



BOSCH

Access Management System

pt-BR Manual de Instalação

Sumário

1	Sobre esta documentação	4
2	Visão geral do sistema AMS	5
3	Instalação	6
3.1	Requisitos do sistema	6
3.2	Instalação do servidor	7
3.3	Desativação do firewall	9
3.4	Instalação do cliente	9
3.5	Verificar se o sistema está instalado	12
3.6	Uso de certificados personalizados	12
3.6.1	Pré-condições	13
3.6.2	Uso de certificados personalizados	13
3.7	Solução de problemas	17
3.8	Atualização do sistema	17
3.9	Desinstalar	20
4	Dados técnicos	22

1 Sobre esta documentação

Este é o principal manual de instalação para o Access Management System.

Documentação relacionada

Os tópicos a seguir são documentados separadamente:

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

2 Visão geral do sistema AMS

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

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

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

3 Instalação

Procedimento geral

A instalação do sistema consiste em dois instaladores diferentes: o servidor e o cliente. A ordem geral de instalação é a seguinte:

1. Verifique os requisitos do sistema
2. Instale o software no servidor e verifique a instalação correta antes de instalar um cliente.
3. Instale o certificado HTTPS na máquina do cliente
4. Instale o cliente

Consulte

- Importar o certificado HTTPS, página 9
- Verificar se o sistema está instalado, página 12

3.1 Requisitos do sistema

Requisitos técnicos mínimos para um servidor AMS

Servidor	
<p>Sistemas operacionais compatíveis. Instalações em outros sistemas operacionais podem funcionar, mas nenhum tipo de garantia é oferecido.</p>	<ul style="list-style-type: none"> – Windows Server 2016 (64 bits, Standard, Datacenter) – Windows 10, version 1903 (LTSC, LTSC) – Observação: O banco de dados padrão fornecido com esse sistema é o SQL Server 2017 Express Edition com serviços avançados
<p>Requisitos mínimos de hardware</p>	<ul style="list-style-type: none"> – Processador Intel i5 com pelo menos 4 núcleos físicos – 8 GB de RAM (32 GB são recomendáveis) – 200 GB de espaço livre no disco rígido (discos SSD são recomendáveis) – Adaptador gráfico com <ul style="list-style-type: none"> – 256 MB de RAM – Resolução de 1280x1024 – Pelo menos 32 k cores – Placa Ethernet de 1 Gbits – Porta USB livre ou compartilhamento de rede para arquivos de instalação

Requisitos técnicos mínimos para um cliente AMS

Cliente	
<p>Sistemas operacionais compatíveis.</p>	<ul style="list-style-type: none"> – Windows 10, versão 1803 (LTSC, LTSC)

Cliente	
Instalações em outros sistemas operacionais podem funcionar, mas nenhum tipo de garantia é oferecido.	
Requisitos mínimos de hardware	<ul style="list-style-type: none"> - Intel i5 ou superior - 8 GB de RAM (16 GB são recomendáveis) - 20 GB de espaço livre no disco rígido - Adaptador gráfico com <ul style="list-style-type: none"> - 256 MB de RAM - Resolução de 1920x1080 - Pelo menos 32 k cores - DirectX® 11 - Placa Ethernet de 1 Gbits - Porta USB livre ou compartilhamento de rede para arquivos de instalação

Requisitos técnicos mínimos para um MAC adicional

Servidor MAC	
Requisitos mínimos de hardware	<ul style="list-style-type: none"> - Intel i5 ou superior - 8 GB de RAM (16 GB são recomendáveis) - 20 GB de espaço livre no disco rígido - Adaptador gráfico com <ul style="list-style-type: none"> - 256 MB de RAM - Resolução de 1280x1024 - Pelo menos 32 k cores - Placa Ethernet de 1 Gbits

3.2 Instalação do servidor

Antes de começar

1. Faça login na máquina do servidor.
2. Verifique se o sistema já está instalado (consulte **Verificar se o sistema está instalado**). Se não estiver, prossiga com a instalação.
3. Copie o pacote de instalação para a máquina do servidor.

Início da instalação do servidor

1. Clique duas vezes no pacote de instalação do software.
2. Clique duas vezes em **Server (Servidor)**.
3. Clique com o botão direito do mouse em **AMS Server Setup.exe** e selecione **Run as administrator (Executar como administrador)** no menu de contexto.
 - O Assistente de preparação de instalação será aberto. Siga as etapas no assistente de preparação de instalação.

