Credential 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 Credential Management e Visitor Management

Credential Management, doravante chamado de CredMgmt, é uma ferramenta de software baseada em navegador que opera em conjunto com um sistema de controle de acesso da Bosch ou ACS. Com uma interface de usuário simples e intuitiva, ela permite que até operadores relativamente inexperientes gerenciem as credenciais de acesso de funcionários e pessoal externo. As credenciais em si podem ser cartões físicos ou credenciais móveis.

Credential Management

No CredMgmt, os operadores de ACS podem gerenciar as credenciais e os registros dos funcionários a quem as credenciais pertencem.

Entidade	Adicionar	Modificar	Excluir	Atribuir/ Cancelar atribuição
Credenciais físicas				Sim
Credenciais virtuais "móveis" (se Mobile Access estiver instalado)	Sim		Sim	Sim
Authorizations (Autorizações)				Sim
Registros de portador de cartão	Sim	Sim	Sim	

Gerenciamento de visitantes

No VisMgmt, os operadores do ACS gerenciam credenciais, registros de visitantes e registros de visitas.

Entidade	Adicionar	Modificar	Excluir	Atribuir/ Cancelar atribuição
Credenciais físicas				Sim
Credenciais virtuais "móveis" (se Mobile Access estiver instalado)	Sim			Sim
Registros de visitantes	Sim	Sim	Sim	
Registros de visitas	Sim	Sim	Sim	

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.

3 Instalação e desinstalação

3.1 Pré-requisitos de software

Você instala o servidor CredMgmt no mesmo computador que o ACS (sistema de controle de acesso principal). Os mesmos requisitos de software e hardware se aplicam.
Se o sistema de controle de acesso principal ainda não estiver instalado, certifique-se de instalá-lo primeiro antes de instalar o Credential 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.

O CredMgmt e os programas de configuração do Mobile Access têm suas próprias mídias de instalação, separadas do ACS. Eles podem ser baixados nos catálogos de produtos online da Bosch.

Aviso!
Necessidade de um certificado raiz estável
Antes de prosseguir com as instalações a seguir, certifique-se de que a instalação do ACS esteja concluída e licenciada, de acordo com seu próprio guia de instalação. Isto inclui uma decisão final sobre o certificado raiz do servidor ACS (seja autoassinado ou baseado em CA) e sua implementação estável. Alterações pós-hoc no certificado raiz do servidor ACS exigiriam a reconfiguração de certificados em todos os computadores e leitores de acesso móvel que participam em seu sistema de controle de acesso.

Requisitos do servidor
O servidor é o computador que executa o ACS e o aplicativo CredMgmt.

Sistemas operacionais	– Windows 11 Professional e Enterprise 23H2; – Windows Server 2019 (Version 1809) (64bit, Standard, Datacenter); – Windows Server 2022 (64 bits, Standard, Datacenter)
Sistemas de gerenciamento de banco de dados	– MS SQL Server 2019 and later 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) Use a versão mais recente do navegador para o seu sistema operacional Windows.

Requisitos do cliente

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

3.2 Pré-requisitos de hardware

Leitores de cadastramento

CredMgmt exige pelo menos um leitor de cadastro para cadastrar cartões físicos. Os leitores de cadastro geralmente são instalados em estações de trabalho clientes. A estação de trabalho cliente se comunica com hardware periférico por meio de um programa chamado `BoschPeripheralDeviceAddon.exe`. A instalação deste programa é descrita abaixo.

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

3.2.1 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.

3.3 Instalação do Credential Management

Introdução

CredMgmt é executado como um aplicativo da Web em conjunto com um sistema de controle de acesso (ACS) da Bosch. As seções a seguir descrevem a instalação do componente back-end que executa este aplicativo da Web.

- Você pode instalá-lo para usar um banco de dados local ou remoto.

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.

3.3.1 Pré-requisitos do CredMgmt

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

O usuário `CMUser` acessa o banco de dados do ACS em nome do aplicativo CredMgmt. Se o CredMgmt for para usar um banco de dados em um servidor de banco de dados remoto, use o procedimento a seguir.

