Installation Instruction

Visionline

ASSA ABLOY
Global Solutions

Experience a safer
and more open world

Copyrights

The information in this document is subject to change at the sole discretion of ASSA ABLOY without notice.

Any use, operation or repair in contravention of this document is at your own risk. ASSA ABLOY does not assume any responsibility for incidental or consequential damages arising from the use of this manual.

All information and drawings in this document are the property of ASSA ABLOY. Unauthorized use and reproduction is prohibited.

June 2021

Table of contents

1. Version

This Visionline system is of version 1.27.x.

Note: The screenshots and search paths etc in this document are for _Windows 10_. Slight differences may appear depending on operating system.

2. Installation

Before starting the installation, make sure that the knowledge requirements in section 2.2 are fulfilled and that the information about minimum hardware in section 2.3 has been considered. Complete all necessary installations in chapter 2 and then continue to chapter 3.

- Single machine installation is not possible; this applies from Visionline 1.20.0 and onwards. Instead, Visionline is always installed in the 'multiple machines' mode.

- To add extra COM ports on your computer, use USB to serial converters.

- If the system should be run with any Inncom technology such as IR4, IR5 or ZigBee, the Inncom software is installed by Inncom staff (contact your distributor for further information). The applicable Inncom option is set in the Visionline software with an option code, and Inncom parameters are entered in Visionline according to the applicable option instruction.

- ASSA ABLOY Global Solutions recommends that Visionline is installed on a separate server (referred to as the ASSA ABLOY Global Solutions server).

- The difference between installing a server with domain account and with local accounts is the location of the Component Account. The Component Account which is added on the clients must have the same user name and password as the Component Account on the ASSA ABLOY Global Solutions server.

2.1 Installer file verification

In order to ensure that our customers operate authentic software free from malware, we scan our releases on a regular basis to detect existing and previously unknown threats. We also sign the installers with our certificates which are publicly recognized and trusted by Microsoft, to allow customers to trust that each release contains authentic software.

1. Follow the instructions in the document *Quick reference guide Checksum comparison* (available in the Visionline bundle) to calculate the checksum for the Visionline installer.
2. Compare the calculated checksum with the one provided in the PDF *Checksum for Visionline vX.XX.X installer* which is located in the same folder as the Visionline installer.
3. See the document *Quick reference guide Checksum comparison* for information on how to proceed after the comparison.

2.2 Knowledge requirements

In order to perform this installation you should be familiar with:
- Windows Explorer
- adding an account using **User Manager**
- viewing the **Event Log** using the **Event Viewer**

2.3 Minimum hardware

- See specification for the operating system which is to run on the Visionline server.
- If the Visionline system should be online, more RAM than what is specified for the operating system is recommended.
- If the number of rooms in the Visionline system is large, more RAM than what is specified for the operating system may be required.
- Depending on the number of days for data storage, more hard disk space that what is specified for the operating system may be required.
- If Data Warehouse is applicable, this should be run on a separate server; see hardware specification for the operating system which is to run on the separate server.

2.4 Command line installation

Microsoft installer (MSI) has the option to install an MSI package from the command line. It can be done either in *silent mode* or with full graphical user interface.

Use the file **msiexec.exe** and a few command line switches.
- msiexec.exe must be run in an elevated process, e.g. right click **command prompt app** and select **Run as administrator**.
- At a silent uninstallation, the database will not be deleted.

2.4.1 Mandatory command line parameters

Parameter	Description
/i <file.msi>	Installs the specified MSI package
/qn **OR** /qf	/qn enables silent mode, while /qf enables installation with full graphical interface
ACCOUNT=<name>	Specifies the component account name
PASSWD=<password>	Specifies the component account password

2.4.2 Optional command line parameters

Parameter	Description
NO_CLIENT=1	The client feature will not be installed.
NO_SERVER=1	The server feature will not be installed.
NO_WEBSERVER=1	The web server (Apache Tomcat) will not be installed.
MY_SERVER=<ip address>	Specifies the server to connect to; this is required if the server feature is not installed.
INSTALLFOLDER=<path>	Specifies an installation folder; default is %ProgramFiles%\ ASSA ABLOY\Visionline.
DATABASEFOLDER=<path>	Specifies a folder for the database; default is %ProgramData%\ ASSA ABLOY\Visionline.

2.4.3 Useful command line parameters

Parameter	Description
/l*v <logfile>	Creates a log file

2.4.4 Examples (for silent mode)

Install server w/o tomcat and client
msiexec /i visionline.msi NO_CLIENT=1 NO_WEBSERVER=1 ACCOUNT=test PASSWD=
Troll1234 /qn

Install client only
msiexec /i visionline.msi NO_SERVER=1 NO_WEBSERVER=1 MY_SERVER=192.168.1.1 ACCOUNT=test
PASSWD=Troll1234 /qn

Install to specified folders
msiexec /i visionline.msi INSTALLFOLDER="C:\Visionline" DATABASEFOLDER="C:\Database" ACCOUNT=test
PASSWD=Troll1234 /qn

Install with default settings and logging
msiexec /i visionline.msi ACCOUNT=test PASSWD=Troll1234 /qn /l*v "c:\temp\install.log"

Install from batch file and wait for process to complete
call msiexec /i "%~dp0visionline.msi" ACCOUNT=test PASSWD=Troll1234 /qn

Install from Power Shell and wait for process to complete
start-process 'c:\windows\system32\msiexec.exe' -argumentlist '/i c:\temp\visionline.msi ACCOUNT=test
PASSWD=Troll1234 /qn' -wait

Uninstall with default settings and logging
msiexec /x visionline.msi /qn /l*v "c:\temp\uninstall.log"

2.5 Installing Omnikey drivers

The reader should not be connected to the PC before the drivers are installed.
1. Locate the **exe** file in the folder **Encoder Drivers** on the Visionline CD.
2. Double click on the **exe** file and follow the instructions on the screen.
   Note that this operation does not install the drivers; it only unzips the
   driver files in a folder of your choice (default folder is created at **C:\Omnikey**).
3. When the unzipping operation is complete, read the information in the
   readme file carefully. The file is available in the folder where the driver files
   have been unzipped.
4. Connect the encoder to an optional USB port on your computer.
5. A dialog **Welcome to the Found New Hardware Wizard** will appear.
6. Follow the instructions on the screen.
7. During the installation of the drivers, the **Diagnostic Tool** is installed as well.
   The **Diagnostic Tool** is reached from the **Control Panel** and shows encoder
   version and status information.

The next time Visionline is started: press **Esc**, go to **File/Select Encoder** and
choose the applicable encoder at 'Smart/RFID card encoder' (or choose encoder
in the startup guide, if it is the first time Visionline is started). At **File/Select
Encoder**, also choose the applicable encoder at 'Magnetic/RFID card encoder'.

