Access Management System

en Installation Guide

Table of contents

1 About this documentation

This is the main installation manual for the Access Management System.

Related documentation

The following are documented separately:

– The configuration and operation of AMS and its auxiliary programs.
– The operation of AMS - Map View.

2 AMS System overview

Access Management System is a powerful, pure access control system, which performs solo or in concert with BVMS, the Bosch flagship video management system.
Its power stems from its unique balance of leading-edge and proven technologies:

- Designed for usability: practical user interface with drag-and-drop Map View, and streamlined biometric enrollment dialogs.
- Designed for data security: supporting the latest standards (EU-GDPR 2018), operating systems, databases and encrypted system interfaces.
- Designed for resilience: middle-layer main access controllers provide automatic failover and replenishment of local access controllers in case of network failure.
- Designed for the future: regular updates and a pipeline full of innovative enhancements.
- Designed for scalability: offering low to high entry levels.
- Designed for interoperability: RESTful APIs, with interfaces to Bosch video management, event handling and specialized partner solutions.
- Designed for investment-protection: allowing you to build on, but boost the efficiency of, your installed access-control hardware.

3 Installation

Overall procedure

The installation of the system consists of two separate installers: the server and the client.
The overall order of installation is as follows:

1. Check the system requirements.
2. Before installing any client workstations:
– Install the software on the server and verify correct installation.
– On the server, create one or more workstation authorizations for the client workstations, and adapt the firewall settings to allow client-server connections.
3. Install the HTTPS Certificate on each client machine.
4. Install the clients.

Notice!

Dedicated servers are recommended
To guarantee the highest levels of operability, availability and performance at all times, install each server system (access management, video management, intrusion detection or third party) on its own dedicated computer.

Refer to

– *Importing the HTTPS certificate, page 10*
– *Checking if the system is installed, page 13*

3.1 System requirements

Minimum technical requirements for an AMS server

Server	
Supported operating systems. Installations on other operating systems may succeed, but are entirely without warranty.	– Windows Server 2016, Windows Server 2019 (64 bit, Standard, Datacenter) – Windows 10 Version 1809 LTSC, Windows 10 Professional and Enterprise, Version 20H2 – **Ensure that the latest software updates are installed.** – **Note:** The default database delivered with this system is SQL Server 2017 Express edition with advanced services

Minimum hardware requirements	– Intel i7 processor generation 8
	– 16 GB RAM (32 GB recommended)
	– 250 GB of free hard disk space
	– Hard disk transfer rate 300 MB/s with < 10 ms average response time (SSD recommended)
	– Graphics adapter with
	  – 256 MB RAM
	  – A resolution of 1280x1024 (Use the graphic resolution recommended for the client if you wish to run the Map View client on the AMS server).
	  – At least 32 k colors
	– 1 Gbit/s Ethernet card

Server	
	– A free USB port or network share for installation files

Minimum technical requirements for an AMS client

Client, including the Map View client	
Supported operating systems. Installations on other operating systems may succeed, but are entirely without warranty.	– Windows 10 Version 1809 LTSC, Windows 10 Professional and Enterprise, Version 20H2 – **Ensure that the latest software updates are installed.**

Minimum hardware requirements	– Intel i5 or higher
	– 8 GB RAM (16 GB recommended)
	– 25 GB of free hard disk space
	– Graphics adapter
	  – 256 MB RAM
	  – To use the AMS Dialog manager, a resolution of 1280x1024 is sufficient.
	  – For AMS Map view, a resolution of 1920x1080 (Full HD) is required.
	  – At least 32 k colors
	– DirectX® 11
	– 1 Gbit/s Ethernet card
	– A free USB port or network share for installation files

Visitor Management client	
Supported browsers.	Google Chrome, Mozilla Firefox, Microsoft Edge (Chromium based)
Minimum recommended screen resolution	Full HD 1920x1080

