BOSCH

Access Management System

AMS Map View

en   Operation manual

Table of contents

1   Using Help

How to use this help file.

Tool bar buttons

Button	Function	Description
	Hide	Click this button to hide the navigation pane (Contents, Index and Search tabs). leaving only the help pane visible.
	Show	When the Hide button is clicked it is replaced by the Show button. Click this button to reopen the Navigation pane.
	Back	Click this button to move back through the chain of topics most recently viewed.
	Forward	Click this button to move forward again through the same chain of topics
	Print	Click this button to print. Choose between "Print the selected topic," and "Print the selected heading and all subtopics".

Tabs

Contents   This tab displays a hierarchical table-of-contents. Click a book icon to open it and then click on a topic icon to view the topic.

Index   This tab displays an index of terms in alphabetical order. Select a topic from the list or type in a word to find the topic(s) containing it.

Search   Use this tab to find any text. Enter text in the field and then click button: **List Topics** to find topics that contain all the words entered.

Resizing the help window

Drag the corner or edge of the window to the desired size.

Further conventions used in this documentation

– Literal text (labels) from the UI appears in **bold**.
  E.g. **Tools, File, Save As…**
– Sequences of clicks are concatenated using the **>** character (the greater-than sign).
  E.g. **File > New > Folder**
– Changes of control-type (e.g. menu, radio-button, check box, tab) within a sequence are indicated just before the label of the control.
  E.g. Click menu: **Extra > Options >** tab: **View**
– Key combinations are written in two ways:

- Ctrl+Z means hold down the first key while pressing the second
- Alt, C means press and release the first key, then press the second
- The functions of icon buttons are added in square brackets after the icon itself.
  E.g. [Save]

2   About this documentation

This is the main software manual for the AMS - Map View auxiliary program of the Access Management System , hereafter referred to as AMS.

- Edit mode: The creation and configuration of maps for interoperability with AMS.
- View mode: The operation of the configured system by operators of AMS - Map View.

Related documentation

The following are documented separately:

- The installation of AMS and its auxiliary programs.
- The configuration and operation of the Access Management System.

3   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.

4   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.

Refer to

4.1   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 (64 bit, Standard, Datacenter) – Windows 10, version 1809 (LTSC) – **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 i5 processor with at least 4 physical cores
	 – 8 GB RAM (32 GB recommended)
	 – 200 GB of free hard disk space (SSD disks 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
	 – 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.	– Windows 10, version 1809 (LTSC) – **Ensure that the latest software updates are installed.**

Client, including the Map View client	
Installations on other operating systems may succeed, but are entirely without warranty.	

Minimum hardware requirements	– Intel i5 or higher
	– 8 GB RAM (16 GB recommended)
	– 20 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

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 (64 bit, Standard, Datacenter) – Windows 10, version 1809 (LTSC) – **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
	  – A resolution of 1280x1024
	  – At least 32 k colors
	– 1 Gbit/s Ethernet card

4.2   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 15*
– *Start the server update, page 20*

4.3 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.

4.4 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!
i	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

1. Go to `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Certificates\Access Management System Internal CA.cer`
2. Copy the certificate to the client machine.
3. In the client machine, double-click the certificate.
   – A certificate dialog box appears.
4. Click **Install Certificate**.
– The Certificate Import Wizard opens.
5. Select **Local Machine** (recommended) and click **Next>**.
6. Select **Place all certificates in the following store** to specify a location for the certificate (recommended).
7. Click **Browse**.
– A dialog box to select the certificate store opens.
8. Select `Trusted Root Certification Authorities` and click **OK** (recommended).
– The dialog box to select the certificate store closes.
9. Click **Next>** in the Certificate Import Wizard.
10. 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 15*
- *Importing the HTTPS certificate, page 13*

4.5 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\`

4.6 Using custom certificates

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

4.6.1 Preconditions

- Have 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)

4.6.2   Using custom certificates

Open a PowerShell session
Run PowerShell as Administrator on the AMS server in the folder: `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Certificates`

Remove the installed certificates
1. Remove the certificates that were installed during the AMS installation.
2. Execute: "`RemoveAceApiCertificates.ps1`" in the opened PowerShell session.

Edit the script for API-Certificate creation
1. Open the PowerShell file "`CreateAceApiCertificatesFromOwnRoot.ps1`" in a text editor and change the following file names to the names of your custom certificates:
– `CustomRootTestCA.pfx`
– `Access Management System Test CA.cer`
    – Note that each file name appears only once in the script.
2. Save the changes.

Run the script for API-Certificate creation
1. Execute: "`CreateAceApiCertificatesFromOwnRoot.ps1`" in the PowerShell session that you opened above.
2. Enter the password for the private certificate.
– The necessary API certificates are created and installed:
– The root certificate is installed.

Verify the installation of the certificates in Windows Certificates for Current User and Local Computer
The certificate is installed if:
– The root certificate is installed under `Current User Personal Certificates, Trusted Root Certificates` and under `Local Computer Trusted Root Certificates`
– The API-Certificates are installed under `Local Computer Personal Certificates`

Update the Thumbprint app settings for each API
For each API, the thumbprint must be updated.

Access API	1. Open `C:\Program Files (x86)\Bosch Sicherheitssysteme \Access Management System\Access API`
	2. Exchange the values in the file `appsettings.json`, line `"Thumbprint"`:
	3. Open **Certificates Local Computer > Personal > Certificates > Friendly Name:** `Access Management System Access API`
	4. Select and open the installed certificate `"Access Management System Access API"` **> Details**
	5. Scroll down in the list to `"Thumbprint"`
	6. Select `Thumbprint.`
	7. Copy the displayed Thumbprint (e.g. `"da"`).
	8. Paste the Thumbprint without spaces into the `appsettings.json` file, in `C:\Program Files (x86)\Bosch Sicherheitssysteme \Access Management System\Access API`
	– (e.g. `"Thumbprint": "53d3588285bd570c9799e883b27ef1b139ba28da"`)

Map API	1. Open `C:\Program Files (x86)\Bosch Sicherheitssysteme \Access Management System\Map API`
	2. Exchange the values in the file `appsettings.json`, line `"Thumbprint"`:
	3. Open **Certificates Local Computer > Personal > Certificates > Friendly Name:** `Access Management System Map API`
	4. Select and open the installed certificate `"Access Management System Map API"` **> Details**
	5. Scroll down in the list to `"Thumbprint"`.
	6. Select `Thumbprint`.
	7. Copy the displayed Thumbprint (e.g. `"e8"`).
	8. Paste the Thumbprint without spaces into the `appsettings.json` file, in `C:\Program Files (x86)\Bosch Sicherheitssysteme \Access Management System\Map API`
	– (e.g. `"Thumbprint": "3cef0c43be36ee01d8a6ea2f59f170cde96168e8"`)

States API	1. Open `C:\Program Files (x86)\Bosch Sicherheitssysteme \Access Management System\States API`
	2. Exchange the values in the file `appsettings.json`, line `"Thumbprint"`:
	3. Open **Certificates Local Computer > Personal > Certificates > Friendly Name:** `Access Management System States API`
	4. Select and open the installed certificate `"Access Management System States API"` **> Details**

