# Visitor Management V5.5

Com Mobile Access

**pt-BR** Manual do usuário

# Sumário

# 1 Segurança

**Use o software mais recente**

Antes de operar o dispositivo pela primeira vez, certifique-se de instalar a versão de software aplicável mais recente. Para obter funcionalidades, compatibilidade, desempenho e segurança consistentes, atualize regularmente o software durante toda a vida útil operacional do dispositivo. Siga as instruções na documentação do produto relativas às atualizações de software.

Os links a seguir fornecem mais informações:

– Informações gerais: https://www.boschsecurity.com/xc/en/support/product-security/
– Avisos de segurança, essa é uma lista de vulnerabilidades identificadas e soluções propostas: https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html

A Bosch não assume qualquer responsabilidade por qualquer dano causado pela operação de seus produtos com componentes de software desatualizados.

# 2 Introdução

## 2.1 Sobre o gerenciamento de visitantes da Bosch

O Visitor Management, doravante chamado de VisMgmt, é uma ferramenta de software baseada em navegador que opera em tandem com os sistemas de controle de acesso da Bosch. Ele gerencia os visitantes de um local com controle de acesso, incluindo a programação de visitas, os dados profissionais dos visitantes, documentos e contratos associados e a atribuição de credenciais temporárias.
A interface de usuário pode ser personalizada e qualquer usuário pode alterar o idioma imediatamente sem se desconectar.
Os principais usuários e casos de uso são:

| Tipo de usuário | Casos de uso |
|---|---|
| Recepcionista | Registro de novos visitantes e visitas<br>Aprovação e recusa de visitas<br>Inclusão de visitantes na lista negra<br>Atribuição e cancelamento de cartões de visitante<br>Gerenciamento dos documentos associados<br>Monitoramento do número de visitantes no local |
| Visitante | Registro próprio e pré-registro<br>Criação e manutenção de um perfil de visitante<br>Assinatura de documentos |
| Host | Gerenciamento de programações e listas de visitas e visitantes<br>Pré-registro de visitas |
| Administrador | Definição de configurações globais<br>Personalização do comportamento da ferramenta e da interface de usuário<br>Adicionalmente:<br>Todos os casos de uso de Recepcionista |

## 2.2 Sobre o Mobile Access

Mobile Access é o controle de acesso de pessoas que usam credenciais virtuais armazenadas em um dispositivo móvel, como um smartphone. As credenciais virtuais são mantidas no sistema de controle de acesso primário, ou ACS.

- Os operadores do ACS geram, atribuem e enviam essas credenciais virtuais a pessoas por meio de um aplicativo Web de cooperação.
- Os portadores de credenciais móveis operam leitores de controle de acesso via Bluetooth por meio de um aplicativo Mobile Access em seus dispositivos móveis.
- Os instaladores de sistemas Mobile Access configuram leitores de controle de acesso via Bluetooth por meio de um aplicativo de configuração especial em seus dispositivos móveis.
- O sistema não armazena dados pessoais em dispositivos móveis.

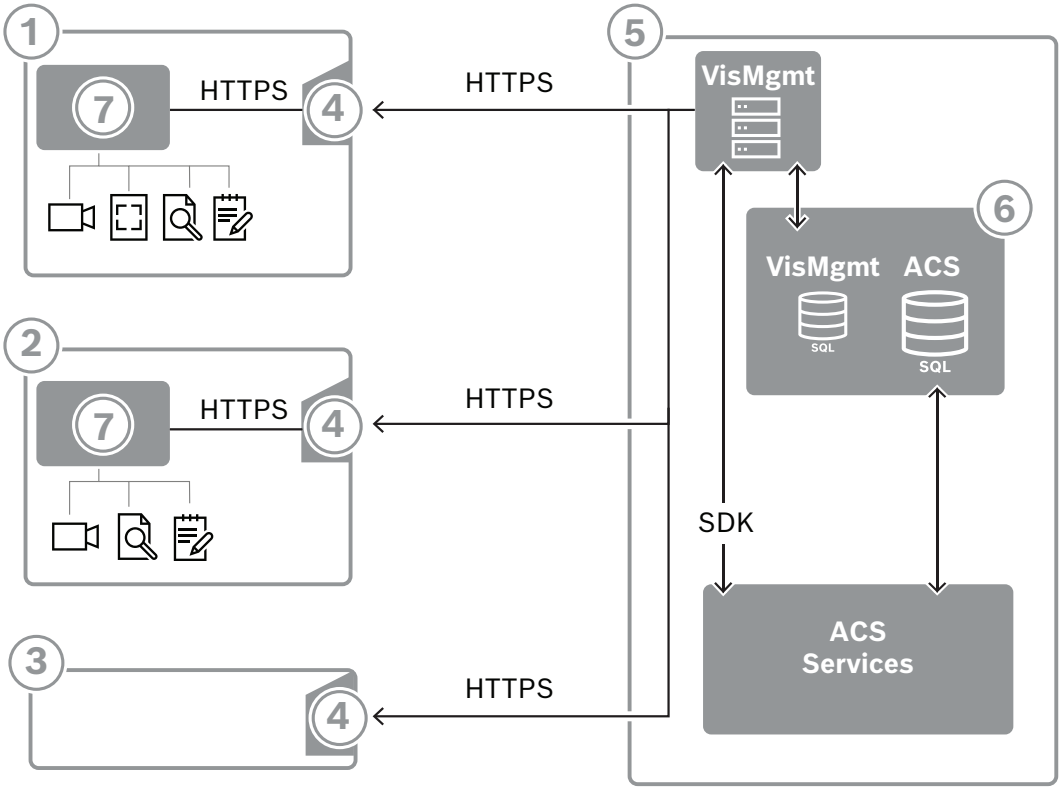
## 2.3 Públicos-alvo

- Instaladores e administradores do Visitor Management
- Os principais tipos de usuários do Visitor Management

## 2.4 Como usar esta documentação

- Use a função **Pesquisar** do visualizador de ajuda para localizar conteúdo relevante.
- As seções de **visão geral, instalação** e **configuração do sistema** destinam-se principalmente aos administradores de sistema
- As seções de **operação** destinam-se principalmente aos usuários do sistema.

# 3 Visão geral do sistema e topologia




| Marcação | Descrição |
|---|---|
| **1** | Estação de trabalho **Recepcionista**. Esta estação de trabalho pode ter hardware periférico opcional, como leitor de inscrição, câmera web e scanners para assinaturas e documentos. |
| **2** | Estação de trabalho do quiosque de **Visitante**, com navegador compatível no modo de quiosque. Esta estação de trabalho pode ter hardware periférico opcional, como uma câmera web e scanners para assinaturas e documentos. |
| **3** | A estação de trabalho **Anfitrião**, ou seja, a estação de trabalho do funcionário que recebe o visitante. |
| **4** | Navegador compatível com o site do VisMgmt |
| **5** | Servidor ACS (BIS ou AMS) |
| **6** | Instância do banco de dados do servidor ACS<br>(Pode estar em um computador separado). |
| **7** | **Complemento de dispositivo periférico Bosch** opcional, que gerencia a comunicação entre o navegador e o hardware periférico. |

A topologia do sistema recomendada tem o servidor VisMgmt no mesmo computador do sistema de controle de acesso principal e o banco de dados na mesma instância do banco de dados.

O complemento de dispositivo periférico Bosch é instalado apenas nas estações de trabalho que requerem acesso a dispositivos periféricos.

A estação de trabalho do host normalmente requer somente acesso por navegador ao servidor VisMgmt.

# 4 Instalação e desinstalação

## 4.1 Requisitos de software e hardware

Instale o servidor VisMgmt no mesmo computador do sistema de controle de acesso principal: os mesmos requisitos de software e hardware são aplicáveis.
Se o sistema de controle de acesso principal ainda não estiver instalado, certifique-se de instalá-lo primeiro antes de instalar o Visitor Management.
Para uma primeira instalação ou para atualizações, a ordem de instalação deve ser a seguinte:

1. Sistema de controle de acesso principal - Access Management System.
2. Credential Management e/ou Visitor Management.
3. Mobile Access.

**Requisitos do servidor**

| | |
|---|---|
| Sistemas operacionais | – Windows 11 Professional e Enterprise 23H2;<br>– Windows Server 2019 (Version 1809) (64bit, Standard, Datacenter);<br>– Windows Server 2022 (64 bits, Standard, Datacenter) |
| Sistemas de gerenciamento de banco de dados | – MS SQL Server 2019 and later<br>Use sempre a mesma instância de banco de dados do ACS (o sistema de controle de acesso primário) |
| Resolução mínima do monitor | Full HD 1920x1080 |
| Navegadores compatíveis | Google Chrome, Mozilla Firefox, Microsoft Edge (baseado em Chromium)<br>Use a versão mais recente do navegador para o seu sistema operacional<br>Windows. |

**Requisitos para o complemento de dispositivos periféricos Bosch**
O **complemento de dispositivos periféricos Bosch** é o programa que trata da comunicação eletrônica entre o navegador e dispositivos periféricos, como leitor de registro, câmera da web, leitor de assinaturas e scanner de documentos.
O computador cliente é o computador que está fisicamente conectado ao hardware periférico. Ele também executa o navegador que se conecta ao servidor VisMgmt.
Embora os dispositivos periféricos não sejam requisitos obrigatórios para instalação, eles são urgentemente recomendados, pois aumentam muito a eficiência do processo de registro de visitantes.

| **Requisito** | **Descrição** |
|---|---|
| Resolução mínima do monitor | Full HD 1920x1080 |
| Navegadores compatíveis | Google Chrome, Mozilla Firefox, Microsoft Edge (Chromium based)<br>Use a versão mais recente do navegador para o seu sistema operacional Windows. |

### 4.1.1 O sistema de controle de acesso principal

**Sem Mobile Access**

Se o Mobile Access não for necessário, o VisMgmt versão 5.5 funcionará com os seguintes sistemas de controle de acesso da Bosch:

– Access Management System (AMS) versões 5.5 e posterior

**Com Mobile Access**

Se Mobile Access for selecionado como uma licença adicional, VisMgmt versão 5.5 funcionará com os seguintes sistemas de controle de acesso da Bosch:

– Access Management System (AMS) versões 5.5 (inclui uma extensão do Mobile Access) e posteriores

Conclua e verifique a instalação do sistema de controle de acesso principal, conforme o guia de instalação, antes de continuar com a instalação do VisMgmt.

### 4.1.2 Uma instância do banco de dados para hospedar o banco de dados do Gerenciador de visitantes

A instalação do sistema principal de controle de acesso cria uma instância de banco de dados que você pode usar para hospedar o banco de dados do VisMgmt, `dbVisitorManagement`.

O nome padrão dessa instância varia, dependendo do ACS

– Para AMS, o nome é `ACE`
– Para BIS ACE, o nome é `BIS_ACE`

### 4.1.3 Um usuário dedicado para acesso ao banco de dados local

O usuário `VMUser` acessa o banco de dados do Gerenciador de visitantes em nome do aplicativo VisMgmt.

A instalação do servidor VisMgmt cria um usuário do Windows `VMUser` no servidor VisMgmt.

### 4.1.4 Um usuário dedicado para acesso ao banco de dados remoto

Se o VisMgmt for usar um banco de dados em um servidor de banco de dados remoto, crie e configure o usuário `VMUser` no Windows e no SQL Server conforme descrito abaixo.

IMPORTANTE: Não execute a configuração do VisMgmt antes de concluir este procedimento.

1. No servidor de banco de dados remoto, crie um usuário Windows com as seguintes configurações:

– **Nome de usuário** (diferencia maiúsculas/minúsculas): `VMUser`
– **Senha**: defina a senha de acordo com as políticas de segurança aplicáveis a todos os seus computadores. Anote-a com cuidado, pois ela será necessária para a configuração do VisMgmt.
– **Membro do grupo**: `Administrators`
– **O usuário deve alterar a senha no login seguinte**: `NO`
– **O usuário não pode alterar a senha**: `YES`
– **A senha nunca expira**: `YES`
– **Login como serviço**: `YES`
– **A conta está desativada**: `NO`

(Adicionar `VMUser` como um login para o SQL Server remoto)

1. Abra o SQL Management Studio

2. Conecte-se à instância SQL remota
3. Acesse **Segurança** > **Login**
4. Adicione o usuário `VMUser` com a função do servidor `sysadmin`

Mais tarde, ao executar a configuração do VisMgmt no servidor VisMgmt, você selecionará a opção para o computador **servidor de banco de dados remoto** e digitará a senha que definiu acima para o `VMUser`.

### 4.1.5 Um usuário dedicado no sistema de controle de acesso principal

1. No sistema de controle de acesso principal, crie um usuário que tenha o recurso **uso de API ilimitado**.
   Para obter instruções detalhadas, consulte o capítulo **Atribuição de perfis de usuário (operador)** no manual do operador do sistema de controle de acesso principal.
2. Se estiver usando o BIS ACE, entre no BIS Classic ou no cliente inteligente uma vez com o usuário, a fim de definir a senha.
3. Anote o nome de usuário e a senha com atenção, pois os assistentes de instalação do VisMgmt precisarão deles.

## 4.2 Instalação do servidor

Não inicie o programa de instalação até satisfazer todos os requisitos de software.
In case of operating AMS, Visitor Management, Credential Management, Mobile Access em um ambiente de rede corporativa, recomenda-se a utilização de certificados emitidos por uma CA (Autoridade Certificadora) corporativa. Os certificados devem ser emitidos antes da instalação de qualquer um dos sistemas back-end. Consulte a seção *Usando certificados personalizados* no manual de instalação do AMS.

### 4.2.1 Execução do programa de instalação do servidor

1. No servidor VisMgmt desejado, como administrador, execute `BoschVisitorManagementServer.exe`.
2. Clique em **Avançar** para aceitar o pacote de instalação padrão.
3. Se você concordar com o Contrato de Licença do Usuário Final (EULA), aceite-o e clique em **Avançar**.
4. Selecione a pasta de destino da instalação. A pasta padrão é recomendada.

– Na tela de **configuração do SQL Server**

5. Selecione se deseja criar o banco de dados na instância local do SQL Server, isto é, na instância do banco de dados no servidor VisMgmt, ou em um computador de servidor de banco de dados remoto.
   – **Observação:** se você escolher um servidor de banco de dados remoto, o programa de instalação solicitará a senha do `VMUser`, o usuário administrador configurado no servidor de banco de dados remoto (consulte a seção Requisitos de software).
6. Verifique e, se necessário, modifique os valores para os seguintes parâmetros:

| | |
|---|---|
| **SQL Server** | O nome do computador do servidor de banco de dados |
| **Instância SQL** | O nome da instância do banco de dados ACS principal. É aqui que o banco de dados de visitantes é criado.<br>Para AMS, o nome é `ACE`<br>Para BIS ACE, o nome é `BIS_ACE` |

| | |
|---|---|
| **Nome de usuário SQL** | O nome de um usuário administrador da instância, normalmente `sa` |
| **Senha SQL** | A senha desse usuário administrador. |

7. Clique em **Testar conexão** para testar se a instância do banco de dados pode ser acessada usando os valores de parâmetro inseridos. Se o teste falhar, verifique os parâmetros novamente.
8. Clique em **Avançar** para continuar

– Na tela de **configuração de acesso do ACS** (onde ACS refere-se ao sistema de controle de acesso principal, AMS ou ACE)

9. Insira valores para os seguintes parâmetros:

| | |
|---|---|
| **Nome de host do ACS** | O nome do computador em que o ACS está em execução |
| **Nome de usuário ACS** | O nome do usuário dedicado do ACS, com uso de API ilimitado. Consulte a seção Requisitos de software. |
| **Senha ACS** | A senha desse usuário dedicado do ACS. |

10. Clique em **Avançar** para continuar

– Na tela de **configuração do servidor de identidades**

11. Digite o URI do servidor de identidade ACS correspondente:
    – AMS: `HTTPS://`<NameOfACSserver>`:44333`
    – BIS: `HTTPS://`<NameOfACSserver>`/BisIdServer`
12. Clique em **Testar conexão** para testar se o servidor de identidades pode ser acessado.
13. Clique em **Avançar** para a tela de resumo e em **Instalar** para iniciar a instalação do servidor VisMgmt.
14. Após a instalação, reinicie o computador.