Minimum technical requirements for an additional MAC

MAC server	
Supported operating systems. Installations on other operating systems may succeed, but are entirely without warranty.	– Windows Server 2016, Windows Server 2019 (64 bit, Standard, Datacenter) – Windows 10 Version 1809 LTSC, Windows 10 Professional and Enterprise, Version 20H2 – **Ensure that the latest software updates are installed.**
Minimum hardware requirements	– Intel i5 or higher – 8 GB RAM (16 GB recommended) – 20 GB of free hard disk space – Graphics adapter with – 256 MB RAM

MAC server	
	– A resolution of 1280x1024 – At least 32 k colors – 1 Gbit/s Ethernet card

3.2 Installing the server

Before you begin

1. Ensure that the hostname of the intended server machine conforms to the rules specified in the notice box below.
2. Ensure that the system is not already installed (see **Checking if the system is installed**).
3. Copy the installation package onto your server machine.

Notice!
NETBIOS conventions for computer names apply, for example:
- The name is no longer than 15 characters,
- The name does **not** start with a digit [0-9].
- The name has only Latin characters, without diacritic marks.
- For details, see: *https://support.microsoft.com/en-us/help/909264/naming-conventions-in-active-directory-for-computers-domains-sites-and*

Start the server installation

1. Double-click the software installation package.
2. Double-click **Server**.
3. Right-click **AMS Server Setup.exe** and select **Run as administrator** from the context menu.
– The installation preparation wizard opens. Follow the installation preparation wizard.
4. Select the required components to be installed and click **Next>**.
– Depending on what is already installed, the wizard presents a list of the software that it will install:
– If there are any non-mandatory components that you do not require, cancel their selections at this point.
5. Read the **End User License Agreement** and click **Accept** to continue. If you do not agree, click **Decline** to abort the installation.
6. Enter the SQL Database Server configuration data.
– SQL Database Server configuration data:
  – SQL Server: The host name where the SQL Server instance will run. Use the local machine.
  – SQL instance: The SQL instance name
  – AMS database: The name of the database
  – SQL user name: The SQL login
7. Click **Next>**.
8. If the default installation path for the server is acceptable, click **Next>**. If you wish to select a different installation path (local drives only), click **Browse**.
– The default installation path *C:\Program Files (86)* is recommended because the files can only be modified by system administrators.

– If you select a different installation path ensure that the path is adequately protected from illicit access.
9. Click **Next>** to continue
– This page configures the API host name.
10. Check the pre-installation summary and click **Install**.
– A summary with all the components you chose to install appears.
11. Observe the installation progress bar.
– Once the moving green bar reaches about the middle of the progress bar, it will take several minutes until it starts to move again. Please wait.
– Another dialog box for the AMS database setup will open.
  – If the database is already installed, it will be updated.
  – Otherwise a new database will be created, and you will be required to create a new password for the *sa* account. **IMPORTANT:** Store this password securely, as it will be required for updates and other operations.
  Database creation can take several minutes. Wait until the dialog box closes.
12. After the operation is completed, click **Next>** and check the post installation summary.
– A summary with all the components that have been installed appears.
13. Click **Finish** to finish the installation.
– A dialog box requesting a restart will open. You must restart the computer to complete the installation of the system.
14. Click **Yes** to restart the PC.
– The PC restarts.
15. Check if the system is installed correctly (see **Checking if the system is installed**).
– If so, the first-time installation of the system application is completed. An icon for the system appears on the desktop.

Logging on for the first time

1. Double-click the application icon of the system on your Desktop.
2. Enter the default user name and password.
  – The default username and password is **Administrator**. Note that the password (but not the username) is case-sensitive.
3. Click **Log in**.
  – A dialog box requesting a password change appears.
  – When logging on for the first time you must change the password in the popup dialog.
4. Click **OK** to log on.

Refer to

– *Checking if the system is installed, page 13*
– *Start the server update, page 15*

3.3 Deactivate the firewall

After successful installation of the server and before installing client workstations, deactivate the firewall. This allows client workstations and external MAC computers to connect to the server easily during initial configuration.