	5. Scroll down in the list to *"Thumbprint"*.
	6. Select *Thumbprint.*
	7. Copy the displayed Thumbprint (e.g. *"e2"*).
	8. Paste the Thumbprint without spaces into the *appsettings.json* file, in *C:\Program Files (x86)\Bosch Sicherheitssysteme \Access Management System\States API*
	– (e.g. "Thumbprint": "37c0bb09d4cab985b620da1c667597ef43b5f8e2"

Identity Server:	1. Open *C:\Program Files (x86)\Bosch Sicherheitssysteme \Access Management System\Identity Server*
	2. Exchange the values in the file *appsettings.json*, line *"Thumbprint"*:
	3. Open **Certificates Local Computer > Personal > Certificates > Friendly Name:** *Access Management System Identity Server*
	4. Select and open the installed certificate *"Access Management Identity Server"* **> Details**
	5. Scroll down in the list to *"Thumbprint"*.
	6. Select *Thumbprint.*
	7. Copy the displayed Thumbprint.
	8. Paste the Thumbprint without spaces into the *appsettings.json* file, in *C:\Program Files (x86)\Bosch Sicherheitssysteme \Access Management System\Identity Server*
	9. Paste the Thumbprints of the other API's in the corresponding Thumbprint entry fields in this file as well.
	– Example:
	– For *"Name": "AccessApi"* *"Thumbprint":* *"53d3588285bd570c9799e883b27ef1b139ba28da"*
	– For *"Name": "MapApi"* *"Thumbprint":* *"3cef0c43be36ee01d8a6ea2f59f170cde96168e8"*
	– For *"Name": "StatesApi"* *"Thumbprint":* *"37c0bb09d4cab985b620da1c667597ef43b5f8e2"*

Stopping and starting services
1. Open Windows services.
2. Right-click the following services and select "Stop" after each one of them:
– Access Management System Access API
– Access Management System Identity Server
– Access Management System Map API
– Access Management System Sates API

– After all four services are stopped, right-click the same services again and select **Start** after each one of them.

Installing the Root Certificate on the client machine
1. Use Windows file Manager to copy your root certificate *"Access Management System Test CA.cer"* and paste it in the client machine, where the client application "Map View" and "AMS" (Dialog Manager) are installed.
   For example, paste it in the Downloads folder.
2. Install the Root Certificate:
– 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 Lock-icon > 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 Lock-icon > 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 Lock-icon > 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 Lock-icon > 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.

4.7 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.

4.8 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 15*

4.9 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

5 Map View basics

Overview

The AMS - Map View is an application of the AMS system that allows the operator to monitor and control building security:

– Upload and configure maps.
– Position and edit devices that were defined in the AMS device editor.
– Monitor device states from a hierarchy of maps and/or schematics.
– Monitor and process alarms, in coordination with other operators.
– Graphically demarcate intrusion detection areas on maps, and configure color changes according to state.
– Send commands to intrusion-detection and access-control devices through the context menus of their map icons.
– Activate and deactivate Threat levels.
– View access events in real time "Swipe ticker".
– View access control areas that were defined in the AMS device editor.

5.1 Getting started

5.1.1 Prerequisites

– The HTTPS certificate must have been imported and installed to the client machine.
– The user must have rights to use the AMS - Map View application.
  The AMS - Map View user rights are set in the AMS Client application: **Main menu > Configuration > Operators and Workstations > User profiles**
  The rights required are **Access Manager Maps** plus one or more of its component rights, which are:

Component	Description
Door commands	Door grant access Enable/Disable unlock Secure/Lock door
Reader commands	Reader grant access Disable/Enable reader
Controller commands	For Access Sequence Monitoring at MAC and reader levels) Grant access Set office mode Secure doors
System commands	Warm and cold start MACs and AMCs, Switch to redundant failover MAC (RMAC) Synchronize MAC with RMAC
Special door commands	Enable and disable manual mode
DOP commands	Turn the digital outputs of controllers on and off
Alarm list commands	Configure alarms

		Handle one or more different categories of alarms, configurable individually Operate the alarm log
	Swipe ticker	Use the Swipe ticker feature
	Intrusion commands	Control intrusion areas, panels and points

5.1.2 Logging on for the first time
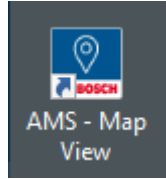
1. ⬛ Double-click the AMS - Map View application icon on the desktop.
–   The log on dialog box opens.
2. Enter the default user name and password.
–   The default username and password for both client applications is **Administrator**. Note that the password (but not the username) is case-sensitive.
3. Click **Logon**.
4. Enter username and password.

–   The main application window of the AMS - Map View opens.

> **Notice!**
> If your logon fails, refer to the error messages displayed in the logon dialog box.

5.2 Display modes: View mode and edit mode

The AMS - Map View application has two modes of operation: **view mode** and the **edit mode**.

Click ✏ in the main tool bar to switch between the two display modes. When the icon is highlighted the application is in **edit mode**.
Note that an operator requires permissions in order to use **edit mode**. For instructions, see *Prerequisites, page 24*

Selecting devices and areas
In both modes, you can select single devices and areas.
For intrusion areas in the areas list, you can also select multiple items:
–   To select multiple items separately, **ctrl-click** each item.
–   To select multiple items contiguously, click the first item, then **shift-click** another item in the same list.

View mode
In view mode, operators cannot edit the devices on the map. They can do the following:
–   Select and give commands to the devices via their context menus
    –   right-click any device to open its context menu
–   Monitor and process alarms.
–   View access control areas and their populations (if this feature is licensed).

Edit mode

In edit mode, the user can edit the maps and the devices but cannot give commands to the devices via their context menus.