4. Selecione os componentes necessários a serem instalados e clique em **Next> (Próximo>)**.
 - Dependendo do conteúdo que já estiver instalado, o assistente mostrará uma lista dos softwares que serão instalados:
 - Se houver componentes não obrigatórios que não são necessários, cancele as seleções neste momento.
5. Leia o **Contrato de licença do usuário final** e clique em **Accept (Aceitar)** para continuar. Se você não concordar, clique em **Decline (Recusar)** para cancelar a instalação.
6. Insira os dados de configuração do SQL Database Server.
 - Dados de configuração do SQL Database Server:
 - SQL Server: o nome do host em que a instância do SQL Server será executada. É recomendável usar a máquina local.
 - SQL instance (Instância do SQL): o nome da instância do SQL
 - AMS database (Banco de dados AMS): o nome do banco de dados
 - SQL user name (Nome de usuário do SQL): o login do SQL
 - SQL password (Senha do SQL): a senha do SQL para o login do SQL. A **senha padrão é: sa_s3k_pw**
7. Após inserir a senha do SQL, clique em **Test Server (Testar servidor)**.
 - Se o teste for bem-sucedido, uma mensagem com fundo verde aparecerá abaixo do campo de senha do SQL.
8. Clique em **Next> (Próximo>)**.
9. Se o caminho de instalação padrão do servidor for aceitável, clique em **Next> (Próximo>)**. Caso queira selecionar outro caminho de instalação (unidades locais apenas), clique em **Browse (Procurar)**.
 - A unidade C:\Program Files do caminho de instalação padrão é recomendada porque os arquivos só podem ser modificados pelos administradores do sistema.
 - Se você selecionar outro caminho de instalação, confirme se ele está adequadamente protegido contra acesso ilícito.
10. Clique em **Next> (Próximo>)** para continuar.
 - Esta página configura o nome de host da API.
 - O nome do servidor não deve ter mais de **16** caracteres. O valor padrão (recomendado) é o nome de host do computador atual em que o instalador está em execução.
11. Verifique o resumo da pré-instalação e clique em **Install (Instalar)**.
 - É exibido um resumo com todos os componentes escolhidos para instalação.
12. Observe a barra de progresso da instalação.
 - Assim que a barra verde em movimento alcançar aproximadamente a metade da barra de progresso, demorará alguns minutos para se movimentar novamente. Aguarde.
 - Será aberta outra caixa de diálogo a respeito da configuração do banco de dados Access Engine (ACE). Essa configuração atualiza o banco de dados ACE. Se o banco de dados já estiver instalado, ele será atualizado. Caso contrário, será criado um banco de dados. Isso pode levar vários minutos. Aguarde o fechamento da caixa de diálogo.
13. Após a conclusão da operação, clique em **Next> (Próximo>)** e verifique o resumo pós-instalação.
 - É exibido um resumo com todos os componentes instalados.
14. Clique em **Finish (Concluir)** para finalizar a instalação.
 - Uma caixa de diálogo solicitando a reinicialização será aberta. É necessário reiniciar o computador para concluir a instalação do sistema.
15. Clique em **Yes (Sim)** para reiniciar o PC.
 - O PC reinicia.

16. Verifique se o sistema está instalado corretamente (consulte **Verificar se o sistema está instalado**).
- Em caso afirmativo, a primeira instalação do aplicativo do sistema estará concluída. O ícone do sistema é exibido na área de trabalho.

Realização do login pela primeira vez

1. Clique duas vezes no ícone do aplicativo do sistema na área de trabalho.
2. Insira o nome de usuário e a senha padrão.
 - O nome de usuário e a senha padrão são **Administrator**. Observe que a senha (mas não o nome de usuário) faz distinção entre maiúsculas e minúsculas.
3. Clique em **Log in (Fazer login)**.
 - É exibida uma caixa de diálogo solicitando a alteração da senha.
 - Ao fazer login pela primeira vez, é necessário alterar a senha na caixa de diálogo pop-up.
4. Clique em **OK** para fazer login.

Consulte

- *Verificar se o sistema está instalado, página 12*
- *Iniciar a atualização do servidor, página 17*

3.3 Desativação do firewall

Após a instalação bem-sucedida do servidor e antes da instalação das estações de trabalho clientes, desative o firewall. Assim, estações de trabalho clientes e computadores MAC externos podem facilmente estabelecer conexão com o servidor durante a configuração inicial.

3.4 Instalação do cliente

Certificado HTTPS para o cliente

O servidor do sistema hospeda diversas APIs, a saber: API de acesso, API de mapa e API de estados. Essas APIs se comunicam via HTTPS e utilizam um certificado autoassinado para estabelecer confiança. O certificado autoassinado é criado pelo instalador do servidor e é instalado na máquina do servidor.

O cliente de Mapa usa essas APIs para funcionar corretamente e, portanto, requer que a máquina do cliente confie nessas APIs. Para permitir isso, um certificado do servidor deve ser copiado e importado manualmente para a máquina do cliente (consulte **Importar o certificado HTTPS**).

Importar o certificado HTTPS

1. Vá para `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Certificates\Access Management System Internal CA.cer`
2. Copie o certificado para a máquina do cliente.
3. Na máquina do cliente, clique duas vezes no certificado.
 - É exibida uma caixa de diálogo do certificado.
4. Clique em **Install Certificate (Instalar certificado)**.
 - O Assistente de importação de certificados abrirá.
5. Selecione **Local Machine (Máquina local)** (recomendado) e clique em **Next> (Próximo>)**.
6. Selecione **Place all certificates in the following store (Colocar todos os certificados no seguinte armazenamento)** a fim de especificar o local para o certificado (recomendado).
7. Clique em **Browse (Procurar)**.