3.4 Installing client workstations

Before you begin

1. Ensure that the hostname of the intended client workstation conforms to the rules specified in the notice box below.
2. Copy the installation package onto your intended client workstation.

Notice!
NETBIOS conventions for computer names apply, for example:
- The name is no longer than 15 characters,
- The name does **not** start with a digit [0-9].
- The name has only Latin characters, without diacritic marks.
- For details, see: *https://support.microsoft.com/en-us/help/909264/naming-conventions-in-active-directory-for-computers-domains-sites-and*

HTTPS certificates for client workstations

The server of the system hosts several APIs. These APIs communicate via HTTPS and use a self-signed certificate. The server setup program creates this self-signed certificate and installs it on the server machine.
To enable secure communication between server and clients, the certificate from the server must be copied and imported manually on each client machine (see **Importing the HTTPS Certificate**).

Importing the HTTPS certificate

The certificate can be found at the following location:

– For AMS *<installation drive>:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Certificates\Access Management System Internal CA.cer*

1. Copy the certificate to the client machine.
2. In the client machine, double-click the certificate.
   – A certificate dialog box appears.
3. Click **Install Certificate**.

– The Certificate Import Wizard opens.

4. Select **Local Machine** (recommended) and click **Next>**.
5. Select **Place all certificates in the following store** to specify a location for the certificate (recommended).
6. Click **Browse**.

– A dialog box to select the certificate store opens.

7. Select *Trusted Root Certification Authorities* and click **OK** (recommended).

– The dialog box to select the certificate store closes.

8. Click **Next>** in the Certificate Import Wizard.
9. Click **Finish** to import the certificate.
   – The certificate import process is finished.

Notice!
If the HTTPS certificate is not installed, it will not be possible to start the application.

Note that you do not have to import the certificate to the server machine, as this is automatically done during the server installation. This applies to separate client workstations only.

AMS API integration with BVMS

To integrate the AMS API with BVMS (Bosch Video Management System) version 10.1 or later, import the self-signed certificate from the AMS server into the BVMS machine (see **Importing the HTTPS Certificate**).

Start the client installation

1. Double-click the software installation package.
2. Double-click **Client**.
3. Double-click **AMS Client Setup.exe**
   – The installation preparation wizard opens. Follow the installation preparation wizard.
4. Select the components that you want to install and click **Next>**.

– Depending on what is already available on the system, the wizard will select required Microsoft packages for Visual C++ and .NET.
– Optional components:
  – Client
  – Map View

5. Read the **End User License Agreement** and click **Accept** to continue. If you do not agree, click **Decline** to go back and cancel the operation.
6. If the default installation path regarding the client workstation is acceptable, click **Next>**. If you wish to select a different installation path (local drives only), click **Browse**.
7. Enter the server address. Address format: *<hostname>:4999/tcp*

– By default, the installation wizard installs the system client in the local *C:\Program Files (86)* folder.
– Files installed under the local *C:\Program Files (86)* folder can only be modified by users with administrator rights, therefore the default folder is strongly recommended.

8. If the default installation path regarding the Map View application is acceptable, click **Next>**.
9. If you wish to select a different installation path (local drives only), click **Browse**.
10. Enter the discovery address.

– By default, the installation wizard installs the Map View application in the local *C:\Program Files (86)* drive (recommended).
– The Map View application will connect to the discovery address to discover the endpoints of the system. This address is an URL containing the server name and the port number where the discovery endpoint is hosted.

11. Check the pre-installation summary and click **Install**.

– A summary with all the components you chose to install appears.

12. Observe the installation progress bar.

– Wait until the operation is completed.

13. After the operation is completed, click **Next>** and check the post installation summary.

– A summary of all installed components appears.

14. Click **Finish** to finish the installation.
15. Restart the computer.
16. Check if the system is installed (see **Checking if the system is installed**).

– If the installation of the AMS client and the Map View is complete, both application icons appear on the desktop. The default username and password is **Administrator**. Note that the password (but not the username) is case-sensitive.