### 4.2.2 Arquivo JSON de configurações do aplicativo

Vários parâmetros de configuração do servidor VisMgmt são armazenados no seguinte arquivo `.JSON`:

`<installation drive>:\Program Files (x86)\Bosch Sicherheitssysteme\Bosch Visitor Management\appsettings.json`

Geralmente, não é necessário alterar os valores padrão, mas pode ser útil ajustar os seguintes parâmetros na seção **Configurações** do arquivo. Se você ajustar os parâmetros, faça uma cópia de backup do arquivo primeiro. O backup ajudará você a reverter as alterações rapidamente se suas alterações causarem mau funcionamento.

Salve as alterações e reinicie o serviço do Windows VisMgmt para que os parâmetros alterados entrem em vigor. O nome do serviço é `Bosch Visitor Management`.

| Nome do parâmetro | Valor padrão | Descrição |
|---|---|---|
| `PageSizeNumberOfVisit` | `20` | O número máximo de registros de visitas que aparecem na tela de uma vez.<br>Conforme o usuário rola, cada nova página é preenchida com esse número de registros, carregados do banco de dados. |

| Nome do parâmetro | Valor padrão | Descrição |
|---|---|---|
| `MaximumUploadFileSizeBytes` | `31457289` | O número máximo de bytes que um arquivo enviado pode conter. |
| `StartoverTimeoutAskSeconds` | `300` | O aplicativo aguardará esse número de segundos se o usuário pausar durante a inserção das informações de login e, em seguida, solicitará informações. |
| `StartoverTimeoutResetSeconds` | `60` | Depois de solicitar, o aplicativo aguardará esse número de segundos antes de redefinir a tela de login. |

## 4.3 Configuração do computador cliente VisMgmt

O complemento de dispositivos periféricos da Bosch pode ser instalado no computador do servidor, mas geralmente é instalado em um computador cliente na mesma rede. Nesse caso, copie o certificado HTTPS do servidor do ACS e instale-o no computador cliente também. Consulte *Certificados de comunicação segura, página 15* abaixo para obter instruções.
O complemento de dispositivos periféricos Bosch é o software de conexão de dispositivos como leitores de inscrição e scanners. Se esses dispositivos não forem necessários, por exemplo, para o usuário do host, o acesso do navegador será suficiente para fazer login e executar o aplicativo VisMgmt.

Os seguintes leitores de cadastro e formatos de cartão são compatíveis.

| | MIFARE DESFire EV1 Bosch Code | MIFARE DESFire EV1 CSN | MIFARE classic CSN | HID Prox 26 bits | iCLASS 26 bits | iCLASS 35 bits | iCLASS 37 bits | iCLASS 48 bits | EM 26 bits |
|---|---|---|---|---|---|---|---|---|---|
| LECTUS enroll ARD-EDMCV002-USB | X | | | | | | | | |
| OMNIKEY 5427 CK | | X | X | X | X | X | X | X | X |

**Consulte**

– *Certificados de comunicação segura, página 15*

### 4.3.1 Configuração do complemento de dispositivos periféricos

O complemento de dispositivos periféricos é necessário somente nos computadores cliente que se conectam a leitores de cadastro, scanners ou outros dispositivos periféricos. Repita o procedimento abaixo em cada computador cliente que tenha esse requisito.

1. No computador cliente desejado, como administrador, execute `BoschPeripheralDeviceAddon.exe` na mídia de instalação.
   – Os componentes principais são listados, isto é, o software cliente e o software para os dispositivos periféricos normais. Recomendamos a instalação de todos os componentes listados, mesmo que você não tenha o hardware disponível no momento.
2. Clique em **Avançar** para aceitar os pacotes de instalação padrão.
3. Na tela **Configuração do cliente**

– **Diretório de instalação:** aceite a opção padrão (recomendado) ou altere conforme necessário.
– **Porta COM:**
  – Se usar um leitor de inscrição LECTUS, digite o número da porta COM, por exemplo `COM3`, à qual o leitor de inscrição está conectado. Verifique esse valor no gerenciador de dispositivos do Windows.
  – Se estiver usando um leitor HID OMNIKEY, deixe este campo em branco.
  – A câmera, o signoPad e o scanner de documentos são “plug-and-play”, por isso não exigem porta COM. Clique em **Permitir** quando o navegador solicitar permissão para se conectar.
– **Endereço do servidor** e **Porta:**
  – Insira o nome de qualquer computador servidor (por padrão, pelo menos o computador servidor do ACS primário), e os números de portas para todos os serviços de back-end que precisam controlar os dispositivos periféricos.
  Em cada caso, clique em **Testar conexão** e aguarde confirmação.
  Clique em **Adicionar** para adicionar mais servidores.
  Clique em **Excluir** para remover servidores.
  – As portas padrão para os serviços de back-end usuais são:
  `5806` para CredMgmt
  `5706` para VisMgmt

4. Clique em **Avançar** para ver um resumo dos componentes a serem instalados.
5. Clique em **Instalar** para iniciar a instalação.
6. Clique em **Finalizar** para concluir a instalação.
7. Após a instalação, reinicie o computador.

### 4.3.2 Certificados de comunicação segura

Para uma comunicação segura entre o navegador na máquina cliente e servidor do ACS, copie o seguinte certificado do servidor do ACS para os computadores clientes. Use uma conta com direitos de administrador do Windows para fazer a instalação.
O caminho normal até o certificado é:

– <drive de instalação>:
`\Bosch Sicherheitssysteme\Access Management System\Certificates\Bosch Security System Internal CA - BISAMS.cer`

**Observação:** Após a rolagem do certificado, reinicie o back-end do Mobile Access ou o serviço do Credential Management da Bosch e o Visitor Management da Bosch.

**Visão geral das transferências de certificados**

| **De →**<br>**Para ↓** | **ACS** | **Back-end de MA**<br>Mobile Access | **DB**<br>Banco de dados | **S**<br>Aplicativo de configuração | **M**<br>Aplicativo de acesso de portador de cartão | **R**<br>Leitor |
|---|---|---|---|---|---|---|
| **ACS** | / | Transferido pelo assistente de configuração (por meio da ferramenta de certificado) | / | / | / | / |
| **Back-end de MA**<br>Mobile Access | Transferido pelo assistente de configuração do MA | / | / | Transferido por cadastro de código QR<br><br>Atualizado via notificação por push | Transferido por cadastro de código QR<br><br>Atualizado via notificação por push | / |
| **DB**<br>Banco de dados | / | / | / | / | / | / |
| **S**<br>Aplicativo de configuração | / | Transferido por cadastro de código QR | / | / | / | / |
| **M**<br>Aplicativo de acesso de portador de cartão | / | Transferido por cadastro de código QR | / | / | / | / |

#### 4.3.2.1 Certificados para o navegador Firefox

Você pode ignorar esta seção se não estiver usando o navegador Firefox.

O navegador Firefox lida com certificados raiz de forma diferente: o Firefox não consulta a loja de certificados do Windows para obter certificados de raiz confiáveis. Em vez disso, cada perfil do navegador mantém sua própria loja de certificados raiz. Para obter mais detalhes, consulte https://support.mozilla.org/en-US/kb/setting-certificate-authorities-firefox Esta página também oferece instruções para forçar o Firefox a usar a loja de certificados do Windows para todos os usuários.

Alternativamente, você pode importar os certificados padrão conforme descrito abaixo.
Nota:
– Você deve importar os certificados para cada usuário e o perfil do Firefox.
– O certificado de servidor descrito abaixo é o certificado padrão criado pela instalação. Se você comprou seu próprio certificado de uma Autoridade certificadora, você pode usá-lo em seu lugar.

**Importação de certificados para a loja de certificados Firefox**
Para acessar o servidor do ACS pelo Firefox no computador cliente, você pode importar o seguinte certificado padrão do servidor:
– <drive de instalação>:
`\Bosch Sicherheitssysteme\Access Management System\Certificates\Bosch Security System Internal CA - BISAMS.cer`
Ou, para o BIS ACE, você também pode baixar o certificado através da web:
– `HTTP://`<Hostname>`/`<Hostname>`.cer`

**Dispositivos periféricos:** para acessar um dispositivo periférico conectado, como um documento ou um leitor de assinaturas, pelo Firefox no computador cliente, você pode usar o certificado padrão. Ele pode ser encontrado no computador cliente no seguinte local:
<drive de instalação>`:\Program Files (x86)\Bosch Sicherheitssysteme\Bosch Peripheral Device Addon\BoschAcePeripheralDeviceAddonHardware CA.cer`

**Procedimento (repetir para cada certificado e perfil do Firefox):**
Use o seguinte procedimento no computador cliente para instalar os certificados necessários:
1. Localize o certificado que deseja instalar.
2. Abra o navegador Firefox e digite `about:preferences` na barra de endereços.
– Uma página de opções é aberta.
3. No campo **Encontrar nas opções**, digite `certificate`
– O botão **Ver certificados** é exibido na página.
4. Clique no botão **Exibir certificados**.
– A caixa de diálogo **Gerenciador de certificados** é aberta com várias guias
5. Selecione a guia **Autoridades**.
6. Clique em **Importar**...
– Um diálogo seletor de certificados é aberto.
7. Selecione o certificado localizado na etapa 1 e clique em **Abrir**.
– A caixa de diálogo **Baixando certificado** é aberta.
8. Selecione **Confiar neste CA para identificar sites** e clique em **OK**.
– A caixa de diálogo **Baixando certificado** se fecha
9. Na caixa de diálogo **Gerenciador de certificados**, clique em **OK**.
– O procedimento de importação do certificado é concluído.

#### 4.3.2.2 Certificados para o navegador Chrome

Você pode ignorar esta seção se não estiver usando o navegador Chrome.
Consulte as notas de versão do seu ACS para conferir as alterações no processamento de certificados no navegador Chrome.
Para instalar um certificado no navegador Chrome no Microsoft Windows:

1. Baixe o arquivo de certificado.
2. Acesse a página de configurações do Chrome (`chrome://settings`) e clique em **Avançado**.
3. Em **Privacidade e segurança**, clique em **Gerenciar certificados**
4. Na guia **Seus certificados**, clique em **Importar** para iniciar o processo de instalação do certificado:

– Um assistente de importação de certificados é exibido.

5. Selecione o arquivo de certificado e conclua o assistente.
6. O certificado instalado será exibido na guia **Autoridades de certificação raiz confiáveis**.

#### 4.3.2.3 Instalação dos aplicativos do Mobile Access

**Introdução**

A Bosch fornece os seguintes aplicativos para Mobile Access

– Bosch Mobile Access: um aplicativo de portador de cartão para armazenar credenciais virtuais e transmiti-las via Bluetooth para os leitores configurados para Mobile Access. Esses leitores concedem ou negam acesso dependendo se uma das credenciais armazenadas do aplicativo é válida para ele.
– Bosch Setup Access: um aplicativo de instalador para fazer a leitura e configurar os leitores via Bluetooth.

Os operadores autorizados de Visitor Management e Credential Management podem enviar credenciais virtuais para aplicativos de portador de cartão e instalador.

Enquanto o aplicativo de portador de cartão estiver em execução e o Bluetooth estiver ativado no dispositivo móvel, você poderá usá-lo como se fosse um cartão físico. Não há necessidade de realizar comandos no aplicativo ou mesmo desbloquear a tela.

**Aviso!**
IMPORTANTE: Não opere os aplicativos de portador de cartão e instalador simultaneamente Certifique-se de que ninguém use o aplicativo de instalador enquanto o aplicativo de portador de cartão estiver em uso, e vice-versa.

**Procedimento**

Os aplicativos Mobile Access da Bosch podem ser baixados das lojas de aplicativos do Google e da Apple e instalados como de costume. Seus nomes nas lojas de aplicativos são:

– Bosch Mobile Access
– Bosch Setup Access

### 4.3.3 Arquivo JSON de configurações do aplicativo

Vários parâmetros de configuração do computador cliente do VisMgmt são armazenados no seguinte arquivo `.JSON`:

<drive de instalação>:`\Program Files (x86)\Bosch Sicherheitssysteme\Bosch Visitor Management\appsettings.json`

Geralmente, não é necessário alterar os valores padrão, mas pode ser útil ajustar os seguintes parâmetros na seção **AppSettings** do arquivo.

Salve as alterações e reinicie o serviço do Windows VisMgmt para que os parâmetros alterados entrem em vigor. O nome do serviço é `Bosch Ace Visitor Management Client`

| Nome do parâmetro | Exemplo | Descrição |
|---|---|---|
| CorseOrigins | "https://my-vm-server:5706" | O endereço e o número da porta do servidor Visitor Management. |
| CardReaderPort | "com3" | O número da porta COM ao qual um leitor de inscrição LECTUS está conectado. Para leitores HID OMNIKEY, este parâmetro pode ficar em branco. |

## 4.4 Verificação da instalação do servidor

Em um computador na mesma rede, usando um dos navegadores compatíveis, abra o seguinte URL:
https://<VisMgmt server computer>:5706/main
Se o servidor estiver em execução, a página de login do aplicativo será exibida.

## 4.5 Instalação do Mobile Access

**Introdução**

O serviço de back-end do Mobile Access fornece funcionalidade de acesso móvel para Credential Management e Visitor Management.
Certifique-se de usar a versão mais recente do sistema de controle de acesso principal e a versão mais recente do back-end do Mobile Access.
**OBSERVAÇÃO**: Se você estiver usando CredMgmt e VisMgmt, precisará instalar o Mobile Access apenas uma vez.

- Você pode instalá-lo no mesmo servidor que o ACS (instalação colocalizada) ou em outro servidor (instalação distribuída).
- Você pode instalá-lo para usar um banco de dados local ou remoto.

**Acessibilidade do serviço de back-end do Mobile Access**

O serviço de back-end do Mobile Access deve estar continuamente acessível para os dispositivos móveis.
Por razões de segurança, é muito improvável que os dispositivos móveis tenham acesso à rede de um servidor do ACS. Portanto, a instalação distribuída é recomendada. Isso permite que você execute o serviço de back-end do Mobile Access em um servidor na “nuvem” com maior disponibilidade.

### 4.5.1 Visão geral da instalação, configuração e uso

O Mobile Access requer que vários componentes funcionem em conjunto. Listamos os estágios gerais aqui e descrevemos seus respectivos pré-requisitos e procedimentos nas seguintes seções deste capítulo:

**Configuração do servidor do ACS**

1. Um ACS está instalado, licenciado e executado com um certificado raiz permanente e leitores de acesso compatíveis. Os operadores estão definidos nele com autorizações para gerenciar o Mobile Access.

**Configuração do Mobile Access**

1. Um administrador de sistema instala um ou ambos os aplicativos Web que usam o Mobile Access, Credential Management ou Visitor Management, no ACS.
2. Um administrador do sistema instala o back-end do Mobile Access.
3. Um administrador do sistema ativa o Mobile Access nos aplicativos Web instalados.

**Configuração de leitores**

1. Um administrador de sistema cria um instalador (uma pessoa autorizada a configurar leitores do Mobile Access) no aplicativo CredMgmt.
2. O instalador baixa o aplicativo de instalador ("Setup Access") em seu dispositivo móvel da loja pública de aplicativos usual do dispositivo.
3. Um administrador do sistema envia um convite para o instalador designado.
4. O instalador aceita o convite no aplicativo de instalador. Este convite autoriza o instalador a configurar leitores de acesso para o Mobile Access.
5. O instalador configura os leitores usando o aplicativo de instalador.

