BioConfig tool

en Operation Manual

Table of contents

1 Introduction

BioIPConfig.exe is an auxiliary program for configuring the network parameters of biometric access control devices, such as the ADR-FBBEW2 series.
After their network parameters have been configured, these access control devices can be used by Bosch access control software, such as the **BIS Access Engine** or the **Access Professional Edition**.
The BioIPConfig tool scans the network for biometric access control devices. The devices that it finds are then listed in the main window of the tool. The user selects devices from the list, and can control and configure them in the following ways:

- Setting IP network parameters
- Upgrading device firmware
- Performing diagnostic functions

2 Getting started

The executable program can be started from the following locations:

BIS ACE

– In the file system under *<Installation drive>:\MgtS\AccessEngine\AC\Bin\BioConfig.exe*
– In the BIS Configuration Browser under **Tools** > **ACE Configuration of fingerprint readers** > Button: **Configuration of fingerprint readers**

AMS

– In the file system under *\Program Files (x86)\Bosch Sicherheitssystems\Access Management System\AccessEngine\AC\Bin\BioConfig.exe*
– In the AMS dialog manager under **Main menu > Configuration > Tools** > **ACE Configuration of fingerprint readers** > Button: **Configuration of fingerprint readers**

The list of devices discovered on the network

The biometric devices found are listed with the following status icons:

Icon	State	Additional information
	Fingerprint reader detected.	Fingerprint reader detected.
	Device connected to a different software/host.	Fingerprint reader detected and connected to a different software/host.
	Device password protected.	Fingerprint reader detected with password protection.
	Device password protected.	User has entered the wrong password.
	SSL enabled and device connectable.	Fingerprint reader detected with SSL.

3 Configuring fingerprint readers

The configuration of biometric devices is performed in two steps

– Scanning the network for fingerprint readers
– Selecting each device that you wish to configure and setting its network parameters

Optionally the tool may be used for updating the firmware and running diagnostics on the devices.

3.1 Scanning the network for fingerprint readers

1. Click the **Scan fingerprint readers** button
   Effect: the network scan begins, and the button label changes to **Abort Scan**
2. Wait for the devices found to appear be listed in the program's main window, or click **Abort Scan** to stop the search.

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

– Network name
– MAC address
– Stored IP address
– DHCP status (yes | no)
– Model name
– Serial number
– OSDP address

Notice!

Discovering devices on the network

The **AccessIPConfig** 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 Setting network parameters on fingerprint readers

1. After scanning for devices, select the row of the device that you wish to modify, and click the **Set IP...** button.
   Result: A popup window appears for editing the device's network parameters.
2. Edit the following device parameters as required for the correct functioning of the device in your network:

Field	Description
Network name	Enter the name of the device as it should appear in the network
Serial number	(read-only field) The serial number of the device.
MAC address	(read-only field) The hardware address of the device.
Model name	(read-only field) The name of the reader model
Radio buttons: Either	Choose whether to use DHCP or static IP addresses,

Field	Description
– **Obtain address via DHCP** – **Static IP address**	
Stored IP address	If you chose **Static IP address** above, enter an IP address here. If you chose the DHCP option, this field shows the address currently assigned to the reader.
Enable subnets – **Subnet mask** – **Default gateway**	Select the check box if you wish to use subnets. If so, enter the subnet mask and the default gateway also. **Note**: some firmware versions do not support communication via gateway / router.
Port	Enter a port number for the device. The default is *51211*
(Purpose of reader) – **Access reader** – **Enrollment reader**	Radio buttons. Define whether the reader is to be used to enroll cards and/or fingerprints, or whether it should be used only for access. Access readers default to the interface *OSDP* mode, but can also use *Wiegand mode* Enrolment readers use only Wiegand mode.
Card data type	Set one of: – *CSN-Code* – *BOSCH Code*
Card type:	Set one of: – *MIFARE Classic* – *MIFARE DESFire EV1*
Interface	Set one of: – *Wiegand Mode* – *OSDP*
OSDP address	If using OSDP, set an address from1 through 8
Baud rate	For OSDP only. Default is *9600*
Password / **Confirm password**	(Optional) enter a password to prevent unauthorized modification of the device's parameters. Every subsequent modification to the parameters of this device will require the operator to enter this password.
Buttons	Click **Reset** to reset the reader to factory defaults
	Click **OK** to confirm and save your settings
	Click **Cancel** to exit the settings dialog without saving

3.3 Upgrading reader firmware

Upgrading the firmware

After a successful scan for reader devices, proceed as described below:

Notice!
IMPORTANT
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.

1. In the main window of the AccessIPConfig tool, select the row of the device that you wish to modify, and click the **Upgrade** button.
2. Read and acknowledge the warning about making sure the device is not used while upgrading its firmware.
   Result: A popup window appears for upgrading the device's firmware. It shows the name of the device, the current application, and an upgraded version, if available.
3. If an upgraded version is available and required, click the **Upgrade>** button at the bottom of the popup window. If a password has been set for this device enter it when prompted.
   – If no upgrade is available or required, click the **Back>** or the **Cancel** button to return to the main tool window.
4. Allow the firmware upgrade to complete before proceeding to other tasks.

3.4 Diagnostics

The AccessIPConfig tool provides a dialog for testing the colored LEDs and the buzzers of fingerprint readers. Proceed as follows:

1. In the main window of the AccessIPConfig tool, select the reader that you wish to test.
2. Click the **Diagnostic** button.
   Result: The **Diagnostic** dialog window appears
3. In the text box **Number of tests**, enter the number of test cycles to be performed. Let this number be N.

LED test

– In the **LED test** pane, click the **Test** button
  Result: the reader's LED displays its range of colors N times and the dialog displays those colors simultaneously.

Buzzer test

– In the **Buzzer test** pane, click the **Test** button.
  Result: the reader plays its range of acoustic signals N times.

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

202105142341