Refer to

–   *Prerequisites, page 24*

5.3   The main application window
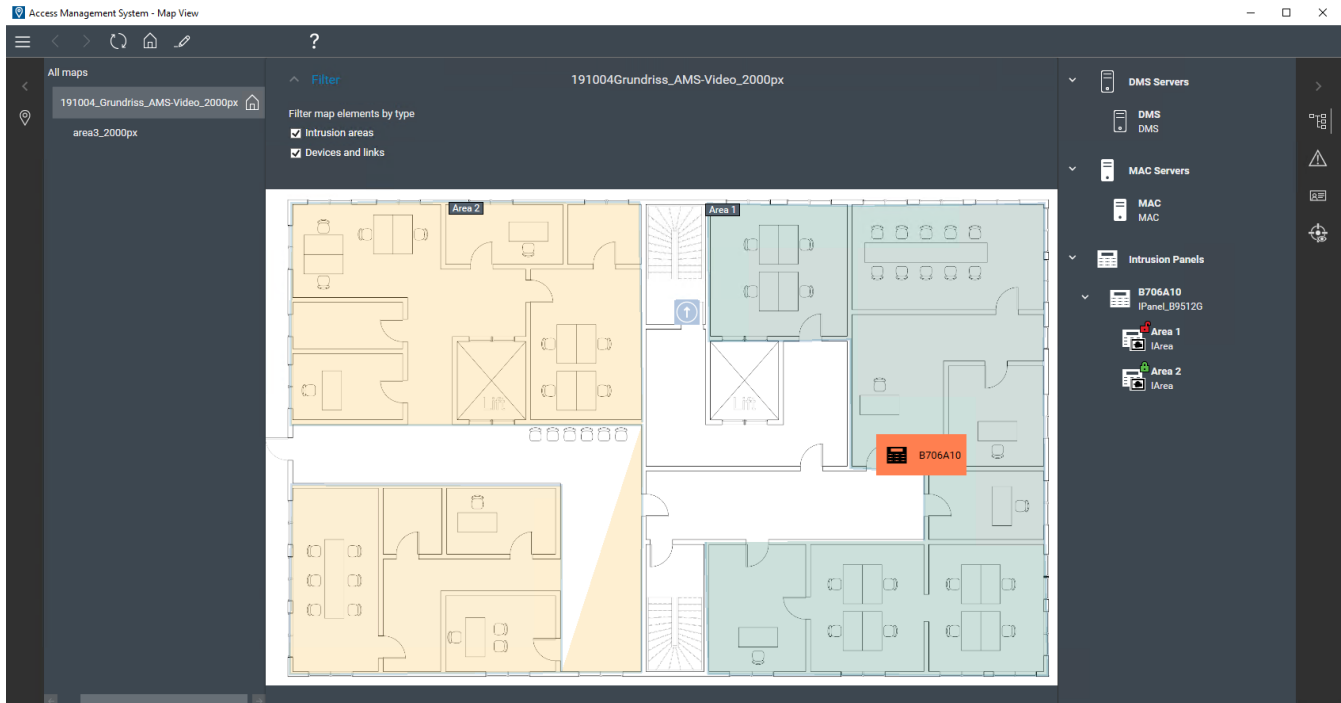
Structure overview

The layout of the main window of the AMS - Map View is as follows:

–   **Top**: The main tool bar
–   **Left**: The map tree menu
–   **Middle**: The map display area
–   **Right**: A column in which to display the applications
–   **Right edge**: The applications menu, including:
     –   The Device tree
     –   The Alarm view
     –   The Swipe ticker
     –   The Areas view

Main tool bar

The main tool bar is situated horizontally at the top of the main application window.

The main tool bar contains the following tools:

Icons	Functions
☰	When clicking this icon, a drop-down menu with two options opens: – Click **About...** to get information about: – Version: Version number of the system

Icons	Functions
	– States API: Version number – Access API: Version number – Build: Installation package number – Operator: Who is logged in – Logon time: Since when the Operator is logged on Click **OK** to close the dialog. – Click **Logout** to log out from the AMS - Map View application.
⟨	Go back to the previous page.
⟩	Go forward to a new page after going back.
↻	Reload the page. A yellow triangle indicates changes that require a reload in order to be displayed.
⌂	Navigate to the home map (view mode).
✎	Switch between display modes (edit mode and view mode).
?	Get information on how to use the application.

Map tree menu

The map tree menu is situated at the left side of the main application window.

It consists of:

– A thin vertical bar with a darker background color that allows you to hide and show the map tree menu.

Icon	Function
⟨	Show the map tree menu.
◎	Show the map tree menu.

– A small horizontal toolbar at the top of the map tree menu. This bar only appears in edit mode.

Icon	Function
+	Add a new map.
✎	Update a map.

Icon	Function
🗑	Delete a map.
	Export a map.
🏠	Set a map as home.

–   The **All maps** function is situated below the small horizontal tool bar. Click 〉 to collapse and expand the map navigation tree.

Applications menu

The applications menu is situated in a column at the right side of the main application window.

The applications menu can be folded and unfolded, and contains the following.

Icon	Function
〉	Show the applications menu.
	Show the device tree.
⚠	Show the alarm list.
	Show the swipe ticker
	Show the access and intrusion areas in tables

–   The device tree displays devices created in the AMS device editor, DevEdit. The contents of the tree are updated by the AMS system.

Icon	Function
〉	Switch between a folded and unfolded view of the device hierarchy.
	A DMS device.
	A MAC device.

Icon	Function
⬚	An AMC device.
🗖	An entrance, which may consist of one or more doors and associated readers.
▯	A door.
▦	An intrusion panel
▦	An intrusion area
▦	An intrusion point. This is the default icon. A selection of more specific icons is available from the context menu, if desired.
K	A turnstile
✲	An assembly point
▤	A reader device.
🕐	A time management reader
P	A parking area.
⊫	A boom barrier.
⬍	An elevator.
▬	A Simons Voss gateway.
⬚	An AMC device with individually configurable digital inputs and outputs (DIPDOP)
⬚	A digital input (DIP). When the digital input is not set the icon is displayed struck through.

Icon	Function
	A digital output (DOP). When the digital output is not set the icon is displayed struck through.

Map display area

The main map display area occupies the center of the main application window. It displays the map that is currently selected in the map tree, along with the intrusion areas and icons for the devices that have been placed on that map.

Use check boxes to hide and unhide map elements: intrusion areas, icons or both.
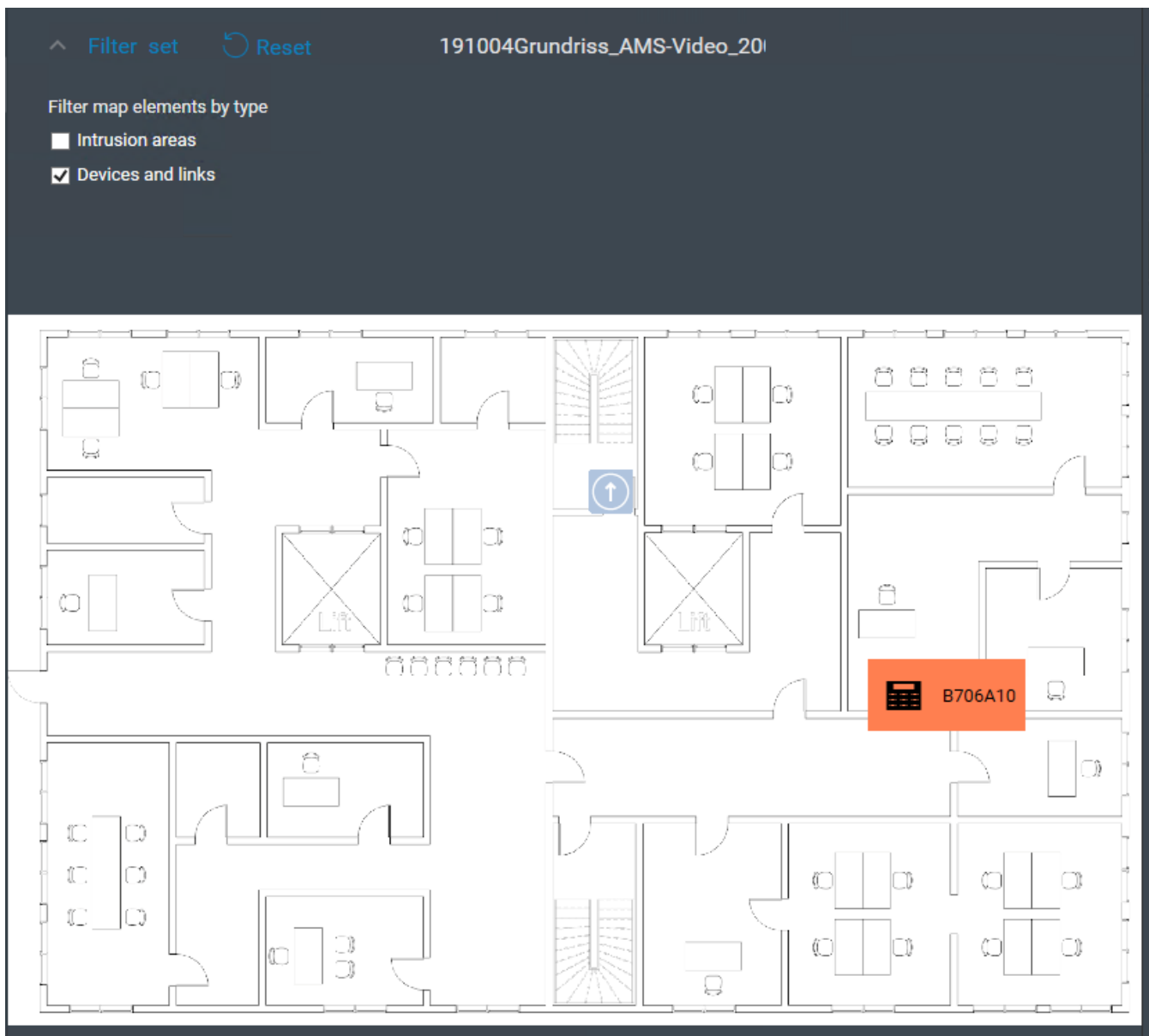
5.4   Configuring alarm sounds