IMPORTANTE: Não execute a configuração do CredMgmt antes de concluir este 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>\`CMUser`

- **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 CredMgmt.
- **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 CMUser 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 CMUser
6. No painel **Selecione uma página**, selecione **Funções de servidor**
7. Marque as caixas de seleção public e dbcreator

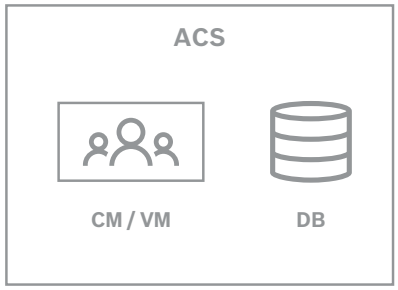
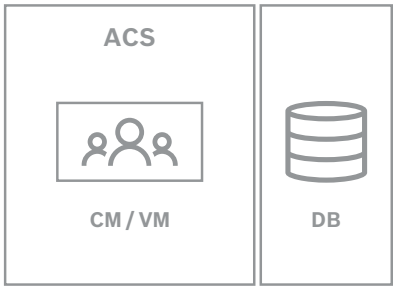
Usuário dedicado para o banco de dados local (somente se você estiver usando um banco de dados local)

O usuário CMUser acessa o banco de dados do ACS em nome do aplicativo CredMgmt. Você NÃO precisa criar esse usuário se o CredMgmt for para usar um banco de dados local, pois o programa de configuração do CredMgmt cria um usuário CMUser do Windows no servidor ACS automaticamente.

Um usuário dedicado no ACS

1. No ACS, crie um usuário que tenha o recurso **de uso ilimitado de API**.
   - Caminho de diálogo no AMS: **Configuração** > **Operadores e estações de trabalho** > **Direitos do usuário** > guia: **Conta de usuário** > **Controle de direitos de acesso à API.** Escolha Unlimited access da lista.
   - Caminho de diálogo no BIS: **Configuração Navegador** > **Administração** > **Operadores** > Selecionar o operador > guia: **Direitos de acesso do ACE API.** Selecione Unlimited access.
   - Para obter instruções mais detalhadas, consulte o capítulo **Atribuição de perfis de usuário (operador)** no manual do operador do ACS.
2. Anote o nome de usuário e a senha com atenção, pois o assistente de instalação do aplicativo da Web irá solicitá-los.

3.3.2 Procedimento de instalação

CredMgmt com DB local	CredMgmt com DB remoto
	

Procedimento

1. No servidor ACS, execute `BoschCredentialManagementServer.exe` como Administrador.

– O programa de instalação é aberto

2. Na tela **Componentes principais**, selecione `Bosch Credential Management` e clique em **Avançar**
3. Leia com cuidado e clique em **Aceitar** se desejar aceitar o Contrato de Licença de Usuário Final (EULA). A instalação só poderá prosseguir se você fizer isso.
4. Procure e selecione uma pasta de destino para a instalação ou aceite a seleção padrão (recomendado), clique em **Avançar**
5. 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)**

6. Na tela **Configuração de acesso ACS**:

– Insira o nome do host do servidor ACS.
– Insira o nome de um usuário do ACS com uso ilimitado de API (consulte Pré-requisitos acima).
– Insira a senha do ACS para este usuário do ACS e confirme-a.

7. 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 o CredMgmt está selecionado e clique em **Instalar**
10. Quando a instalação for concluída, inicie o CredMgmt com a seguinte URL:
`https://` <NameOfACSserver>`:5806`

3.4 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.

3.4.1 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.

3.4.2 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

3.4.3 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:

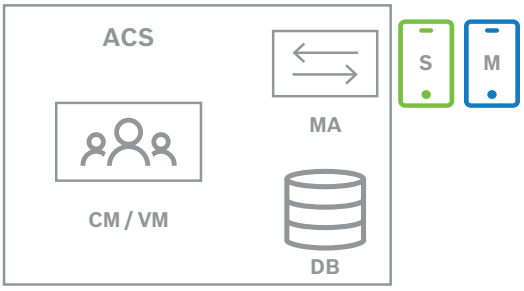
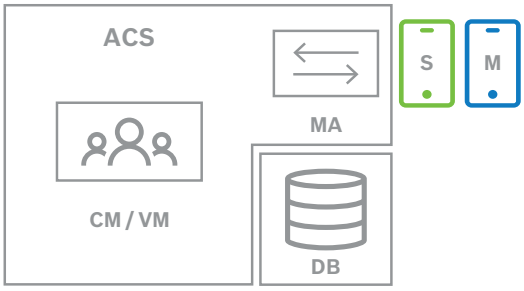
1. Abra o SQL Management Studio
2. Conecte-se à instância SQL remota
3. Acesse **Segurança** > **Login**
4. No painel **Selecione uma página**, selecione **Geral**

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.