Before starting the client

Before logging on to the client, you need to configure the client workstation on the server. Follow the procedure below:

1. Start the client on the server machine.
2. Click **Configuration>Device Data**

– A new dialog box opens.

3. In the top toolbar select the **Workstations** icon.
4. In the top toolbar select the **New** icon.
5. In the **Workstation** tab fill in the empty fields.

– The fields:
  – **Name**: Insert the host name of the client workstation (mandatory)
  – **Description**: Insert a description (optional)
  – **Login via reader**: Perform the login via the reader (optional)
  – **Automatic Logout after: X seconds** (optional). Set an automatic log out if you want the application to log out automatically after a specific amount of time

– Note that the underlined fields are mandatory.

6. In the top toolbar click the **Save** icon to save the changes.

– You can now log on from the client workstation.

Logging on for the first time

1. Double-click the application icon on your Desktop.
2. Enter the default user name and password.
   – The default username and password for both client applications is **Administrator**. Note that the password (but not the username) is case-sensitive.
3. Click **Log on**.
   – When logging on for the first time you must change the password. A dialog box appears.
4. Click **OK** to enter a new password in the next dialog box.
   – Use a strong password of at least 8 characters.
5. Enter your new password and click **Change**. Click **Cancel** to cancel the password change.
   – A dialog box confirming the password change appears.
6. Click **OK** to log on.

Notice!

Both the server and the client must be of the same AMS version. Do not try to access the server from a client of a different AMS version.

Refer to

– *Checking if the system is installed, page 13*
– *Importing the HTTPS certificate, page 10*

3.5 Checking if the system is installed

Checking if the system is installed

The system is installed if:

– The icons of the system are visible on the desktop.
– The following services are in the Windows Services application (**Start** > **Search** > *service.msc*): DMS, MAC Access PI, Identity service, MAP API, State API.
– The system is in the default installation path: *C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System*

3.6 Using custom certificates

AMS APIs can be configured to use custom certificates rather than the self-signed certificates that are automatically created during the setup.
This is beneficial when an organization already has a public key infrastructure (PKI) that has its own Certificate Authority (CA).

3.6.1 Prerequisites

– You have acquired a trusted root certificate file.
– The public and private parts of the certificate have to be placed on the AMS server directory
C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Certificates

Examples of public and private parts of a certificate:

– *Access Management System Test CA.CER* (public part)
– *CustomRootTestCA.PFX* (private part)

3.6.2 Using the Access Certificate Tool

Procedure

1. Navigate to the *Certificates* subfolder of your installation folder:
2. Run as Administrator *AcessCertificateTool.exe*
3. Select the check box **Delete old access certificates**
4. Select the check box **Custom root certificate**
5. In the text field **Certificate location**, enter the location of your PFX file
6. Enter the password, that you received from your Certificate Authority (CA)
7. In the text field **Output folder**, select the *Certificates* subfolder of your installation folder
8. Click **Generate**

– The tool generates your certificate *.CER* file
– Note: If the generation fails repeatedly, contact technical support.

9. Reboot your system.
10. Proceed to install this certificate on your client machines.

3.6.3 Installing and testing

Installing the root certificate on the client machines

1. Use Windows file Manager to copy your root certificate *"Access Management System Test CA.cer"* and to the client machine, where the client applications "Map View" and "AMS" (Dialog Manager) are installed.
2. Install the Root Certificate as follows:

– In the File Manager, right-click the **certificate file** and select **Install Certificate > Current User > Next >** Select **"Place all certificates in the following store" > Browse >** Select **"Trusted Root Certification Authorities" > Next > Finish > OK**

Testing the API certificates on the client machine.
The API-Certificates have to be tested on the client machine, where the client application Map View and AMS (Dialog Manager) are installed.