**Como usar o Mobile Access**

1. Os portadores de credenciais elegíveis para usar o Mobile Access baixam o aplicativo de portador de credencial ("Mobile Access") em seus dispositivos móveis da loja pública de aplicativos usual do dispositivo.
2. Os operadores de CredMgmt e/ou VisMgmt enviam credenciais móveis por código QR ou e-mail para os portadores de credenciais elegíveis.
3. Os portadores de credenciais leem o código QR ou o e-mail no aplicativo de portador de credencial ("Mobile Access"). Isso permite que o dispositivo móvel funcione como uma credencial física quando o aplicativo estiver em execução.

### 4.5.2 Pré-requisitos de hardware do Mobile Access

O Mobile Access requer leitores de acesso com um módulo BLE. Os seguintes leitores da Bosch são adequados:

ARD-SELECT -BOM, -WOM, -BOKM, -WOKM

- B e W significam a cor, preto ou branco
- O significa OSDP
- K significa a presença de um teclado
- M significa adequação para Mobile Access

### 4.5.3 Pré-requisitos de configuração do Mobile Access

**Usuário dedicado para um banco de dados remoto (se você estiver usando um banco de dados remoto)**

Se o Mobile Access for usar um banco de dados em um servidor de banco de dados remoto, crie e configure um usuário administrador chamado `MAUser` nesse servidor remoto, tanto para Windows como para SQL Server. Durante a configuração descrita abaixo, selecione a opção de servidor de banco de dados remoto e insira a senha definida para `MAUser`.

IMPORTANTE: Não execute a configuração do Mobile Access antes de concluir este procedimento.

**Procedimento**

1. No servidor de banco de dados remoto, crie um usuário de domínio do Windows no mesmo domínio que o ACS. Use as seguintes configurações:

- **Nome de usuário** (o nome de usuário diferencia maiúsculas de minúsculas): <ACS-Domain>\MAUser
- **Senha**: defina a senha de acordo com as políticas de segurança aplicáveis a todos os seus computadores. Anote-a com cuidado, pois ela será necessária para a configuração do Mobile Access.
- **O usuário deve alterar a senha no login seguinte**: NO
- **O usuário não pode alterar a senha**: YES
- **A senha nunca expira**: YES
- **Login como serviço**: YES
- **A conta está desativada**: NO

Depois, adicione MAUser como login para o SQL Server remoto da seguinte maneira:

1. Abra o SQL Management Studio
2. Conecte-se à instância SQL remota
3. Acesse **Segurança** > **Login**
4. No painel **Selecione uma página**, selecione **Geral**
5. Selecione o usuário MAUser
6. No painel **Selecione uma página**, selecione **Funções de servidor**
7. Marque as caixas de seleção public e dbcreator

**Um usuário dedicado para o banco de dados local (se você estiver usando um banco de dados local)**

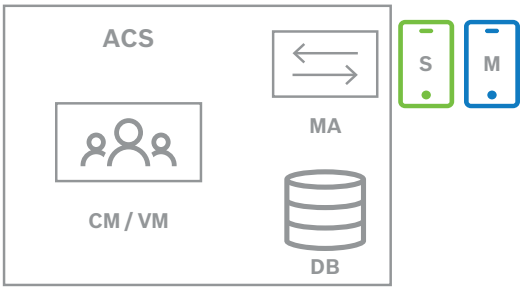
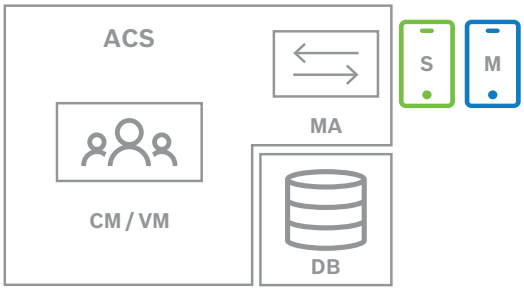
O usuário MAUser acessa o banco de dados do ACS em nome do aplicativo Mobile Access. Você NÃO precisará criar esse usuário se estiver usando um banco de dados local. O programa de instalação do Mobile Access criará um usuário do Windows MAUser no servidor do ACS automaticamente.

### 4.5.4 Procedimento para instalação colocalizada

**Instalação colocalizada** significa que o serviço de back-end do Mobile Access é executado no mesmo servidor do ACS.

**Instalação distribuída** significa que o serviço de back-end do Mobile Access é executado em um servidor diferente, por exemplo, um servidor na nuvem.

Para a opção distribuída, consulte a próxima seção **Procedimento para instalação distribuída**.

| Colocalizada com banco de dados local | Colocalizada com banco de dados remoto |
|---|---|
|  |  |



| Chave | Significado |
|---|---|
| ACS | O sistema de controle de acesso primário, AMS ou BIS-ACE |
| CM/VM | Back-end para o aplicativo Web: Credential Management ou Visitor Management |

| Chave | Significado |
|---|---|
| DB | Banco de dados do ACS principal |
| MA | Back-end do Mobile Access |
| S | Aplicativo de instalador “Setup Access” para dispositivos móveis de instaladores e configuradores de sistema |
| M | Aplicativo de acesso “Mobile Access” para dispositivos móveis de portadores de credenciais normais. |

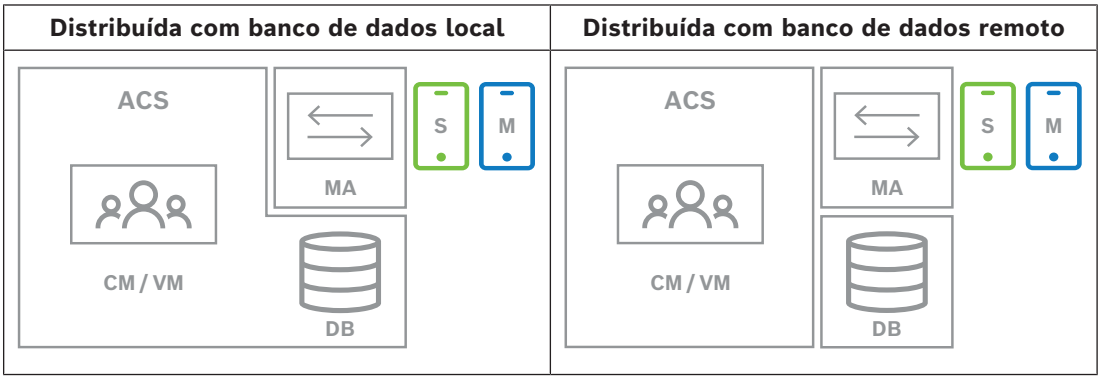
**Procedimento**

1. No servidor do ACS, que também é o servidor do Mobile Access em caso de instalações colocalizadas, execute `BoschMobileAccessBackend.exe` como administrador
– O programa de instalação é aberto
2. Na tela **Local**, selecione o tipo de configuração: **Colocalizada**
3. Na tela **Componentes**, verifique se o `Bosch Mobile Access` está selecionado e clique em **Avançar**
4. Na tela do **EULA**, leia atentamente e clique em **Aceitar** se quiser aceitar o Contrato de Licença de Usuário Final (EULA). A instalação só poderá prosseguir se você fizer isso.
5. Na tela **Diretório de instalação**:
– Procure e selecione uma pasta de destino para a instalação ou aceite a seleção padrão (recomendado)
– Insira o nome da sua empresa na forma como ele deve ser exibido no aplicativo móvel e nos modelos de e-mail HTML
– Clique em **Next (Próximo)**
6. Na tela **Certificado**
– Insira o nome do host em que o back-end do Mobile Access deverá ser executado
– Se desejar, ou se a rede não fornecer resolução de nome de host, insira o endereço IP desse host
– Clique em **Next (Próximo)**
7. Na tela **SQL Server**, selecione uma das duas alternativas para o local do banco de dados. As configurações são ligeiramente diferentes. Escolha uma alternativa para a próxima etapa:
– ALTERNATIVA 1 **Banco de dados local**:
  – O programa de instalação localiza o banco de dados local e o pré-seleciona.
  – Insira a senha SQL para um usuário administrador (o padrão é `sa`)
  – Clique em **Testar conexão**
  – Clique em **Next (Próximo)**
– ALTERNATIVA 2 **Banco de dados remoto**
  – Insira o nome do SQL Server que está na rede
  – Insira o nome da instância SQL
  – Insira a senha SQL para um usuário administrador (o padrão é `sa`)
  – Clique em **Testar conexão**
  – Verifique o nome de usuário e insira a senha do usuário administrador do Windows e SQL que você criou para usar banco de dados remoto (consulte os pré-requisitos acima)
  – Clique em **Next (Próximo)**
8. Na tela de **configuração do servidor de identidades**
– O servidor de identidade padrão (pré-selecionado) é o servidor do ACS primário com porta `44333` `https://`<NameOfACSserver>`:44333`

– Clique em **Testar conexão**
– Se o teste falhar, verifique novamente a disponibilidade do servidor de identidade.
– Clique em **Next (Próximo)**
9. Na tela **Componentes principais**, confirme se **Bosch Mobile Access** está selecionado e clique em **Instalar**
– O assistente de instalação é concluído
10. Clique em **Next (Próximo)**
11. Na tela **Componentes principais**, verifique se a instalação foi concluída com êxito e clique em **Concluir**
12. No aplicativo `Services` do Windows, verifique se o serviço `Bosch Mobile Access` está em execução.

### 4.5.5 Procedimento para instalação distribuída

**Instalação colocalizada** significa que o serviço de back-end do Mobile Access é executado no mesmo servidor do ACS.
**Instalação distribuída** significa que o serviço de back-end do Mobile Access é executado em um servidor diferente, por exemplo, um servidor na nuvem.
Para a opção colocalizada, consulte a seção anterior **Procedimento para instalação colocalizada**.
Em um servidor back-end do Mobile Access distribuído, o pré-requisito a seguir é necessário antes de iniciar uma instalação do Mobile Access ou ao atualizar o sistema. Isso não é necessário em ambiente colocalizado:
– Instale o **ASP.NET Core 8.0 Runtime (v8.0.2) Hosting Bundle** no servidor back-end do Mobile Access distribuído antes de iniciar o instalador do Mobile Access.
– Use o link a seguir para baixar o pacote de hospedagem necessário: https://dotnet.microsoft.com/en-us/download/dotnet/thank-you/runtime-aspnetcore-8.0.2-windows-hosting-bundle-installer.




| Chave | Significado |
|---|---|
| ACS | O sistema de controle de acesso primário, AMS ou BIS-ACE |
| CM/VM | Back-end para o aplicativo Web: Credential Management ou Visitor Management |
| DB | Banco de dados do ACS principal |
| MA | Back-end do Mobile Access |
| S | Aplicativo de instalador “Setup Access” para dispositivos móveis de instaladores e configuradores de sistema |

| Chave | Significado |
|---|---|
| M | Aplicativo de acesso “Mobile Access” para dispositivos móveis de portadores de credenciais normais. |

**Procedimento**

Certifique-se de ter a versão mais recente do sistema de controle de acesso principal.

1. No servidor de back-end do Mobile Access, execute `BoschMobileAccessBackend.exe` como administrador
– O programa de instalação é aberto
2. Na tela **Local**, selecione o tipo de configuração: **Distribuída**
3. Na tela **Host**, selecione **Mobile Access Back-end** e clique em **Avançar**
– Observação: a opção **ACS** será usada posteriormente neste procedimento, quando instalarmos o Mobile Access no servidor do ACS.
4. Na tela **Componentes**, verifique se **Bosch Mobile Access** está selecionado e clique em **Avançar**
5. Na tela do **EULA**, leia atentamente e clique em **Aceitar** se quiser aceitar o Contrato de Licença de Usuário Final (EULA). A instalação só poderá prosseguir se você fizer isso.
6. Na tela **Diretório de instalação**:
– Procure e selecione uma pasta de destino para a instalação ou aceite a seleção padrão (recomendado)
– Insira o nome da sua empresa na forma como ele deve ser exibido no aplicativo móvel e nos modelos de e-mail HTML
– Clique em **Next (Próximo)**
7. Na tela **SQL Server**, selecione uma das duas alternativas para o local do banco de dados. As configurações são ligeiramente diferentes. Escolha uma alternativa para a próxima etapa:
– ALTERNATIVA 1 **Banco de dados local**:
  – O programa de instalação localiza o banco de dados local e o pré-seleciona.
  – Insira a senha SQL para um usuário administrador (o padrão é `sa`)
  – Clique em **Testar conexão**
  – Clique em **Next (Próximo)**
– ALTERNATIVA 2 **Banco de dados remoto**
  – Insira o nome do SQL Server que está na rede
  – Insira o nome da instância SQL
  – Insira a senha SQL para um usuário administrador (o padrão é `sa`)
  – Clique em **Testar conexão**
  – Verifique o nome de usuário e insira a senha do usuário administrador do Windows e SQL que você criou para usar banco de dados remoto (consulte os pré-requisitos acima)
  – Clique em **Next (Próximo)**

*Neste ponto da instalação distribuída, você deve trocar para o computador em que o servidor do ACS está sendo executado e configurar o* Mobile Access *nele, para que ele possa se comunicar posteriormente com o back-end do* Mobile Access *no computador local.*
*Depois de concluir as etapas indicadas nele, o programa de instalação vai guiar você de volta para o servidor local para confirmar e prosseguir.*

1. No computador servidor do ACS, execute `BoschMobileAccessBackend.exe` como administrador

– O programa de instalação é aberto
2. Na tela **Local**, selecione o tipo de configuração: **Distribuída**
3. Na tela **Host**, selecione **ACS** e clique em **Avançar**
4. Na tela **Assistente complementar**, leia o texto explicativo e clique em **Avançar**
5. Na tela **Certificado**
– Insira o nome do host em que o back-end do Mobile Access deverá ser executado
– Se desejar, ou se a rede não fornecer resolução de nome de host, insira o endereço IP desse host
– Clique em **Next (Próximo)**
6. Na tela de **configuração do servidor de identidades**
– O servidor de identidade padrão (pré-selecionado) é o servidor do ACS primário com porta `44333` `https://`<NameOfACSserver>`:44333`
– Clique em **Testar conexão**
– Se o teste falhar, verifique novamente a disponibilidade do servidor de identidade.
– Clique em **Next (Próximo)**
7. Na tela **Criar arquivo**
Aqui podemos criar um arquivo de configuração em um arquivo ZIP protegido por senha, disponibilizando-o para o back-end do Mobile Access.
– **Senha de usuário**: insira uma senha para o arquivo ZIP
– **Arquivo de configuração**: insira ou navegue até uma pasta para armazenar o arquivo ZIP. Observe que essa pasta deve estar acessível ao computador em que o back-end do Mobile Access está sendo executado. Caso contrário, você deverá transferir o arquivo ZIP para esse computador por outros meios.
– Clique em **Criar arquivo de configuração**
– Clique em **Next (Próximo)**
8. Na tela **Alternar máquina**
As etapas de instalação no servidor do ACS estão concluídas.
– Clique em **Confirmar** para encerrar o procedimento

*Neste ponto da instalação distribuída, você retorna ao programa de instalação no computador de back-end do* Mobile Access .