3.4.4 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
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**

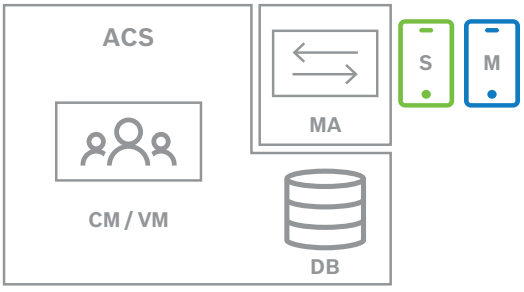
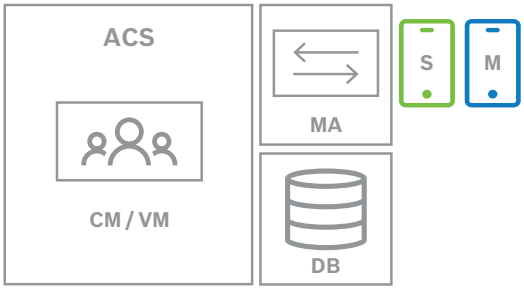
4. Na tela do **EULA**, leia atentamente e clique em **Aceitar** se quiser aceitar o Contrato de Licença de Usuário Final (EULA). A instalação só poderá prosseguir se você fizer isso.
5. Na tela **Diretório de instalação**:
– Procure e selecione uma pasta de destino para a instalação ou aceite a seleção 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.

3.4.5 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.

Distribuída com banco de dados local	Distribuída 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
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
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.

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

3.5.1 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.

3.5.2 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**.

3.5.3 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

3.6 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.

3.7 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.

4 Visão geral do Credential Management

A seguir ilustramos possíveis topologias de instalações do Credential Management, com e sem o Mobile Access. Cada caixa anexa representa um computador separado.

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
M	Aplicativo de acesso “Mobile Access” para dispositivos móveis de portadores de credenciais normais.

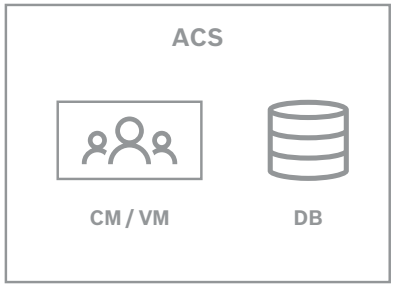
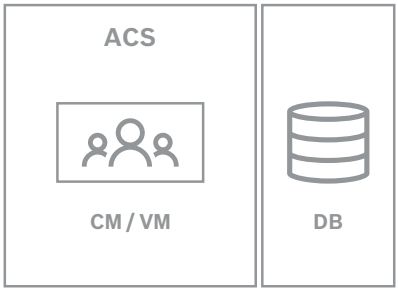
Credential Management, DB local	Credential Management, DB remoto
	

Tabela 4.1: Topologias do Credential Management

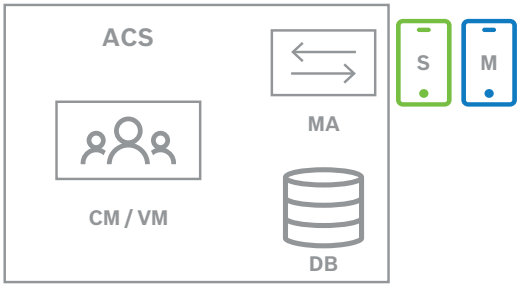
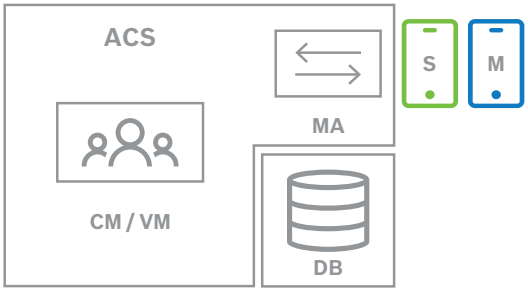
Mobile Access, colocalizado, DB local	Mobile Access, colocalizado, DB remoto
	

Tabela 4.2: Topologias colocalizadas de Mobile Access

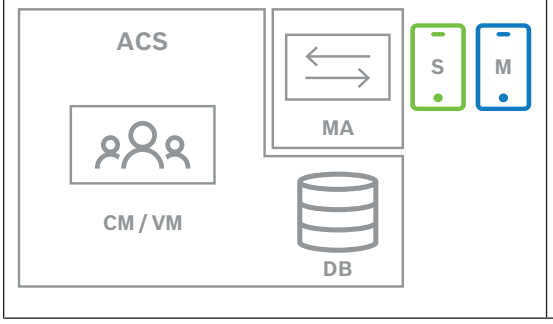
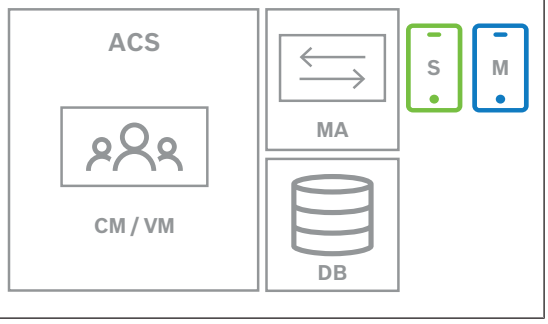
Mobile Access, distribuído, DB local	Mobile Access, distribuído, DB remoto
	