Introduction

AMS Map view provides a fully customizable way of playing different alarm sounds to the operator, depending on the severity of the alarm.

Procedure

1.   Place up to four files of type `.WAV` in the following folder:

       `<installation drive>:\Program Files (x86)\Bosch Sicherheitssysteme`
       `\Access Management System\Map View\`
       Note that sample files are available from
       `<installation drive>:\Program Files (x86)\Bosch Sicherheitssysteme`
       `\Access Management System\Map View\Sample Sounds\`

2.   Each file name must be one of:

`Threat.wav`
`Critical.wav`
`Warning.wav`
`Maintenance.wav`

Note that, as the whole `.WAV` file is played, Bosch recommends that it be of short duration, for example one or two seconds.

Process

1.   Whenever an alarm is raised, Map view looks to see whether a `.WAV` file of the corresponding severity is present in the `Map view\` folder.
       –   If so then the file is played via the computer's default playback device.
       –   If not then no sound is played.

6 Configuring maps with Edit mode

Introduction to edit mode

Edit mode is the mode for making changes to the maps and their device links, as opposed to operating the devices.

Note that an operator requires permissions in order to use **edit mode**. For instructions, see *Prerequisites, page 24*

The following sections describe the tasks that can be performed in edit mode.

6.1 Uploading a map

Supported image formats

Before uploading a map image to the AMS - Map View application, make sure that the image file fulfills the following requirements:

Minimum technical requirements to add a map image file	
Supported image file format	*.bmp, *.jpg, *.png
Maximum supported map dimension	2000 x 2000

Upload a map as follows:

1. Click ✎ to enter edit mode.
– The map editing toolbar appears
2. Select a node in the map tree to be the parent of the new node.
3. In the map tree menu, click ┼
– A dialog box appears
4. Fill in the empty entry fields:
– Image file: Click **...** to upload an image file from your computer. Select the desired map image in the **Save As** dialog box, and click **Open**.
– Name: The system assumes the name of the uploaded file by default. Change the name if desired.
– Description: Add a description if desired.
– If you are authorized for more than one division, select the division from the list.
5. Click **OK**.
– The map image appears in the map display area.
– The name of the uploaded map appears as a subnode beneath the currently selected node in the map tree.

> **i** **Notice!**
> The map tree nodes are ordered alphabetically by default.

6.2   Updating a map

To update a map:

–   Select a map in the map navigation tree.

1.   Click ✎ to enter edit mode.
–   The map editing toolbar appears
2.   Right-click a map node and select **Edit map** from the context menu
–   A dialog box appears.
3.   Fill in the empty entry fields.
–   **Image file:** Click **...** to upload a different image file from your computer, if desired. Select the desired map image file and click **Open**.
–   **Name**: Change the name of the map, if desired.
–   **Description**: The system assumes the description of the previously uploaded file by default. Change the description if desired.
–   (Only if Divisions are licensed and in operation)
        Division: Select a new division for the map, if desired.
4.   Click **OK.**
–   The dialog box closes.
–   The new map image replaces the previously selected map.

6.3   Deleting a map

To delete a map from the map tree:

1.   Click ✎ to enter edit mode.
–   The map editing toolbar appears
2.   Select a map from the map navigation tree.

3.   Click 🗑 to delete the selected map.
–   A new dialog appears asking for your confirmation.
4.   Click **OK** to confirm that you want to remove the map.
–   The map has been deleted.

---

i   **Notice!**
          All links that have been added to the map will be deleted along with it.

6.4   Exporting a map

To export a map from the map tree:

1. Click ✎ to enter edit mode.
– The map editing toolbar appears
2. Select a map from the map navigation tree.

3. Click 🖼 to export the selected map.
– The **Save As** dialog box appears.
4. Select the location to which you want to save the map.
5. Click **Save** to save the map in the chosen location.
– The map has been exported.

> **ⓘ**
>
> **Notice!**
> Editing and uploading an exported map again
> It is possible to edit an exported map outside AMS and upload it again into the map tree.
> (Right-click the map in the map tree, select **Edit map** and locate the edited file for upload from the file system.)
> If you use the same scale for the upload, the device icons previously placed on the map will reappear in the same positions. If you use a different scale, then the positions of icons will need to be adjusted manually.

6.5 Setting a map as your home map

Introduction
The home map is that map that is displayed first, when you log on.

Procedure

1. Click ✎ to enter edit mode.
– The map editing toolbar appears
2. Select a map in the map navigation tree.

3. Click 🏠 in the map editing toolbar to set a map as your home map
– A dialog box appears informing you that the selected map has been set as your home map.
4. Click **OK** to close the dialog box.

6.6 Adding devices to the map

You can add any type of device to a map in the map display area.
Devices are grouped as follows: DMS Servers, MAC Servers, AC Controllers, Entrance (including Doors and Readers)
Each device can only appear once on the same map.

Add a device to the map as follows:

1. Click ✎ to enter edit mode.

2. Click ⛶ to open the device browser

3. Locate the desired device in the device browser.

– Note that if Divisions are licensed and in operation, you will see only the devices for which you are authorized.

4. Drag the device and place it on the desired area of the map in the map display area.

5. Release the mouse button.

– The icon appears on the map.

Notice!

If someone may have configured devices in the AMS dialog manager during your Map view session, click reload ↻ to ensure that any changes are propagated immediately to Map view.

Changing the properties of a device

Change the properties of a device as follows:

1. Click a device in the map display area.

– A properties dialog box appears below the device tree.

2. Change the properties as desired. Note that the number and types of editable properties depends on the type of the device selected.

Device properties table

Property	Function
Name	Change the name of the device.
Show name	Select the check box to display the name of the device on the map. Clear the check box to hide the name of the device on the map.
Icon size	The icons appear in size **Medium** by default. 1. Change the size of the icon on the map. 2. Click **Medium**. – A drop-down list appears. 3. Select one of the sizes: **Small**, **Medium**, **Large**. – The size of the icon changes on the map.
Position	Drag and drop the device on the map to change its position.
Angle	Change the display angle of a device icon as it appears on the map. – Click the spin-box arrows to change the degree of the angle, or – Type the angle directly into the numeric field. The angle increases clockwise from 0 (vertical), or – Click the icon and rotate the wheel button, if available.
Icon	(Not available for all devices)

Property	Function
	Select an icon to appear on the map to represent this device. In the case of DIP/DOP devices a wide choice of icons is offered
Color Background color	Change the color of the device icon on the map. In the case of DIP/DOP devices different colors can be selected for ON (set) and OFF (not set) states

6.7   Arranging the map tree

Moving or creating subnodes within the map tree

There are two different ways of creating subnodes in the map tree:

Option 1 - Turn an already existing map into a subnode.
1. Select a node in the map tree.
2. Drag the node and place it over another node in the map tree.
3. Release the mouse button.
– The released node appears as a subnode in the map tree.

