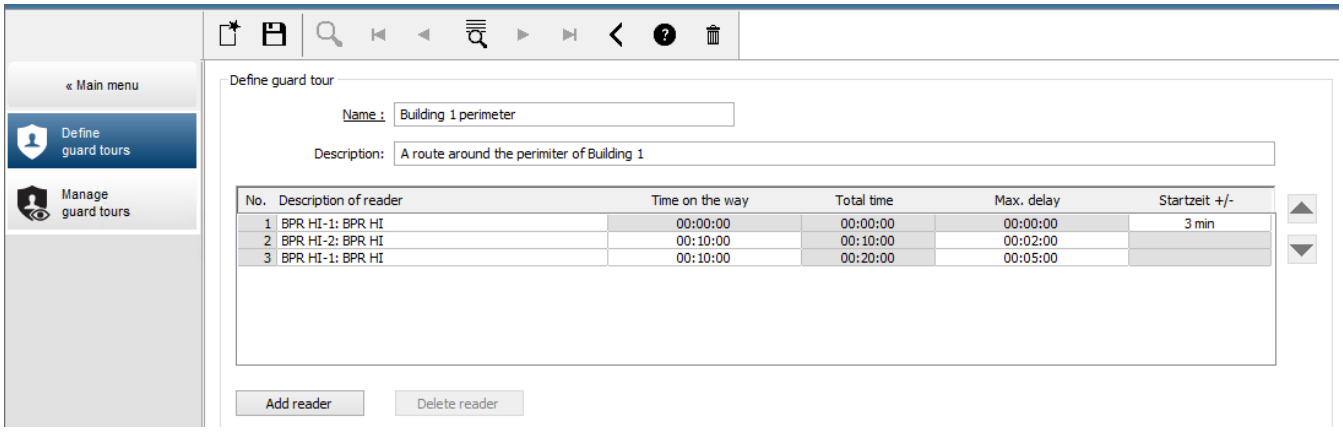
A Ronda de segurança consiste em uma série de leitores com tempos de caminhada aproximados entre eles. O atraso máximo tolerável entre leitores, e o desvio tolerável (+/-) desde a hora de início, também são atributos da Ronda de segurança. Desvios fora dessas tolerâncias definidas podem acionar alarmes 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.

21.1 Definição de rondas de segurança

Selecione **Guard tours (Rondas de segurança)** > **Define guard tours (Definir rondas de segurança)**



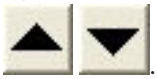
- No campo de texto **Name (Nome)**, insira um nome para a Ronda de segurança
- No campo de texto **Description (Descrição)**, insira uma descrição mais detalhada da rota (opcional).

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  .

21.2 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 –  . 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.