Tabela 4.3: Topologias distribuídas de Mobile Access

Versões compatíveis de software relacionado

A tabela a seguir lista as versões de ferramentas de software auxiliares compatíveis com esta versão do sistema.

Componente	Versão	Localização
Access Management System (AMS)	5.5 (inclui extensão para Mobile Access)	Baixar Loja/Catálogo de Produtos
Visitor Management (VisMgmt)	5.5 (inclui extensão para Mobile Access)	Baixar Loja/Catálogo de Produtos

Aviso!

Divisões

Credential Management, Visitor Management e Mobile Access não suportam o recurso "Divisões" dos sistemas de controle de acesso da Bosch, onde um (ACS) administra o controle de acesso de vários locatários independentes.

5 Configuração

5.1 Criação de usuários do Credential Management no ACS

No ACS (ACE ou AMS), cada usuário do Credential Management deve ser um titular de cartão com uma definição de Operador separada.

Essas definições de Operador contêm direitos de CredMgmt especiais na forma de **perfis do usuário**.
É necessário definir um Operador separado para cada titular de cartão que trabalhe no CredMgmt. Não é possível atribuir vários portadores de cartões ao mesmo operador.
Consulte a ajuda on-line em seu ACS para obter informações detalhadas e instruções sobre os **perfis de Usuários**.
Os usuários do Credential Management devem ser criados no AMS:

Caminho da caixa de diálogo
Configuração > **Operadores e estações de trabalho** > **Perfis de usuário**

Procedimento

1. Clique em  para criar um novo perfil
2. Insira um nome para o perfil no campo **Profile Name (Nome do perfil)** (obrigatório)
3. Insira uma descrição para o perfil no campo **Description (Descrição)** (opcional, porém recomendado)
4. Clique em  ou **Apply (Aplicar)** para salvar as alterações
5. Escolha a função de acordo com o tipo de perfil:
   - No painel da lista, selecione as funções (primeira coluna) e os recursos dentro da função (**Execute (Executar)**, **Change (Alterar)**, **Add (Adicionar)**, **Delete (Excluir)**) que devem ser acessíveis para esse perfil. Clique duas vezes neles para alternar suas definições para `Yes`.
   - Da mesma forma, verifique se todas as funções que não deve ser acessíveis estão definidas como `No`.
6. Clique em  ou **Apply (Aplicar)** para salvar as alterações

Para obter mais informações sobre funções de usuários para o Credential Management, consulte *Visão geral das funções do usuário.*

5.2 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 CredMgmt seguido por dois pontos e pelo número da porta (o padrão é `5806`)
   `https://`<My_CredMgmt_server>`:5806`
   A tela **Fazer login** é exibida
2. Faça login como usuário **administrador** do CredMgmt.
3. Clique em  para abrir o menu **Configurações**.

5.3 Uso do menu Configurações para configuração

Geral	– **Período de retenção (dias)**: essa configuração controla o processamento de registros das pessoas. – Quando o período expira pela primeira vez, o aplicativo torna o registro anônimo. – Quando o período expira pela segunda vez, o aplicativo exclui o registro. O valor padrão é `365`. Defina como 0 para desativar o período de retenção completamente. Nesse caso, os registros serão retidos indefinidamente. – **Logotipo**: Marque ou desmarque a caixa de seleção que determina se as caixas de diálogo exibem um logotipo personalizado ou o logotipo padrão. – Para conferir os critérios para arquivos de logotipo personalizados, consulte: *Personalização do logotipo da empresa, página 29* – **Supergráfico:** Marque ou desmarque a caixa de seleção que determina se as caixas de diálogo exibem o supergráfico da Bosch. – **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.

5.3.1 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.
Depois de baixá-los no menu **Configurações** os modelos são armazenados 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.

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

Marcador de posição	Description (Descrição)
{{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

5.3.2 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**.

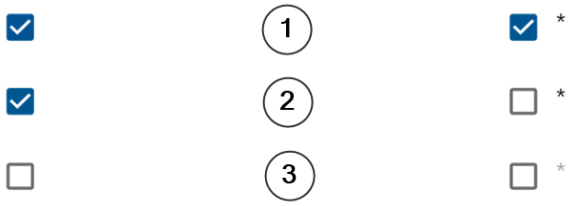
5.4 Personalização da interface de usuário

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

5.4.1 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.