2.6 New installation
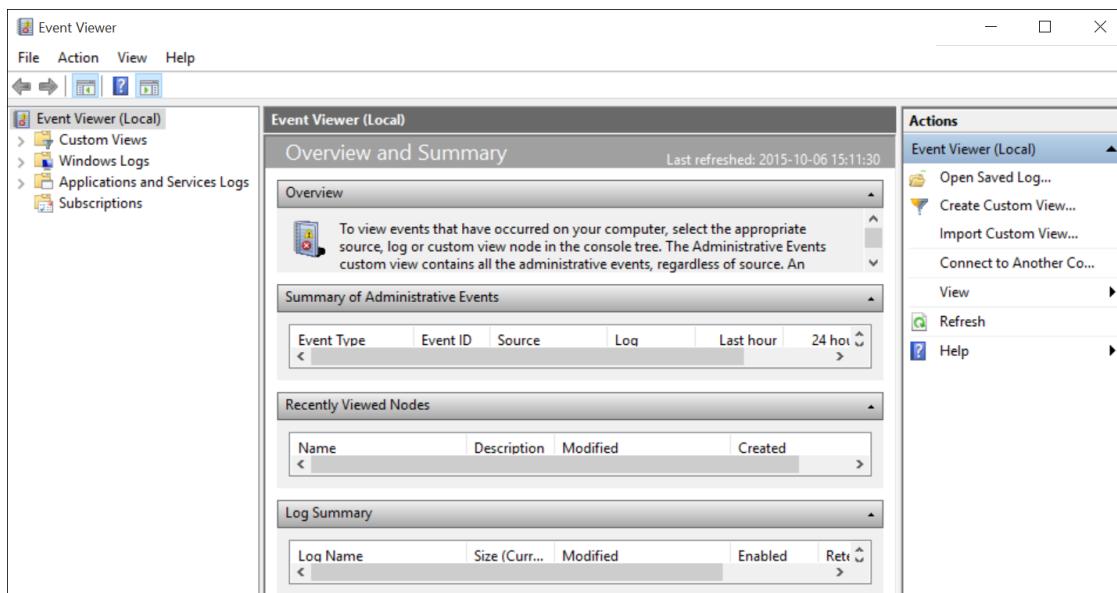
Important: See information about minimum hardware in section 2.3.

1. Visionline setup will automatically add exceptions in Windows Firewall for some of the files in the installation folder, and also for the DCOM command port 135. If 'Web server' is chosen during the installation, there will automatically be an exception also for port 443.

2. If a 3rd party firewall application is used instead of Windows Firewall, please see chapter 10 for a list of files that need to be added to the firewall. *Note:* If Visionline cannot be run even though exceptions have been made for the concerned exe files, it is recommended to log what the firewall blocks; see instruction in section 10.1.
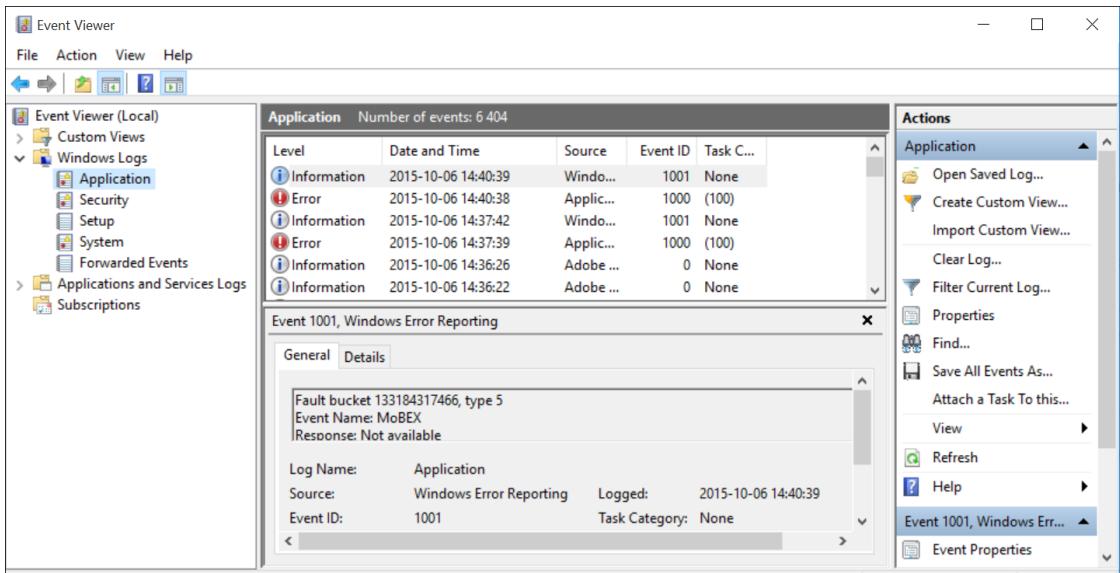
   The following exceptions in the firewall (Windows or other) are not done automatically: exceptions for all TCP ports in the Visionline device list that are used (example: 7799 for ZigBee gateway, if this is applicable); see details on how to set this up in chapter 11.