1. Retorne ao programa de configuração `BoschMobileAccessBackend.exe` no computador servidor do Bosch Mobile Access.
2. Na página **Alternar máquina**
– marque a caixa de seleção **Eu já concluí as etapas necessárias na máquina do ACS**
– Clique em **Next (Próximo)**
3. Na tela **Carregar arquivo**
– **Carregar arquivo de configuração:** selecione o arquivo de configuração que você criou no servidor do ACS
– **Verificação de senha:** insira a senha definida para o arquivo ZIP no servidor do ACS
– Depois de inserir a senha correta, clique em **Avançar** para ler o arquivo de configuração
4. Na tela **Componentes principais**, confirme se **Bosch Mobile Access** está selecionado e clique em **Instalar**
– O assistente de instalação é concluído
5. Clique em **Next (Próximo)**
6. Na tela **Componentes principais**, verifique se a instalação foi concluída com êxito e clique em **Concluir**

7. No aplicativo `Services` do Windows, verifique se o serviço `Bosch Mobile Access` está em execução.

## 4.6 Instalação dos aplicativos do Mobile Access

**Introdução**

A Bosch fornece os seguintes aplicativos para Mobile Access

- Bosch Mobile Access: um aplicativo de portador de cartão para armazenar credenciais virtuais e transmiti-las via Bluetooth para os leitores configurados para Mobile Access. Esses leitores concedem ou negam acesso dependendo se uma das credenciais armazenadas do aplicativo é válida para ele.
- Bosch Setup Access: um aplicativo de instalador para fazer a leitura e configurar os leitores via Bluetooth.

Os operadores autorizados de Visitor Management e Credential Management podem enviar credenciais virtuais para aplicativos de portador de cartão e instalador.

Enquanto o aplicativo de portador de cartão estiver em execução e o Bluetooth estiver ativado no dispositivo móvel, você poderá usá-lo como se fosse um cartão físico. Não há necessidade de realizar comandos no aplicativo ou mesmo desbloquear a tela.

**Aviso!**
IMPORTANTE: Não opere os aplicativos de portador de cartão e instalador simultaneamente Certifique-se de que ninguém use o aplicativo de instalador enquanto o aplicativo de portador de cartão estiver em uso, e vice-versa.

**Procedimento**

Os aplicativos Mobile Access da Bosch podem ser baixados das lojas de aplicativos do Google e da Apple e instalados como de costume. Seus nomes nas lojas de aplicativos são:

- Bosch Mobile Access
- Bosch Setup Access

## 4.7 Hardware periférico

Os dispositivos USB periféricos a seguir foram testados e aprovados para uso com o VisMgmt e o CredMgmt no momento da publicação. Para ver uma lista de dispositivos compatíveis atualizada constantemente, consulte a ficha técnica do sistema de controle de acesso principal.

| | |
|---|---|
| Leitor de inscrição do cartão | LECTUS enroll ARD-EDMCV002-USB, HID OMNIKEY 5427 CK |
| Scanner de documentos de identidade | ARH Combo, ARH Osmond |
| Scanner de assinatura | signotec LITE, signotec Omega |

Siga as instruções do fabricante para conectar esses dispositivos aos computadores cliente.

**Leitores de cadastramento**

Os seguintes leitores de cadastro e formatos de cartão são compatíveis.

| | MIFARE DESFire EV1 Bosch Code | MIFARE DESFire EV1 CSN | MIFARE classic CSN | HID Prox 26 bits | iCLASS 26 bits | iCLASS 35 bits | iCLASS 37 bits | iCLASS 48 bits | EM 26 bits |
|---|---|---|---|---|---|---|---|---|---|
| LECTUS enroll ARD-EDMCV002-USB | X | | | | | | | | |
| OMNIKEY 5427 CK | | X | X | X | X | X | X | X | X |

### 4.7.1 Registro de hardware periférico com o computador cliente

Para registrar o hardware periférico com o computador cliente do VisMgmt, execute o programa de instalação de dispositivos periféricos Bosch, `BoschPeripheralDeviceAddon.exe`, no cliente. Para obter instruções, consulte *Configuração do complemento de dispositivos periféricos, página 14*.

**Consulte**

– *Configuração do complemento de dispositivos periféricos, página 14*

## 4.8 Reparar instalações do Mobile Access

**Introdução**

Para atualizar os binários ou recriar o certificado do Mobile Access, você pode executar o instalador da versão atual ou de uma versão posterior do Mobile Access em uma instalação existente:

**Procedimento**

1. No servidor do back-end do Mobile Access, execute a nova versão do `BoschMobileAccessBackend.exe` como administrador.
– Observe que, para instalações colocalizadas, o servidor de back-end do Mobile Access é o mesmo servidor do ACS.
2. Siga o assistente de configuração, definindo as mesmas configurações da instalação original.
– Para recriar o certificado, na tela **Certificados**, selecione o botão de opção **Recriar certificado.**
3. Após a conclusão do programa de configuração, reinicie o servidor.
4. Inicie uma nova sessão de login em cada aplicativo Web que esteja usando o Mobile Access (CredMgmt ou VisMgmt, ou ambos).
– O aplicativo Web usará os novos binários.
– Se você selecionou **Recriar certificado**, todos os convites adicionais enviados aos usuários e instaladores do Mobile Access serão baseados no novo certificado do Mobile Access.

## 4.9 Desinstalação do software

Para desinstalar o software do servidor ou cliente:

1. Com direitos de administrador do Windows, inicie o programa Windows **Adicionar ou remover programas**.
2. Selecione o programa (servidor ou cliente) e clique em **Desinstalar**.
3. (Para gerenciamento de visitantes, e somente no servidor) Decida se deseja remover o banco de dados de gerenciamento de visitantes e o programa.

– **Observação**: o banco de dados registra todas as visitas registradas durante o uso do programa. É recomendável arquivar o banco de dados ou transferi-lo para outra instalação.

4. Decida se deseja remover os arquivos de log.
5. Conclua a desinstalação normalmente.
6. (Recomendado) Reinicialize o computador para garantir uma modificação completa do Registro do Windows.

**Observação:** Depois de desinstalar o back-end do Mobile Access, os seguintes vestígios de configuração devem ser removidos manualmente, se desejado:

– **MAUser** - este usuário permanece após a desinstalação. Um administrador deve removê-lo manualmente.
– **Certificados** - use *Gerenciar certificados do computador* para remover manualmente todos os certificados instalados devido à instalação do Mobile Access.
– **Configuração do servidor de ID do Mobile Access** - arquivo *appsettings.Extension.MobileAccessBackend* permanece após a desinstalação do back-end. Excluí-lo manualmente.

# 5 Configuração

## 5.1 Criação de usuários de gerenciamento de visitantes no ACS

**Introdução**

Cada usuário administrador, recepcionista ou anfitrião do VisMgmt deve ser um portador de cartão com uma definição de Operador separado no ACS, ou seja, o sistema de controle de acesso principal.

Essas definições de Operador contêm direitos de VisMgmt especiais na forma de **perfis do usuário**. Consulte a ajuda on-line em seu ACS para obter informações detalhadas e instruções sobre os **perfis de Usuários**.

– É necessário definir um operador separado para cada portador do cartão que trabalhe no gerenciamento de visitantes. Não é possível atribuir vários portadores de cartões ao mesmo operador.

**Aviso!**

Segurança de TI e contas de usuários

De acordo com as melhores práticas de segurança de TI, recomendamos que cada usuário recepcionista, anfitrião e administrador trabalhe sob sua própria conta do Windows.

**Criação de perfis de usuários para gerenciamento de visitantes**

1. Faça login no sistema de controle de acesso principal com privilégios de administrador.
2. Crie um ou mais perfis de usuário (operador) para os usuários do VisMgmt.
   Caminho da caixa de diálogo:
– **Configuração > Operadores e estações de trabalho** > **Perfis de usuário**
– Navegador de configuração > **Administração** > **Perfis de usuário do ACE**
3. Atribua um dos seguintes direitos de usuário a esses perfis.
– Administrador: `Visitor Management > Administrator`
– Host: `Visitor Management > Host`
– Recepcionista: `Visitor Management > Receptionist`

Depois de criar os perfis de usuário necessários para as várias funções do VisMgmt (Administrador, Recepcionista, Host), você pode atribuir cada perfil a vários operadores.

**Atribuição de perfis de usuários a operadores e portadores de cartões do ACS**

Caminho da caixa de diálogo:
– **Configuração** > **Operadores e estações de trabalho** > **Direitos de usuário**
– Navegador de configuração > **Administração** > **Operadores**

1. Adicione um novo tipo de operador (Clique em  ou em  , dependendo do ACS) e forneça um nome claramente relacionado a uma das funções do VisMgmt (Administrador, Host ou Recepcionista).
2. Na guia **Configurações gerais de operador**, selecione `Operator ACE` na lista de autorizações.
3. Na guia **Configurações de operador do ACE**, use os botões de seta para atribuir o **perfil de usuário do ACE** criado acima.
   Cancele a atribuição do perfil padrão `UP-Administrator`, exceto no caso improvável de que o portador do cartão precise de direitos gerais de administrador no ACS.
4. Ainda na guia **Configurações de operador do ACE**, use o painel **Atribuir pessoa** para encontrar o portador do cartão no sistema que deve ter a função VisMgmt.

5. Clique em **Atribuir pessoa** para concluir a atribuição ao portador do cartão selecionado.

– É necessário definir um operador separado para cada portador do cartão que trabalhe no gerenciamento de visitantes. Não é possível atribuir vários portadores de cartões ao mesmo operador.

## 5.2 Criação de autorizações e perfis de visitantes no ACS

**Introdução**

O recepcionista ou o administrador do sistema VisMgmt seleciona para cada novo visitante um **Tipo de visitante**. O tipo de visitante se baseia em um **Tipo de pessoa** predefinido denominado **Visitante** no sistema de controle de acesso principal (ACS), ou em um subtipo de **Visitante** criado pelos administradores do ACS.

Esses administradores também precisam configurar o Tipo de pessoa **Visitante** e seus subtipos no ACS com perfis de acesso. Os perfis de acesso permitem que esses tipos de pessoas operem portas físicas do local.

## 5.3 Configuração do computador do recepcionista

O computador do recepcionista executa o complemento de **dispositivos periféricos Bosch**, que permite realizar conexões físicas com dispositivos periféricos para ler cartões, digitalizar documentos de identidade e assinaturas.

Conecte todos os dispositivos periféricos necessários antes de instalar o software cliente. Verifique se o computador e os dispositivos periféricos estão devidamente protegidos contra o acesso não autorizado.

## 5.4 Configuração de um computador de quiosque para visitantes

**Introdução**

Os visitantes normalmente registram as visitas e criam seus próprios perfis em um computador com livre acesso na área da recepção do local com controle de acesso. Por motivos de segurança, o navegador da Web do computador é executado no modo de quiosque, que permite o acesso somente ao VisMgmt e não a várias guias, configurações do navegador ou ao sistema operacional do computador. Todos os navegadores compatíveis oferecem o modo de quiosque, mas a configuração exata depende do navegador.

O computador do quiosque executa o software cliente do complemento de **dispositivos periféricos Bosch**, o que permite realizar conexões físicas com dispositivos periféricos para digitalizar documentos de identidade e assinaturas.

– O URL do modo de quiosque é `https://`<My_VisMgmt_server>`:5706`

**Configuração de navegadores para o modo de quiosque**

Os links a seguir descrevem a configuração do modo de quiosque para os navegadores compatíveis com o VisMgmt

| | **Instruções para configurar o modo de quiosque** |
|---|---|
| **Chrome** | https://support.google.com/chrome/a/answer/9273974 |
| **Firefox** | https://support.mozilla.org/en-US/kb/firefox-enterprise-kiosk-mode |
| **Edge** | https://docs.microsoft.com/en-us/deployedge/microsoft-edge-configure-kiosk-mode |

**Aviso!**
Por motivos de segurança, sempre desabilite a opção de navegador para salvar senhas automaticamente.

## 5.5 Como fazer login para tarefas de configuração

Para tarefas de configuração e administração, use um computador que seja fisicamente protegido contra o acesso não autorizado.

1. No navegador, insira o endereço HTTPS do servidor VisMgmt seguido por dois pontos e pelo número da porta (o padrão é `5706`)
   `https://`<My_VisMgmt_server>`:5706/main`
   A tela **Fazer login** é exibida
2. Faça login como usuário **administrador** do VisMgmt.
3. Clique em  para abrir o menu **Configurações**.

## 5.6 Uso do menu Configurações para configuração

O menu **Configurações** contém subseções que permitem realizar as seguintes etapas de configuração:

| | |
|---|---|
| **Configurações gerais** | – **Período de retenção (dias)**: essa configuração rege o processamento de registros de visitas.<br>– Quando o período expira pela primeira vez, o aplicativo torna o registro anônimo.<br>– Quando o período expira pela segunda vez, o aplicativo exclui o registro.<br>O valor padrão é `365`.<br>Defina como 0 para desativar o período de retenção completamente. Nesse caso, os registros das visitas serão retidos indefinidamente.<br>– **Modo de armazenamento de documentos**: defina se os documentos serão armazenados como arquivos impressos ou digitais.<br>– **Número máximo de visitantes** permitidos no local simultaneamente.<br>O valor padrão é `100`.<br>Defina como `0` para desativar completamente os contadores de visitantes no painel.<br>– **Período de validade do documento (dias)**: digite por quanto tempo os documentos carregados, como contratos de não divulgação (NDA) e termos de uso, permanecerão válidos. O período é pertinente a arquivos impressos e digitais.<br>Depois desse período, os documentos serão marcados como expirados no perfil do visitante (ícone de relógio com um ponto vermelho).<br>O valor padrão é `365` |

- **Período de aviso de expiração de documento (dias)**: insira a duração do período de aviso antes da data de expiração.
  Durante esse período de aviso, os documentos serão marcados no perfil do visitante (ícone de relógio com um ponto laranja). Antes do período de aviso, o ícone de relógio apresenta um ponto verde.
- **Logotipo:** marque ou desmarque as caixas de seleção que determinam se as caixas de diálogo exibirão um logotipo personalizado ou o logotipo padrão, bem como se deseja exibir o **supergráfico** da Bosch.
  - Para conferir os critérios para arquivos de logotipo personalizados, consulte: *Personalização do logotipo da empresa, página 37*
- Clique em **Visualizar** para mostrar a página da caixa de diálogo conforme seria exibida com essas configurações. Consulte a próxima seção para obter mais detalhes sobre o modo de visualização.
- **Idiomas**:
  selecione quais idiomas deverão estar disponíveis na interface do usuário, com seus formatos de **data** e **hora** preferenciais.
- **Servidor de e-mail**
  Insira o endereço IP, o número da porta e os detalhes da conta do seu servidor de e-mail a fim de habilitar o envio de e-mails do aplicativo. Caso o servidor de e-mail externo exija um certificado SSL/TSL extra, importe-o para a máquina que executa o back-end de acesso móvel. Após a importação, é necessário reiniciar o `VisitorManagerServer`.
- **Modelos de e-mail**
  São fornecidos vários modelos de e-mail em HTML que você personaliza conforme suas próprias necessidades. Para obter mais detalhes, consulte a seção de **modelos de e-mails** abaixo.
- **Mobile Access**
  Marque a caixa de seleção **Mobile Access** para ativar o Mobile Access.

  **Conexão**: insira o endereço do servidor de Mobile Access (endereço do serviço de registro).
  `https://`<MyMobileAccessBackendServer>`:5700`
  Use um (FQDN) para <MyMobileAccessBackendServer> em ambientes de vários domínios.

  **Observação:** Para usar um endereço IP em vez de um FQDN, insira o endereço IP em **Criação de certificado** ao executar o assistente de instalação para o back-end do Mobile Access.