5.4.2 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>
   ```

5.4.3 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

5.5 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

Saída do servidor	Porta de saída	Entrada do servidor	Porta de entrada	Protocolo	Comentários
					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.

5.5.1 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

Programa	**Local do arquivo**
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

Serviço	Local do arquivo
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]\

5.5.2 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.

5.6 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:

5.6.1 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.

5.6.2 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.

5.6.3 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.

5.7 Privacidade e proteção de dados na Bosch

Introdução

Em todos os processos corporativos e em conformidade com os requisitos legais aplicáveis, garantimos que a privacidade é salvaguardada, os dados pessoais são protegidos e as informações comerciais são mantidas seguras. Técnica e organizacionalmente, e especialmente no que diz respeito à proteção contra acesso não autorizado e perda, aplicamos um padrão adequado que reflete a tecnologia de ponta e leva em conta os riscos associados. Ao desenvolver produtos Bosch e novos modelos de negócios, garantimos que os requisitos legais que controlam a proteção de dados e a segurança das informações sejam levados em conta em uma fase inicial.

Além da organização de conformidade e do departamento jurídico, o principal contato para dúvidas sobre como lidar adequadamente com os dados é o responsável pela segurança de dados.

Processando dados pessoais no aplicativo Mobile Access e no sistema back-end do Mobile Access

- Categorias de dados pessoais

  - Os aplicativos Mobile Access contêm dados pessoais. Esta é a informação do número do cartão usada para obter acesso aos leitores. O acesso aos dados reais de pessoas reais só é possível através da utilização adicional dos programas AMS, ACE ou do Visitor Management.
  - O procedimento de registro do Instalador no menu **Configurações** não precisa armazenar dados pessoais. No entanto, algumas informações de usuários, como endereços de e-mail, podem ser armazenadas opcionalmente.
  - O servidor back-end do aplicativo Mobile Access armazena dados pessoais para gerenciamento de credenciais.
- Transferência de dados
  - As informações de credenciais são transferidas entre o sistema back-end, o aplicativo Mobile Access e o sistema Visitor Management para controlar o acesso aos leitores.
- Registro de dados
  - O aplicativo Mobile Access mantém registros técnicos. Esses registros são armazenados localmente no dispositivo móvel e podem ser enviados a terceiros, como suporte técnico, se necessário.
  - O servidor back-end também mantém registros técnicos. Os dados são armazenados localmente no sistema do servidor.
  - Por padrão, o servidor back-end não exclui arquivos de log automaticamente. No entanto, a exclusão automática pode ser configurada com base na capacidade de armazenamento restante ou em um cronograma.

O que fizemos para tornar a proteção de dados do produto amigável?

Os sistemas de controle de acesso da Bosch gerenciam os direitos de acesso das pessoas. Para proteger estas pessoas, a Bosch toma medidas para integrar os requisitos de GDPR (General Data Protection Regulation, Regulamento Geral de Proteção de Dados) diretamente no desenvolvimento dos produtos, seguindo uma abordagem de “privacidade desde a concepção”.

- É usada criptografia de última geração.
- As informações de credenciais são pseudonimizadas.
- O usuário do aplicativo não é obrigado a inserir informações pessoais para receber credenciais virtuais via QR-Code ou e-mail.
- A exclusão de informações de credenciais é possível a partir dos aplicativos Mobile Access, dos sistemas primários de controle de acesso e de aplicativos auxiliares como Visitor Management e Credential management.
- As credenciais podem ser bloqueadas pelos operadores dos sistemas de controle de acesso primários e aplicativos auxiliares a qualquer momento.
- Os dados de telemetria são anonimizados por design.
- Os arquivos de log não são transferidos de dispositivos móveis para terceiros, como Suporte Técnico, sem o consentimento e cooperação ativos do usuário.
- A exclusão automática programada de arquivos de log é configurável no sistema de controle de acesso primário.
- A Bosch não exige registro na app store ou no aplicativo. A App Store não encaminha dados pessoais para a Bosch.
- O aplicativo requer Bluetooth para funcionar, mas solicita e exige que o usuário ative o Bluetooth manualmente.

Outras perguntas