21.3 Monitoramento de rondas (anteriormente controle de caminhos)

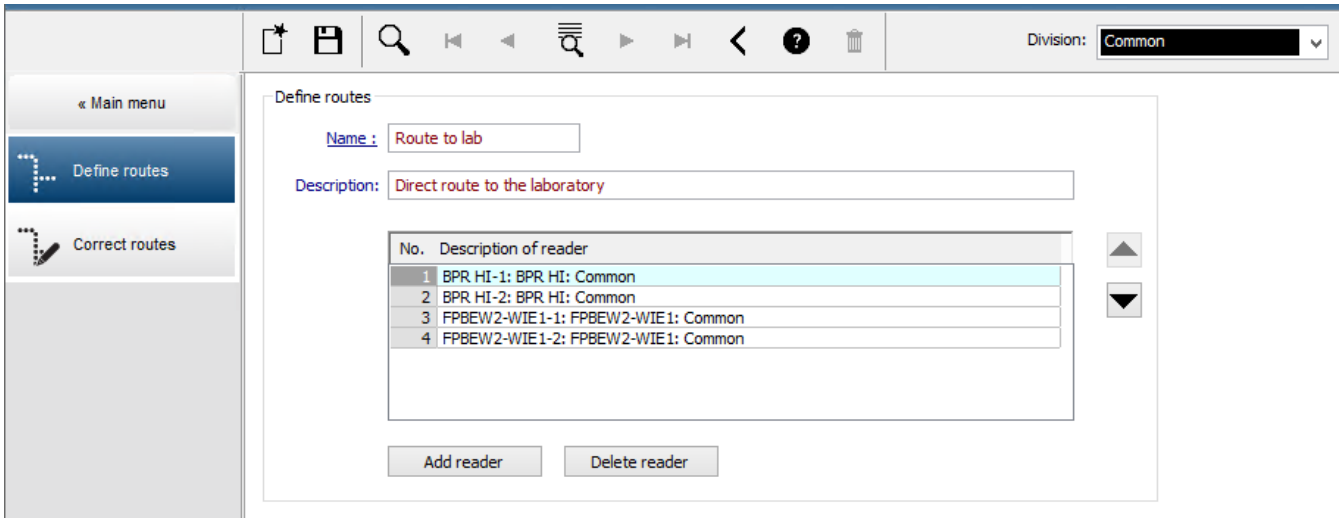
Introdução

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)**.

22 Triagem aleatória de funcionários

O processo de triagem aleatória

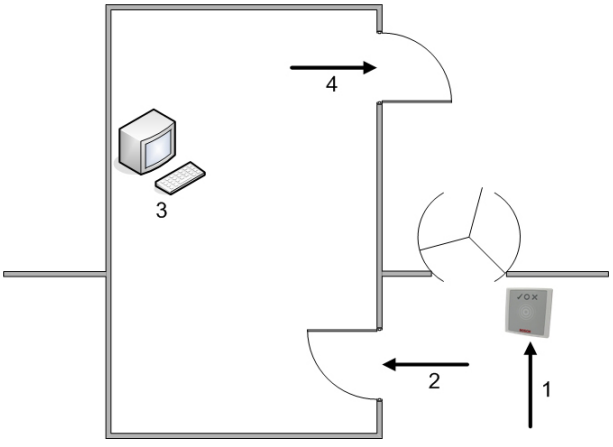
1. Um titular do cartão exibe seu cartão em um leitor configurado para triagem aleatória.
   Observação
   Só as pessoas autorizadas a passar através da entrada no sentido definido podem ser selecionadas aleatoriamente. Como as autorizações são verificadas antes da triagem aleatória ser feita, qualquer pessoa não autorizada será imediatamente barrada, e não será incluída no processo de seleção.
2. Se a seleção aleatória selecionar esta pessoa para a triagem, o seu cartão será bloqueado no sistema inteiro.
   - O evento é registrado no histórico de eventos do sistema.
   - A caixa de diálogo **Blocking (Bloqueio)** recebe um registro de duração ilimitada marcado em **Random screening (Triagem aleatória)**. [Figura abaixo – número 1]
   - A barra de status das caixas de diálogo de dados de funcionários do Access Engine exibe os "LEDs" Bloqueado (vermelho) e a Triagem aleatória junto com ele (piscando em violeta).

Aviso!
As pessoas para as quais o parâmetro **Excluded from random screening (Excluído da triagem aleatória)** foi definido (na caixa de diálogo **Cards (Cartões)**, guia **Other data (Outros dados)**) não serão incluídas no processo de triagem.

3. A pessoa selecionada aleatoriamente é convidada a passar por controles adicionais em uma cabine de segurança separada.
4. Após a realização destes controles, o vigilante de segurança redefine o bloqueio na caixa de diálogo **Blocking (Bloqueio)** da seguinte forma:
   - Selecione o bloqueio apropriado na lista de controle **Blocking (Bloqueio)**.
   - Clique no botão **Delete (Excluir)**.
   - Confirme a exclusão clicando em **Yes (Sim)**.

A pessoa triada aleatoriamente agora pode usar seu cartão novamente em todos os leitores para os quais estiver autorizada.

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.

23 Usando o visualizador de eventos

Introdução

O Visualizador de eventos permite que operadores devidamente autorizados examinem eventos registrados pelo sistema e produzam relatórios, impressos ou na tela.

Para recuperar e exibir os registros desejados do banco de dados do Log de eventos, defina critérios de filtragem e clique em **Refresh (Atualizar)**  .