- Uma caixa de diálogo para seleção do armazenamento do certificado abrirá.
- 8. Selecione `Trusted Root Certification Authorities` e clique em **OK** (recomendado).
- A caixa de diálogo para seleção do armazenamento do certificado fechará.
- 9. Clique em **Next> (Próximo>)** no Assistente de importação de certificados.
- 10. Clique em **Finish (Concluir)** para importar o certificado.
 - O processo de importação do certificado concluirá.

**Aviso!**

Se o certificado HTTPS não for instalado, não será possível iniciar o aplicativo.

Observe que não é necessário importar o certificado para a máquina do servidor, pois isso é feito automaticamente durante a instalação do servidor. Isso se aplica somente a estações de trabalho do cliente.

Integração da API de acesso ao BVMS

Para integrar a API de acesso do AMS ao BVMS (Bosch Video Management System), versão 9.1 ou superior, importe o certificado descrito na última seção para a máquina do BVMS (consulte **Importar o certificado HTTPS**).

Sistema operacional compatível

O sistema operacional compatível para o cliente é o **Windows 10, versão 1803 (LTSC, LTSC)**.

**Aviso!**

Instalar o cliente fora deste escopo pode resultar em problemas de compatibilidade.

Iniciar a instalação do cliente

1. Clique duas vezes no pacote de instalação do software.
2. Clique duas vezes em **Client (Cliente)**.
3. Clique duas vezes em **AMS Client Setup.exe**
 - O Assistente de preparação de instalação será aberto. Siga as etapas no assistente de preparação de instalação.
4. Selecione os componentes que deseja instalar e clique em **Next> (Próximo>)**.
 - Dependendo do conteúdo que já estiver disponível, o assistente marcará os seguintes softwares de pré-requisito obrigatórios:
 - Microsoft Visual C++ 2010 Redistributable
 - Microsoft Visual C++ 2015 Redistributable
 - Microsoft Visual C++ 2017 Redistributable
 - .NET 4.8
 - Componentes opcionais:
 - Cliente
 - Map View

- Para cada componente opcional, é possível escolher se deseja instalar ou ignorar.
- 5. Leia o **Contrato de licença do usuário final** e clique em **Accept (Aceitar)** para continuar. Se você não concordar, clique em **Decline (Recusar)** para voltar e cancelar a operação.
- 6. Se o caminho de instalação padrão para a estação de trabalho cliente for aceitável, clique em **Next> (Próximo>)**. Caso queira selecionar outro caminho de instalação (unidades locais apenas), clique em **Browse (Procurar)**.
- 7. Insira o endereço do servidor. Formato do endereço: Hostname:4999/tcp
 - Por padrão, o assistente de instalação instala o cliente do sistema na unidade `C:\Program Files local` (recomendado).
 - Arquivos instalados na unidade `C:\Program Files local` só podem ser modificados por usuários com direitos de administrador. Isso proporciona segurança, pois garante que usuários sem direitos de administrador não modifiquem arquivos relacionados ao sistema.
 - Caso queira selecionar outro caminho de instalação, as vantagens oferecidas serão perdidas.
- 8. Se o caminho de instalação padrão do aplicativo Map View for aceitável, clique em **Next> (Próximo>)**.
- 9. Caso queira selecionar outro caminho de instalação (unidades locais apenas), clique em **Browse (Procurar)**.
- 10. Insira o endereço de descoberta.
 - Por padrão, o assistente de instalação instala o aplicativo Map View na unidade `C:\Program Files local` (recomendado).
 - O aplicativo Map View estabelecerá conexão com o endereço de descoberta para descobrir os endpoints do sistema. Esse endereço é um URL que contém o nome do servidor e o número da porta em que o endpoint de descoberta está hospedado.
- 11. Verifique o resumo da pré-instalação e clique em **Install (Instalar)**.
 - É exibido um resumo com todos os componentes escolhidos para instalação.
- 12. Observe a barra de progresso da instalação.
 - Aguarde o término da operação.
- 13. Após a conclusão da operação, clique em **Next> (Próximo>)** e verifique o resumo pós-instalação.
 - É exibido um resumo com todos os componentes instalados.
- 14. Clique em **Finish (Concluir)** para finalizar a instalação.
- 15. Reinicie o PC (recomendado).
- 16. Verifique se o sistema está instalado (consulte **Verificar se o sistema está instalado**).
 - Em caso afirmativo, a instalação do cliente e do Map View (opcional) estará concluída. Os ícones dos dois aplicativos do cliente aparecem na área de trabalho. O nome de usuário e a senha padrão são **Administrator**. Observe que a senha (mas não o nome de usuário) faz distinção entre maiúsculas e minúsculas.