3. If this has not been done on the machine before: configure the **Application Event Log** (found in the **Event Viewer**) to **Overwrite events as needed**. *Note:* If this is not done, the event log will overflow and the system can stop.
   - Go to **Control Panel/System and Security/Administrative Tools/ Event Viewer**.
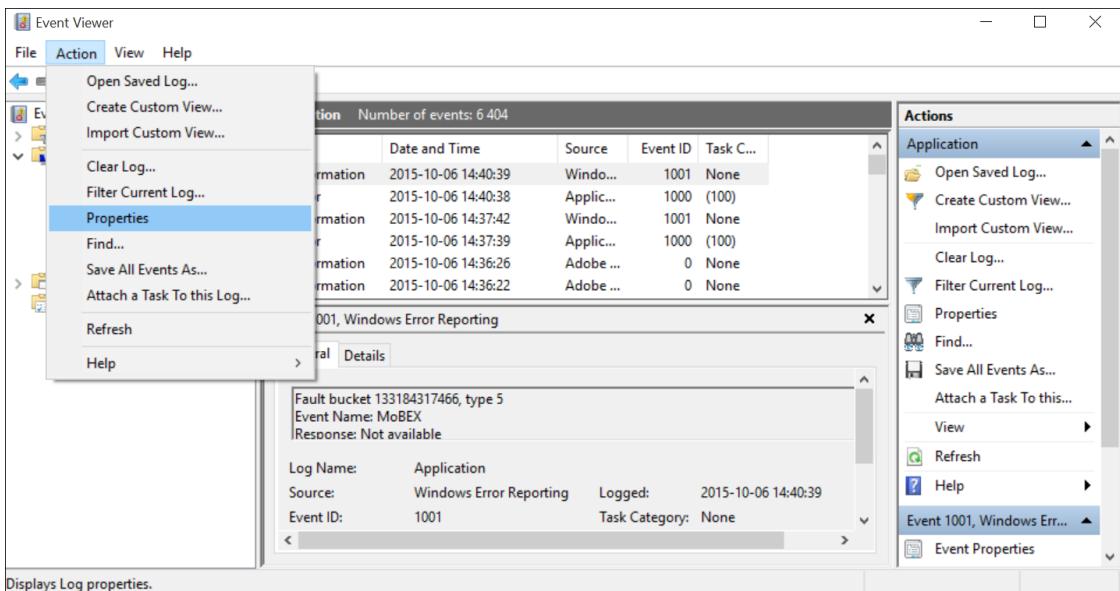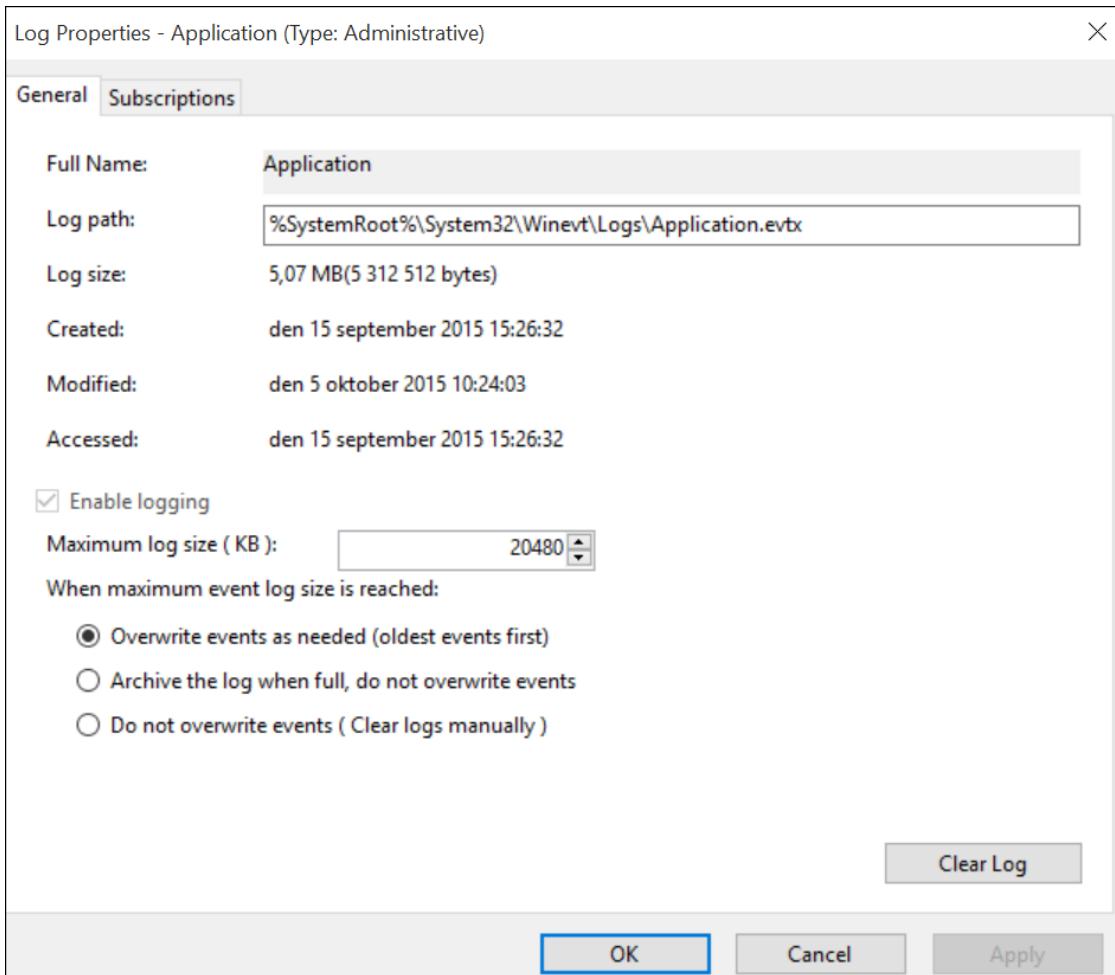
- Expand **Windows Logs** in the left window by clicking on the arrow.

- Mark **Application**.
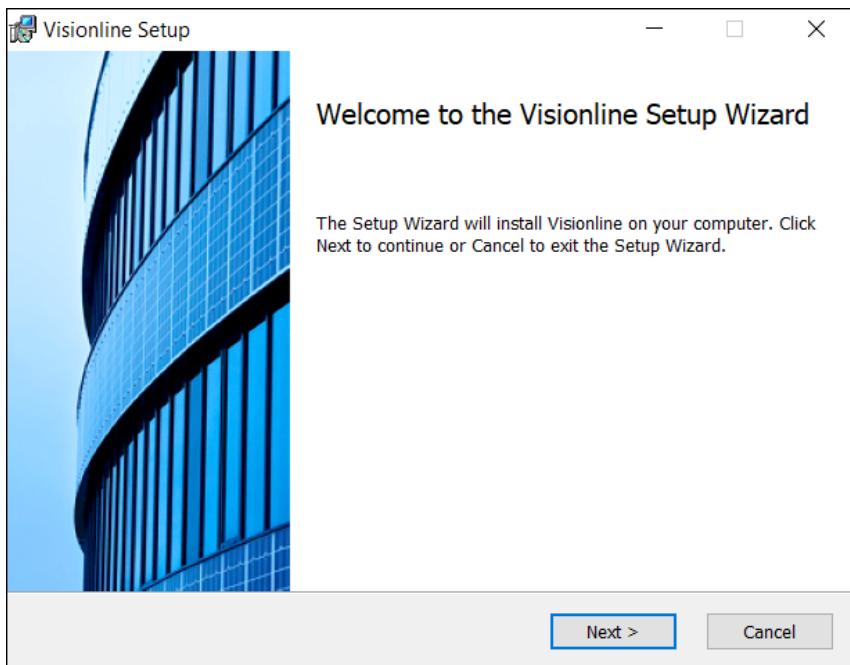
- Go to the menu **Action** and choose **Properties**.

Log Properties - Application (Type: Administrative)

General | Subscriptions

Full Name:	Application
Log path:	%SystemRoot%\System32\Winevt\Logs\Application.evtx
Log size:	5,07 MB(5 312 512 bytes)
Created:	den 15 september 2015 15:26:32
Modified:	den 5 oktober 2015 10:24:03
Accessed:	den 15 september 2015 15:26:32

☑ Enable logging

Maximum log size (KB):   20480

When maximum event log size is reached:

◉ Overwrite events as needed (oldest events first)

○ Archive the log when full, do not overwrite events

○ Do not overwrite events (Clear logs manually)

Clear Log

OK   Cancel   Apply

- Mark the radio button 'Overwrite events as needed' and click **OK**.

4. If domain user account is applicable (else go directly to step 5) and this has not been done on the machine before: add a user account on the domain, to be used by Visionline internally.
   Note: This is referred to as the **Component Account**. This is the only account that will handle contacts with the Visionline database. The **Component Account** should be dedicated for Visionline and not be used for anything else.

5. If **Lock Application Starter** is running, it must be stopped; see details here.

6. Terminate all active Windows programs before starting the installation on the server. **Note:** Do not forget to deactivate all antivirus programs and other monitoring applications during the installation, since these programs can disturb the installation process. When the installation is finished, ASSA ABLOY Global Solutions strongly recommends that some folders are excluded from the antivirus scanning to enhance the Visionline operation; follow the instructions in step 20 below.