Os critérios de filtragem podem ser definidos de diversas formas:

Relative (Relativo)	Para selecionar eventos relativos ao momento atual.
Interval (Intervalo)	Para selecionar eventos dentro de um intervalo de tempo qualquer
Total	Para selecionar eventos independentemente do momento 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)**

23.1 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)
   - Code data (Data do código)
   - 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.

23.2 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)
   – Code data (Data do código)
   – 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.

23.3 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)
   – Code data (Data do código)
   – 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.

24 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)**.

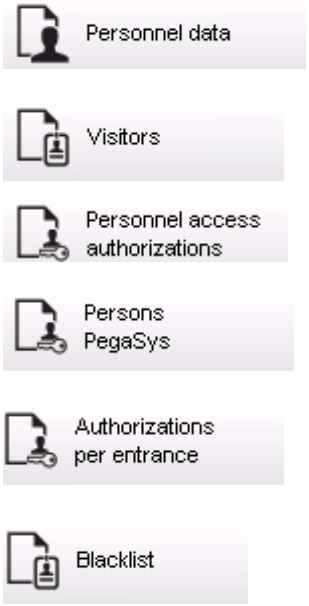
Uso da barra de ferramentas de relatórios

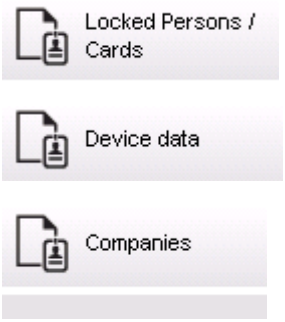
Clique em  para exibir uma visualização antes de imprimir.
A visualização tem sua própria barra de ferramentas:

- 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.

24.1 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.

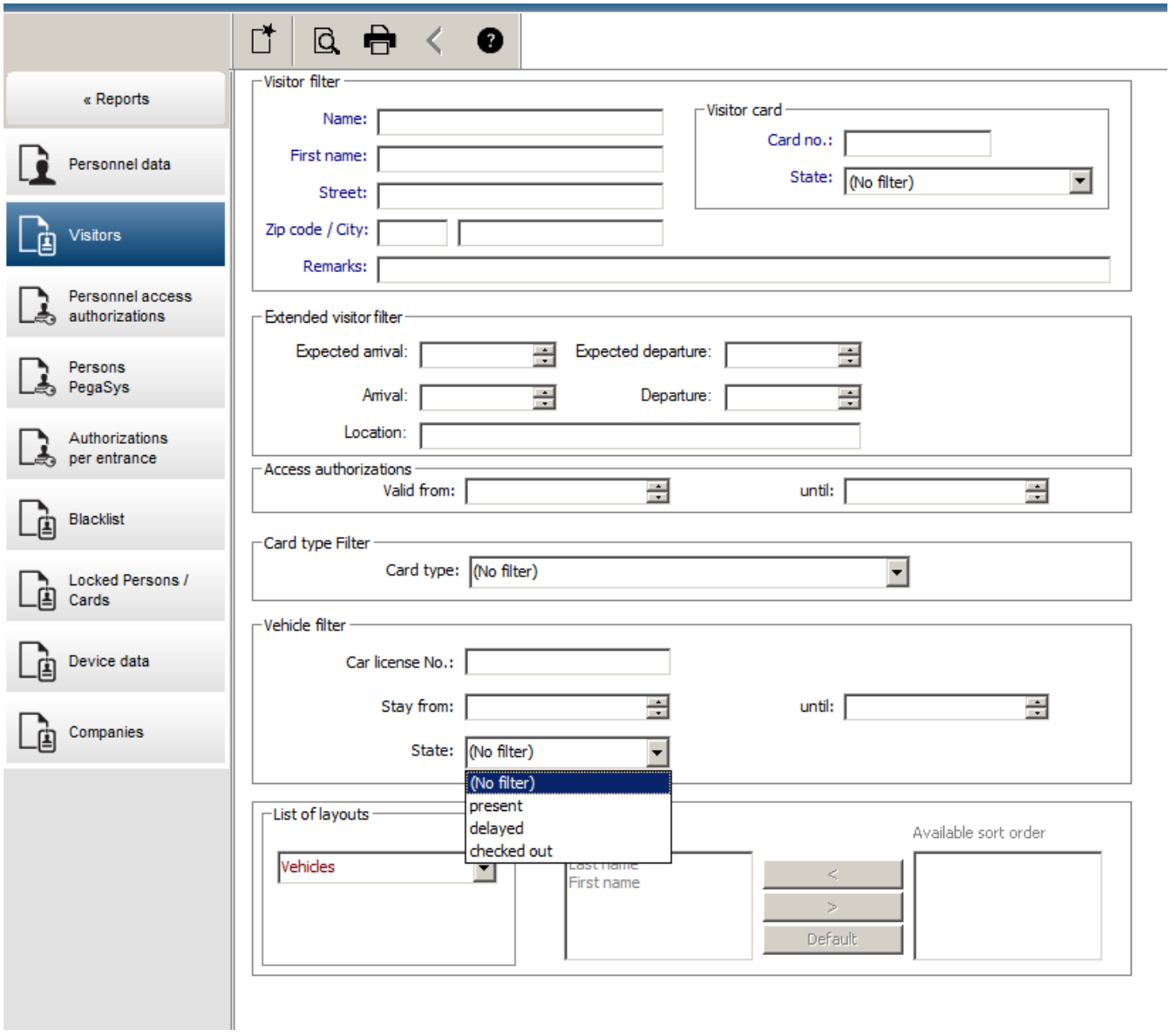
Utilize asteriscos, por exemplo, para encontrar empresas que começam com uma letra específica.