Antes de iniciar o cliente

Antes de fazer login no cliente, você deve configurar a estação de trabalho cliente no servidor. Siga o procedimento abaixo:

1. Inicie o cliente na máquina do servidor.
2. Clique em **Configuration (Configuração) > Device Data (Dados do dispositivo)**
 - Uma nova caixa de diálogo será aberta.
3. Na barra de ferramentas superior, selecione o ícone **Workstations (Estações de trabalho)**.

4. Na barra de ferramentas superior, selecione o ícone **New (Novo)**.
5. Na guia Workstation (Estação de trabalho), preencha os campos vazios.
 - Os campos:
 - Name (Nome): insira o nome de host da estação de trabalho cliente (obrigatório)
 - Description (Descrição): insira uma descrição (opcional)
 - Login via reader (Login via leitor): faça o login por meio do leitor (opcional)
 - Automatic Logout after (Logout automático depois de): X segundos (opcional). Defina um logout automático se desejar que o aplicativo encerre a sessão automaticamente após um tempo especificado.
 - Observe que os campos sublinhados são obrigatórios.
6. Na barra de ferramentas superior, clique no ícone **Save (Salvar)** para salvar as alterações.
 - Agora, você já pode fazer login com êxito pela estação de trabalho cliente.

Efetuando login pela primeira vez

1. Clique duas vezes no ícone do aplicativo do sistema na área de trabalho.
2. Insira o nome de usuário e a senha padrão.
 - O nome de usuário e a senha padrão para ambos os aplicativos do cliente são **Administrator**. Observe que a senha (mas não o nome de usuário) faz distinção entre maiúsculas e minúsculas.
3. Clique em **Log on (Fazer login)**.
 - É exibida uma caixa de diálogo solicitando a alteração da senha.
 - Ao fazer login pela primeira vez, é necessário alterar a senha.
4. Clique em **OK** para inserir uma nova senha na caixa de diálogo.
5. Insira a nova senha e clique em **Change (Alterar)**. Clique em **Cancel (Cancelar)** para cancelar a alteração da senha.
 - É exibida uma caixa de diálogo confirmando a alteração da senha.
6. Clique em **OK** para fazer login.



Aviso!

O servidor e o cliente devem ser instalados na mesma versão. Não tente acessar o servidor com uma versão de cliente diferente.

Consulte

- *Verificar se o sistema está instalado, página 12*
- *Importar o certificado HTTPS, página 9*

3.5

Verificar se o sistema está instalado

Verificar se o sistema está instalado

O sistema estará instalado se:

- Os ícones do sistema estiverem visíveis na área de trabalho.
- Os serviços a seguir estão no aplicativo Windows Services (**Iniciar > Pesquisar > service.msc**): DMS, MAC Access PI, Identity service, MAP API, State API.
- O sistema está no caminho de instalação padrão: C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\

3.6

Uso de certificados personalizados

As APIs do AMS podem ser configuradas para usar certificados diferentes em vez de usar os certificados autoassinados criados automaticamente durante a instalação. Isso é útil quando uma organização já tem uma infraestrutura de chaves públicas (ICP) que possui sua própria Autoridade certificadora (AC).

3.6.1 Pré-condições

- Ter um arquivo de certificado raiz confiável.
- As partes pública e privada do certificado precisam ser colocadas no diretório do servidor do AMS `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Certificates`

Exemplos das partes pública e privada de um certificado:

- `Access Management System Test CA.cer` (parte pública)
- `CustomRootTestCA.pfx` (parte privada)

3.6.2 Uso de certificados personalizados

Abrir uma sessão do PowerShell

Abra uma sessão do PowerShell no servidor do AMS no diretório `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Certificates`

Remover os certificados instalados

1. Remova os certificados que foram instalados durante a instalação do AMS.
2. Execute: `"RemoveAceApiCertificates.ps1"` na sessão aberta do PowerShell.

Editar o script para criação de certificados da API

1. Abra o arquivo do PowerShell `"CreateAceApiCertificatesFromOwnRoot.ps1"` em um editor de texto e renomeie os seguintes arquivos para os nomes dos seus arquivos:
 - `CustomRootTestCA.pfx`
 - 2. `Access Management System Test CA.cer`
 - Observe que os nomes de arquivos aparecem apenas uma vez no script.
 - 3. Salve as alterações.

Executar o script para criação de certificados da API

1. Execute: `"CreateAceApiCertificatesFromOwnRoot.ps1"` na sessão do PowerShell aberta na etapa 1.
2. Insira a senha para o certificado privado.
 - Os seguintes certificados da sub-API foram criados e instalados:
 - API de acesso do Access Management System
 - Servidor de identidade do Access Management System
 - API de mapa do Access Management System
 - API de estados do Access Management System
 - O certificado raiz é instalado.

Verifique a instalação dos certificados em Certificados do Windows para o usuário atual e o computador local

O certificado estará instalado se:

- O certificado raiz estiver instalado em Current User Personal Certificates, Trusted Root Certificates e em Local Computer Trusted Root Certificates
- Os certificados de API estiverem instalados em Local Computer Personal Certificates

Atualizar as configurações do aplicativo Thumbprint para cada API

O thumbprint deverá ser atualizado para cada API.