On the client machine, start the Google Chrome browser.
– To test the Identity Server, enter the following address: *https://[ServerHostname]:44333/.well-known/openid-configuration*
  – Right-click the website information padlock icon, select **Verify Certificate (Valid)** and check if the correct certificate is being used under **Issued by**.
– To test the Access API, enter the following address: *https://[ServerHostname]:44347/swagger*
  – Right-click the website information padlock icon, select **Verify Certificate (Valid)** and check if the correct certificate is being used under **Issued by**.
– To test the States API, enter the following address: *https://[ServerHostname]:62901/swagger*
  – Right-click the website information padlock icon, select **Verify Certificate (Valid)** and check if the correct certificate is being used under **Issued by**.
– To test the Map API, enter the following address: *https://[ServerHostname]:61801/$metadata*
  – Right-click the website information padlock icon, select **Verify Certificate (Valid)** and check if the correct certificate is being used under **Issued by**.

Using the certificate in AMS.
Start the Map View application on the Client machine and log on.

3.7 Troubleshooting

If the installation fails the progress bar turns red. Additional error text may be displayed. Click **Next>** to proceed to the summary page that will display which component has failed.

3.8 Updating the system

Before you begin
1. Log on to the server machine.
2. Check if the previous version of the system is installed (see **Checking if the system is installed**).
3. Copy the new installation package into your server machine.

Notice!
Both the server and the client must be of the same AMS version. Do not try to access the server from a client of a different AMS version.

Start the server update

1. Double-click the new version of the software installation package.
2. Select the interface language.
3. Double-click **Server**.
4. Right-click **AMS Server Setup.exe** and select **Run as administrator** from the context menu.

– The installation preparation wizard opens.
– Select the components that you desire to update and click **Next>**.
– Depending on what is already available, the wizard marks the components that can be updated by default.
– You can choose whether to update or skip the update of components.
– Components that cannot be updated will be marked as **Skip** by default.

5. Read the **End User License Agreement** and click **Accept** to continue. If you do not agree, click **Decline** to go back and cancel the operation.
6. Enter the SQL Database Server configuration data.

– SQL Database Server configuration data:
  – SQL Server: The host name where the SQL Server instance runs i.e., the local machine (recommended)
  – SQL instance: The SQL instance name
  – AMS database: The name of the database
  – SQL user name: The SQL login

7. Click **Next>**.

– The next dialog shows the installation path where the server of the system will be kept.
– By default, the installation wizard installs the server of the system in the local *C:\Program Files (86)* drive (recommended).
– Files installed under the local *C:\Program Files (86)* drive can only be modified by users with administrator rights. This offers security by ensuring that users without administrator rights cannot modify files related to the system.

8. Click **Next>** to continue.
9. Check the pre-update installation summary and click **Install**.

– A summary with all the components you chose to update appears.

10. Observe the installation progress bar.

– Once the moving green bar reaches about the middle of the progress bar, it will take several minutes until it starts to move again. Please wait.
– Another dialog box for the AMS database setup will open.
  – If the database is already installed, it will be updated.
  – Otherwise a new database will be created, and you will be required to create a new password for the *sa* account. **IMPORTANT:** Store this password securely, as it will be required for updates and other operations.
    Database creation can take several minutes. Wait until the dialog box closes.

11. After the operation is completed, click **Next>** and check the post-update installation summary.

– A summary with all the components that have been updated appears.

12. Click **Finish** to finish the installation of the updated version of the system.
13. Restart the PC (recommended).

– The PC restarts.

14. Check if the system is installed (see **Checking if the system is installed**).

– If so, the installation of the updated version of the system application is completed.

– The default username and password is **Administrator**. Note that the password (but not the username) is case-sensitive.

Start the client update

1. Double-click the new version of the software installation package.
2. Select the interface language.
3. Double-click **Client**.
4. Right-click **AMS Client Setup.exe** and select **Run as administrator** from the context menu.

– The installation preparation wizard opens.
– Select the components that you desire to update and click **Next>**.
– Depending on what is already available, the wizard marks the components that can be updated by default.
– You can choose whether to update or skip the update of components:
– Components that cannot be updated will be marked as **Skip** by default.