24.1.1 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:

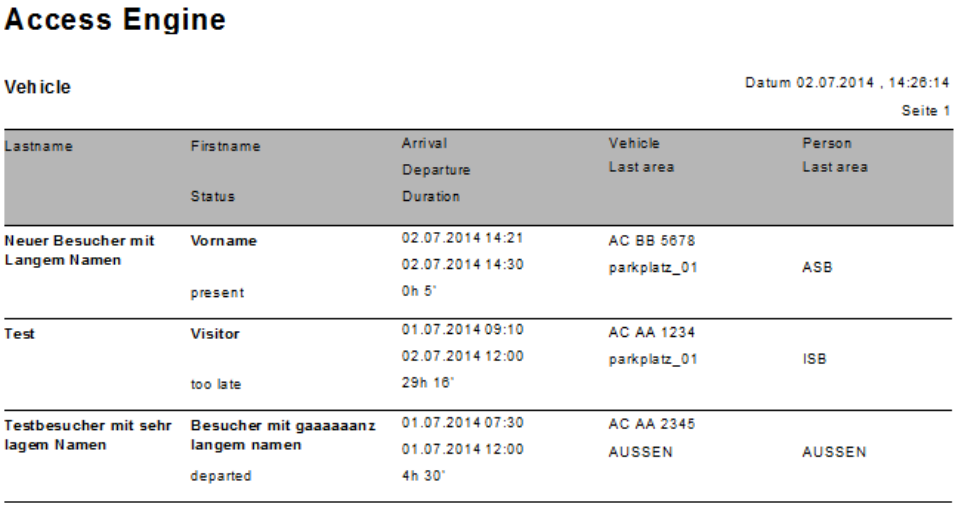
– Presente: Visita ainda não é terminada e o tempo ainda não é esgotado.
– Atrasada: Visita ainda não é terminada, mas tempo já está esgotado.
– Saída registrada: O visitante devolveu todos os cartões de acesso.



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

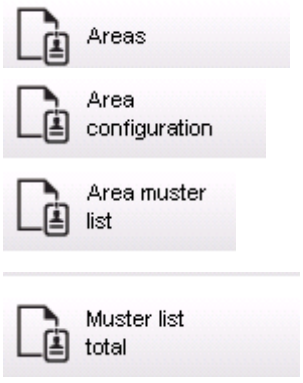
Datum 02.07.2014 , 14:26:14
Seite 1

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

24.2 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.

