BOSCH

APE 3.8

Secure Operation Concept

en English

Table of contents

1 Product

1.1 Product Information

This software provides access control for small and medium-sized companies. The installation is simple and fast. It is easy to use and enables a user with minimal training to create badges and administer access rights. Specific event logging and reporting provide an easy overview of access rights and access data. You can choose your readers and cards from the same bundle of devices that are supported by Bosch's medium to large scale BIS/ACE Access Engine systems.

The Access Modular Controller (AMC) family, including Wiegand protocol and OSDPv2 via RS485 protocol, is fully supported by the software, offering highest flexibility in system design.

The software includes card personalization, providing you with the means to create IDs, design badges and capture image with USB cameras.

1.2 Scope of Product

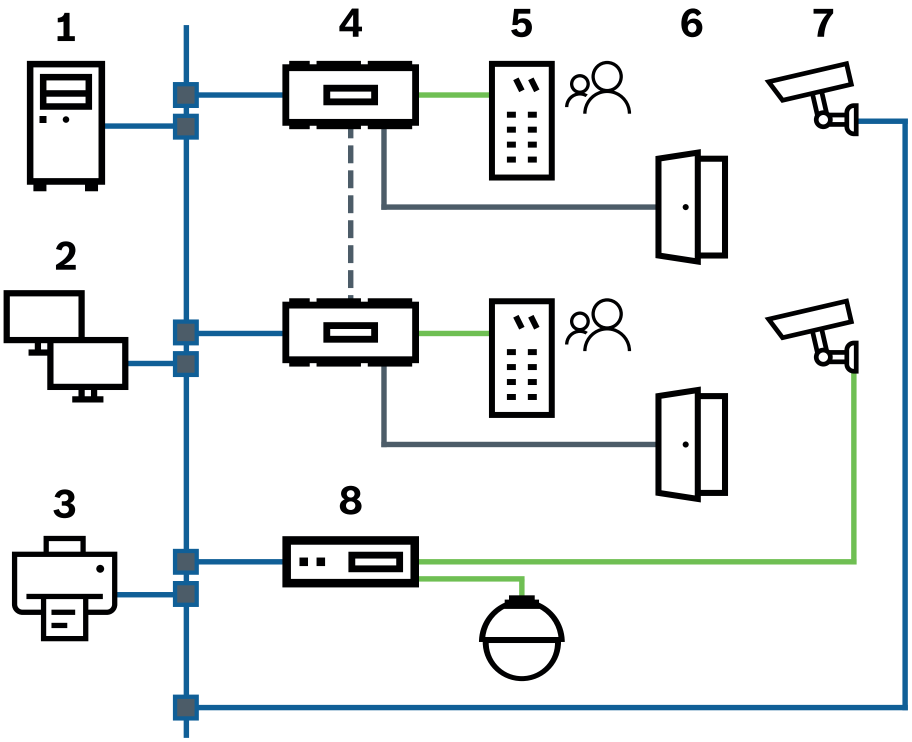


Figure 1.1: Pos. Description

1	Server with Access PE Software	2	Workstations
3	Printer	4	AMC2 - access controller
5	Reader	6	Door strikes
7	Camera	8	DVR or encoder