Option 2 - Upload a new map into an existing map node.
Before uploading a map image to the AMS - Map View application, make sure that the image file fulfills the following requirements:

Minimum technical requirements to add a map image file	
Supported image file format	*.bmp, *.jpg, *.png
Maximum supported map dimension	2000 x 2000

To upload a new map into an existing map node:
1. In the map tree, right-click the map node to which you want to add a sub node.
2. Click **Add scene...**
– A dialog box appears.
3. Fill in the empty entry fields:
– Image file: Click **...** to upload an image file from your computer. Select the desired map image in the **Save As** dialog box, and click **Open**.
– Name: The system assumes the name of the uploaded file by default. Change the name if desired
– Description: Add a description if desired.
4. Click **OK**.
– The map appears as a subnode of the node that you selected initially.

Promoting a subnode
Turn a subnode into a node as follows:
1. In the map tree, select a node of your choice
2. Drag the node and place it over **All maps** in the map tree.
3. Release the mouse button.
– The released subnode appears as a node in the map tree.

6.8   Linking map scenes together

You can create and place links on map scenes that serve as hyperlinks to other scenes.
The **Links to scenes** function is positioned below the device tree.

Icon	Function
⬀	Link a map to another map.

Click **Links to scenes** to hide and show the ⬀ **Icon link** tool.:

1. Click the ⬀ **Icon link** tool.
2. Drag the Icon link tool and place it on the desired area of the map in the map display area.
3. Release the mouse button.
– The icon appears on the map.
– A properties dialog box appears at the bottom of the device tree menu.
4. Change the general properties as required. See *Device properties table, page 35*
5. Change the properties that are specific to **Icon link**

Property	Function
Referenced scene	The name of the map which will be displayed when you click the icon link in **View mode**.
Symbol	From the drop-down list, change the appearance of the symbol to reflect the link's direction of virtual movement within the hierarchy of maps.

6.9   Linking access areas to maps

Access areas are linked to maps via the **readers** of the entrances which have that area as their **destination**. Location and destination are assigned to readers in the device editor of the AMS application.

Procedure

To link a reader and its access areas to a map do the following:

1. Click the ✏ icon to enter **edit mode**
2. Drag and drop one of the reader devices onto the map of your choice.
3. (Optional) Change the properties of the icon in the popup window, if desired.
4. Repeat the steps above, if desired, to place icons of the same reader on multiple maps in the map tree.

5. Click the highlighted ✏ icon to leave **edit mode**
– The reader icons on the maps now have context menus in **view mode**.
– The destination area of the reader in the areas tree has a context menu containing the element **Go to map**. Use this to open any of the maps that contain this reader.

6.10   Linking intrusion areas to maps

In contrast to access areas you can delimit Intrusion areas as polygons on maps in Map view. Later, in view mode, you can right-click these polygons to invoke context menus for their intrusion areas. The context menu contains commands to arm and disarm (partially or totally, delayed or instantly)

Prerequisites
–   You have configured intrusion panels and areas in the AMS dialog manager. See the AMS Configuration and Operation help for details.
–   You have uploaded at least one map to Map view.

Dialog path
Map view Device tree > **Intrusion Panels**

Procedure to delimit an intrusion area on a map

1.   Click the ✏ icon to enter **edit mode**
2.   In the Map view device tree, under **Intrusion Panels**, expand a panel to see the intrusion areas that are defined on it.
3.   Drag and drop one of the intrusion areas onto a map of your choice
     –   A popup window explains how to delimit a polygon to represent an intrusion area on the map.
4.   With a series of left clicks set the perimeter of an intrusion area on the map.
5.   Complete the series with a right click:
     –   The polygon is the area now colored blue.
     –   A properties pane for the polygon appears in the Device tree.
6.   In the properties pane edit the following properties as desired, or simply accept the default values.

Property	Description
Name	(Text field) The label of the delimited area on the map
Label position	(List) Select whether the name of the area should be left-justified, right-justified or centered
Stroke thickness	(List) Select the line thickness of the perimeter of the polygon.
Opacity	(List) Select the opacity of the polygon fill-color, in percent.
NOTE	The background color cannot be selected in the properties pane. The background color is determined by the mode (edit or view mode) and arming status of the area. See *Intrusion area background colors (View mode), page 45*

7.   Click the highlighted ✏ icon to leave **edit mode**

Procedure to remove an intrusion area from a map

1.   Click the ✏ icon to enter **edit mode**
2.   In the Map view main pane, click anywhere inside the area that you want to remove:
     –   The vertices of the area appear as red squares
     –   The top right corner of the area is marked with an **X** in a gray square.

3. Click the X in the gray square
   - A confirmation popup window appears
4. In the popup window, click **OK** to confirm that you want to remove the area
   - The area is removed from the map.

5. Click the highlighted icon to leave **edit mode**

7 Interplay of Maps and Divisions

This section is only relevant if the AMS Divisions feature is licensed and in operation.

In the map tree and the map itself

Map view operators can only edit and view the scenes of the Divisions for which they are authorized.

– In **View mode**,
  – Scenes for which they are not authorized do not appear in the **All maps** tree.
  – If an operator places a device link on a map, and the device is subsequently moved to a division for which that operator is not authorized, then the orphaned link will no longer work, and will raise a popup window: **The item assigned could not be found**.
– In **Edit mode**:
  – Scenes that do not belong to authorized divisions are not displayed except by a name with a padlock icon in the maps tree.
  – Scenes that are hierarchically **below** the selected scene, and do not belong to authorized divisions, are not displayed. A warning triangle in the scene name, and a tool tip, inform the operator of subordinate scenes that they cannot edit or view.
    Note: In such cases the selected scene cannot be deleted or moved by this operator.

In the device tree

Map view operators can only view the devices of Divisions for which they are authorized.

In the alarm list and swipe ticker

Map view operators can only view events in the Alarm list and Swipe ticker for devices in Divisions for which they are authorized.
If the cardholder involved is from another division, then the event is displayed and the cardholder's data are anonymized.

Divisions of **operator**	Division of **reader**	Division of **cardholder**	Display of event in **Map view** (Alarm list or Swipe ticker)
A	A	A	All details displayed
A	A	B	Event with anonymized details of cardholder
A	B	A	Not displayed
A	B	B	Not displayed

Tab. 7.1: Access events

8   Operating maps and devices with View mode

Introduction to view mode

View mode is the mode for browsing the maps and operating their devices, as opposed to configuring them by adding, modifying and deleting. Depending on the permissions assigned to them in the AMS client (Dialog manager), operators can uses the following applications in view mode:

– Device tree

– Alarms list

– Swipe ticker

– Areas view

8.1   Using the Device tree

Introduction

The Device tree allows you to locate, monitor and operate devices. The devices in the view are grouped as follows:

DMS servers

MAC servers

Access controllers

Entrances
– Doors
– Readers

Intrusion Panels
– Panels
    – Areas

Locating the devices

1. Click   to open the Device tree.
2. Unfold the device tree to locate the desired device.
3. (Optional) Right-click the device and select **Show on map** to locate icons of a device that have been placed on a map.