Para obter mais informações sobre privacidade de dados, consulte o aviso de privacidade de dados no aplicativo Mobile Access ou entre em contato com a equipe de projetos da Bosch.

5.8 Autorizações de alta segurança

5.8.1 Princípio de duas pessoas

A partir do AMS 5.5 e posterior, é possível ativar o princípio de Duas Pessoas. O principal objetivo desta funcionalidade é reforçar a segurança ao atribuir autorizações adicionando um aprovador. No Credential Management, um operador pode atribuir uma ou mais autorizações a uma determinada pessoa. Ao contrário de uma atribuição de autorização típica, na qual é atribuída imediatamente à pessoa, as autorizações com o princípio de duas pessoas ativado são enviadas como uma solicitação a um operador diferente que tem o direito de aprovar ou recusar a solicitação de autorização. Isto evitará atribuições indevidas, pois pode ser usado para proteger autorizações para áreas sensíveis, ou seja, autorizações que podem ser atribuídas a um funcionário somente se dois operadores aprovarem (o solicitante e o aprovador).

5.8.2 Configurando autorizações de alta segurança

Para permitir o princípio das Duas Pessoas, os seguintes requisitos são obrigatórios:

– Ter um AMS atualizado com a versão mais recente.
– Ser um administrador do AMS.

Criação de autorizações de acesso com princípio de duas pessoas

No sistema de controle de acesso principal:

Caminho da caixa de diálogo

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

1. Limpe os campos de entrada clicando em **New (Novo)** da barra de ferramentas.

   Como alternativa, clique em **Copy (Copiar)** para criar uma nova autorização com base em outra existente.
2. Digite um nome único para a autorização
3. (Opcional) Digite uma descrição
4. (Opcional) Selecione um modelo de tempo para governar essa autorização
5. (Opcional) Escolha um **Limite de inatividade** da lista.
6. (Obrigatório) Atribua pelo menos uma **Entrada**.
7. Marque a caixa de seleção **Aprovação necessária** (esta opção ativa o Princípio de Duas Pessoas).
8. Clique em salvar para salvar a autorização.

Aviso!

Recomendação de segurança

Este recurso é aplicável apenas para o Credential Management. No AMS, os administradores devem atribuir e configurar perfis de usuário para operadores de maneira adequada para tornar os diálogos inacessíveis. Isto evitará que os operadores normais atribuam autorizações de alta segurança sem o princípio das duas pessoas.

Para obter mais informações, consulte a versão mais recente do Manual do software *Access Management System Configuration and Operation.*

6 Operação

6.1 Visão geral das funções de usuário

As capacidades dos usuários do Credential Management são determinadas pelos seus Perfis de usuário no ACS:

Tipo de usuário	Casos de uso
Administrador	Definição de configurações globais Personalização do comportamento da ferramenta e da interface de usuário mais Todos os casos de uso de Operadores
Operador	Atribuição e cancelamento de atribuição de cartões de acesso físico e credenciais virtuais para acesso móvel
Princípio de duas pessoas: Solicitante	Solicitar autorizações de alta segurança
Princípio de duas pessoas: Aprovador	Aprovar ou negar autorizações de alta segurança Remover autorizações normais

Consulte

– *Criação de usuários do Credential Management no ACS, página 26*

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.

Uso geral da tabela de pessoal

Cada linha da tabela representa uma pessoa. São funcionários internos ou externos que necessitam de credenciais para acessar as instalações.

- Você pode selecionar pessoas individuais ou várias pessoas 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 pessoas à tabela
- Você pode atribuir e cancelar atribuições de credenciais clicando nos botões de ação
  - Atribuir uma credencial física
  - Atribuir uma credencial virtual (para acesso móvel)
  - Editar detalhes da pessoa
- 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.

As funções do painel

Marcação	Função
(1) N **entradas**	O número total N de pessoas (cada pessoa é uma linha na tabela).
(2) **Pesquisar**	Procurar texto arbitrário entre as pessoas na tabela
(3) 	Selecione todos os itens da lista
(4)  **Excluir**	Exclui os itens selecionados
(5)  **Mais recentes**	Mostrar as pessoas que foram adicionadas mais recentemente à tabela.
(6)  **Redefinir**	Redefina a tabela para a visualização padrão e reverta todos os filtros.
(7)  **Cancelar atribuição do cartão**	Abra uma caixa de diálogo para cancelar os cartões atribuídos usando um leitor de inscrição conectado.
(8) **. . .**	Clique no símbolo de elipse para um menu para exportar as pessoas e também documentos, para vários formatos de arquivos, como, por exemplo `CSV` e `.XLSX`. 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.
(9) 	Abrir uma caixa de diálogo para criar uma nova pessoa

As colunas do painel

Coluna	Descrição
Name (Nome)	Clique no hiperlink para ver os detalhes da pessoa.