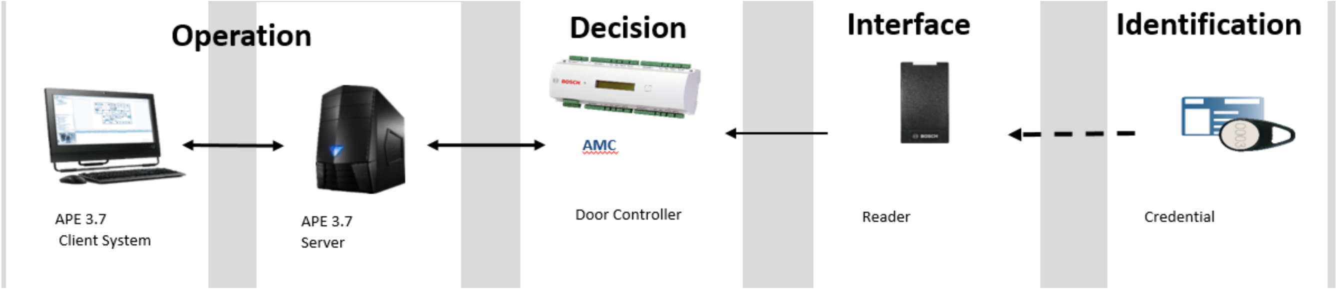


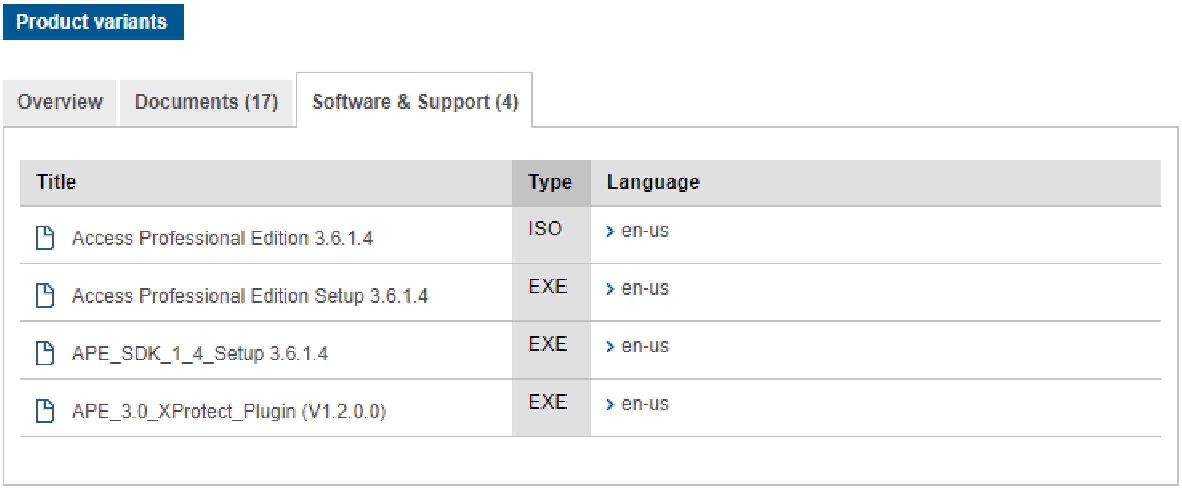
Figure 1.2: APE 3.8 scope

2 Secure Delivery

The ISO image includes the APE setup, documentation files, third-party products setups and drivers.
All executables of the APE are signed by Microsoft Authenticode by Verisign with a BOSCH specific certificate.

Notice!
APE is distributed by download from the BOSCH catalog.

In addition to the PDF documentation for installation and operation, the software executables can be downloaded directly from the catalogue.



Title	Type	Language
Access Professional Edition 3.6.1.4	ISO	› en-us
Access Professional Edition Setup 3.6.1.4	EXE	› en-us
APE_SDK_1_4_Setup 3.6.1.4	EXE	› en-us
APE_3.0_XProtect_Plugin (V1.2.0.0)	EXE	› en-us

Figure 2.1: APE 3.8 executables

3 Secure Operation

3.1 Secure Installation and Configuration

The installation of Access PE requires:

One of the following operating systems:

- Windows 2016 R2 Server
- Windows 10 X64 professional

Minimum Hardware Requirements

Both Server and Client require a Standard Windows PC with:

- 2 GHz quad core or 3 GHz dual core CPU
- At least 4 GB RAM
- 20 GB free disk space (Server)
- 1 GB free disk space (Client)
- 100 Mbit Ethernet Network Card (PCI)
- Graphical adapter with 1024x768 resolution and 32k colors
- Resolution support:
  - 1024 by 768/1280 by 1024/1920 by 1080/2560 by 1080

Restrictions for low-end hardware:

- Use fixed IP addresses.
- Disable all power saving options.
- Select a high performance power plan.
- Disable power savings within the USB settings.
- Disable Hibernate functions.
- Disable automatic Windows operating system updates.
- Apply a USB Ethernet Adapter if the Wi-Fi connection is unstable.
- Ensure that the screen resolution matches the SBC hardware requirements. For the exemplary tested device, the recommended resolution is 1920x1080.
- Ensure that there is sufficient memory available. We recommend a free memory of 5GB for installing and operating the APE software. Use an external hard disk or apply a microSD to the SBC if the internal memory is not sufficient.
- Create Windows recovery CDs and save entry points on a regular basis.