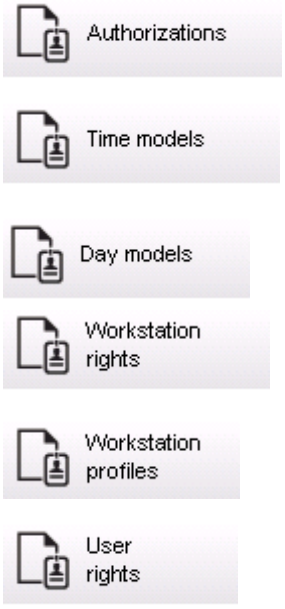
Relatório: Configuração de áreas
As áreas definidas e suas subáreas com um marcador que representa estacionamentos e o número máximo de pessoas ou carros.

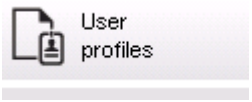
Relatório: Lista de convocação da área
Além de serem listadas de acordo com dados puramente numéricos, as pessoas de uma área também podem ser listadas por nome.
Com os tempos de leitura das áreas individuais, estes relatórios também contêm os tempos de cada pessoa individual.

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.

24.3 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.

25 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 116*

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 116*

25.1 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.

25.2 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 121*

25.3 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.

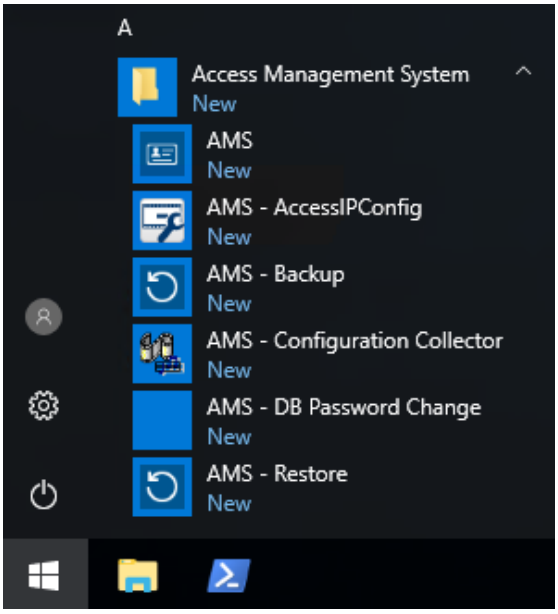
Consulte

- *Criação de um cartão de alerta, página 136*

26 Backup e restauração

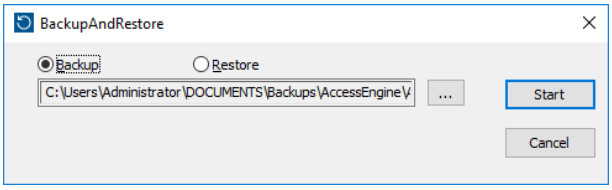
A função **Backup and Restore (Backup e restauração)** permite reconstruir a instalação em um computador diferente se o computador original falhar.
Backup and Restore (Backup e restauração) só pode ser iniciado em uma máquina onde o servidor AMS estiver instalado. Para conveniência, dois atalhos são criados:

– **AMS - Backup** para criação de um backup
– **AMS - Restore** para restauração de um backup:

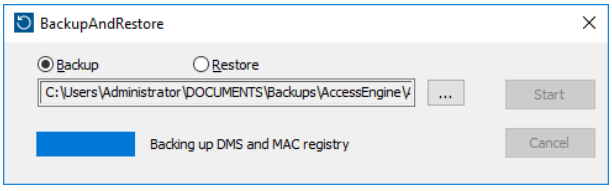


26.1 Procedimento de backup

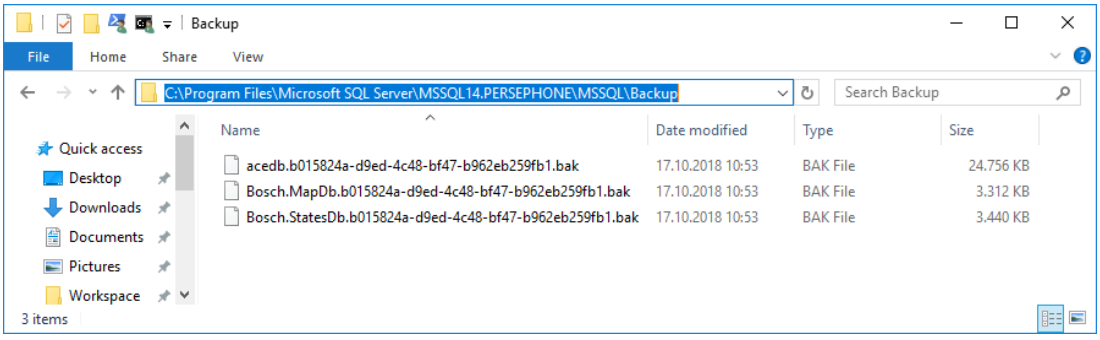
1. Clique no atalho **AMS - Backup**.
   Isso iniciará a ferramenta **Backup and Restore (Backup e restauração)**:



2. Insira um caminho onde o arquivo GZIP deve ser salvo.
3. Clique em **Start (Iniciar)** para iniciar o backup.
   Uma barra de progresso será exibida.
   Ao concluir, o arquivo GZIP será criado.



O local de backup do banco de dados depende da versão do SQL Server e do nome da instância de banco de dados.
Por exemplo, se o nome da instância do SQL Server do AMS for "PERSEPHONE", o backup estará localizado em:



IMPORTANTE: para garantir a segurança dos dados, a Bosch recomenda fortemente que você copie essa pasta e o arquivo GZIP para um lugar seguro e remoto. Não deixe a única cópia do backup no computador do servidor DMS.

Aviso!
O log de eventos é salvo no seguinte caminho padrão (o instalador poderá escolha um caminho diferente):
`C:\Program Files (x86)\Access Management System\Access Engine\AC\LgfLog\`

26.2 Procedimento de restauração

Pré-requisitos

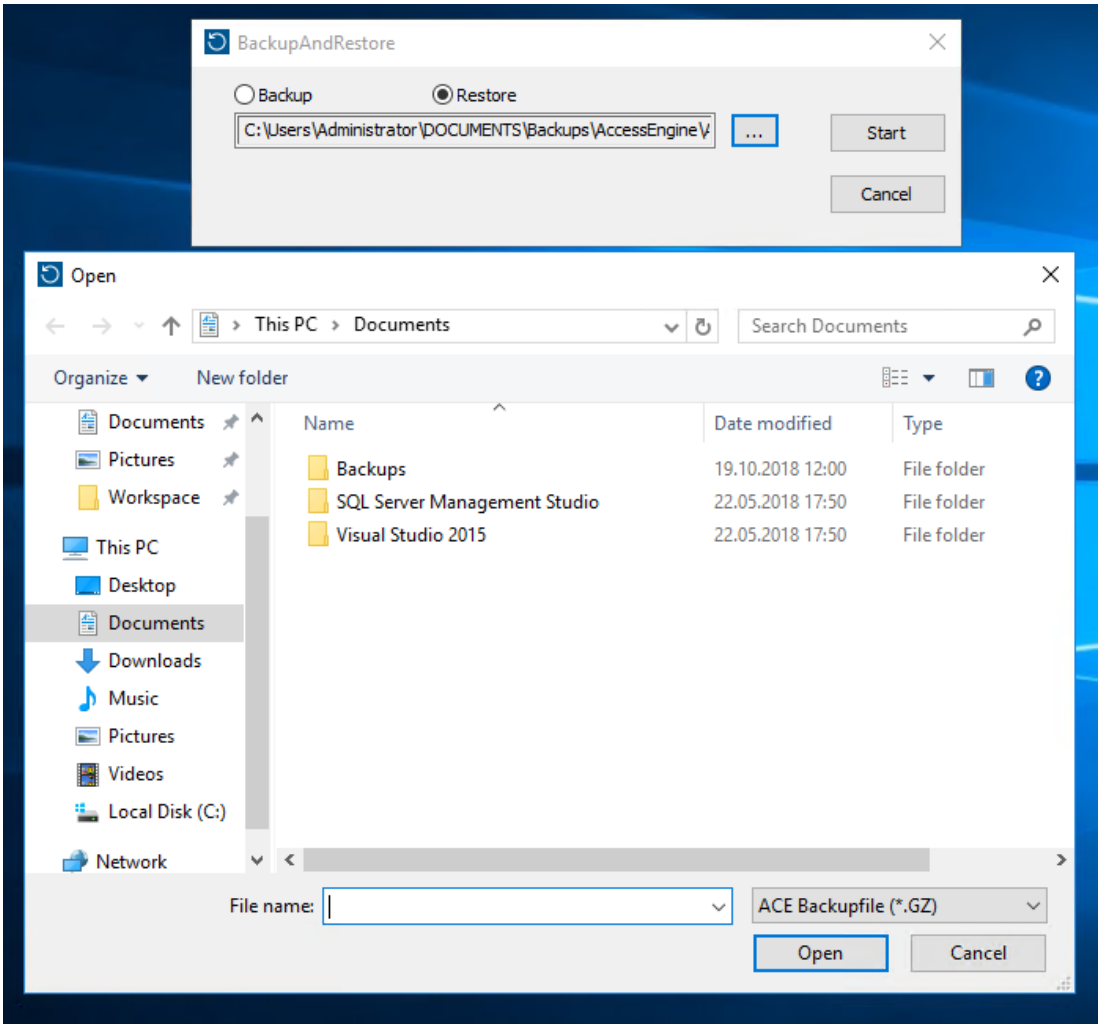
- O arquivo GZIP criado pela ferramenta **Backup and Restore (Backup e restauração)**.
- Os dados de backup criados pelo SQL Server na pasta de backup do SQL Server.
- Uma conta do SQL com direitos **sysadmin**, como `sa`.