  **Integração de instalador:** selecione as informações necessárias dos instaladores para que eles possam configurar leitores de acesso móvel usando o Bosch Setup Access.

| | |
|---|---|
| | Saia do aplicativo Web e faça login novamente para usar o recurso Mobile Access imediatamente. |
| **Recepcionista** | – Essa tela de configuração contém duas caixas de seleção para cada campo de dados nas caixas de diálogo de registro do visitante do recepcionista.<br>– Marque ou desmarque a primeira caixa de seleção para definir se o campo de dados deve ficar **visível** em todas as caixas de diálogo de registro.<br>– Marque ou desmarque a segunda caixa de seleção (marcada com um asterisco) para indicar se o campo de dados é **obrigatório** ou não.<br>– Personalize os textos de cabeçalho padrão nas caixas de diálogo de coleta de dados.<br>Para mais detalhes, consulte *Personalização da interface de usuário, página 36* abaixo. |
| | **Opção especial: habilitar check-in/check-out sem cartão**<br>Se os visitantes tiverem acompanhantes próximos ou estiverem restritos a espaços públicos, cartões individuais para visitantes podem ser desnecessários. Para esses casos existe a opção de fazer check-in e check-out de visitantes sem cartões. Por questões de segurança, essa opção fica desativada por padrão. Selecione a caixa de seleção para habilitá-la:<br>– **Observação:** se a opção estiver ativada, qualquer **Visitante** que se cadastrar no computador do quiosque aprovará e fará automaticamente o check-in da própria visita no mesmo momento.<br>– Consulte o capítulo **Operação** *Check-in e check-out sem cartão, página 54* deste documento para obter detalhes sobre como um usuário **recepcionista** processa visitantes sem cartões. |
| **Anfitrião**<br>**Visitante** | As configurações dos usuários **Host** e **Visitante** continuam sendo somente leitura até você editar e salvar as configurações para **Recepcionista**.<br>Os campos marcados como não visíveis nas configurações de **Recepcionista** são definidos automaticamente como não visíveis para **Host** e **Visitante**.<br>Depois disso, o procedimentos de configuração é idêntico. |

**Consulte**
- *Atribuição de credenciais físicas, página 50*
- *Personalização da interface de usuário, página 36*

### 5.6.1 Modelos de e-mail

São fornecidos vários modelos de e-mail em HTML que você personaliza conforme as necessidades da sua empresa. Para cada modelo, você pode armazenar endereços de e-mails para CC, BCC e um destinatário de teste, para quem você possa enviar um e-mail de teste imediatamente. Quando você baixa um modelo para edição, ele é armazenado na pasta de downloads padrão do seu navegador.

- `MobileAccess.html` Um convite para um titular de cartão usar credenciais baseadas em smartphones.
- `SetupAccess.html` Um convite para um instalador configurar leitores para Mobile Access.
- `VisitorInvite.html` Um convite para alguém visitar seu site, com a opção de anexar um arquivo iCalendar ao e-mail.
- `InformHostAboutCheckin.html` Um e-mail para informar o anfitrião que um visitante chegou.

**Espaços reservados para uso em modelos de e-mails**

Os modelos de e-mail fornecem vários espaços reservados de texto para incluir campos de banco de dados no texto. Esses espaços reservados são descritos nas tabelas a seguir, de acordo com os modelos nos quais podem ser usados.

**Mobile Access**

E-mail que é enviado para um portador de cartão (para o aplicativo Mobile Access) quando o acesso móvel é concedido a ele

| Marcador de posição | Description (Descrição) |
|---|---|
| `{{Title}}` | título da pessoa (Sr., Sra., Dr., Dra. etc.) |
| `{{FirstName}}` | nome da pessoa |
| `{{LastName}}` | sobrenome da pessoa |
| `{{CompanyName}}` | empresa da pessoa |
| `{{QrcodeLink}}` | código QR correspondente ao link que oferece ao portador do cartão acesso móvel pelo aplicativo |
| `{{InviteLink}}` | link que oferece ao portador do cartão acesso móvel pelo aplicativo |

**Setup Access (Acesso à configuração)**

E-mail que é enviado para um instalador de Mobile Access (para o aplicativo Setup Access) quando o acesso móvel é concedido a ele para configurar leitores.

| Marcador de posição | Description (Descrição) |
|---|---|
| `{{Title}}` | título do instalador (Sr., Sra., Dr. etc.) |
| `{{FirstName}}` | nome do instalador |
| `{{LastName}}` | sobrenome do instalador |
| `{{CompanyName}}` | empresa do instalador |
| `{{QrcodeLink}}` | código QR correspondente ao link que oferece ao instalador acesso móvel para configurar leitores pelo aplicativo Setup Access |
| `{{InviteLink}}` | link que oferece ao instalador acesso móvel para configurar leitores pelo aplicativo Setup Access |

**Convite do visitante**

E-mail que é enviado ao visitante quando uma visita é criada ou editada.

| Marcador de posição | Description (Descrição) |
|---|---|
| {{VisitorID}} | código do ID do visitante, gerado pelo aplicativo VisMgmt |
| {{Title}} | título do visitante (Sr., Sra., Dr. etc.) |
| {{FirstName}} | nome do visitante |
| {{LastName}} | sobrenome do visitante |
| {{CompanyName}} | empresa do visitante |
| {{HostFirstName}} | nome do anfitrião |
| {{HostLastName}} | sobrenome do anfitrião |
| {{ExpArrivalDate}} | data planejada da visita |

**Visitante chegou**

E-mail que é enviado ao host quando a recepção aprova a visita

| Marcador de posição | Description (Descrição) |
|---|---|
| {{VisitorID}} | código do ID do visitante, gerado pelo aplicativo VisMgmt |
| {{Title}} | título do visitante (Sr., Sra., Dr. etc.) |
| {{FirstName}} | nome do visitante |
| {{LastName}} | sobrenome do visitante |
| {{CompanyName}} | empresa do visitante |
| {{HostFirstName}} | nome do anfitrião |
| {{HostLastName}} | sobrenome do anfitrião |
| {{ExpArrivalDate}} | data planejada da visita |
| {{ArrivalDate}} | data real de visita |

**Passe de visitante**

Documento que pode ser impresso e entregue a um visitante. Pode conter um mapa do prédio ou uma lista de verificação.

| Marcador de posição | Description (Descrição) |
|---|---|
| {{VisitorID}} | código do ID do visitante, gerado pelo aplicativo VisMgmt |
| {{Title}} | título do visitante (Sr., Sra., Dr. etc.) |
| {{FirstName}} | nome do visitante |
| {{LastName}} | sobrenome do visitante |
| {{CompanyName}} | empresa do visitante |
| {{HostFirstName}} | nome do anfitrião |
| {{HostLastName}} | sobrenome do anfitrião |

| Marcador de posição | Description (Descrição) |
|---|---|
| {{ExpArrivalDate}} | data planejada da visita |
| {{ArrivalDate}} | data real de visita |

### 5.6.2 Modo de visualização

Alguns conjuntos de opções têm um botão **Visualização** que ativa o modo de visualização para permitir que você veja as caixas de diálogo conforme apareceriam com essas opções definidas.

No modo de visualização, as seguintes condições são aplicadas:

– Um banner aparece na parte superior do painel.


– As alterações feitas no painel ou nos menus **não** são salvas.
– Clique em **Fechar modo de visualização** no banner para fechar o modo de visualização
– Use a lista **Alterar função** dentro do banner para ver a aparência da interface para os diferentes tipos de usuário.

### 5.6.3 Modelos de documento

Para os diversos documentos e e-mails, você pode baixar modelos e carregar versões personalizadas desses modelos na caixa de diálogo **Painel** > **Configurações > Geral**.

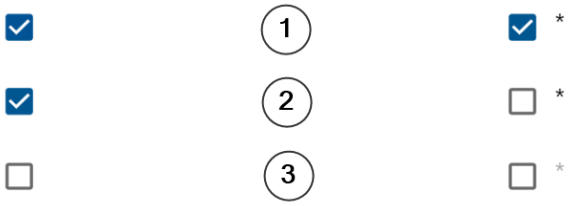
## 5.7 Personalização da interface de usuário

Personalize a interface de usuário nas caixas de diálogo **Painel** > **Configurações**.

### 5.7.1 Definição de opções visíveis, invisíveis e obrigatórias

Selecione quais campos de dados estarão visíveis nas caixas de diálogo e quais dados são obrigatórios.

Exemplo:




– (1) é visível e obrigatório.
– (2) é visível, mas não obrigatório.
– (3) não é visível.

### 5.7.2 Personalização de textos da interface de usuário para localização

É possível personalizar com facilidade os textos da interface do usuário com base em idioma.

Por padrão, o **texto de localização** contém os cabeçalhos padrão dos blocos de campos de dados nas caixas de diálogo de coleta de dados.

Como personalizar esses cabeçalhos de acordo com os requisitos locais:

1. Selecione um idioma de interface do usuário na lista.

2. Substitua os textos na caixa de texto.
   Você pode usar tags HTML para formatação simples, por exemplo:
   `<b>this text will appear bold </b>`
   `<i>italics</i>`
   `<u>underline</u>`


### 5.7.3 Personalização do modo quiosque

Se o seu site não tiver dispositivos de hardware periféricos, por exemplo, um scanner de documentos, você poderá personalizar o processo de autorregistro do visitante no modo quiosque. Para isso, desmarque as caixas de seleção das etapas de registro correspondentes.

### 5.7.4 Personalização do logotipo da empresa

Os arquivos gráficos que você carrega para o logotipo da sua empresa devem atender aos seguintes critérios:

| | |
|---|---|
| Formatos compatíveis | PNG, JPEG, JPG |
| Largura exata (pixels) | 125 |
| Altura exata (pixels) | 63 |
| Tamanho máximo (MB) | 1 |

## 5.8 Configurações de firewall

Adicione aplicativos auxiliares à configuração de firewall dos computadores cliente e servidor:

1. Inicie o Firewall do Windows: clique em Iniciar > **Painel de controle** > **Firewall do Windows**
2. Selecione **Configurações avançadas**
3. Selecione **Regras de entrada**
4. No painel **Ações**, selecione **Nova regra...**
5. Na caixa de diálogo **Tipo de regra**, selecione **Porta** e clique em **Avançar >**
6. Na próxima página, selecione **Portas TCP e locais específicas**
7. Permita a comunicação pelas seguintes portas:

– No computador, ou computadores, servidor

<nome do servidor>:`44333` — usado pelo servidor de identidade do AMS **(*)**

<nome do servidor>:`5706` — usado pelo servidor do VisMgmt

<nome do servidor>:`5806` — usado pelo servidor do CredMgmt

<nome do servidor>:`5701` — usado pelo servidor do Mobile Access

– Nos computadores clientes

`localhost:5707` - usado pelo complemento do dispositivo periférico Bosch

**(*)** Nós usamos os servidores de identidade AMS e BIS conforme descrito nos respectivos manuais de instalação.

**Uso de portas no sistema**

| Saída do servidor | Porta de saída | Entrada do servidor | Porta de entrada | Protocolo | Comentários |
|---|---|---|---|---|---|
| VisMgmt ou CredMgmt | * | Back-end do Mobile Access | 5701 | HTTPS | Comandos do aplicativo Web para criar e/ou excluir credenciais móveis |
| Dispositivos móveis da Internet | * | Back-end do Mobile Access | 5701 | HTTPS | Os dispositivos móveis recebem credenciais móveis pela Internet |
| Back-end do Mobile Access | * | Google Firebase (Internet) | * | HTTPS | Os dispositivos móveis recebem notificações por push, consulte a documentação do Google Firebase sobre as configurações de firewalls<br><br>https://firebase.google.com/docs/cloud-messaging/concept-options |
| Computador cliente do usuário do VisMgmt | * | Back-end do VisMgmt | 5706 | HTTPS | Comandos do computador cliente do VisMgmt para o back-end do VisMgmt |
| Computador cliente do usuário do CredMgmt | * | Back-end do CredMgmt | 5806 | HTTPS | Comandos do computador cliente do CredMgmt para o back-end do CredMgmt |
| Computador administrador | * | Back-end do Mobile Access | 3389 | Área de Trabalho Remota (RDP) | Por motivos de segurança, você deve conceder acesso de administrador ao computador do back-end do Mobile Access apenas temporariamente. |

**Aviso!**
Observe que o Mobile Access e o ACS não têm conexão direta, nem de entrada, nem de saída.

### 5.8.1 Programas e serviços como exceções de firewall

Você também pode configurar o firewall adicionando programas e serviços como exceções

1. Inicie a interface de usuário do Firewall do Windows, selecione **Iniciar > Configurações > Painel de Controle > Firewall do Windows**.
2. Selecione a guia **Permitir um aplicativo ou recurso através do Firewall do Windows**.
3. Selecione **Permitir outro aplicativo** (se esta opção estiver esmaecida, habilite-a selecionando **Alterar configurações**).
4. Você pode adicionar os seguintes programas:

**Programas**

O caminho de instalação padrão é `C:\Program Files (x86)\Bosch Sicherheitssysteme\`

| **Programa** | **Local do arquivo** |
|---|---|
| acsp.exe | [caminho-instalação]\AccessEngine**AC**\BIN |
| ACTA-3.exe | [caminho-instalação]\AccessEngine**AC**\BIN |
| BioVerify.exe | [caminho-instalação]\AccessEngine**AC**\BIN |
| BioIdentify.exe | [caminho-instalação]\AccessEngine**AC**\BIN |
| Bosch.Ace.CredentialManagement.exe | [caminho-instalação]\Bosch Credential Management |
| Bosch.Access.MobileAccessBackend.exe | [caminho-instalação]\Bosch Mobile Access |
| Bosch.Ace.VisitorManagement.exe | [caminho-instalação]\Bosch Visitor Management |
| CalTa-3.exe | [caminho-instalação]\AccessEngine**AC**\BIN |
| CDTA-1.exe | [caminho-instalação]\AccessEngine**AC**\BIN |
| EMDP.exe | [caminho-instalação]\AccessEngine**AC**\BIN |
| KCKemas.exe | [caminho-instalação]\AccessEngine**AC**\BIN |
| KCS.exe | [caminho-instalação]\AccessEngine**AC**\BIN |
| Loggifier-2.exe | [caminho-instalação]\AccessEngine**AC**\BIN |
| PictureServer.exe | [caminho-instalação]\AccessEngine**AC**\BIN |
| ReplServer.exe | [caminho-instalação]\AccessEngine**AC**\BIN |
| reps.exe | [caminho-instalação]\AccessEngine**AC**\BIN |
| TAccExc.exe | [caminho-instalação]\AccessEngine**AC**\BIN |
| EMAILSP.exe | [caminho-instalação]\AccessEngine**AC**\BIN |
| master-3.exe | [caminho-instalação]\AccessEngine**AC**\BIN |
| querySrv-2.exe | [caminho-instalação]\AccessEngine**AC**\BIN |
| webSrv-1.exe | [caminho-instalação]\AccessEngine**AC**\BIN |
| LicenseGateway.exe | [caminho-instalação]\AccessEngine**AC**\BIN |
| DMS.exe | [caminho-instalação]\AccessEngine**MAC**\BIN |
| lac.exe | [caminho-instalação]\AccessEngine**MAC**\BIN |

**Serviços**

O caminho de instalação padrão é `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System`

| Serviço | Local do arquivo |
|---|---|
| Bosch.States.Api | [caminho-instalação]\States API |
| Bosch.Map.Api | [caminho-instalação]\Map API |
| Bosch.MapView.Api | [caminho-instalação]\Map View API |
| Bosch.Events.Api | [caminho-instalação]\Events API |
| Bosch.Alarms.Api | [caminho-instalação]\Alarms API |
| Bosch.Ace.IdentityServer | [caminho-instalação]\Identity Server |
| Bosch.Ace.Api | [caminho-instalação]\Access API |
| Bosch.DialogManager.Api | [caminho-instalação]\Dialog Manager API |
| Bosch.Intrusion.Api | [caminho-instalação]\Intrusion API |
| Bosch Ace Visitor Management | [caminho-instalação-VM] |
| Bosch Ace Visitor Management Client | [caminho-instalação-cliente-VM]\ |
| Bosch.OSS-SO | [caminho-instalação]\OSS-SO |
| Bosch.OSS-SO.Configurator | [caminho-instalação]\OSS-SO.Configurator |
| Bosch.Access.ProductApi.Api | [caminho-instalação]\ProductApi |
| Bosch.MUM | [MUM-install-path]\ |

### 5.8.2 Mobile Access API

A partir do lançamento do Mobile Access 5.2 e posterior, Credential Management 5.2 e posterior e Visitor Management 5.2 e posterior, a API do Mobile Access Backend foi dividida em uma parte de canal frontal e uma parte de canal traseiro. Supostamente, o canal frontal deve se comunicar com telefones celulares enquanto o canal traseiro se comunica com o Credential Management e/ou Visitor Management.
Isso permite definir regras e rotas de firewall para controlar o tráfego de rede, a fim de fortalecer a segurança de TI. A divisão da API vem com dois números de porta separados. Ou seja, o número da porta de telefones celulares é 5700, enquanto que a porta de endereço do Credential Management e do Visitor Management é 5701.
Tanto o Credential Management como o Visitor Management têm duas configurações separadas para a URL do canal frontal e a URL do canal traseiro, respectivamente. A interface do usuário os chama de "Endereço de serviço administrativo" (canal traseiro) e "Endereço de serviço de registro" (canal frontal).
A porta padrão para "Endereço de serviço administrativo" (canal traseiro) é 5701. Em uma regra de firewall específica do cliente, essa porta deve ser configurada apenas para comunicação com a máquina que está executando o back-end do Credential Management e/ou Visitor Management, que é o Servidor AMS na maioria dos casos.