API de acesso	<ol style="list-style-type: none"> 1. Abra C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Access API 2. Troque os valores no arquivo appsettings.json, linha "Thumbprint": 3. Abra Certificates Local Computer > Personal > Certificates > Friendly Name (Certificados computador local > Pessoal > Certificados > Nome amigável): Access Management System Access API 4. Selecione e abra o certificado instalado "Access Management System Access API" > Details (Detalhes) 5. Role a lista para baixo até "Thumbprint" 6. Selecione Thumbprint. 7. Copie o Thumbprint exibido (por exemplo, "da"). 8. Cole o Thumbprint sem espaços no arquivo appsettings.json, em C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Access API <p>- (por exemplo, "Thumbprint": "53d3588285bd570c9799e883b27ef1b139ba28da")</p>
---------------	--

API de mapa	<ol style="list-style-type: none"> 1. Abra C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Map API 2. Troque os valores no arquivo appsettings.json, linha "Thumbprint": 3. Abra Certificates Local Computer > Personal > Certificates > Friendly Name (Certificados computador local > Pessoal > Certificados > Nome amigável): Access Management System Map API 4. Selecione e abra o certificado instalado "Access Management System Map API" > Details (Detalhes) 5. Role a lista para baixo até "Thumbprint". 6. Selecione Thumbprint. 7. Copie o Thumbprint exibido (por exemplo, "e8"). 8. Cole o Thumbprint sem espaços no arquivo appsettings.json, em C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Map API <p>- (por exemplo, "Thumbprint": "3cef0c43be36ee01d8a6ea2f59f170cde96168e8")</p>
-------------	---

--	--

API de estados	<ol style="list-style-type: none">1. Abra C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\States API2. Troque os valores no arquivo appsettings.json, linha "Thumbprint":3. Abra Certificates Local Computer > Personal > Certificates > Friendly Name (Certificados computador local > Pessoal > Certificados > Nome amigável): Access Management System States API4. Selecione e abra o certificado instalado "Access Management System States API" > Details (Detalhes)5. Role a lista para baixo até "Thumbprint".6. Selecione Thumbprint.7. Copie o Thumbprint exibido (por exemplo, "e2").8. Cole o Thumbprint sem espaços no arquivo appsettings.json, em C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\States API <ul style="list-style-type: none">- (por exemplo, "Thumbprint": "37c0bb09d4cab985b620da1c667597ef43b5f8e2")
----------------	---

Servidor de identidade:	<ol style="list-style-type: none">1. Abra C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Identity Server2. Troque os valores no arquivo appsettings.json, linha "Thumbprint":3. Abra Certificates Local Computer > Personal > Certificates > Friendly Name (Certificados computador local > Pessoal > Certificados > Nome amigável): Access Management System Identity Server4. Selecione e abra o certificado instalado "Access Management Identity Server" > Details (Detalhes)5. Role a lista para baixo até "Thumbprint".6. Selecione Thumbprint.7. Copie o Thumbprint exibido.8. Cole o Thumbprint sem espaços no arquivo appsettings.json, em C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Identity Server9. Cole os Thumbprints das outras APIs nos campos de entrada de Thumbprint correspondentes nesse arquivo também. <ul style="list-style-type: none">- Exemplo:<ul style="list-style-type: none">- Para "Name": "AccessApi" "Thumbprint": "53d3588285bd570c9799e883b27ef1b139ba28da"
-------------------------	---

	<ul style="list-style-type: none"> - Para "Name": "MapApi" "Thumbprint": "3cef0c43be36ee01d8a6ea2f59f170cde96168e8" - Para "Name": "StatesApi" "Thumbprint": "37c0bb09d4cab985b620da1c667597ef43b5f8e2"
--	---

Iniciar e parar serviços

1. Abra os serviços do Windows.
2. Clique com o botão direito nos serviços a seguir e selecione "Parar" em cada um deles:
 - API de acesso do Access Management System
 - Servidor de identidade do Access Management System
 - API de mapa do Access Management System
 - API de estados do Access Management System
 - Depois que todos os quatro serviços forem interrompidos, clique com o botão direito nos mesmos serviços novamente e selecione **Iniciar** em cada um deles.

Instalar o certificado raiz na máquina do cliente

1. Use o Gerenciador de arquivos do Windows para copiar o certificado raiz "Access Management System Test CA.cer" e cole-o na máquina do cliente, onde o aplicativo do cliente "Map View" e o "AMS" (Dialog Manager) estão instalados. Por exemplo, cole-o na pasta Downloads.
2. Instale o certificado raiz:
 - No Gerenciador de arquivos, clique com o botão direito no **arquivo do certificado** e selecione **Install Certificate > Current User > Next (Instalar certificado > Usuário atual > Próximo) > Selecione "Place all certificates in the following store" > Browse ("Colocar todos os certificados no seguinte armazenamento" > Procurar) > Selecione "Trusted Root Certification Authorities" > Next > Finish > OK ("Autoridades de certificação raiz confiáveis" > Próximo > Concluir > OK)**

Teste os certificados de API na máquina do cliente.