8.1.1   Monitoring device states

The states of the devices are displayed in the form of a small icon that overlays the main device icon.

Icon	State
▯	Door Closed (white icon)
▯	Door Open (white icon)
⊘	Device (usually a reader) disabled (red icon)
✋	Manual Mode (orange icon)
🔓	Door unlocked ("permanent open") (red icon)

Tab. 8.2: Main icon states

Icon	State
▸▮◂	Access Sequence Monitoring ON (green icon)
📇	Whitelist activated(white icon)
🛡	Intrusion area armed

Tab. 8.3: Top left states

Icon	State
⚡	Battery power failure (red icon)
⚡	CMOS Battery insufficient (red icon)
⚡	DC power failure (red icon)
⚡	Power failure (red icon)
⚡	Battery of reader alarm (red icon)
▭	Battery level of reader (red icon)
🛡	Threat level activated

Tab. 8.4: Top right states

Icon	State
🔑	Mac Switch Master (yellow icon)
🔑	Mac Switch Slave (grey icon)
🔫	Tamper alarm (red icon)

Tab. 8.5: Bottom left states

Icon	State
⚠️	Connection Down (yellow icon)

Tab. 8.6: Bottom right states

8.1.2   Controlling devices via context menus

1. To operate a device, right-click its icon on the map or in the Device tree.
2. A context menu appears. The contents of the menu vary depending on the type of device, its current state, and the operator's permissions.
    If the command cannot be carried out on the device in its current state, then the menu item is grayed out.
    If the command cannot be carried out by the operator for lack of permissions, then the menu item is hidden.
3. Click the desired command to execute it.

The following tables list the main commands for the device types.

MAC commands

Command	Description
Cold start MAC	This command deletes all locally stored data and restarts the device. On startup, a configuration is requested from the parent device again.
Warm start MAC	This command restarts the device, but keeps the locally stored data.
Synchronize MAC	Starts a synchronization of all the MAC database tables with the DMS.
Switch MAC	This command switches between primary and secondary MAC. The active MAC has the state "Master". The standby MAC has the state "Slave".
Enable Access Sequence Monitoring	This Access Sequence Monitoring check can be enabled for a controller or globally switched off on the MAC level. The check can only be performed if it is enabled on MAC and on AMC level.
Disable Access Sequence Monitoring	This command disables the Access Sequence Monitoring check.

Tab. 8.7: MAC commands

AMC commands

Command	Description
Cold start controller	This command deletes all locally stored data and restarts the device. On startup, the configuration is reloaded from the parent device.

Command	Description
Warm start controller	This command restarts the device, but keeps the locally stored data.

Tab. 8.8: AMC commands

Door or entrance commands

Command	Description
Enable Manual Mode	The door taken out of AMS control (no reporting of events and no execution of commands).
Disable Manual Mode	The door is put back under AMS control, and locked for normal mode.
Note that in the following commands the inbound/outbound distinction applies only to directional entrances such as turnstiles.	
Grant access inbound normal	Cycle a door from locked to unlocked and back to locked state.
Grant access inbound extended	Slow-cycle a door from locked to unlocked and back to locked state. The signal is longer than normal, to allow more time for persons with disabilities.
Grant access outbound normal	Cycle a door from locked to unlocked and back to locked state.
Grant access outbound extended	Slow-cycle a door from locked to unlocked and back to locked state. The signal is longer than normal, to allow more time for persons with disabilities.
Enable Permanent Open	Unlock a door for a period of uncontrolled access.
Disable Permanent Open	Lock the door for normal mode, that is, to grant access for valid credentials only.
Block door	Secure the door. Normal mode is suspended. The door can be unlocked only by special credentials or direct command from AMS.
Unblock door	Lock the door for normal mode, that is, to grant access for valid credentials only.

Tab. 8.9: Door or entrance commands

Reader commands

Command	Description
Enable Access Sequence Monitoring	This Access Sequence Monitoring check is enabled for an individual controller or globally at the MAC level. Enabling at reader level can only function if it is also enabled on both MAC and AMC levels.
Disable Access Sequence Monitoring	This command disables Access Sequence Monitoring .
Grant access normal	Cycle a door from locked to unlocked and back to locked state
Grant access extended	Slow-cycle a door from locked to unlocked and back to locked state. The signal is longer than normal, to allow more time for persons with disabilities.
Enable Manual Mode	The reader taken out of AMS control (no event logging and no execution of commands).
Disable Manual Mode	The reader is put back under AMS control, and locked for normal mode.
Block reader	Secure the door by suspending normal mode. The reader will respond only to special credentials or direct command from the main system.
Unblock reader	Change the door to locked state and normal mode, where the reader will grant access for valid credentials only

Tab. 8.10: Reader commands

Intrusion functionality

Intrusion areas that are delimited on maps have different background colors depending on the state of the area.

Note that in **Edit mode** all intrusion areas have a blue background color.

Intrusion area background colors (View mode)

Color	Description
Blue	Not ready to arm. Disarmed
Green	Ready to arm. Disarmed
Yellow	Armed.
Red	An alarm has been triggered for this area.
Light gray	State unknown.

Tab. 8.11: Intrusion area background colors (View mode)

Intrusion area commands

Command	Description
Activate area alarm bell	Sound the alarm bell for the selected intrusion area.
Silence area alarm bell	Silence the alarm bell for the selected intrusion area.
All On Delay	Allow the personnel time to exit, then arm all points in the intrusion area.
All On Instant	Arm all points in the intrusion area immediately.
Part On Delay	Allow the personnel time to exit, then arm only the perimeter points in the selected intrusion area. Partial arming leaves the personnel free to move within the area without triggering an alarm.
Part On Instant	Arm only the perimeter points in the selected intrusion area immediately. Partial arming leaves the personnel free to move within the area without triggering an alarm.
Disarm area	Disarm all points in the intrusion area immediately.
Reset sensors in area	Arm all the points in the intrusion area, then disarm them all immediately.
Show in device tree	Highlight the selected area in the Map view device tree.

Tab. 8.12: Intrusion area commands

Intrusion panel commands

Command	Description
Show in device tree	Highlight the selected panel in the Map view device tree.

Tab. 8.13: Intrusion panel commands

Intrusion point commands

Command	Description
Bypass point	Ignore alarms from this point until the bypass is removed.
Un-Bypass point	Stop ignoring alarms from this point. Remove the bypass.

Tab. 8.14: Intrusion point commands

Digital input/output (DIP/DOP) commands

Command	Description
Set digital output	Sets the digital output on the AMC to 1
Clear digital output	Sets the digital output on the AMC to 0

Command	Description
Show on map	Highlights the device on the map that you select from a drop-down list.