3.1.1 Access PE ports

The individual processes and applications in Access PE use the following network connections:

Connection between	Source Port/Protocol	Destination Port/Protocol
APE-Client-Application - LacSp-Service	any/TCP	43434/TCP (LACSP)
	43434/TCP (LACSP)	any/TCP
AcPers - CP (on same Host)	any/TCP	20005/TCP (CP)
	20005/TCP (CP)	any/TCP

LacSp - AMC	54545/UDP and above (LacSp)	10001/UDP (AMC)
	10001/UDP (AMC)	54545/UDP and above (LacSp)
Video verification	See VSDK Document	

3.1.2 External Firewall

On an external firewall, the allowed connections can be configured as a VPN-Connection between the used PCs or as OSI-Layer-3 definitions. One of the OSI-Layer-3 definitions has to be described as:

- Source IP, Port and Protocol (like 192.168.172.001:43434/TCP)
- Destination IP, Port and Protocol (like 192.168.192.201:any/TCP)

3.1.3 Windows Firewall

The connections in the Windows Firewall can be configured in a process-based way for the following processes:

LacSp.exe (PE LAC-Subprocess-Service)	Any connection with TCP and UDP
AcPers.exe (PE Personal-Management)	Any connection with TCP
AcConfig.exe (PE Configuration)	Any connection with TCP
AcViv.exe (PE Video-Verification)	Any connection with TCP
AcAlarm.exe (PE Alarm-Management)	Any connection with TCP
Stm4App.exe (CP Card Personalization)	Any connection with TCP

3.1.4 Shared Folder Security

APE client installations require access to shared folders on the server side. The authentication is done via a user which is generated during the APE server installation. On the client installation, this user is retrieved from the server and created identically on the Client-PC. Thus when installing the client, the LacSp-Service must be running on the server.
The access over network to the shared folder is done by Windows with the SMB network protocol (Server Message Block). Both SMB client and SMB server must support SMB 3.0 or higher to take advantage of the SMB Encryption functionality. The Configuration of SMB should follow the recommendations from Windows.

- Security enhancements in Windows Server 2012
- How to detect, enable and disable SMBv1, SMBv2, and SMBv3 in Windows and Windows Server

The following table describes the used SMB versions between different Windows versions.

Windows version	Windows 10/2016	Windows 8.1/2012 R2	Windows 7/2012	Windows 7/2008 R2	Windows Vista/2008	Other versions
Windows 10/2016	3.1.1	3.0.2	3.0	2.1	2.0.2	1.x
Windows 8.1/2012 R2	3.0.2	3.0.2	3.0	2.1	2.0.2	1.x
Windows 7/2012	3.0	3.0	3.0	2.1	2.0.2	1.x
Windows 7/2008 R2	2.1	2.1	2.1	2.1	2.0.2	1.x
Windows Vista/2008	2.0.2	2.0.2	2.0.2	2.0.2	2.0.2	1.x
Other versions	1.x	1.x	1.x	1.x	1.x	1.x

3.2 Hardening

Some recommendations:

- Anti-virus and anti-spyware software shall be installed and kept up to date.
- The windows software patches and updates shall be installed and kept up to date.
- In order to prevent attacks on the server, the USB ports and the CD/DVD drive shall be disabled.

TLS-Versions communication between Client and Server (1.0/1.1)

SMB V3.0:

- On Setup the **SmbShare** parameter “**EncrypData**” is set to **$True** for shared folder “**APEData$**”.
- The **SmbServerConfiguration** parameter “**RejectUnencryptedAccess**” is not changed. Default setting is **$True**.

4 Security Update Management

APE does not work with an update mechanism or patches.
With each release, the software should be uninstalled first and then reinstalled with the new version.
The setup provides the possibility to export the database and the configuration. During the reinstallation, the operator will be asked if he wants to import the existing data/configuration.

5 Secure Disposal

When uninstalled, the whole software and data will be deleted.

Only the following registry keys remain:

HKLM\Bosch\Access Professional Edition \SaveData	Folder with saved data - needs to be reinstalled.
HKLM\Bosch\Access Professional Edition\IPC	IP-Connect information for APE and SDK.
HKLM\Bosch\Access Professional Edition \Security	Security Information of shared folder user - needs to be reinstalled.

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