A porta padrão para o "Endereço do serviço de registro" (canal frontal) é 5700. Em uma regra de firewall específica do cliente, essa porta deve ser configurada para ser acessada pelos aplicativos Mobile Access. Em muitos cenários, esse end-point seria acessível de fora. No entanto, isso depende muito do cenário do cliente.
Se o cliente estiver atualizando de uma versão anterior para a versão mais recente do AMS, as configurações do Credential Management e do Visitor Management precisarão ser ajustadas. Esta configuração está acessível para a função de administrador do Visitor Management e do Credential Management na página de configurações.
O canal traseiro deve ser protegido para não ser acessível pela Internet pública ou por qualquer rede não autorizada.

## 5.9 Segurança de TI

A segurança do sistema de controle de acesso de uma organização é uma parte essencial da infraestrutura. A Bosch recomenda seguir rigorosamente as diretrizes de segurança de TI prescritas para o país de instalação.
A organização que opera o sistema de controle de acesso é responsável pelo menos por:

### 5.9.1 Responsabilidades de hardware

- A prevenção do acesso físico não autorizado a componentes de rede, como conexões RJ45.
  - Os invasores precisam de acesso físico para realizar ataques man-in-the-middle.
- A prevenção do acesso físico não autorizado ao hardware do controlador AMC2.
- Uso de uma rede dedicada para controle de acesso.
  - Os invasores podem obter acesso por meio de outros dispositivos na mesma rede.
- O uso de credenciais seguras como **DESFire** com o código da Bosch e autenticação multifatorial com biometria.
- O cadastro imediato, por meio do aplicativo **Setup Access**, de leitores de acesso móvel com módulos BLE (Bluetooth Low Energy). Leitores não cadastrados e ligados são vulneráveis à invasão por terceiros. Para remediar esse tipo de invasão, consulte o manual de instalação do leitor para obter instruções sobre como redefinir os padrões de fábrica.
- Fornecer um mecanismo de failover e uma fonte de alimentação de backup para o sistema de controle de acesso.
- O rastreamento e a desativação de credenciais perdidas ou inseridas incorretamente.
- A desativação adequada de hardware que não está mais em uso, especificamente a redefinição para os padrões de fábrica e a exclusão de dados pessoais e informações de segurança.

### 5.9.2 Responsabilidades de software

- Manutenção, atualização e funcionamentos corretos do firewall da rede de controle de acesso.
- O monitoramento de alarmes que indicam quando componentes de hardware, como leitores de cartão ou controladores AMC2, ficam off-line.
  - Esses alarmes podem indicar uma tentativa de trocar componentes de hardware.
- O monitoramento de alarmes de detecção de fraude acionados por contatos elétricos no hardware de controle de acesso, por exemplo, controladores, leitores e gabinetes.
- A limitação de transmissões UDP na rede dedicada.

- Atualizações, especialmente atualizações e patches de segurança, no software de controle de acesso.
- Atualizações, especialmente atualizações e patches de segurança, no firmware do hardware.
  - Até mesmo hardware entregue recentemente pode exigir uma atualização de firmware. Consulte o manual do hardware para obter instruções.
  - A Bosch não se responsabiliza pelos danos causados por produtos colocados em operação com firmware desatualizado.
- O uso da comunicação de canal seguro OSDPv2.
- O uso de senhas fortes.
- A imposição do *Princípio de privilégio mínimo* para garantir que usuários individuais tenham acesso somente aos recursos necessários para fins legítimos.
- A atribuição e configuração adequada de perfis de usuário para operadores, a fim de evitar que operadores normais atribuam autorizações de alta segurança sem o princípio das duas pessoas.

### 5.9.3 Tratamento seguro de credenciais móveis

- Não deixe leitores do Mobile Access não configurados desprotegidos.
  - Um invasor pode apropriar um leitor para outro ACS. Isso exigiria uma redefinição de fábrica de alto custo.
- Se um dispositivo móvel com credenciais móveis for perdido ou roubado, trate esse dispositivo como um cartão perdido: bloqueie ou exclua todas as credenciais móveis associadas a ele o quanto antes.
- Para ambientes de alta segurança, a Bosch recomenda a implantação de autenticação de dois fatores. Isso requer que o portador da credencial desbloqueie o dispositivo móvel antes de usá-lo como uma credencial.
- As credenciais móveis não são restauradas quando um telefone é restaurado de um backup. Se um portador de credencial móvel receber um novo dispositivo móvel, você deverá reenviar todos os convites atuais.
- Um invasor pode usar um bloqueador de comunicação para bloquear a comunicação com leitores de acesso móvel. Os funcionários cujo acesso às áreas é essencial devem portar credenciais físicas como backup.
  - Como backup para o Mobile Access, use apenas cartões físicos com uma codificação segura (como o código da Bosch).
- Proteja o servidor do Mobile Access contra acesso físico não autorizado. A Bosch recomenda medidas adicionais, como criptografia de disco BitLocker.
- Proteja o servidor do Mobile Access contra ataques de negação de serviço (DoS). Ele deve fazer parte de um ambiente de rede seguro que forneça proteções, como um limitador de taxa.
- Trate os códigos QR de convite do instalador como credenciais de administrador. Um smartphone de instalador roubado, com credenciais de instalador ativas, pode permitir que um invasor reconfigure os leitores do Mobile Access de maneira mal-intencionada.
  - Envie convites aos instaladores apenas com antecedência suficiente para a configuração do leitor e certifique-se de que excluam essas credenciais assim que a instalação for concluída.
  - Use a função “Leitura de códigos QR da tela” em vez de convites por e-mail. Certifique-se de que o instalador pretendido carregue a credencial imediatamente.

## 5.10 Backup do sistema

VisMgmt é um aplicativo da Web auxiliar para um sistema de controle de acesso principal. Consulte a documentação do sistema de controle de acesso principal sobre o backup dos bancos de dados de sistema.

# 6 Operação

## 6.1 Visão geral das funções de usuário

| Tipo de usuário | Casos de uso |
|---|---|
| Recepcionista | Registro de novos visitantes e visitas<br>Aprovação e recusa de visitas<br>Inclusão de visitantes na lista negra<br>Atribuição e cancelamento de cartões de visitante<br>Gerenciamento dos documentos associados<br>Monitoramento do número de visitantes no local |
| Visitante | Registro próprio e pré-registro<br>Criação e manutenção de um perfil de visitante<br>Assinatura de documentos |
| Host | Gerenciamento de programações e listas de visitas e visitantes<br>Pré-registro de visitas |
| Administrador | Definição de configurações globais<br>Personalização do comportamento da ferramenta e da interface de usuário<br>Adicionalmente:<br>Todos os casos de uso de Recepcionista |

## 6.2 Uso do painel

O painel é a tela inicial, uma caixa de diálogo central que leva a todas as outras caixas de diálogo.

**Visão geral e filtros rápidos**

A parte superior do painel contém uma visão geral breve das visitas do dia. Isso permite que o usuário monitore com facilidade o número de visitantes do local.

| Visitantes esperados hoje: _% | Visitantes que fizeram check-in: _% | Visitantes que ainda farão check-out hoje | Visitantes atrasados para check-out |
|---|---|---|---|
| `<current count> / <total capacity>` | `<current count> / <total capacity>` | `<current count>` | `<current count>` |

Clique em qualquer cabeçalho para filtrar a tabela de visitas de acordo com o significado do cabeçalho. Por exemplo, clique em **Visitantes que fizeram check-in** para ver somente os visitantes aos quais um cartão foi atribuído.

O valor de `<total capacity>` é uma configuração definida pelo administrador do sistema. Consulte *Uso do menu Configurações para configuração, página 31*.

### 6.2.1 Visão geral da página da pessoa

No painel, clique no nome de uma determinada pessoa; uma caixa de diálogo com dados pessoais é aberta. Na página de dados. Nesta visão geral da página pessoal, há quatro seções de campos de dados pessoais:

- Imagem de ID
- Documento de identidade
- Informações gerais
- Documentos

## 6.2.2 A tabela de visitas

Cada linha da tabela representa uma visita marcada.

- Você pode classificar a tabela por qualquer coluna clicando no cabeçalho da coluna.
- Você pode selecionar visitas individuais ou várias visitas ao mesmo tempo, usando as expressões de teclado-mouse:
  - Ctrl + clique para a seleção múltipla de linhas individuais.
  - Shift + clique em uma linha já selecionada para removê-la da seleção.
  - Shift + clique para a seleção múltipla de linhas contíguas
- É possível adicionar novas visitas à tabela
- Você pode processar visitas e detalhes do visitante clicando nos botões de ação
  - Aprovar visita
  - Recusar visita
  - Atribuir cartões ao visitante
  - Editar detalhes do visitante e visitas
- Você pode exportar todos os dados para um arquivo .CSV ou .XLSX. Se desejar apenas alguns dados específicos, use a função de filtro. Não é possível exportar os dados desejados selecionando-os. Somente as linhas atualmente filtradas podem ser exportadas para um arquivo .CSV ou .XLSX.

A barra de ferramentas horizontal tem as seguintes funções:


| Marcação | Função |
|---|---|
| 1 N **entradas** | O número total N de visitas (cada visita é uma linha na tabela). |
| 2 **Pesquisar** | Procurar texto arbitrário entre as visitas na tabela |
| 3 | Mostre as visitas que foram adicionadas mais recentemente à tabela. |
| 4 | Abrir uma caixa de diálogo para selecionar critérios de filtragem |
| 5 | Redefina a tabela para a visualização padrão e reverta todos os filtros. |
| 6 **Cancelar atribuição do cartão** | Abra uma caixa de diálogo para cancelar os cartões atribuídos usando um leitor de inscrição conectado. |

| Marcação | Função |
|---|---|
|  | Abrir uma caixa de diálogo para criar uma nova entrada de visita na tabela |
| ... | Clique no símbolo de elipse para um menu para exportar as visitas filtradas atualmente, e também documentos, para vários formatos de arquivo, como, por exemplo `CSV` e `.XLSX`.<br>Observe que, por razões de segurança de dados, você só pode exportar se seu cliente estiver executando em uma conexão HTTPS segura, com um certificado. |

## 6.2.3 Colunas da tabela e ações

**Colunas**

| Coluna | Valor | Descrição |
|---|---|---|
| **Status** |  Visita esperada<br>  Visita aprovada<br>  Visita recusada<br>  Cartão atribuído<br>  Cartão expirou<br>  Visita encerrada (o visitante não tem mais cartões e saiu do local) | Um ícone que reflete o status da visita |
| **Nome** | O nome do visitante como um hiperlink | Clique no hiperlink para ver os detalhes do visitante e da visita atual. |
| **Chegada esperada** | Data e hora | A data e a hora esperadas da chegada do visitante |
| **Partida esperada** | Data e hora | A data e a hora esperadas da partida do visitante |
| **Check-in** | Data e hora | A data e a hora da atribuição do primeiro cartão para o visitante. |

| Coluna | Valor | Descrição |
|---|---|---|
| **Check-out** | Data e hora | A data e a hora do cancelamento do último cartão do visitante. |
| **Números de cartão** | Numérico | Os números dos cartões atribuídos a esse visitante. |
| | | |
| **Ações** | Ícones | Veja a tabela separada abaixo |

**Ações**

| Ícone | Função |
|---|---|
|  | **Aprove** a visita.<br>OBSERVAÇÃO: não é possível atribuir um cartão a visitantes da lista negra. Remova o visitante da lista negra primeiro ou libere-o temporariamente.<br>Consulte *Adição, remoção e isenção na lista negra, página 55* |
|  | **Recuse** a visita.<br>Esse botão é desativado depois que o visitante faz check-in, isto é, quando ele já tem um cartão. |
|  | **Atribuir** um ou mais cartões ao visitante |
|  | **Editar** o evento da visita e/ou as credenciais do visitante |

## 6.3 Recepcionista

### 6.3.1 Login na função de recepcionista

1. No navegador, abra `https://`<My_VisMgmt_server>`:5706/main/` para a tela de login.
2. Insira o nome de usuário de uma conta com os direitos necessários para sua função. Consulte o administrador do sistema se você não tiver uma conta.
3. Insira a senha.
4. Clique em **Login**.

### 6.3.2 Pesquisa e filtragem de visitas

No painel do VisMgmt, na barra de ferramentas acima da tabela de visitas.

**Pesquisar**

Para pesquisar nomes e hosts, insira um texto alfanumérico na caixa de pesquisa e pressione Return.

**Filtragem**

- Para ver as visitas mais próximas da hora atual, clique em **Mais recentes**
- Para criar um filtro complexo a partir do status da visita, das datas de check-in e check-out e dos números de cartão, clique em **Filtrar**.
  - Insira os critérios de filtro desejados na caixa de diálogo pop-up

- Clique em **Aplicar**
  O sistema reduz a tabela de visitas somente aos compromissos que satisfazem os critérios de filtro.
- Para excluir todos os critérios de filtro, clique em **Redefinir**

### 6.3.3 Registro de visitas

**Introdução**

Um recepcionista tem dois cenários básicos para registrar visitas:

- **A:** quando um visitante usa o quiosque para criar seu próprio ID de visitante e enviar documentos, o recepcionista só precisa preencher as informações necessárias e assinaturas que ainda estão faltando e atribuir um cartão ao visitante.
- **B:** quando um visitante ignora o quiosque e vai diretamente para a recepção, o recepcionista pode registrar a visita do zero: coletar as informações necessárias, coletar assinaturas para os documentos necessários e atribuir um cartão ao visitante.

O cenário **A** é um subconjunto do cenário **B**, de modo que o cenário **B** completo é descrito aqui. O uso do modo de quiosque por um visitante é descrito em uma seção separada. Consulte *Apresentação do modo de quiosque, página 58*.

**Procedimento**

No painel do VisMgmt, na barra de ferramentas acima da tabela de visitas.

1. Clique em  para adicionar uma visita marcada à tabela.
2. Na caixa de diálogo **Dados pessoais**, insira os dados que o local exige dos visitantes.
   Os campos obrigatórios são marcados com um asterisco (*).
   Você pode inserir os dados manualmente, mas é mais rápido e preciso usar um scanner de documentos para isso, se disponível na estação de trabalho do recepcionista.
   Consulte *Hardware periférico, página 26* para obter detalhes sobre os dispositivos periféricos compatíveis.