Tab. 8.15: Digital input/output (DIP/DOP) commands

Simons Voss Reader commands

Command	Description
Activate Whitelist	Activates the whitelist feature
Deactivate Whitelist	Deactivates the whitelist feature
Delete Whitelist	Deletes all entries from the whitelist
Synchronize Whitelist	Synchronizes entries of the whitelist with the MAC

Tab. 8.16: Simons Voss Reader commands

8.2   Using the Alarm list

The **Alarm list** view displays system events that require attention by operators. It has the following applications:

Application	Purpose
	Displays unhandled alarms
	Opens the alarms audit trail for browsing through past events
	Opens the alarm categories tool for setting the relative urgency of system events, that is, deciding which should be treated as alarms, and if so, with what priority:

When operators start Map view they are asked whether they wish to view immediately the unhandled alarms produced since the last start of Map view.

Prerequisites

Permissions can be assigned separately for all alarm categories.
In order to use this feature, the operator requires permissions for at least one alarm category under **Access Manager Maps** in their operator profile. Categorizing alarms requires its own permission.
Contact your system administrator, or consult the AMS Configuration and Operation help, section **Creating user (operator) profiles**

Refer to
– *Prerequisites, page 24*

8.2.1   Operating the Unhandled alarms list

This dialog is opened automatically when Map view is started, and unhandled alarms exist. Unhandled alarms are events that have occurred while no Map view was open, or which no Map view operator has yet handled.

If you are starting Map view,

▶   Select **Show unhandled alarms** after entering your operator name and password.

If Map view is already running,

1.   Click ⚠ to open the alarm list

2.   Click 🕐 to display the unhandled alarms.

Handling alarms

To handle an alarm in Map view means to Accept (acknowledge) it, to take appropriate action if necessary, and then to delete it from the list when finished.

–   For multiple selection use the usual Windows key combinations:
     Ctrl-a to select all,
     Shift-click for contiguous selection,
     Ctrl-click for discrete selection and deselection

Prerequisite: The alarm list is open.

1.   Select the alarm or alarms that you wish to handle.
      The alarm is highlighted in the list
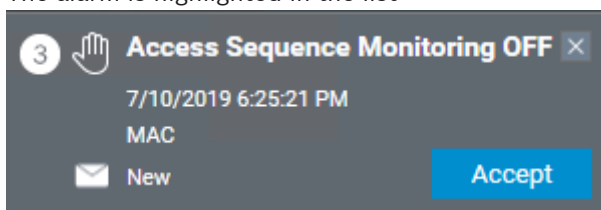
If the alarm originates from a device which is linked to a map, then the map view switches to the corresponding map and flashes the device icon. The device icon is overlayed with a warning triangle and an envelope, which is open or closed depending on whether an operator has accepted the alarm.

Conversely, if you click a device icon marked with a warning triangle on the map, the corresponding alarm is highlighted in the alarm list.

2.   To delete the alarm, click the **x** button in the top-right corner.
      The alarm disappears from the list
      Although an alarm disappears from the alarm list, all actions are protocolled in the main AMS system, and in the Map view alarm change log.

3.   To begin handling the alarm, click **Accept**
      The **Accept** button changes to **Done**
      The alarm is now your responsibility. Other Map view operators in the system will no longer see it in their Map views.

4.   Take appropriate action to respond to the alarm

5.   When your actions are complete, click **Done**
      The alarm disappears from the list
      Although an alarm disappears from the alarm list, all actions are protocolled in the main AMS system, and in the Map view alarm change log.

8.2.2   Using the alarm audit trail dialog

The alarm audit trail contains the history of the handling of alarms by operators.

Procedure

1. Click ⚠ to open the alarm list

2. Click 📄 to display the alarm Change Log

3. Use the entry fields to restrict the list of alarms to those that interest you, then click **Apply**
    Range of **dates**:
    Range of **times**: From the list, select whether the beginning and end times apply to each day in the range of dates, or to the first and last day respectively.
    Operator: the name of the operator who performed the action
    Category: the category of the alarm

4. Click **OK** to close the window when finished.

8.2.3   Categorizing alarms

Alarms can be sorted into categories depending on their degree of urgency at your site. Categorizing the alarms changes the way they are prioritized in the alarm list.
The default categories from most to least urgent are:

1. Duress

2. Critical

3. Warning

4. Maintenance

–   (no alarm)

To change categories from their default values, proceed as follows:

1. Click ⚠ to open the alarm list

2. Click ⚙ to display the alarm categories.
    Each event type is displayed alongside a drop-down list containing its current category.

3. Select the event type that you wish to modify and then select a different category from its drop-down list.

4. Repeat for as many event types as required

5. Click **OK** to save the assignments of category, or **Cancel** to abort without saving changes.

8.3   Triggering and cancelling a threat alert via UI command

This section describes how to trigger a threat alert in AMS Map View.

Dialog path

–   AMS Map view >   (Device tree)

Prerequisites
–   At least one threat level has been defined
–   At least one threat level has been marked with Active in the device editor.
–   You as a Map View and AMS operator have the necessary permissions:
    –   to operate Threat levels
    –   to view the MAC or MACs in the Division where the threat alert is to be triggered.

Procedure to trigger a threat alert
1.   In the device tree in AMS Map view, right click the MAC device where the threat alert is to be triggered.
    –   A context menu appears, containing the commands that you are authorized to execute on that MAC
    –   If no threat level is yet in operation, the menu will include one or more items labeled **Activate Threat level** '*<name>*', where is the name of the threat level defined in the device editor.
2.   Select the threat level that you wish to trigger.
    –   The threat level goes into operation.

Procedure to cancel a threat alert
Prerequisite: A threat level is already in operation.
1.   In the device tree in AMS Map view, right click the MAC device where the threat alert is to be cancelled.
    –   A context menu appears, containing the commands that you are authorized to execute on that MAC
2.   Select **Deactivate Threat level**. From the context menu.
    –   The currently threat level is deactivated.

8.4   Operating Swipe ticker

Introduction
Swipe ticker is a tool that helps Map view operators to monitor, in real time, who is entering or leaving the premises.

Overview
Swipe ticker is an application, within AMS Map view, that displays the last 10 minutes of access events in a dynamic scrolling list. Up to 50 access events are displayed, and events older than 10 minutes are automatically dropped from the list. The operator can monitor all readers in the system, or select a subset.
Each record in the list contains details of the event and the credential used, for example:
–   The name of the cardholder and their stored photo, for visual confirmation of identity.
–   A time stamp.
–   Company and/or department name, if stored.

- – The entrance and the reader at which the credential was used
- – An event category with a colored label:
  - – Green: A completed access with a valid credential
  - – Yellow: An incomplete access with a valid credential, for example, the cardholder cycled the lock but did not open the door
  - – Red: A failed attempt to access with an invalid credential. The type of invalidity is shown, for example, the credential is blacklisted, unknown or expired

Swipe ticker does not keep its own archives, it extracts and displays access events from the system database. The dynamic scrolling can be paused for closer study, or opened in a separate window for parallel use with other Map view applications.

|	
i	**Notice!** Latency after edits Changes to ID photos in AMS typically need a few minutes to propagate to the Swipe ticker.

Prerequisites

The User profile of the operator requires a special authorization to run Swipe ticker.
1. In the main AMS application, navigate to the menu: **Configuration** > **User profiles**
2. Load the profile name of the desired operator
3. In the table, select **Access Manager Maps** > **Special functions** > Swipe ticker

Starting Swipe ticker

▸ In Map view, click [icon] to start the tool.