7. Double click on the file **Visionline.msi**.

8. **Welcome to the Visionline Setup Wizard** – click **Next>**.
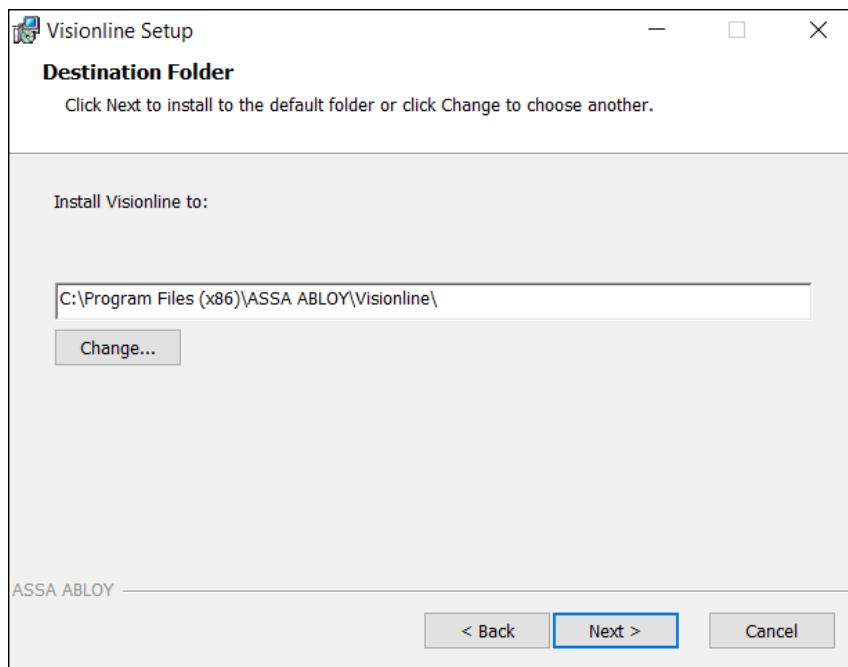
9. **License Agreement** – read carefully, mark the checkbox 'I accept the License Agreement' and then click **Next**.
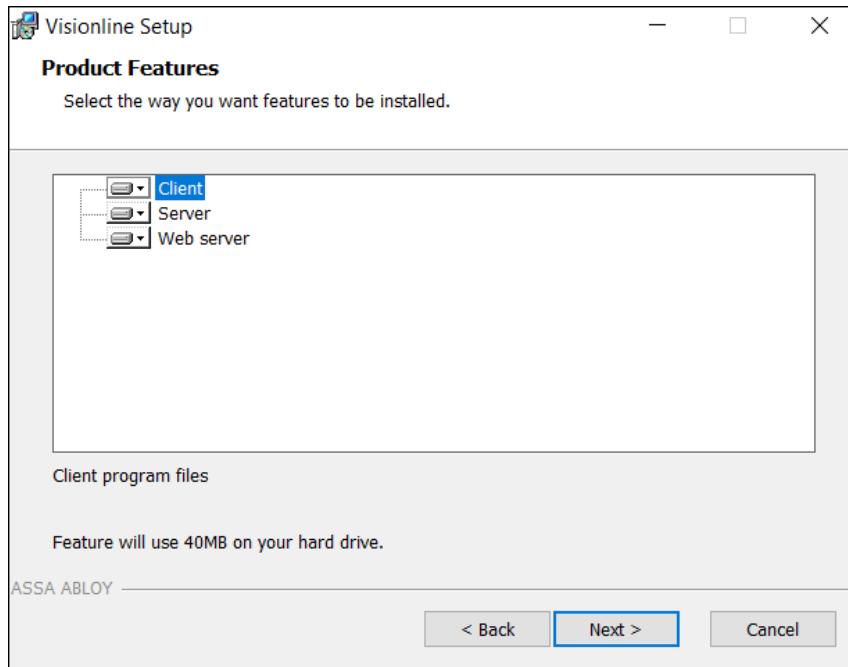

10. **Choose Destination Location** – a default folder is shown, but you can click **Browse** and choose another folder where the files should be installed.

Click **Next>**.

11. **Product Features** – mark which one or ones of the parts *client*, *server* and *web server* that should be installed; see details in step 10. For the features which should NOT be installed, 'The feature will not be installed' must be chosen.
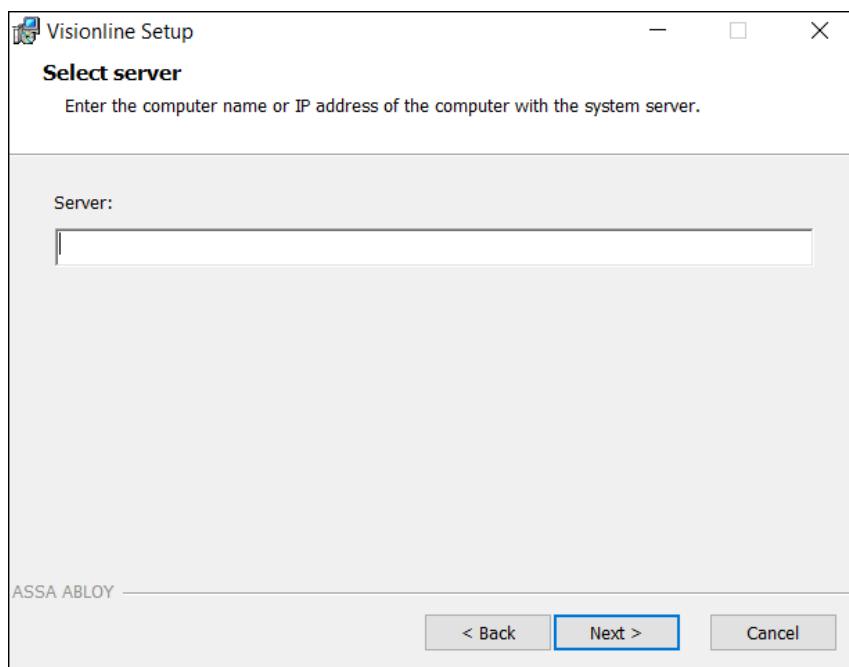
12. For each of the features *client*, *server* and *webserver*, it is possible to choose between the below alternatives. Mark the desired alternative for each feature
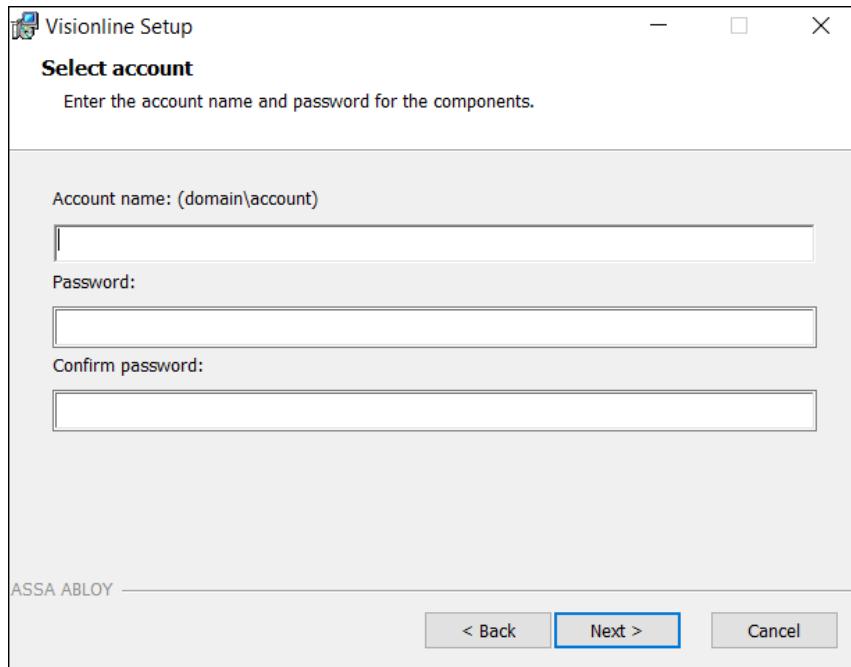
(note that you must make a choice also for features that should not be installed, or be installed when needed) and then click **Next>**.