5. Read the **End User License Agreement** and click **Accept** to continue. If you do not agree, click **Decline** to go back and cancel the operation.

– The next dialog shows the installation path where the client of the system will be kept.
– By default, the installation wizard installs the client of the system in the local *C:\Program Files (86)* drive (recommended).
– Files installed under the local *C:\Program Files (86)* folder can only be modified by users with administrator rights.

6. Enter the server address. Address format: *<hostname>:4999/tcp*
7. Click **Next>** to continue.

– The next dialog shows the installation path where the Map View application of the system will be kept.
– By default, the installation wizard installs the Map View application of the system in the local *C:\Program Files (86)* drive (recommended).

8. Enter the discovery address.

– The Map View application will connect to the discovery address to discover the endpoints of the system. This address is an URL containing the server name and the port number where the discovery endpoint is hosted.

9. Check the pre-update installation summary and click **Install**.

– A summary with all the components you chose to update appears.

10. Observe the installation progress bar.

– Wait until the operation is completed.

11. After the operation is completed, click **Next>** and check the post-update installation summary.

– A summary with all the components that have been updated appears.

12. Click **Finish** to finish the installation of the updated version of the system.
13. Restart the PC (recommended).

– The PC restarts.

14. Check if the system is installed (see **Checking if the system is installed**).

– If so, the installation of the updated version of the system application is completed.
– The default username and password is **Administrator**. Note that the password (but not the username) is case-sensitive.

Refer to

– *Checking if the system is installed, page 13*

3.9 Uninstalling

To remove the software of the system, follow the steps below:

Uninstalling the server

1. Click the Windows **Start** button.
2. Search **Control Panel** and double-click to open it.
3. Follow the path: **Programs** > **Programs and Features** > **Uninstall a program**

– A list of installed programs opens.

4. Right-click **Access Management System** - **Server** and select **Uninstall** from the context menu.

– The uninstallation wizard of the system opens.

5. Select the components that you want to uninstall and click **Next>**. Click **Cancel** to cancel the process.

– You can choose whether to uninstall or skip components. Most components are mandatory and cannot be skipped.

6. Select the components that you want to uninstall and click **Next>**. After entering the **SQL password**, click **Test Server.**

– SQL Database Server configuration data:
  – SQL Server: The host name where the SQL Server runs i.e., the local machine
  – SQL instance: The SQL instance name.
  – AMS database: The name of the database that you created.
  – SQL user name: The SQL login that you created.
  – SQL password: The SQL password that you created for the SQL login.

7. Click **Next>**.
8. Observe the uninstallation progress bar.
9. After the operation is completed, click **Next>** and check the post-uninstallation summary.

– A summary with all the components that were uninstalled or skipped will appear.

10. Click **Finish** to finish the server uninstallation.

– The uninstallation wizard closes.
– The system disappears from the installed programs list.
– The icon of the system disappears from the desktop.

Uninstalling the client

1. Click the Windows **Start** button.
2. Search **Control Panel** and double-click to open it.
3. Follow the path: **Programs** > **Programs and Features** > **Uninstall a program**

– A list of installed programs opens.

4. Right-click **Access Management System** - **Client** and select **Uninstall** from the context menu.

– The uninstallation wizard of the system opens.

5. Select the components that you want to uninstall and click **Next>**. Click **Cancel** to cancel the process.

– You can choose whether to uninstall or skip components. Most components are mandatory and cannot be skipped.

6. Observe the uninstallation progress bar.

7. After the operation is completed, click **Next>** and check the post-uninstallation summary.
– A summary with all the components that were uninstalled or skipped will appear.
8. Click **Finish** to finish the client uninstallation.
– The installation wizard closes.
– The system disappears from the programs list.
– The icon of the system disappears from the desktop.

To complete the deinstallation process, delete the folder *C:\Program Files (x86)\Bosch Sicherheitssysteme*

4 Technical data

Notice!
Both the server and the client must be of the same AMS version. Do not try to access the server from a client of a different AMS version.

Glossary

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

202110302335