Selecting readers to monitor

If readers have not already been selected, or if you wish to change the selection, proceed as follows:

1. In the Swipe ticker window, click [icon] (settings).
   The **Filter devices** window opens.
2. From the tree of devices, select the check boxes of the entrances or readers that you wish to monitor. The check boxes behave as follows:
   If you select an entrance, then all its subordinate devices will be selected by default.
   The check boxes of individual subordinate devices can then be cleared if not required.
   If **all** children of a parent device are selected, then the parent's check box is white. If only **some** are selected, then the parent's check box is gray.
3. Click **OK** to finish selecting readers and close the **Filter devices** window.

Displaying selected readers on the map

▸ Double-click a record in the Swipe ticker.
✓ The swipe ticker is automatically paused.
✓ Map view displays, in the main window, the first relevant map scene in its map hierarchy, and highlights the reader that you double-clicked.

Pausing the Swipe ticker

▸ In the Swipe ticker window, click ⏸ , or double-click a record in the list, to pause the dynamic display
✓ The dynamic display freezes. Incoming event records are buffered but not displayed.
✓ A notice is placed at the top of the list, that the event stream has been paused.

Resuming a paused Swipe ticker

▸ In the Swipe ticker window, click ▷ to resume the dynamic display
✓ The dynamic list displays in chronological order (newest first) all access events that have occurred at the selected readers in the last 10 minutes, up to a maximum of 50.
✓ Access events that are older than the 50 newest, or older than 10 minutes, are removed from the list.
✓ New access events are again displayed in real time as they occur.

Duplicating Swipe ticker in a separate window
Note that only one duplicate ticker window can be opened at a time.

1. In the Swipe ticker window, click ⊞ (additional window).
   The separate window is a duplicate and **not** independent of the ticker in the main window. It obeys the same settings.
   Other Map view applications, such as the alarm list, can now be operated in parallel in the main window.
2. When you are finished with the separate window use the title bar to close it.

Refer to
– *Prerequisites, page 24*

8.5 Monitoring access areas

Introduction
When you have added and saved access areas in the AMS client (Dialog manager) they will be displayed in the Map view areas list.

▸ Click 🎯 to display the areas list.
A search bar is available for locating areas in large area trees.
Access areas are displayed as an indented list in a table. The table contains columns for the following.
– **Name** of the area
– **Type** of the area. This will be determined by the type of the corresponding entrance in the device editor, or else Default for normal entrances.
The next two columns are only significant if the population count feature has been activated for the entrance in the device editor:
– **Count**:The current count of persons (or vehicles in the case of parking lots) in the area.
– **Max. count**: The maximum number of persons (or vehicles) for the area.
– **State**: the current state of the area.

> **Notice!**
> Reloading to refresh the view
> If Map View was running while you making changes in the AMS client (Dialog manager), then
>
> click reload ⟲ to ensure that all changes are reflected.

8.6   Monitoring and controlling intrusion areas

Introduction

When you have added and saved the credentials of the intrusion panels in the AMS client (Dialog manager) they will be displayed in the Map view areas list. Here you can monitor the status of the intrusion areas and send commands to them.

8.6.1   Monitoring intrusion areas

Procedure

1.   Click ⊕ to display the Intrusion and Access areas tables.
2.   (Optional) Use the search bar, if necessary, to locate the areas of interest in large area tables.
–   Intrusion areas are displayed in a table. The table contains columns for the following:
      –   **Name:** Name of the intrusion area
      –   **Panel:** Name of the intrusion panel to which the area belongs
      –   **State:** The current state of the intrusion area
      –   A button for a default command
      –   An ellipsis [...] button for a context menu of commands

8.6.2   Controlling intrusion areas

Procedure

1. Click ⊕👁 to display the Intrusion and Access areas tables.
2. (Optional) Use the search bar, if necessary, to locate the areas of interest in large area tables.
– Intrusion areas are displayed in a table. The table contains columns for area **Name**, **Panel** and current **State**, plus the following command buttons:

    – A button, such as **Disarm area** for the default command in the context of the current state.
    – An ellipsis [**...**] button that invokes a context menu containing all the applicable commands for the area.

3. Click the button to give the default command.
   Alternatively, make a single or multiple selection and right-click the ellipsis button to select a command from the context menu. Note that with multiple selections the context menu contains only those commands that are executable for all devices in the selection.
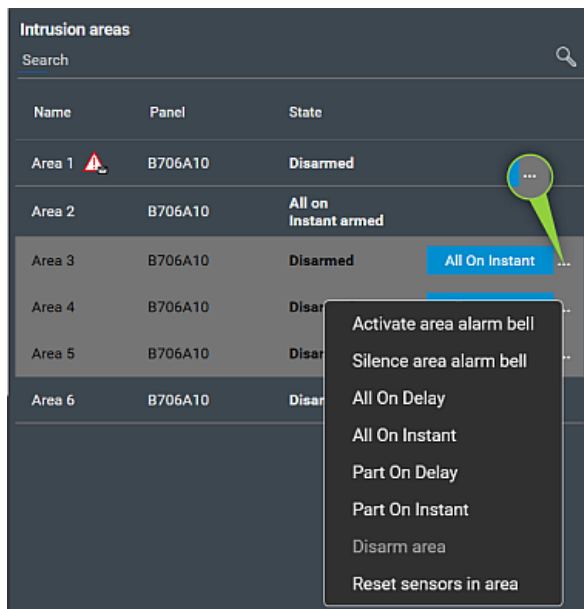
Note

In View mode you can invoke the same context menu by right clicking the area in a map. To locate the area on a map, click the ellipsis button in the Intrusion areas table, and select **Show on map** from the context menu.

Glossary

Access Sequence Monitoring

The tracking of a person or vehicle from one defined Area to another by recording each scan of the ID card, and granting access only from Areas where the card has already been scanned.

Area (Access control)

In access control systems an Area is the virtual space into which a cardholder passes when they successfully use a reader which has that Area defined as its destination.

Area (Intrusion)

In intrusion detection systems an Area is the set of those points (i.e. intrusion sensors) that can detect an intrusion into a particular physical area.

Cold start MAC

The MAC performs the following steps: 1) Stop services 2) Delete own database 3) Clear own data buffers 4) Restart services 5) Rebuild own database 6) Request all data tables from the DMS, 7) Refill all data tables with DMS data, 8) Overwrite all data tables of its subordinate AMCs.

Data Management System (DMS)

A top-level process for managing access control data in the system. The DMS supplies data to main access controllers (MAC), which in turn supply data to local access controllers (usually AMC).

DMS server

Hardware: A computer that hosts the Data Management System (DMS) of the access control system.

Entrance

The term Entrance denotes in its entirety the access control mechanism at an entry point: It includes the readers, some form of lockable barrier and an access procedure as defined by sequences of electronic signals passed between the hardware elements.

Local Access Controller (LAC)

A hardware device that sends access commands to peripheral access control hardware, such as readers and locks, and processes requests from

that hardware for the overall access control system. The most common LAC is an Access Modular Controller or AMC.

MAC (Main Access Controller)

In access control systems a server program that coordinates and controls the Local Access Controllers, usually AMCs (Access Modular Controller)

manual mode

the mode of a door that is cut off from the access control system, and can only be locked and unlocked by a key or similar physical means

Point

A sensor to detect intrusion into an intrusion-controlled area. In some contexts points may be called zones or sensors.

Warm start MAC

The MAC performs the following steps: 1) Request all data tables from the DMS, 2) Refill all data tables with DMS data, 3) Send all data to its subordinate AMCs.