13. If either 'The feature will be installed when needed' or 'The feature will not be installed' was chosen for **Server**, the following dialog will be shown. Follow the instructions and click **Next>**.
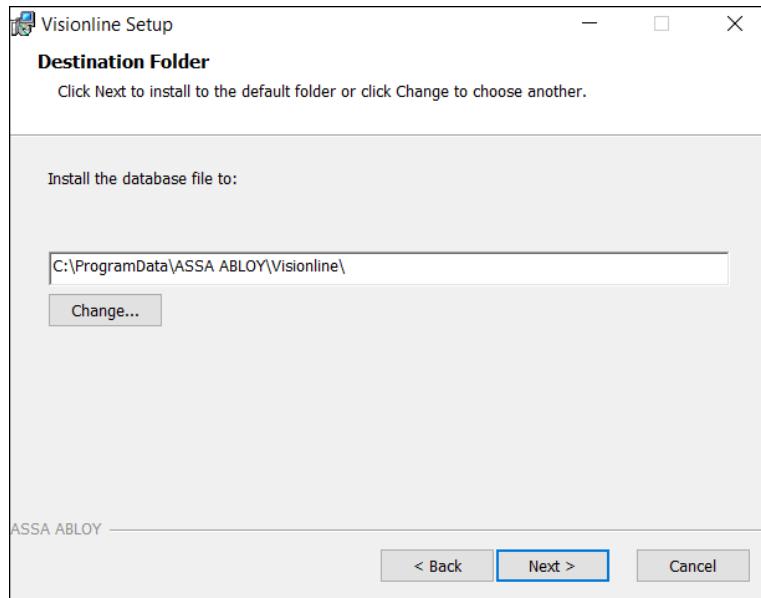
14. **Select Account** – enter the name and password for the **Component Account**. If the account is located on the domain, the account name must be preceded by the domain name and a backslash; thus **Domain\Account**. Click **Next>** to start the file copy process.
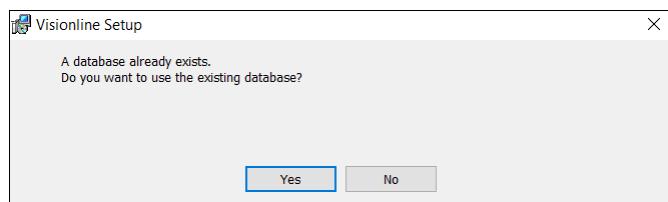
15. If the **Component Account** is a domain account, you will get the option to specify the group. **_Note:_** If no group is specified in this step, the group **Everyone** will be given access to our components as previously.
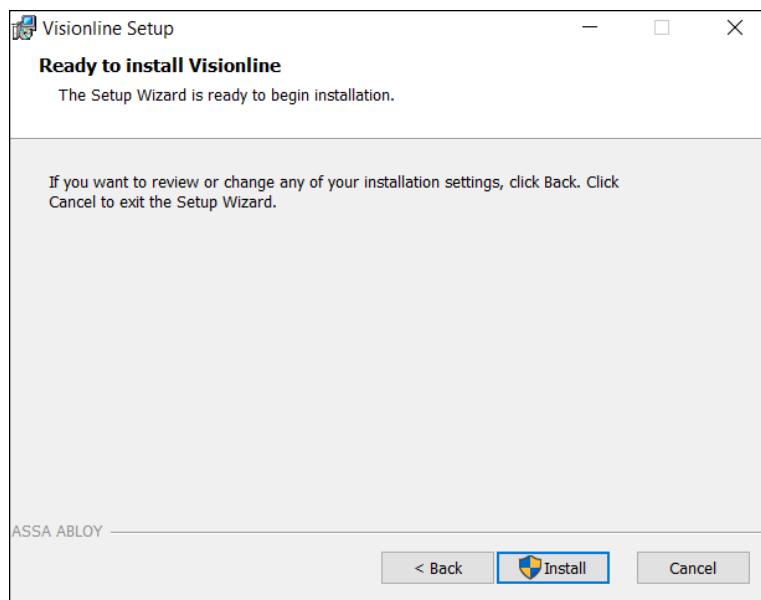

16. A default folder is shown, but you can click **Browse** and choose another folder where the database should be installed. Click **Next>**. **_Note_**: Make sure that the database is placed where the **Component Account** has authority to read and write.
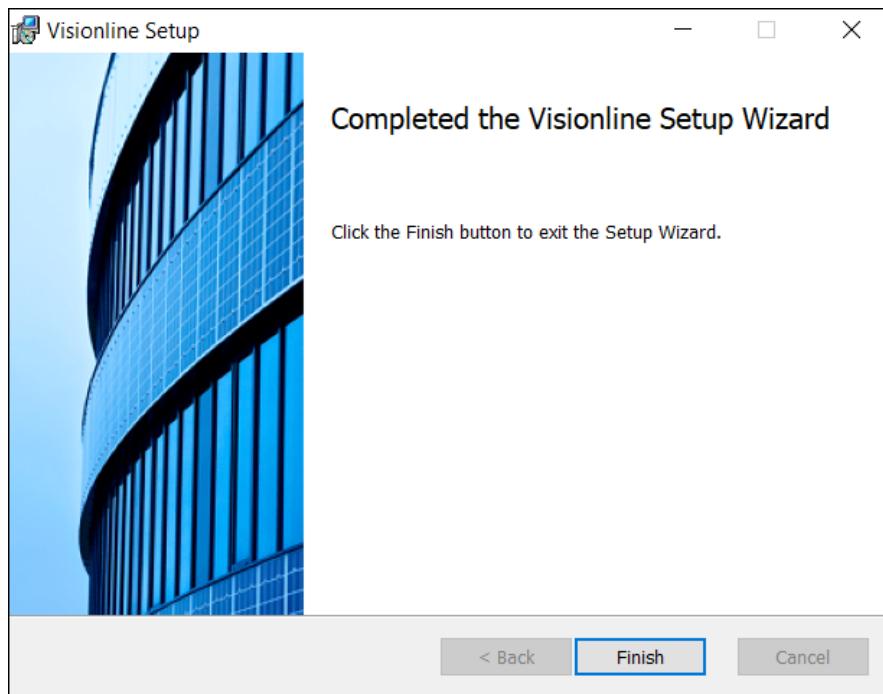
17. If a database already exists, you will get the below dialog; make the applicable choice **Yes** or **No**.

18. The following dialog will be shown, where you click **Install** unless any settings need to be changed.

66 5013 142-8

19. **InstallShield Wizard Complete** – click **Finish** to exit the installation program.

20. If any antivirus programs are used: make exceptions in the antivirus scanning for
    - the Visionline installation folder
    - the Visionline database folder
    since these folders are used extensively when Visionline is running.

21. Start the required services *, either by
    - restarting the computer **OR**
    - selecting **Control Panel/System and Security/Adminstrative Tools/ Services**; mark the service and then right click on it to choose **Stop**.

*) The service **Lock Application Starter** should always be started.
The service **Lock Application Card Updater** should be started if any of the below scenarios
are applicable:
    - interface to Visionline via web API
    - interface to Visionline via PMS
    - auto-update

2.7 Upgrade installation

2.7.1 Preparations

The operations described below are required for both upgrade scenarios in sections 2.7.2-2.7.3.

