AMCIPConfig tool

en Operation Manual

Table of contents

1 Introduction

The **AMC IP Configuration tool** *Bosch.AMCIPConfig.exe* is an auxiliary program for configuring the credentials and network parameters of local access controllers, such as the Bosch AMC2 controller series.
After their network parameters have been configured, these access controllers can be used by Bosch access control software, such as the **BIS Access Engine (ACE)** or the **Access Management System (AMS)**.

Intended Audience
Persons who install, configure or administer the networks of access control systems that use Bosch local access controllers.

2 Getting started

This section contains a brief overview of the tool and its main functions.

2.1 Prerequisites

One of the following is installed on your system

- The Access Engine (ACE) of the Bosch Building Integration System (BIS) version 4.9 or later.
- Bosch Access Management System version 3.0.1 or later

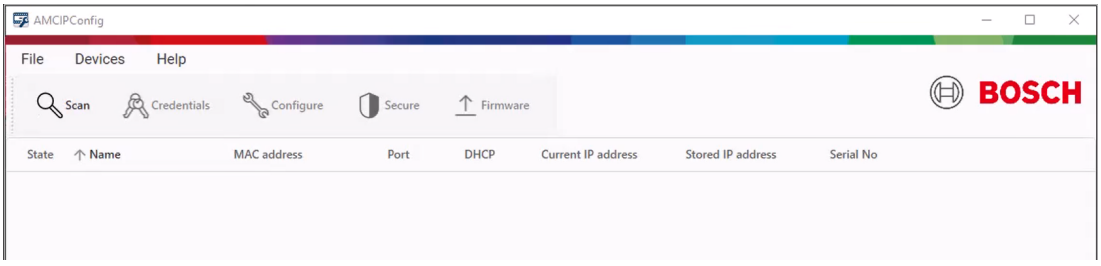
2.2 Starting the tool

Start the executable of the AMC IP Configuration tool *Bosch.AMCIPConfig.exe* from one of the following locations:

BIS ACE

- In the file system under *<Installation drive>:\MgtS\AccessEngine\AC\Bin\Bosch.AMCIPConfig.exe*
- In the BIS Configuration Browser under **Tools** > **ACE Configuration AMC IP addresses** > Button: **Configuration AMC IP addresses**

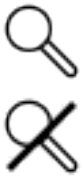
2.3 Main functions of the tool



The AMC IP Configuration tool scans the network for local access controllers. The devices that it finds it lists in the main window of the tool along with the following properties:

- **State** - an icon showing the current state of the device
- **Name** - the name that the operators have assigned to the device
- **MAC address** - the media access control address of the device
- **Port** - the network port that the device is using
- **DHCP** - whether the IP address of the device is assigned by Dynamic Host Configuration Protocol
- **Current IP address** - the IP address currently assigned by DHCP
- **Stored IP address** - the IP address that the operators have stored on the device
- **Serial Number** - the serial number of the device

The user selects one or more devices from the list, and can control and configure them using the following functions:

Function	Name	Description
	**Scan**	Scans or aborts the scan of controllers on the network.

	**Credentials**	Sets credentials (for example, passwords) for the AMCIPConfig application, to permit it to modify the controllers. Single or multiple selection is possible.
	**Configure**	Sets the IP network parameters and other properties listed above. Only single selection is possible.
	**Secure**	Sets credentials on the controller devices themselves. Single or multiple selection is possible.
	**Firmware**	Updates the firmware of selected controller or controllers.

3 Scanning and configuring AMC devices

General procedure to configure AMC devices on the network:

1. Scan the network for AMC devices
2. Select the device or devices that you wish to configure
3. Apply the tool's functions to the selection.

The following sections describe these steps in more detail.

3.1 Scan: Discovering AMC devices on the network

1. Click the **Scan** button 

   The network scan begins, and the button label changes to **Abort Scan** 
2. Wait for the devices found to appear in the program's main window, or click **Abort Scan** to stop the search.

   Zero or more AMCs are discovered on the network and presented in a list in the tool's main window, with columns for the following attributes:

- **State** - an icon showing the current state of the device
- **Name** - the name that the operators have assigned to the device
- **MAC address** - the media access control address of the device
- **Port** - the network port that the device is using
- **DHCP** - whether the IP address of the device is assigned by Dynamic Host Configuration Protocol
- **Current IP address** - the IP address currently assigned by DHCP
- **Stored IP address** - the IP address that the operators have stored on the device
- **Serial Number** - the serial number of the device

Reading the states of discovered devices

State	Description
	The device is on the network without a password.
	The device has a credential and the IPConfig tool has stored it.
	The device has a credential and the IPConfig tool has **not** stored it. In this case, a popup window will prompt you for a credential for the device when you try to change its configuration.
	The configuration of the device has changed. Scan the devices again to update the information in the list of discovered devices.

Limiting the scan time

To set a timeout for the scanning process:

1. From the **File** menu select **Options**
2. In the **Options** popup window, enter a number of seconds under **Device scan timeout (s)**:

Logging of AMC network communication

To enable logging:

1. From the **File** menu select **Options**

2. In the **Options** popup window, select the **Enable logging** check box.

To access AMC communication logs:

1. From the **File** menu select **Options**
2. In the **Options** popup window, click **Open folder**.

Notice!