Os certificados de API precisam ser testados na máquina do cliente, onde o aplicativo do cliente Map View e o AMS (Dialog Manager) estão instalados.

Na máquina do cliente, inicie o navegador Google Chrome.

- Para testar o Servidor de identidade, insira o seguinte endereço: `https://[ServerHostname]:44333/.well-known/openid-configuration`
 - Clique com o botão direito no ícone de cadeado de informações do site > Verifique "Certificado (válido)" e verifique se o certificado correto está sendo usado em "Issued by"
- Para testar a API de acesso, insira o seguinte endereço: `https://[ServerHostname]:44347/swagger`
 - Clique com o botão direito no ícone de cadeado de informações do site > Verifique "Certificado (válido)" e verifique se o certificado correto está sendo usado em "Issued by"

- Para testar a API de estados, insira o seguinte endereço: `https://[ServerHostname]:62901/swagger`
 - Clique com o botão direito no ícone de cadeado de informações do site > Verifique "Certificado (válido)" e verifique se o certificado correto está sendo usado em "Issued by".
- Para testar a API de mapa, insira o seguinte endereço: `https://[ServerHostname]:61801/odata/$metadata`
 - Clique com o botão direito no ícone de cadeado de informações do site > Verifique "Certificado (válido)" e verifique se o certificado correto está sendo usado em "Issued by"

Use os certificados no AMS.

Inicie o aplicativo Map View na máquina do cliente e faça login.

3.7 Solução de problemas

Se a instalação falhar, a barra de progresso ficará vermelha. Texto de erro adicional poderá ser exibido.

Clique em **Next> (Próximo>)** para prosseguir até a página de resumo que exibirá qual componente falhou.

3.8 Atualização do sistema

Antes de começar

1. Faça login na máquina do servidor.
2. Verifique se a versão anterior do sistema está instalada (consulte **Verificar se o sistema está instalado**).
3. Copie o novo pacote de instalação na máquina do servidor.



Aviso!

O servidor e o cliente devem ser instalados na mesma versão. Não tente acessar o servidor com uma versão de cliente diferente.

Iniciar a atualização do servidor

1. Clique duas vezes na nova versão do pacote de instalação do software.
2. Selecione o idioma da interface.
3. Clique duas vezes em **Server (Servidor)**.
4. Clique com o botão direito em **AMS Server Setup.exe** e selecione **Run as administrator** (Executar como administrador) no menu de contexto.
 - O assistente de preparação de instalação é aberto.
 - Selecione os componentes que deseja atualizar e clique em **Next> (Próximo>)**.
 - Dependendo do que já estiver disponível, o assistente marcará os componentes que podem ser atualizados por padrão.
 - Você pode optar por atualizar ou ignorar a atualização dos componentes.
 - Os componentes que não puderem ser atualizados serão marcados como **Skip (Ignorar)** por padrão.

5. Leia o **Contrato de licença do usuário final** e clique em **Accept (Aceitar)** para continuar. Se você não concordar, clique em **Decline (Recusar)** para voltar e cancelar a operação.
6. Insira os dados de configuração do SQL Database Server.
 - Dados de configuração do SQL Database Server:
 - SQL Server: o nome do host onde a instância do SQL Server é executada, isto é, a máquina local (recomendado)
 - Instância do SQL: o nome da instância do SQL
 - Banco de dados AMS: o nome do banco de dados
 - Nome de usuário do SQL: o login do SQL
 - Senha do SQL: a senha do SQL para o login do SQL. A senha padrão é: `sa_s3k_pw`
7. Após inserir a senha do SQL, clique em **Test Server (Testar servidor)**.
 - Se o teste for bem-sucedido, uma mensagem com fundo verde aparecerá abaixo do campo de senha do SQL.
 - Se o banco de dados já existir, haverá uma tentativa de migrá-lo.
8. Clique em **Next> (Próximo>)**.
 - O próximo diálogo mostra o caminho de instalação onde o servidor do sistema será mantido.
 - Por padrão, o assistente de instalação instala o servidor do sistema na unidade `C:\Program Files local` (recomendado).
 - Arquivos instalados na unidade `C:\Program Files local` só podem ser modificados por usuários com direitos de administrador. Isso oferece segurança ao garantir que usuários sem direitos de administrador não possam modificar arquivos relacionados ao sistema.
9. Clique em **Next> (Próximo>)** para continuar.
10. Verifique o resumo de instalação pré-atualização e clique em **Install (Instalar)**.
 - É exibido um resumo com todos os componentes escolhidos para atualização.
11. Observe a barra de progresso da instalação.
 - Assim que a barra verde em movimento alcançar aproximadamente a metade da barra de progresso, demorará alguns minutos para se movimentar novamente. Aguarde.
 - Será aberta outra caixa de diálogo a respeito da configuração do banco de dados Access Engine (ACE). Essa configuração atualiza o banco de dados ACE. Se o banco de dados já estiver instalado, ele será atualizado. Caso contrário, será criado um novo banco de dados. Isto pode demorar vários minutos. Aguarde até que a caixa de diálogo feche.
12. Após a conclusão da operação, clique em **Next> (Próximo>)** e verifique o resumo pós-atualização.
 - É exibido um resumo com todos os componentes atualizados.
13. Clique em **Finish (Concluir)** para concluir a instalação da versão atualizada do sistema.
14. Reinicie o PC (recomendado).
 - O PC reinicia.
15. Verifique se o sistema está instalado (consulte **Verificar se o sistema está instalado**).
 - Se sim, a instalação da versão atualizada do aplicativo do sistema estará concluída.
 - O nome de usuário e a senha padrão são **Administrator**. Observe que a senha (mas não o nome de usuário) faz distinção entre maiúsculas e minúsculas.