1. Disable DCOM (Distributed COM):
   - In the Windows **Run** command prompt, enter 'dcomcnfg' and click **OK**.
   - In the left pane of the **Component Services** dialog, click the arrow to the left of **Component Services** and the arrow to the left of **Computers**.
   - Right click on **My Computer** and choose **Properties**.
   - In the **My Computer Properties** dialog, choose the **Default Properties** tab.
   - Unmark the checkbox 'Enable Distributed COM on this computer'.
   - Click **OK**.
2. If the Visionline client is running, go to the menu **File** and choose **Exit**.
3. If SysMon (*System Monitor*) is open, go to the menu **File** and choose **Exit**.
   Note: If SysMon has been set up to pop up each time PMS Plus sends information about a card/tag etc that is to be encoded (applicable if the *RFID KDE network encoder* is used), the SysMon shortcut in the **Startup** folder must be removed as well.
4. Stop **Lock Application Starter**:
   - Go to **Control Panel/System and Security/Adminstrative Tools/Services**.
   - Mark **Lock Application Starter**.
   - Right click on **Lock Application Starter** and choose **Stop**.
5. Stop **Lock Application Card Updater**:
   - Go to **Control Panel/System and Security/Adminstrative Tools/Services**.
   - Mark **Lock Application Card Update**.
   - Right click on **Lock Application Card Update** and choose **Stop**.
6. Wait 1 minute for all Visionline processes to terminate.
7. If you get a message when starting the upgrade installation according to any of the sections 2.7.2-2.7.3 that one or more Visionline processes are running, double click on **KAS.BAT** in the Visionline installation folder.

If you are upgrading from a non-released version, also perform the steps below:

1. If the old database should be kept: Make a backup copy of the database.
2. Uninstall the old Visionline version.
3. Install the new Visionline version.
4. Replace the new, empty database with the old, backed-up one.
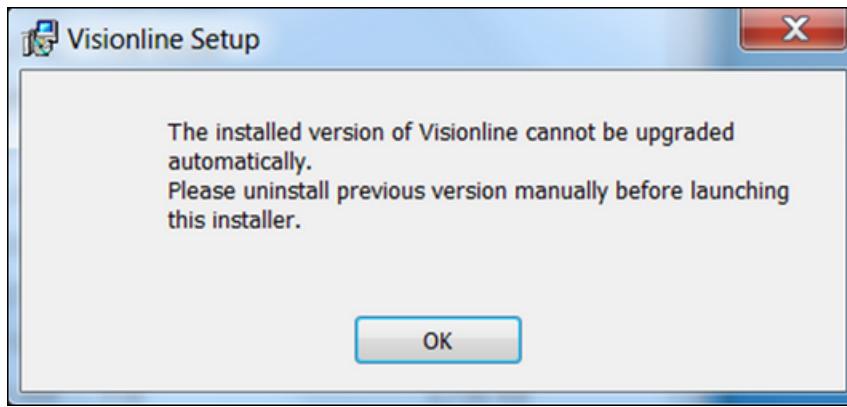
2.7.2 Upgrade installation from Visionline 1.20.x

If you are upgrading from a Visionline 1.20.x version, the 1.27.x version can be installed directly over the 1.20.x version without uninstalling it.

2.7.3 Upgrade installation from a version prior to 1.20.0

If you are upgrading from a Visionline version prior to 1.20.0, you must in addition to the preparations in section 2.7.1 make sure that you have a license upgrade code available since the system will otherwise not work. Contact Technical Support to get a license upgrade code. At first logon to the software after installation, the license upgrade code should be entered in the dialog which pops up and requests you to do this.

From Visionline 1.20.0, WiX installer is used instead of InstallShield installer. Upgrade to a Visionline version based on the WiX installer from any previous Visionline version based on the InstallShield installer is not possible (if you try, a screenshot as below will be shown).

Instead follow the steps below:
1. Uninstall the Visionline version which is based on the InstallShield installer (without deleting the database).
2. Install the Visionline version which is based on the WiX installer.

2.8 Uninstallation

For uninstallation of Visionline, three alternatives are available:
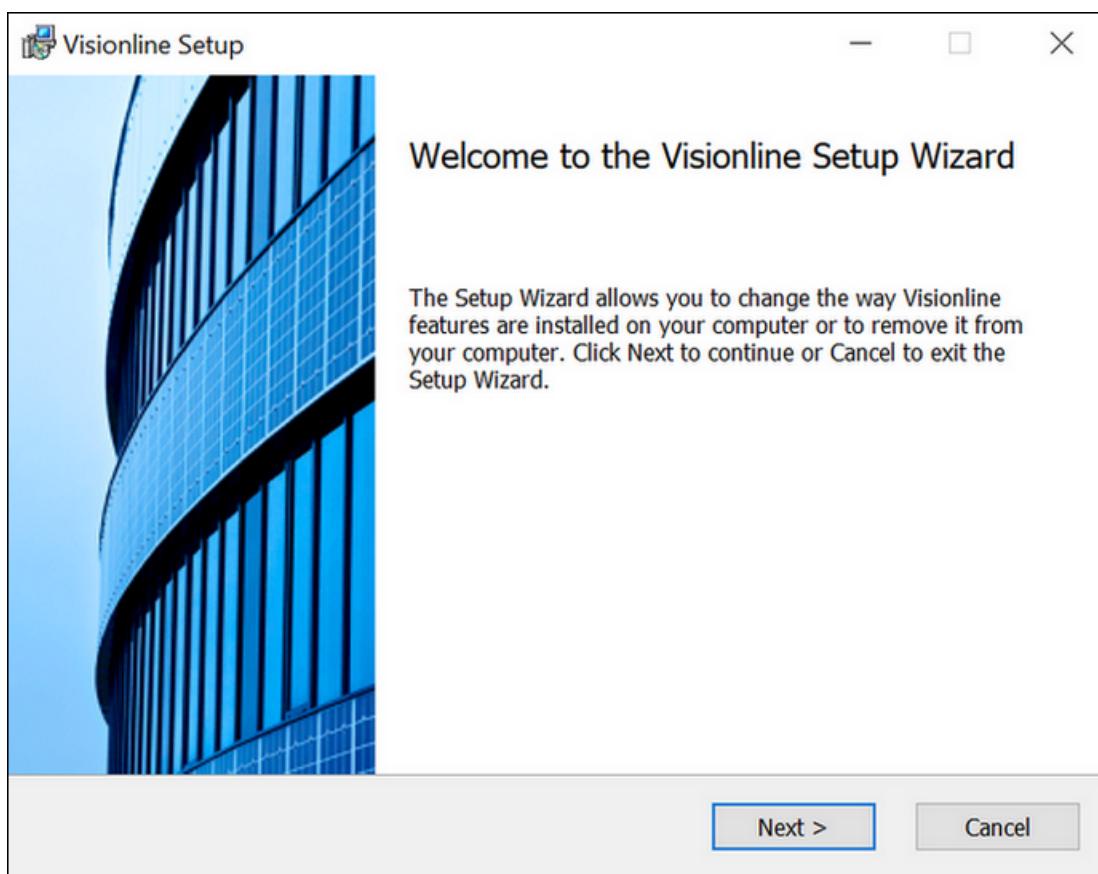
- Right-click on the file **Visionline.msi** and choose **Uninstall**.