Email	
Department (Departamento)	
Position (Posição)	
Company (Empresa)	
Números de cartão	Os números dos cartões atribuídos a essa pessoa.
Ações	Veja a tabela separada abaixo

Ações a serem executadas em registros pessoais na tabela do painel

Ícone	Ações
	**Atribuir** um ou mais cartões físicos para a pessoa
	**Atribuir** uma credencial virtual para a pessoa para acesso móvel
	**Editar** os detalhes pessoais da pessoa. As alterações são propagadas para o ACS. As alterações feitas no ACS são propagadas para o aplicativo CredMgmt.

6.2.1 Visão geral da página da pessoa

Após clicar no nome de uma determinada pessoa, é aberta uma caixa de diálogo com dados pessoais. Nesta caixa de diálogo existem campos onde as informações principais da pessoa podem ser exibidas e editadas, mas as informações pessoais básicas são exibidas permanentemente no lado esquerdo da caixa de diálogo.

As informações sobre entradas na lista negra - se existirem - aparecem na parte inferior desta coluna de informações pessoais básicas.

Dica: o campo **Título** permite texto livre além das opções disponíveis na lista suspensa.

Na mesma caixa de diálogo, existem três guias com sua própria visualização: **Detalhes, Credenciais, Autorizações**.

No Credential Management, se esta pessoa for bloqueada, um aviso laranja aparecerá com a expressão **Na lista negra**. Ele também exibe o motivo e quem atribuiu a lista negra.

Um administrador e um operador com direitos podem bloquear a pessoa clicando no botão **Lista negra.**

– Uma janela de aviso é aberta

1. Clique em **Sim**
2. No assistente **Motivo**, digite o motivo > **Salvar > Ok**

Observe que uma pessoa na lista negra ainda mantém as autorizações atribuídas. No entanto, esta pessoa não poderá abrir uma entrada/porta.
Para remover a pessoa da lista negra, basta clicar no botão **X Remover da lista negra**.
Configure os direitos corretamente. Para obter mais informações sobre os direitos do usuário**,** consulte o *Manual do software Access Management System Configuration and Operation*.

Details (Detalhes)
Nesta guia é possível inserir os dados pessoais que não precisam estar constantemente visíveis.

PIN
Nesta guia **Detalhes**, é possível visualizar e alterar PINs (PIN de verificação)[1] para um titular de cartão. É possível especificar uma data de validade ao alterar o PIN.
Observação: se o PIN for alterado ou sua configuração for alterada, será necessário digitar novamente o PIN para confirmação.
Se existir um ou mais bloqueios de **PIN** para as credenciais da pessoa selecionada, um aviso aparecerá na parte inferior da coluna de informações pessoais básicas. Quando o operador clica neste aviso, a guia **Credenciais** é selecionada e o operador consegue ver mais informações sobre o bloqueio do **PIN** .
Observe que se houver um erro de validação em uma guia, não será possível selecionar outra página até que o erro seja solucionado.
[1]Credential Management suporta apenas PIN padrão. PINs de identificação E PINs de IDS/ PINs de armação separados não são suportados.
Para obter mais informações sobre os **Códigos PIN**, consulte o *Manual do Software Access Management System Configuration and Operation*.

Credenciais
Nesta guia é possível atribuir um cartão físico clicando no botão **Ler cartão** ou atribuir uma credencial móvel clicando no botão **Adicionar acesso móvel**. Para obter mais informações, consulte *Atribuição de credenciais móveis* e *Atribuição de credenciais físicas*.
Observação: se um ponto laranja aparecer no ícone do telefone, significa que a credencial já está no celular, mas precisa da aprovação do suporte de acesso móvel. Somente após essa aprovação o ponto ficará verde.

Authorizations (Autorizações)
Nesta guia é possível visualizar todas as autorizações atribuídas e modificar autorizações.
Para obter mais informações, consulte *Atribuir autorizações na página de informações pessoais.*.
Observe que em qualquer caixa de diálogo das guias, o botão **Salvar e Fechar** redireciona para a caixa de diálogo **Painel**.

6.3 Atribuindo autorizações

Atribuindo autorizações na página de informações pessoais.
– Na caixa de diálogo do painel, aparece uma lista de pessoas.
1. Clique no nome da pessoa.

– A caixa de diálogo de informações da pessoa é aberta.
1. No canto superior direito da caixa de diálogo, clique na guia **Autorizações**.
2. Para atribuir uma nova autorização, clique em **Modificar autorizações**

Um assistente com uma lista de todas as autorizações é exibido. Estas autorizações são todas previamente configuradas no Access Management System. A partir desta etapa, escolha quais autorizações atribuir.

1. Clique em  > **Confirmar** > **Salvar**.

Observação: autorizações de alta segurança, ou seja, com a funcionalidade Princípio de duas pessoas habilitada, aparece com  .