Iniciar a atualização do cliente

1. Clique duas vezes na nova versão do pacote de instalação do software.
2. Selecione o idioma da interface.
3. Clique duas vezes em **Client (Cliente)**.

4. Clique com o botão direito em **AMS Client Setup.exe** e selecione **Run as administrator (Executar como administrador)** no menu de contexto.
 - O Assistente de preparação de instalação será aberto.
 - Selecione os componentes que deseja atualizar e clique em **Next> (Próximo>)**.
 - Dependendo do conteúdo que já estiver disponível, o assistente marcará os componentes que podem ser atualizados por padrão.
 - Você pode optar por atualizar ou ignorar a atualização dos componentes:
 - Por padrão, os componentes que não puderem ser atualizados serão marcados como **Skip (Ignorar)**.
5. Leia o **Contrato de licença do usuário final** e clique em **Accept (Aceitar)** para continuar. Se você não concordar, clique em **Decline (Recusar)** para voltar e cancelar a operação.
 - A próxima caixa de diálogo mostra o caminho de instalação em que o cliente do sistema será mantido.
 - Por padrão, o assistente de instalação instala o cliente do sistema na unidade C : \Program Files local (recomendado).
 - Arquivos instalados na unidade C : \Program Files local só podem ser modificados por usuários com direitos de administrador. Isso proporciona segurança, pois garante que usuários sem direitos de administrador não modifiquem arquivos relacionados ao sistema.
6. Insira o endereço do servidor. Formato do endereço: Hostname:4999/tcp
7. Clique em **Next> (Próximo>)** para continuar.
 - A próxima caixa de diálogo mostra o caminho de instalação em que o aplicativo Map View do sistema será mantido.
 - Por padrão, o assistente de instalação instala o aplicativo Map View do sistema na unidade C : \Program Files local (recomendado).
8. Insira o endereço de descoberta.
 - O aplicativo Map View estabelecerá conexão com o endereço de descoberta para descobrir os endpoints do sistema. Esse endereço é um URL que contém o nome do servidor e o número da porta em que o endpoint de descoberta está hospedado.
9. Verifique o resumo de instalação pré-atualização e clique em **Install (Instalar)**.
 - É exibido um resumo com todos os componentes escolhidos para atualização.
10. Observe a barra de progresso da instalação.
 - Aguarde o término da operação.
11. Após a conclusão da operação, clique em **Next> (Próximo>)** e verifique o resumo de instalação pós-atualização.
 - É exibido um resumo com todos os componentes atualizados.
12. Clique em **Finish (Concluir)** para finalizar a instalação da versão atualizada do sistema.
13. Reinicie o PC (recomendado).
 - O PC reinicia.
14. Verifique se o sistema está instalado (consulte **Verificar se o sistema está instalado**).
 - Em caso afirmativo, a instalação da versão atualizada do aplicativo do sistema estará concluída.
 - O nome de usuário e a senha padrão são **Administrator**. Observe que a senha (mas não o nome de usuário) faz distinção entre maiúsculas e minúsculas.

Consulte

- *Verificar se o sistema está instalado, página 12*

3.9 Desinstalar

Para desinstalar completamente o software do sistema, siga as etapas abaixo:

Desinstalação do servidor

1. Clique no botão **Iniciar** do Windows.
2. Pesquise **Painel de Controle** e clique duas vezes para abri-lo.
3. Siga o caminho: **Programas > Programas e Recursos > Desinstalar um programa**
 - Uma lista dos programas instalados abrirá.
4. Clique com o botão direito em **Access Management System - Server** (Servidor) e selecione **Uninstall** (Desinstalar) no menu de contexto.
 - O assistente de desinstalação do sistema abrirá.
5. Selecione os componentes que deseja desinstalar e clique em **Next> (Próximo>)**. Clique em **Cancel (Cancelar)** para cancelar o processo.
 - Você pode escolher se deseja instalar ou ignorar os componentes. A maioria dos componentes são obrigatórios e não podem ser ignorados.
6. Selecione os componentes que deseja desinstalar e clique em **Next> (Próximo>)**. Após inserir a **senha do SQL**, clique em **Test Server (Testar servidor)**.
 - Dados de configuração do SQL Database Server:
 - SQL Server: o nome do host onde o SQL Server é executado, isto é, a máquina local
 - Instância do SQL: o nome da instância do SQL.
 - Banco de dados AMS: o nome do banco de dados criado.
 - Nome de usuário do SQL: o login do SQL criado.
 - Senha do SQL: a senha do SQL criada para o login do SQL.
7. Clique em **Next> (Próximo>)**.
8. Observe a barra de progresso da desinstalação.
9. Após a conclusão da operação, clique em **Next> (Próximo>)** e verifique o resumo pós-desinstalação.
 - Será exibido um resumo com todos os componentes desinstalados ou ignorados.
10. Clique em **Finish (Concluir)** para finalizar a desinstalação do servidor.
 - O assistente de desinstalação fechará.
 - O sistema desaparece da lista de programas instalados.
 - O ícone do sistema desaparece da área de trabalho.

Desinstalação do cliente

1. Clique no botão **Iniciar** do Windows.
2. Pesquise **Painel de Controle** e clique duas vezes para abri-lo.
3. Siga o caminho: **Programas > Programas e Recursos > Desinstalar um programa**
 - Uma lista dos programas instalados abrirá.
4. Clique com o botão direito em **Access Management System - Client** (Cliente) e selecione **Uninstall** (Desinstalar) no menu de contexto.
 - O assistente de desinstalação do sistema abrirá.
5. Selecione os componentes que deseja desinstalar e clique em **Next> (Próximo>)**. Clique em **Cancel (Cancelar)** para cancelar o processo.
 - Você pode escolher se deseja instalar ou ignorar os componentes. A maioria dos componentes são obrigatórios e não podem ser ignorados.
6. Observe a barra de progresso da desinstalação.

7. Após a conclusão da operação, clique em **Next> (Próximo>)** e verifique o resumo pós-desinstalação.
 - Será exibido um resumo com todos os componentes desinstalados ou ignorados.
8. Clique em **Finish (Concluir)** para finalizar a desinstalação do cliente.
 - O assistente de instalação fechará.
 - O sistema desaparece da lista de programas instalados.
 - O ícone do sistema desaparece da área de trabalho.

Para concluir o processo de desinstalação, vá para `Program Files (x86)` na sua unidade `C:` local e exclua a pasta `Bosch Sicherheitssysteme`.

4 Dados técnicos

Servidor	
<p>Sistemas operacionais compatíveis. Instalações em outros sistemas operacionais podem funcionar, mas nenhum tipo de garantia é oferecido.</p>	<ul style="list-style-type: none"> - Windows Server 2016 (64 bits, Standard, Datacenter) - Windows 10, version 1903 (LTSC, LTSC) - Observação: O banco de dados padrão fornecido com esse sistema é o SQL Server 2017 Express Edition com serviços avançados
<p>Requisitos mínimos de hardware</p>	<ul style="list-style-type: none"> - Processador Intel i5 com pelo menos 4 núcleos físicos - 8 GB de RAM (32 GB são recomendáveis) - 200 GB de espaço livre no disco rígido (discos SSD são recomendáveis) - Adaptador gráfico com <ul style="list-style-type: none"> - 256 MB de RAM - Resolução de 1280x1024 - Pelo menos 32 k cores - Placa Ethernet de 1 Gbits - Porta USB livre ou compartilhamento de rede para arquivos de instalação
Cliente	
<p>Sistemas operacionais compatíveis. Instalações em outros sistemas operacionais podem funcionar, mas nenhum tipo de garantia é oferecido.</p>	<ul style="list-style-type: none"> - Windows 10, versão 1803 (LTSC, LTSC)
<p>Requisitos mínimos de hardware</p>	<ul style="list-style-type: none"> - Intel i5 ou superior - 8 GB de RAM (16 GB são recomendáveis) - 20 GB de espaço livre no disco rígido - Adaptador gráfico com <ul style="list-style-type: none"> - 256 MB de RAM - Resolução de 1920x1080 - Pelo menos 32 k cores - DirectX® 11 - Placa Ethernet de 1 Gbits - Porta USB livre ou compartilhamento de rede para arquivos de instalação
Servidor MAC	
<p>Requisitos mínimos de hardware</p>	<ul style="list-style-type: none"> - Intel i5 ou superior - 8 GB de RAM (16 GB são recomendáveis) - 20 GB de espaço livre no disco rígido - Adaptador gráfico com <ul style="list-style-type: none"> - 256 MB de RAM

Servidor MAC	
	<ul style="list-style-type: none">- Resolução de 1280x1024- Pelo menos 32 k cores- Placa Ethernet de 1 Gbits

**Aviso!**

O servidor e o cliente devem ser instalados na mesma versão. Não tente acessar o servidor com uma versão de cliente diferente.



Bosch Security Systems B.V.

Torenallee 49

5617 BA Eindhoven

Netherlands

www.boschsecurity.com

© Bosch Security Systems B.V., 2020