- Double click on the file **Visionline.msi** to start an uninstallation; the three below dialogs will be shown. The database is by default saved (see second screenshot; if it should be deleted, mark 'Delete the database file'). If hovering over the checkboxes, a more detailed explanation is shown:
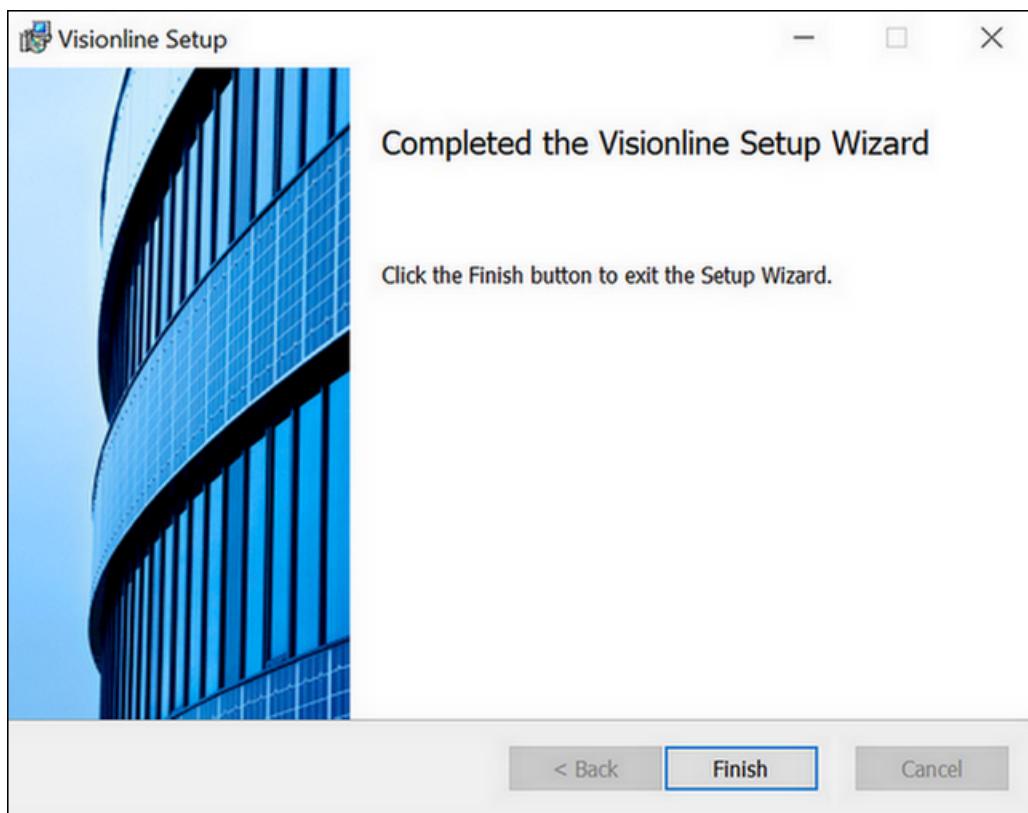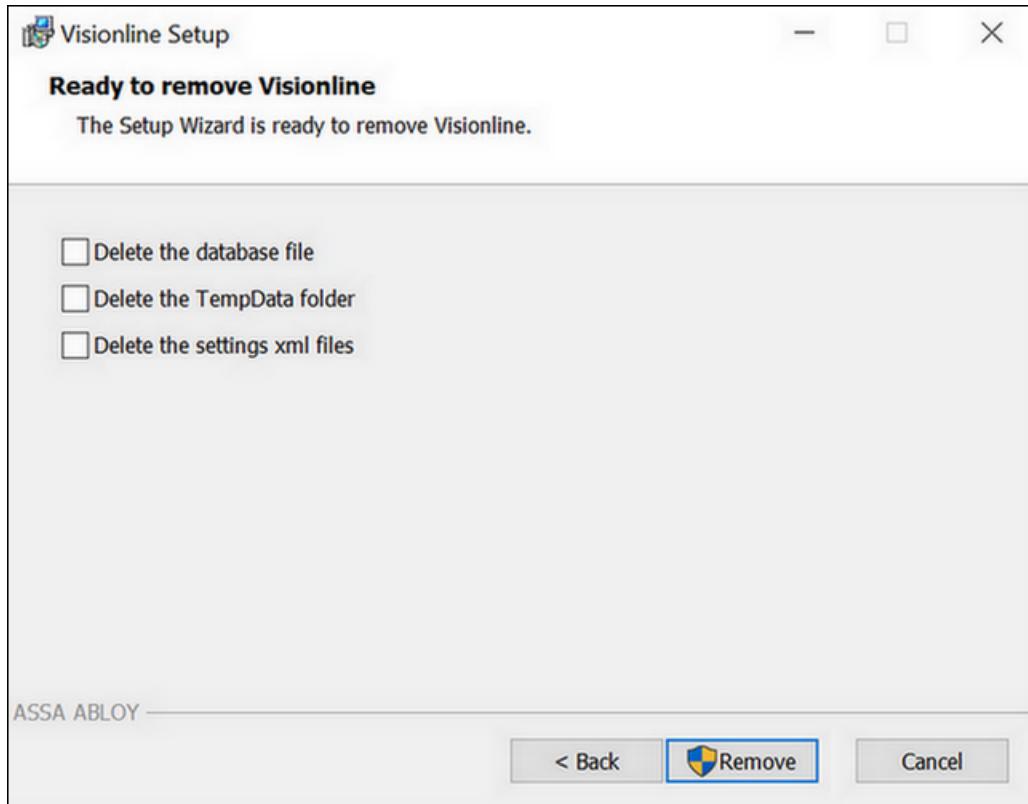
  Delete the database file: This will remove the database permanently without the possibility to recover. Only check this if you are sure you have a backup or will never use this database again.

  Delete the TempData folder: This will remove all the temporary files used by Visionline. Doing this may have a minor impact in online installations, but for the most part, it is safe to do this.

  Delete the settings xml files: This will remove all settings made in Visionline.

- Go to **Control Panel/Programs and Features**; right-click on Visionline and select **Change**; this will lead to the same three dialogs below.

66 5013 142-8

Visionline Setup

Ready to remove Visionline

The Setup Wizard is ready to remove Visionline.

☐ Delete the database file

☐ Delete the TempData folder

☐ Delete the settings xml files

ASSA ABLOY

< Back | Remove | Cancel

Visionline Setup

Completed the Visionline Setup Wizard

Click the Finish button to exit the Setup Wizard.

< Back | Finish | Cancel

3. Event log

The event log shows errors and important events. It is found in the **Application Log** of the built-in **Event Log**.

4. Backup

When the Visionline system has been set up with doors, users, time schedules etc (see *Setup manual Visionline* for details), a backup of the database should be made:

1. Click the **Start** button and choose **Programs/Visionline/Tools/ Backup database**.
2. Mark the applicable radio button 'To diskette' or 'To folder'.
3. Click **Backup**. If 'To folder' is chosen, browse to the desired folder/USB memory tc and click **OK**. If 'To diskette' is chosen, follow the instructions on the screen. This procedure requires a number of diskettes; how many depends on the size of the database.
4. At **Tools/Options/System/Database backup**, it will at 'Last run' be shown when backup to diskette or folder was last done (shown with date and time).

To set up a backup folder for automatic backup:

1. Go to **Tools/Options/System/Database backup** and browse to a suitable backup folder (should be located where regular backup is made). If no file server is available, a USB memory can be used for backup.
    Note: The database will automatically be copied to the chosen folder after each housekeeping. Before the database is copied, a compression of the database is automatically performed.