- **Informações gerais**
  - Localize e carregue um perfil de visitante inteiro criado em uma visita anterior.
    Para localizar perfis, clique no ícone  (pesquisar), localizado no campo **Sobrenome***.
    Quando um perfil de visitante é criado, ele recebe um código alfanumérico exclusivo que o visitante deve guardar com cuidado, para agilizar o processo de registro em visitas futuras.
  - Também é possível inserir dados manualmente.
- **Fotos de identificação**
  - **Envie** uma foto do sistema de arquivos.
  - **Tire** fotos do visitante com uma câmera da Web conectada.
- **Documentos de identidade**
  - Clique em **Digitalizar documento** para ler dados de um scanner de documentos (se disponível) e preencher automaticamente os campos de dados relevantes na caixa de diálogo.
  - Também é possível inserir dados manualmente, caso o sistema não tenha um scanner de documentos.
- **Documentos legais**
  - Carregue os documentos que o visitante assinou eletronicamente no quiosque.

- Se o sistema não tiver um quiosque de visitantes, imprima e registre (com a assinatura do visitante) os documentos PDF necessários armazenados no sistema de arquivos.

3. Clique em **Avançar** para continuar na caixa de diálogo **Visitas**.
4. Na caixa de diálogo **Visitas**, no painel **Visita atual**, insira os dados exigidos pelo local. Os campos obrigatórios são marcados com um asterisco (*).

- Selecione um **Tipo de visitante**.
  Existe um **Visitante** (padrão) ou uma subclasse personalizada de **Visitante**, definido como **Tipo de pessoa** no sistema de controle de acesso principal.
- Selecione em **Anfitrião** o nome do funcionário a ser visitado.
  - Observe que você só pode selecionar os titulares de cartão do sistema de controle de acesso principal.
  - Uma dica de ferramenta exibe o endereço de e-mail da pessoa como um auxílio à identificação.
- Se o visitante precisar de um acompanhante enquanto estiver no local, selecione o nome do funcionário acompanhante em **Acompanhante**.
  - Observe que você só pode selecionar os titulares de cartão do sistema de controle de acesso principal.
  - Uma dica de ferramenta exibe o endereço de e-mail da pessoa como um auxílio à identificação.
- Se o visitante precisar de mais tempo para passar por uma porta, marque a caixa de seleção **Tempo de abertura da porta estendido**

5. Clique em **Salvar**.
   Você não poderá salvar os dados até preencher todos os campos obrigatórios.

**Consulte**

- *Hardware periférico, página 26*

### 6.3.4 Aprovação e recusa de visitas

**Contexto: aprovação de cartões físicos**

É necessário aprovar uma visita antes de atribuir cartões a um visitante.

**Contexto: aprovação de credenciais móveis**

Você pode criar e compartilhar uma credencial móvel no dia da visita, de maneira semelhante à atribuição de um cartão físico.

- **Observação:** A credencial móvel não funcionará até que você aprove a visita.

*Como alternativa*, você pode criar a credencial móvel e compartilhá-la com antecedência. Quando o visitante chegar à recepção, aprove a visita, conforme descrito abaixo, para ativar a credencial.

- **Observação:** A credencial móvel não funcionará até que você aprove a visita.
- Se você definiu um horário de partida esperado para a visita, esse horário será aplicado.
- Se você não tiver definido um horário de partida esperado, um número padrão de horas (8) será aplicado. Os administradores podem alterar esse padrão no menu **Configurações**.

**Procedimentos de aprovação e negação**

Existem dois lugares para aprovar ou recusar uma visita:

- na tabela de visitas no painel

– no editor de visitas

**Na tabela de visitas no painel:**

– **Aprovar**: na tabela de visitas, selecione uma linha na tabela e clique em  . Depois de um menu pop-up de confirmação, o ícone fica cinza para mostrar que a visita foi aprovada.

– **Recusar**: na tabela de visitas, selecione uma linha na tabela e clique em  . Após um pop-up de confirmação, o ícone **Aprovar** é restaurado para azul, para mostrar que a visita ainda precisa ser aprovada.

**No editor de visitas:**

1. No painel, na tabela de visitas, selecione uma linha na tabela e clique em  para editar a visita.
2. Na caixa de diálogo **Dados pessoais**, clique em **Avançar**.
3. Na caixa de diálogo **Visitas**, clique no botão **Aprovar** ou **Recusar**.
4. Confirme sua ação na janela pop-up.

## 6.3.5 Atribuição de credenciais físicas

**Introdução**

Atribua um cartão para cada visitante que pode entrar no local. É possível atribuir vários cartões a um único visitante, se necessário.

– A hora do **Check-in** de uma visita é a hora da atribuição do primeiro cartão.
– A hora do **Check-out** de uma visita é a hora do cancelamento do último cartão que ainda está atribuído ao visitante.

O recepcionista pode atribuir e cancelar cartões com facilidade no painel, se um leitor de cartões de inscrição estiver conectado ao computador do recepcionista.
No entanto, o editor de visitas permite a atribuição de números de cartão, caso nenhum leitor esteja disponível.

**Aviso!**
As pessoas incluídas na lista negra não podem receber cartões
Não é possível atribuir cartões a visitantes que estão na lista negra. Remova o visitante da lista negra, ou crie uma isenção temporária para o visitante, antes de tentar atribuir um cartão.

**Atribuição de um cartão no painel (requer um leitor de inscrição)**

1. Tenha um cartão de visitante físico pronto para apresentar ao leitor de inscrição.
2. Na tabela de visitas, aprove a visita. Consulte *Aprovação e recusa de visitas, página 49*
3. Selecione a linha da visita e clique em 

4. Siga as instruções no menu pop-up para usar o leitor de inscrição.

**Cancelamento de um cartão no painel (requer um leitor de inscrição)**

1. Recolha o cartão físico do portador e deixe-o pronto para apresentar ao leitor de cadastramento.
2. Na barra de ferramentas, clique em **Cancelar cartão**. 
3. Siga as instruções no menu pop-up para usar o leitor de inscrição.

**Atribuição de um cartão no editor de visitas**

1. No painel, na tabela de visitas, selecione uma linha na tabela e clique em  para editar essa visita.
2. Na caixa de diálogo **Dados pessoais**, clique em **Avançar**
3. Na caixa de diálogo **Visitas**, se a visita ainda não tiver sido aprovada, clique em **Aprovar**.
4. Se houver um leitor de cadastramento conectado, clique em **Ler cartão** e siga as instruções do menu pop-up para usar o leitor de cadastramento.

– Caso contrário, clique em **Mostrar cartões livres** para exibir uma lista dos cartões de visitantes ainda disponíveis.
  Como alternativa, se você tiver cartões físicos não classificados com números impressos, selecione qualquer cartão e use a ferramenta de **Pesquisa** para encontrar o número dele rapidamente na lista.
– Clique em  ao lado de um número de cartão para atribuir o cartão em questão ao visitante atual.
– Repita as últimas etapas para atribuir outros cartões, se necessário.

5. Clique em **Salvar** para salvar a visita atual com as atribuições de cartão.

**Cancelamento de um cartão no editor de visitas**

1. No painel, na tabela de visitas, selecione uma linha na tabela e clique em  para editar essa visita.
2. Na caixa de diálogo **Dados pessoais**, clique em **Avançar**
3. Na caixa de diálogo **Visitas**, no painel Cartões de visitante, clique em  ao lado do cartão que deseja cancelar e confirme a ação na janela pop-up.
   Repita essa etapa até cancelar todos os cartões desejados.
4. Clique em **Salvar** para salvar a visita atual com as atribuições de cartão.
5. Ao cancelar o último cartão atribuído ao visitante, o sistema registra essa data e hora como a hora do check-out do visitante.

   Na tabela de visitas, o status desse registro de visita se torna 

**Consulte**

- *Uso do menu Configurações para configuração, página 31*
- *Registro de visitas, página 48*
- *Aprovação e recusa de visitas, página 49*

### 6.3.6 Atribuição de credenciais móveis

**Pré-requisitos**

- O Mobile Access está instalado e configurado no seu sistema.
  - Para obter instruções, consulte a seção relevante no capítulo de instalação deste documento.
- A pessoa destinatária instalou o aplicativo Mobile Access e ele está em execução em seu dispositivo inteligente.
  - Para obter instruções, consulte a seção relevante no capítulo de instalação deste documento.

**Procedimento**

É possível atribuir credenciais móveis diretamente do ícone do painel ou da visão geral da página pessoal.

No **Painel**:

1. Selecione a linha da pessoa que vai receber credenciais móveis
2. Na linha selecionada, clique em 

Na visão geral da página pessoal:

1. No **Painel**, selecione o nome da pessoa e a visão geral da página da pessoa é aberta.
2. Selecione a guia **Credencia**l > **Adicionar acesso móvel.**

Prossiga com as seguintes instruções:

1. Selecione um dos ícones grandes para as opções:

- **Código QR**

  ou

- **E-mail de convite**

2. Se você selecionou a **opção de código QR**:

- O sistema exibe um código QR
- A pessoa faz a leitura do código QR com o aplicativo Mobile Access em seu dispositivo móvel
- Para que a credencial funcione, você deve **aprovar** a visita.
  Para obter instruções, consulte a seção *Aprovação e recusa de visitas, página 49*
- O dispositivo móvel funciona como um cartão de acesso físico, desde que o aplicativo esteja em execução

3. Se você selecionou a **opção de e-mail de convite**:

- Por padrão, o programa seleciona o endereço de e-mail definido para a pessoa selecionada. Insira um endereço de e-mail alternativo, se necessário
- O sistema envia um e-mail para o endereço selecionado
- A pessoa recebe o e-mail em seu dispositivo móvel, que está executando o aplicativo Mobile Access
- A pessoa abre o link no e-mail
- Para que a credencial funcione, você deve **aprovar** a visita.
  Para obter instruções, consulte a seção *Aprovação e recusa de visitas, página 49*
- O dispositivo móvel funciona como um cartão de acesso físico, desde que o aplicativo esteja em execução

**Procedimento nas caixas de diálogo de edição**

1. Selecione a linha da pessoa que vai receber credenciais móveis
2. Na linha selecionada, clique em 
– A caixa de diálogo de edição é aberta
3. No VisMgmt, clique em **Avançar** para prosseguir para a tela **Detalhes da visita**
4. Clique no botão **Adicionar Mobile Access**
5. Selecione um dos ícones grandes para as opções:
– **Código QR**
ou
– **E-mail de convite**
6. Se você selecionou a **opção de código QR**:
– O sistema exibe um código QR
– A pessoa faz a leitura do código QR com o aplicativo Mobile Access em seu dispositivo móvel
– Para que a credencial funcione, você deve **aprovar** a visita.
Para obter instruções, consulte a seção *Aprovação e recusa de visitas, página 49*
– O dispositivo móvel funciona como um cartão de acesso físico, desde que o aplicativo esteja em execução
7. Se você selecionou a **opção de e-mail de convite**:
– Por padrão, o programa seleciona o endereço de e-mail definido para a pessoa selecionada. Insira um endereço de e-mail alternativo, se necessário
– O sistema envia um e-mail para o endereço selecionado
– A pessoa recebe o e-mail em seu dispositivo móvel, que está executando o aplicativo Mobile Access
– A pessoa abre o link no e-mail
– Para que a credencial funcione, você deve **aprovar** a visita.
Para obter instruções, consulte a seção *Aprovação e recusa de visitas, página 49*
– O dispositivo móvel funciona como um cartão de acesso físico, desde que o aplicativo esteja em execução

**Consulte**

– *Instalação do Mobile Access, página 19*
– *Instalação dos aplicativos do Mobile Access, página 18*

## 6.3.7 Cancelar atribuição de credenciais

**Cancelamento de um cartão no painel (requer um leitor de inscrição)**

1. Recolha o cartão físico do portador e deixe-o pronto para apresentar ao leitor de cadastramento.
2. Na barra de ferramentas, clique em **Cancelar cartão**. 
3. Siga as instruções no menu pop-up para usar o leitor de inscrição.

**Cancelamento de um cartão no editor de credenciais**

1. No painel, selecione uma linha da tabela principal e clique em  para editar esse portador de cartão.
2. Na caixa de diálogo de edição, na coluna **Cartões de funcionário**, clique em  ao lado do cartão que deseja cancelar e confirme a ação na janela pop-up.
   Repita essa etapa até cancelar todos os cartões desejados.
3. Clique em **Salvar** para salvar a visita atual com as atribuições de cartão.

## 6.3.8 Check-in e check-out sem cartão

**Introdução**

Se os visitantes tiverem acompanhantes próximos ou estiverem restritos a espaços públicos, cartões individuais para visitantes podem ser desnecessários. Para esses casos existe a opção de fazer check-in e check-out de visitantes sem cartões. Por questões de segurança, essa opção fica desativada por padrão.

**Pré-requisito.**

O administrador do sistema habilitou a opção especial **Check-in/check-out sem cartão** na caixa de diálogo **Configurações** > **Recepcionista > Visitas**. Consulte o capitulo de configuração *Uso do menu Configurações para configuração, página 31* para mais instruções.

**Processamento**

Quando a opção é ativada, ocorre o seguinte:

– Qualquer visitante que se cadastra no computador do quiosque aprova automaticamente a visita e faz check-in ao mesmo tempo.
– O sistema define a data e a hora do check-in para o momento da inscrição.
– O botão de alternar **check-in/check-out sem cartão** aparece no editor de visitas e no painel de instrumentos para a mesma visita.

**Procedimento: check-in de um visitante sem cartão**

Se um visitante não conseguir se cadastrar no quiosque, mas deve fazer o check-in sem um cartão:

1. registre a visita manualmente, como descrito no capítulo *Registro de visitas, página 48*
2. No painel, na tabela de visitas, clique no nome do visitante na tabela ou em  para editar a visita.
3. Na caixa de diálogo **Dados pessoais**, clique em **Avançar**
4. No diálogo **Visitas**, no painel **Cartões de visitantes**, clique em **Entrada sem cartão**

**Procedimento: check-out de visitante sem cartão**

Se um visitante sem cartão sair do local:

1. No painel, na tabela de visitas, clique no nome do visitante na tabela ou em  para editar a visita.

2. Na caixa de diálogo **Dados pessoais**, clique em **Avançar**
3. No diálogo **Visitas**, no painel **Cartões de visitantes**, clique em **Check-out sem cartão**

**Consulte**

– *Registro de visitas, página 48*

## 6.3.9 Adição, remoção e isenção na lista negra

Os visitantes que não são bem-vindos no local podem ser colocados em uma lista negra. Enquanto o visitante estiver na lista negra, não será possível atribuir um cartão a essa pessoa. Você pode remover o visitante da lista negra a qualquer momento, ou conceder uma isenção temporária, para atribuir um cartão.

**Inclusão na lista negra**

1. No painel, na tabela de visitas, selecione uma linha na tabela e clique em  para editar uma visita.
2. Na caixa de diálogo **Dados pessoais**, clique em **Lista negra**.
3. Na janela pop-up, confirme que você deseja incluir essa pessoa na lista negra.
4. Na próxima janela pop-up, insira um motivo para a inclusão e confirme.

– Um banner **Incluído na lista negra** aparece no editor de visitantes,


– Dois botões aparecem sob o banner: um para remover o visitante da lista negra e um para conceder uma isenção temporária.
– Na tabela de visitas, o nome de cada visitante incluído na lista negra aparece com um triângulo de advertência. Por exemplo: 


**Remoção e isenção**

1. No painel, na tabela de visitas, selecione uma linha na tabela onde o visitante está marcado como incluído na lista negra e clique em  para editar a visita.
2. Na caixa de diálogo **Dados pessoais**, clique em um destas opções:

– **Remover** para remover o visitante permanentemente da lista negra.
– **Isentar** para manter o visitante na lista negra, mas permitir a atribuição de um cartão somente para essa visita.