Observações sobre o computador de destino

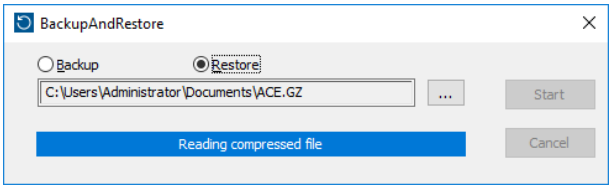
- Para executar a configuração restaurada, o computador de destino (onde o backup é restaurado) exigirá pelo menos licenças equivalentes àquelas do computador onde o backup foi criado.
- Todos os clientes do computador de destino exigirão os certificados gerados pela instalação no computador de destino, não aqueles gerados pela instalação no computador original.
  Consulte o guia de instalação para instalação dos certificados de cliente.

Procedimento

1. No programa AMS, clique em **File (Arquivo)** > **Exit (Sair)** para encerrar todos os serviços em execução.
2. Quando o programa for encerrado, execute o aplicativo Windows **Services** e verifique se todos os serviços do `Access Engine` e `Access Management System` foram encerrados.
3. Clique no botão Iniciar do Windows > **AMS - Restore**
4. Clique no botão **[...]** para localizar e selecionar o arquivo de backup GZIP.



5. Clique em **Start (Iniciar)** para iniciar o processo de restauração.
6. Insira as credenciais de login **SQL sysadmin**.
   O processo de restauração é iniciado



7. Quando o processo de restauração for concluído, execute o aplicativo Windows **Services** e verifique se todos os serviços do `Access Engine` e `Access Management System` foram reiniciados.
   Se não, reinicie-os manualmente.
8. Inicie o **AMS Map View** na área de trabalho.
9. Localize e clique com o botão direito no MAC no Map View.
10. Selecione **Cold start MAC (Executar o arranque a frio do MAC)** para sincronizar novamente os dados do backup com os dados do sistema atual.

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.

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.

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.

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.

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 (Controlador de acesso principal)

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 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 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.

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.

Servidor MAC

Hardware: um computador em uma rede do Access Engine, separado do servidor DMS, onde um MAC ou um RMAC é executado.

Sistema de gerenciamento de dados (DMS)

Um processo de nível superior para gerenciamento de dados do controle de acesso no Access Engine. O DMS fornece dados aos MACs que, por sua vez, fornecem dados aos AMCs.

Sistema de gerenciamento de dados (DMS)

Um processo de nível superior para gerenciamento de dados do controle de acesso no Access Engine. O DMS fornece dados aos MACs que, por sua vez, fornecem dados aos AMCs.

SmartIntego

Sistema de bloqueio digital da SimonsVoss Technologies. O SmartIntego já vem integrado em alguns sistemas de controle de acesso da Bosch.

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