A caixa de diálogo do painel é aberta. Caso tenha sido atribuída uma autorização normal, é possível verificar se a autorização foi realmente atribuída clicando novamente no nome da pessoa e verificando a guia **Autorizações**.
Se a autorização com o princípio de Duas Pessoas tiver sido atribuída, o resultado será diferente. Ou seja, a autorização não estará ativa imediatamente depois de salva, mas apenas solicitada. Nas colunas **Autorizações** e **Ações**, é possível visualizar quem solicitou a autorização.
Na guia **Autorizações**, as autorizações com o princípio de duas pessoas parecem ter sido aprovadas ou negadas. É possível ver quem solicitou em qual data e horário passando o mouse sobre o nome da autorização. Uma dica de ferramenta é exibida.

Dependendo do tipo de autorização e da função e direitos do usuário, os botões **Ações** exibidos podem ser os seguintes:

Solicitação
Recolher - cancelar minha própria solicitação de atribuição de autorização, que ainda não foi aprovada.
Aprovar - aprovar pedido de atribuição de autorização por outro operador.
Recusar - recusar pedido de atribuição de autorização por outro operador.
Remover - remover a autorização atribuída. Isto é válido para autorizações normais e de alta segurança.

Observação: nenhuma ação é válida apenas clicando no botão de ação. Sempre clique em **Salvar.**
Consulte *Visão geral das funções do usuário* para obter mais informações.

No AMS, os **Perfis de usuários** devem ser configurados adequadamente com os direitos disponíveis para o princípio de duas pessoas:
– Administrador
– Operador
– Princípio de duas pessoas: Solicitante
– Princípio de duas pessoas: Aprovador

Para obter mais informações sobre como configurar **Perfis de usuários**, consulte a versão mais recente do manual do Software *Access Management System Configuration and Operation*.

Solicitações de autorização pendentes

Um Operador com direitos de aprovador ou solicitante e um Administrador podem visualizar as **Solicitações de Autorização** no menu. Nesta caixa de diálogo, é possível ver todas as **Solicitações de Autorização Pendentes** em uma única visualização, sem a necessidade de navegar pelo nome de cada pessoa.
Um aprovador do Operador pode aprovar autorizações por meio desta caixa de diálogo e um Administrador pode retirar autorizações. Um solicitante Operador só pode visualizar as autorizações pendentes. Um Operador sem direitos de aprovador e solicitante não pode visualizar esta caixa de diálogo.
Observação: nenhuma ação é válida apenas clicando no botão de ação. Após clicar no botão de ação, ele fica cinza e depois clique em **Salvar.**

6.4 Atribuição de credenciais físicas

Pré-requisitos
É altamente recomendável atribuir credenciais novas a novos funcionários, usando um cartão novo, uma impressora de cartões e um leitor de registro.

Atribuindo um cartão (requer um leitor de inscrição)
Procedimento
É possível atribuir um cartão a partir do ícone do painel diretamente ou a partir da visão geral da página pessoal.
No **Painel**:
1. Tenha um cartão de acesso físico pronto para apresentar ao leitor de inscrição.
2. Selecione a linha da pessoa e clique em 
3. Siga as instruções no menu pop-up para usar o leitor de inscrição.

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 **Credencial** > **Ler cartão**.

Atribuindo um cartão no editor de credenciais (requer um leitor de inscrição)

1. No painel, na tabela de pessoas, selecione uma pessoa e clique em  para editar as credenciais dessa pessoa.
2. Clique em **Ler cartão** e siga as instruções no pop-up para uso do leitor de inscrição.
– Repita as últimas etapas para atribuir outros cartões, se necessário.
3. Clique em **Salvar** para salvar a pessoa atual com as atribuições de cartão.

6.5 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
– 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
– 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
– 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
– O dispositivo móvel funciona como um cartão de acesso físico, desde que o aplicativo esteja em execução

Consulte
– *Instalação do Mobile Access, página 13*
– *Instalação dos aplicativos do Mobile Access, página 22*

6.6 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.

6.7 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.

6.7.1 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.

6.8 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.

6.8.1 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).

GDPR

O Regulamento Geral de Proteção de Dados (GDPR, General Data Protection Regulation) é uma lei de privacidade e segurança elaborada pela União Europeia (UE) e que entrou em vigor em 2018. Ele impõe obrigações às organizações em qualquer lugar que coletam dados relacionados a pessoas na UE.

Mobile Access

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

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

202405132119