3. Confirme sua ação na janela pop-up.

## 6.3.10 Manutenção dos perfis de visitante

O sistema mantém os perfis de visitante até que sejam excluídos pelos próprios visitantes, recepcionistas ou administradores.
Depois de um período de retenção definido nas configurações do sistema (valor padrão de 12 meses), o sistema exclui os registros da visita.
Quando um visitante ou recepcionista cria um novo perfil de visitante, o perfil recebe um código alfanumérico exclusivo. Os visitantes podem fazer login com esse código no quiosque e, assim, obter acesso para manter seus próprios perfis.

**Aviso!**
Proteger IDs de visitante
Proteja os IDs de visitantes com cuidado contra o acesso não autorizado, pois eles fornecem acesso a dados pessoais.

### 6.3.11 Visualização de registros de visita

1. No painel, na tabela de visitas, selecione uma linha na tabela e clique em  para editar essa visita.
2. Na caixa de diálogo **Dados pessoais**, clique em **Avançar**
3. Na caixa de diálogo **Visita atual**, clique em **Mostrar todas as visitas**
   A caixa de diálogo **Visita atual** mostra uma lista das visitas anteriores.

## 6.4 Host

Os hosts são funcionários que recebem visitas. Eles podem registrar seus próprios compromissos e procurar no sistema detalhes de visitantes e registros de visitas: passadas, presentes e futuras.

### 6.4.1 Login na função de host

1. No navegador, abra `https://<My_VisMgmt_server>:5706/main/` para a tela de login.
2. Insira o nome de usuário de uma conta com os direitos necessários para sua função. Consulte o administrador do sistema se você não tiver uma conta.
3. Insira a senha.
4. Clique em **Login**.

### 6.4.2 Pesquisa e filtragem


A barra de ferramentas do painel Host contém as seguintes funções:

| Marcação | Função |
|---|---|
| 1 N **entradas** | O número total N de visitas (cada visita é uma linha na tabela). |
| 2 **Pesquisar** | Procurar texto arbitrário entre as visitas na tabela |
| 3 | Mostre as visitas que foram adicionadas mais recentemente à tabela. |
| 4 | Abrir uma caixa de diálogo para selecionar critérios de filtragem |

| Marcação | Função |
|---|---|
|  | Redefina a tabela para a visualização padrão e reverta todos os filtros. |
|  | Abrir uma caixa de diálogo para criar uma nova entrada de visita na tabela |

**Pesquisar**

Para pesquisar nomes e hosts, insira um texto alfanumérico na caixa de pesquisa e pressione Return.

**Filtragem**

- Para ver as visitas mais próximas da hora atual, clique em **Mais recentes**
- Para criar um filtro complexo a partir do status da visita, das datas de check-in e check-out e dos números de cartão, clique em **Filtrar**.
  - Insira os critérios de filtro desejados na caixa de diálogo pop-up
  - Clique em **Aplicar**
    O sistema reduz a tabela de visitas somente aos compromissos que satisfazem os critérios de filtro.
- Para excluir todos os critérios de filtro, clique em **Redefinir**

## 6.4.3 Registro de visitas

Para registrar uma visita marcada de um visitante pela primeira vez:
No painel do VisMgmt, na barra de ferramentas acima da tabela de visitas.

1. Clique em  para adicionar uma linha à tabela de visitas
2. Na caixa de diálogo **Dados pessoais**, na seção **Informações gerais**, insira os dados pessoais que o local exige dos visitantes.
3. Na seção **Detalhes da visita**, insira os detalhes necessários, normalmente as horas esperadas de chegada e partida, além do motivo da visita.
4. Clique em **Salvar** para salvar a visita marcada.
   A visita aparece no painel como uma linha na tabela de visitas.

## 6.4.4 Cópia de visitas marcadas

Para programar outra visita do mesmo visitante

1. No painel do VisMgmt, encontre um compromisso existente do mesmo visitante na tabela de visitas.
2. Clique no ícone  menor no final da linha.
3. Na caixa de diálogo **Dados pessoais**, na seção **Detalhes da visita**, insira os detalhes necessários, normalmente as horas esperadas de chegada e partida, além do motivo da visita.

4. Clique em **Salvar** para salvar a visita marcada.
   A visita aparece no painel como uma linha na tabela de visitas.

## 6.5 Visitante

Os visitantes podem usar o sistema no modo de quiosque no local para criar seus próprios perfis de visitante e assinar os documentos necessários antes de se dirigirem à recepção para pegar os cartões de visitante.

### 6.5.1 Apresentação do modo de quiosque

Os visitantes normalmente registram as visitas e criam seus próprios perfis em um computador com livre acesso na área da recepção do local com controle de acesso. Por motivos de segurança, o navegador da Web do computador é executado no modo de quiosque, que permite o acesso somente ao VisMgmt e não a várias guias, configurações do navegador ou ao sistema operacional do computador. Todos os navegadores compatíveis oferecem o modo de quiosque, mas a configuração exata depende do navegador.
O computador do quiosque executa o software cliente do complemento de **dispositivos periféricos Bosch**, o que permite realizar conexões físicas com dispositivos periféricos para digitalizar documentos de identidade e assinaturas.

– O URL do modo de quiosque é `https://`<My_VisMgmt_server>`:5706`
– Em contrapartida, o URL para fazer login como administrador, recepcionista ou host é `https://`<My_VisMgmt_server>`:5706/main/`

### 6.5.2 Criação de um perfil de visitante: check-in automático

**Visitantes pela primeira vez**

O procedimento exato depende dos dispositivos periféricos, como scanners de documentos e assinaturas e câmeras fotográficas, disponíveis para o computador do quiosque.

1. Na tela de boas-vindas no computador do quiosque, clique em **Continuar sem ID do visitante.**
2. Na próxima tela, clique em **Check-in automático**.
3. Na próxima tela, selecione **Digitalizar documento**.
4. Siga as instruções na tela para requisitos específicos do local, como:
– digitalização de documentos de identidade,
– assinatura de qualquer outro documento legal necessário,
– captura de uma foto.
5. O sistema exibe as informações coletadas para você corrigir e preencher.
6. O sistema pergunta se você precisa de autorizações de acesso especiais e comunica isso para a recepção, se necessário.
7. No final do processo de check-in, a tela exibe um ID de visitante exclusivo.
   Leve esse ID para a recepção para receber seu cartão de visitante.

**Aviso!**
Seu ID de visitante exclusivo
Anote com atenção o ID de visitante e proteja-o contra uso não autorizado. Ele fornece acesso ao seu perfil de visitante. Você pode usá-lo para fazer login no computador do quiosque e, assim, agilizar seu próximo check-in.

**Visitantes frequentes**

1. Faça login no quiosque com seu ID de visitante exclusivo.
2. O sistema exibe as informações coletadas para você corrigir e preencher, se necessário.
3. Vá para a recepção pegar seu cartão de visitante.

## 6.6 Autorização de instaladores de leitores de acesso móvel

**Introdução**

Os instaladores de leitores de acesso móvel usam o Bosch Setup Access para fazer a leitura e configurar os leitores via BLE.

Os operadores autorizados do **Credential Management** e **Visitor Management** enviam credenciais virtuais para o aplicativo de instalador a fim de autorizar o instalador. Esta seção descreve esse procedimento.

**Pré-requisitos**

- O Mobile Access está instalado e configurado no seu sistema.
  - Para obter instruções, consulte a seção relevante no capítulo de instalação deste documento.
- Verifique se o instalador que está recebendo a autorização instalou o Bosch Setup Access, e se ele está em execução em seu dispositivo inteligente.
  - Para obter instruções, consulte a seção relevante no capítulo de instalação deste documento.

**Procedimento**

1. No menu principal, clique em  para abrir a caixa de diálogo **Integração de instalador**.
2. Clique em **Adicionar** para adicionar um instalador à lista ou clique em  para excluir um instalador existente

- A janela pop-up **Adicionar instalador** é exibida.

3. Na janela pop-up **Adicionar instalador**, insira os detalhes necessários, por exemplo:

- Nomes pessoais, nome de empresa, endereço de e-mail, número de telefone
- Observação: Você pode clicar em  para modificar os detalhes de um instalador selecionado posteriormente

4. Clique em **Next (Próximo)**
5. Selecione um dos ícones grandes para as opções:

- **Código QR**

  ou

- **E-mail de convite**

6. Se você selecionou a **opção de código QR**:

- O sistema exibe um código QR
- A pessoa faz a leitura do código QR com o aplicativo Mobile Access em seu dispositivo móvel
- Isso conclui o processo de registro do instalador
- Ele permite que o dispositivo móvel procure leitores de acesso móvel e os configure via BLE, desde que o aplicativo esteja em execução

7. Se você selecionou a **opção de e-mail de convite**:

– Por padrão, o programa seleciona o endereço de e-mail definido para a pessoa selecionada. Insira um endereço de e-mail alternativo, se necessário
– O sistema envia um e-mail para o endereço selecionado
– A pessoa recebe o e-mail em seu dispositivo móvel, que está executando o Bosch Setup Access
– A pessoa abre o link no e-mail
– Isso conclui o processo de registro do instalador
– Ele permite que o dispositivo móvel procure leitores de acesso móvel e os configure via BLE, desde que o aplicativo esteja em execução

**Reenvio de convites**

1. Na caixa de diálogo de integração de instalador, selecione o instalador desejado
2. Clique em  na mesma linha para reenviar a autorização para o instalador selecionado por código QR ou e-mail.
   **OBSERVAÇÃO:** Você só poderá reenviar a autorização se o instalador ainda não tiver ativado ela.

### 6.6.1 Redefinição de leitores do Mobile Access

Pode ser necessário redefinir leitores de acesso para os padrões de fábrica com o intuito de reconfigurá-los.
Por exemplo, se um instalador precisar reconfigurar leitores do Mobile Access que já foram configurados para um local diferente, esses leitores exigirão redefinição.
Consulte o manual do leitor do LECTUS select para obter uma descrição de como redefinir o leitor usando os interruptores DIP.

## 6.7 Como usar os aplicativos do Mobile Access em dispositivos móveis

**OBSERVAÇÃO:** O uso dos aplicativos do Bosch Mobile Access está descrito em detalhes para os respectivos usuários em **Guias Rápidos** separados. Estes documentos estão disponíveis no catálogo de produtos online da Bosch.

**Introdução**

A Bosch fornece os seguintes aplicativos para Mobile Access

– Bosch Mobile Access: um aplicativo de portador de cartão para armazenar credenciais virtuais e transmiti-las via Bluetooth para os leitores configurados para Mobile Access. Esses leitores concedem ou negam acesso dependendo se uma das credenciais armazenadas do aplicativo é válida para ele.
– Bosch Setup Access: um aplicativo de instalador para fazer a leitura e configurar os leitores via Bluetooth.

Os operadores autorizados de Visitor Management e Credential Management podem enviar credenciais virtuais para aplicativos de portador de cartão e instalador.

**Aviso!**
IMPORTANTE: Não opere os aplicativos de portador de cartão e instalador simultaneamente Certifique-se de que ninguém use o aplicativo de instalador enquanto o aplicativo de portador de cartão estiver em uso, e vice-versa.

### 6.7.1 Definição de limites RSSI no aplicativo Setup Access

**Introdução**

O limite RSSI e a faixa de BLE podem ser considerados conceitos praticamente equivalentes no contexto do Bosch Mobile Access.

Os dispositivos de acesso móvel transmitem sinais de BLE para leitores próximos. Uma parte importante da configuração do leitor é a definição de um limite RSSI para cada leitor. Esse limite é a intensidade mínima do sinal de BLE, medida em dBm, que o leitor (R) deve aceitar como uma solicitação de acesso. O leitor deve ignorar todos os sinais de BLE mais fracos.


Os valores de RSSI podem variar muito dependendo de diversos fatores, incluindo o tipo de dispositivo de transmissão, o nível da bateria e o material e a espessura das paredes nos arredores. Não há relação linear entre o valor de RSSI e a distância entre o transmissor e o receptor.

Por esse motivo, o aplicativo Setup Access fornece uma ferramenta para medir o RSSI do leitor a partir da posição atual do dispositivo móvel. O procedimento abaixo descreve como usar essa ferramenta.

Quando você encontrar um valor de limite adequado para o intervalo de BLE, use o aplicativo Setup Access para armazenar esse valor na configuração do leitor.

**Procedimento**

Configure a **faixa de BLE** usando uma das seguintes opções, A ou B:

**A:** Usar valores de RSSI refletidos pelo leitor

1. Posicione-se diante do leitor, no lugar em que você espera que o usuário de credencial móvel esteja.
2. Toque em **Verificar e usar a faixa atual**

– Uma mensagem pop-up será exibida. Toque em **OK**

3. Um valor de RSSI aparecerá.

– Recomendado: Repita este passo algumas vezes na mesma posição para ter uma ideia do grau de variância na intensidade do sinal percebido.

4. Quando você encontrar um valor de limite adequado, toque em **Salvar.**

**B:** Definir o limite RSSI manualmente

1. Insira um valor no limite RSSI.
   Consulte a tabela de limites típicos abaixo
2. Toque em **Salvar**

**Valores típicos de limite (apenas aproximados):**

| Distância esperada entre o dispositivo móvel e o leitor | Limite RSSI sugerido |
|---|---|
| Baixa (5 cm a 10 cm) | -30 ... -40 dBm |
| Média (0,5 m a 2 m) | -50 ... -60 dBm |
| Alta (>2 m) | -70 ... -90 dBm |

**Aviso!**
Os valores de RSSI podem variar muito dependendo de diversos fatores, incluindo o tipo de dispositivo de transmissão, o nível da bateria e o material e a espessura das paredes nos arredores.

# Glossário

**ACS**

termo genérico para um sistema de controle de acesso (Access Control System) da Bosch, por exemplo, AMS (Access Management System) ou ACE (BIS Access Engine).

**BLE**

Bluetooth Low Energy é uma tecnologia de rede sem fio que fornece um alcance de comunicação semelhante ao Bluetooth, mas com consumo de energia mais baixo.

**FQDN**

Um nome de domínio totalmente qualificado é um nome de domínio de rede que expressa seu local absoluto na hierarquia do sistema de nome de domínio (DNS).

**host**

no contexto do gerenciamento de visitantes, o host é o visitado, isto é, a pessoa que recebe o visitante.

**Mobile Access**

controle de acesso de pessoas que usam credenciais virtuais armazenadas em um dispositivo móvel, como um smartphone.

**modo de quiosque**

Um modo extremamente restrito de uso do navegador que normalmente permite o acesso apenas a um único aplicativo da Web, e não às configurações do navegador, várias guias ou ao sistema operacional do computador.

**OSDP**

Open Supervised Device Protocol (Protocolo de dispositivo supervisionado aberto) é um padrão de comunicações de controle de acesso lançado em 2011 pela Security Industry Association (SIA). Ele oferece vantagens em relação a protocolos mais antigos nas áreas de criptografia, biometria, facilidade de uso e interoperabilidade.

**RSSI**

o indicador de intensidade do sinal recebido (RSSI) é a intensidade de sinal percebida por um dispositivo receptor, medida em dBm. Os dispositivos móveis normalmente exibem o RSSI em um gráfico de barra de intensidade de sinal.

**Bosch Security Systems B.V.**
Torenallee 49
5617 BA  Eindhoven
Países Baixos
**www.boschsecurity.com**


**Soluções prediais para uma vida melhor**

202405131940