Discovering devices on the network

The tool only finds devices on the subnet where it is running. If the scan results do not include the device you require, try running the tool in the subnet of the devices, or use the Windows *arp* command to associate an IP address with physical Ethernet (MAC) address of the device.

arp –s <IP address> <physical Ethernet (MAC) address>

3.2 Selecting devices

To select one or multiple devices from the list of discovered devices:

- **Single selection**: Click the device in the list.
- **Discrete multiple selection**: Hold the Ctrl key and click two or more devices anywhere in the list.
- **Contiguous multiple selection**: Click any device in the list, then hold the Shift key and click another device in the list.
  The two devices and all intervening devices are selected.

Creating an inventory of selected devices.

When you have made a selection, press Ctrl -C to copy the selected lines to the Windows paste buffer. You can then paste the lines into a text editor, and save them as a .CSV file, where the data are separated by tab characters. The .CSV file can easily be imported into a spreadsheet program for further processing.

3.3 Credentials: Storing credentials for use by the tool

About Credentials

The **Credentials** function in the tool stores credentials only for the duration of the current session. For security reasons, the tool forgets all credentials when you close it.
Credentials can currently be only passwords, but future versions may provide alternative means of authentication.

Disambiguation

The **Credentials** menu stores device credentials temporarily, for use by the IPConfig tool in the current session.
The **Secure** menu sets persistent credentials on the devices directly.

Procedure

1. Select one or more devices and click **Credentials** 
   A popup window lists the selected devices. It indicates in each case whether a credential is available, that is, stored in the tool.
2. Setting and changing credentials:
   Changes will apply to all the selected devices. The possibilities that the tool offers depend on whether the tool has stored credentials for the selected devices:

If the tool has no stored credentials for the selected device or devices	
You wish to store the credential for the selected device or devices.	Click **Provide credential** enter the credential and confirm it in the popup window.

If the tool has stored credentials for the selected device or devices	
You wish to force users of the tool within this session to enter credentials whenever they configure the selected devices:	Click **Forget credential**

3.4 Configure: Setting network parameters on AMC devices

1. Select only one device from the list, and click **Configure** 
   A popup window appears for editing the device's network parameters.
2. If the device requires a credential for editing, enter the credential in the popup window.
3. Edit the following device parameters as required for the correct functioning of the device in your network:

Field	Description
Name	Enter the name of the device as it should appear in the network
DHCP	Select the check box to enable DHCP.
Static IP address	If not using DHCP, enter the static IP address here.
Use gateway	Select the check box to enable use of a network gateway.
– **Default gateway** – **Subnet mask**	If using a gateway, enter the address of the default gateway, and a subnet mask.
Port	Enter a port number for the device. The default is *10001*

3.5 Secure: Setting credentials on the devices

Disambiguation

The **Credentials** menu stores device credentials temporarily, for use by the IPConfig tool in the current session.

The **Secure** menu sets persistent credentials on the devices directly.

Procedure

1. Select one or more devices and click **Secure** 
   A popup window appears, listing the selected devices. It indicates in each case whether the device has a credential, and whether there is a pending credential change that needs to be saved.
2. Changing and resetting credentials:
   Changes will apply to all the selected devices.

You wish to change credentials that are already assigned to the selected devices:	Click **Change credential** enter a credential and confirm it in the popup window.
You wish to delete the credentials from the selected devices.	Click **Reset credential**

3.6 Firmware: Upgrading AMC firmware

Precautions before upgrading

Before you upgrade the bootloader or firmware of an AMC device, temporarily disconnect it from the ACE system.as follows:

1. In the BIS Configuration Browser go to the **Connections** menu
2. In the **Connection servers** tree, select the **AccessEngine** node under your connection server
3. In the **Device data** tree, select the AMC device whose firmware you wish to upgrade.
4. On the first tab in the device editor pane, clear the check box **Communication to host enabled**.
5. Click the **Apply** button to save this change

Notice!

Ensure reliable connections to power and network

Ensure that the device's power supply and network are reliably connected, as an interruption to either during the upgrade process can put the device in an inconsistent and unusable state.

Procedure

1. Select one or more devices and click  **Firmware**.
2. Read and acknowledge the warning about disconnecting the AMC device from the system before upgrading its firmware. See the previous section **Precautions before upgrading AMC firmware**.
3. Click **Next** to continue
   A popup window appears for upgrading the device's firmware. For each device it shows the following details:

– **Name**: the name of the device as seen on the network
– One of the following:
  – **Current bootloader**: The version of the currently installed bootloader .
  – **Current application**: the firmware version that is currently installed on the device.
– **Upgrade to version**: The version number of the bootloader or firmware to which you can upgrade the device.

4. If you have a file containing an upgraded version of the firmware, click **Select Firmware** and locate the file in the file system, using the popup file explorer.
   – If no upgrade is available or required, click **Back** or **Cancel** to return to the tool's main screen.
5. Click **Next** to proceed with the upgrade
   A popup window monitors the upgrade process, including verification.

6. Allow the firmware upgrade and its verification to complete before proceeding to other tasks. The message **Upgrade successful** should appear for each device.
   – If a failure message appears, click **Back** once and repeat the upgrade procedure from the previous screen.
7. Click **Close** to close the popup window.
8. On the main screen of the IPConfig tool the state icons of the modified devices will have a yellow warning triangle  . Scan again to refresh the data in the device list.
9. Remember to reconnect the upgraded devices in the BIS Configuration Browser **Connections** menu, by re-selecting the check box **Communication to host enabled**.

Glossary

Credential

any means of authenticating the identity and thereby the access rights of a person or a computer. Credentials can be physical, biometric or intellectual, for example an ID card, a fingerprint or a password respectively.

LAC bootloader

The BIOS (Basic I/O System) of a Local Access Controller (LAC).

LAC firmware

application running on a LAC (Local Access Controller), to provide access control funtionality.

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

202105142245