Important: **ASSA ABLOY Global Solutions recommends that a database backup is made every day. If a backup folder is set up according to above, this is automatically the case since housekeeping is run every day.**

5. Start-up

To start Visionline, go to **Start/Programs/Visionline/Visionline**. At first start-up, there is a startup guide; here you choose to run in licensed or unlicensed mode, and you also choose encoder (in unlicensed mode, it is possible to run without operator cards or without card encoders). If licensed mode is chosen, a license code should be entered. When starting in licensed mode, an operator card for system manager should be encoded. Log on with the card; the user ID is *sym* and the password is *sym*. Change password for system manager in the **Operator details** dialog which is shown. You will also get a message with a link to register the installation; click the link and enter the required information.

The start-up guide will be shown at each start-up until a license code is entered. It is not possible to go back to unlicensed mode once the system ID has been set. In unlicensed mode, cards can only be made for a maximum of 28 days and the only guest rooms that cards can be issued for are 101-110.

It is important that software, door units and service device have the same status, either unlicensed or with system ID. It is possible to initiate door units in unlicensed mode and keep the initiation when shifting to system ID; please see *Setup manual Visionline* for more detailed instructions.

Note: **Keep the software CD and the system cards in a safe place.**

6. Power down cards

To every guest room, there must be a pre-encoded power down card. The power down cards are given to new guests if there is a power failure and guest cards cannot be issued. Whenever a power down card has been used, a new one must replace it as soon as card encoding is possible again. Please see *User manual Visionline* for more detailed instructions.

7. Options

If any software options have been ordered together with the system, they are included in the license code for the system and will be set in the software when entering the license code. If any options are ordered later on, when system ID has been set, they are delivered as option codes and must be installed manually. Please see the respective option instruction for more detailed instructions.

8. Service device

Before a service device can be used, a service device host must be added to the device list. The service device must also be registered.

1. Select **Device...** from the **Add new** menu.
2. Enter a name for the service device host.
3. Enter an optional description of the service device host.
4. Select 'Service device host' as type.
5. A default IP address is shown; change this to the IP address of the PC at the selected **Location**. If possible, use the default port.
6. Select **Service device...** from the **Add new** menu. A notice with a registration code will be shown. Please note that the registration code must be entered in the service device within a given time interval. When the code has been entered, the service device will appear in the service device list. See *Quick reference guide Lock Service* or *Quick reference guide Lock Service 3G* for more information about the registration. Also follow the steps in *Quick reference guide Lock Service/Quick reference guide Lock Service 3G* for server connections.

9. PMS

Before the PMS interface can be used, a device must be added in the device list:

1. Select **Device...** from the **Add new** menu.
2. Enter a name of the PMS device.
3. Enter an optional description of the PMS device.
4. Select 'PMS/PMS Plus' for type.
5. Specify the COM port where the PMS is to be connected.
6. Enter the name of the computer where the PMS is to be connected or click on **Server** if the PMS is to be connected to a COM port on the server.
7. In order to make the PMS device listen for PMS commands on the COM port, the device must be started (***Note:*** **not needed if Visionline is installed on a standalone machine**). This is done with the service **Lock Application Starter**. Once Visionline has been installed, **Lock Application Starter** is automatically started every time the computer is restarted.

Lock Application Starter is found at

Control Panel/System and Security/Administrative Tools/Services/ Lock Application Starter

The event log shows whether the device was successfully started or not.

10. Exe files

See below an explanation of the Visionline exe files for which firewall exceptions are automatically made.

Note: All calls between machines are made through DCOM (_Distributed Component Object Model_). In many ways, DCOM works like the FTP protocol.The DCOM command port is TCP 135 (for FTP, it is normally 21). Once a command arrives at port 135, a temporary port (ephemeral port) is randomized within a specific port range; this range depends on the Windows version. The DCOM call is then processed on the ephemeral port so that the command port is free for other incoming DCOM requests; this is the same procedure as when FTP randomizes a data port to transfer the files on.
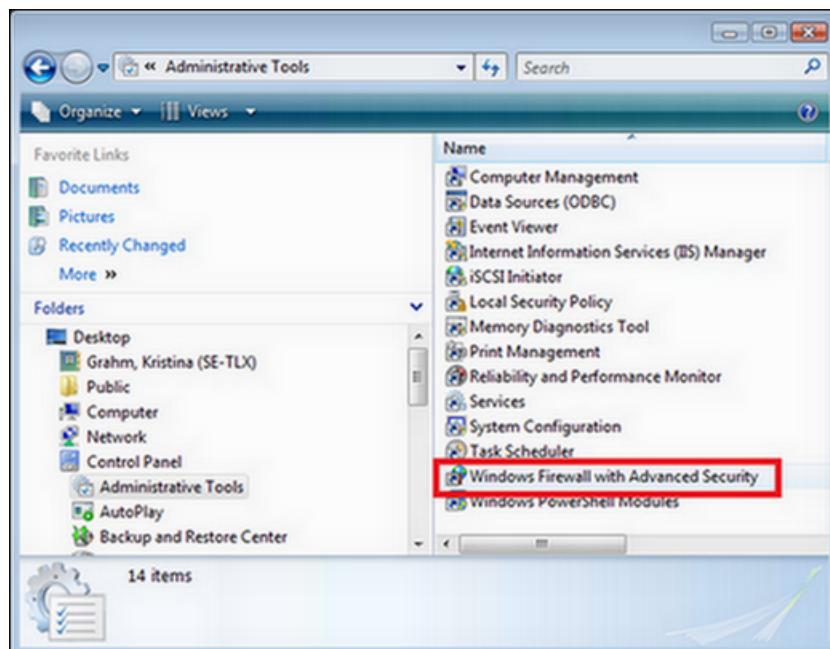
Name	Description
AppAlarm.exe	• Manages alarm triggering and revoking
AppAuth.exe	• Manages authority for operators • Assures that all devices on a client are started when the client starts
AppCamera.exe	• Manages communication with IP cameras
AppCard.exe	• Manages encoding and encryption of cards
AppCath.exe	• Manages housekeeping and storing of events in the database • Creates reports
AppDB.exe	• Queues database requests • Assures that the database only sees one user • Manages Data Warehouse
AppEv.exe	• Receives events from all components and passes them on to the Event Log • Feeds SysMon with events, cards, PMS requests and Data Warehouse statistics.
AppMail.exe	• Manages sending and receiving of e-mails (plain or SSL)
AppMessage.exe	• Formats e-mails and text messages • Manages integration to HotSOS
AppOnline.exe	• Handles online communication including ZigBee network management
AppPMS.exe	• Handles Handles PMS interface • Validates PMS requests • Calls AppCard to produce cards
AppTLCode.exe	• Generates commands to Lock Service/Lock Service 3G/Orion Service • Loads events
AppUpdate.exe	• Manages auto-update of cards
AppWebService.exe	• Manages the web service
AppXml.exe	• Handles non-volatile storage of XML data
Cards.exe	• Buffers requests for cards issued from the client • Displays the card-encoding window.
CardUpdate.exe	• Service that keeps AppUpdate running
CEMag.exe	• Communicates with MCE and CE as well as with ACE emulating MCE/Omron

DBServer.exe	• Buffers database calls • Manages compression, repair and backup of database
DeviceMUX.exe	• Manages start and stop of devices as well as queuing
HCU.exe	• Communicates with Lock Service/Lock Service 3G/Orion Service
NGStarter.exe	• Service that runs on W7/W8/W10/2008/2012/2016 • Also called Lock Application Starter • Activates Online, PMS and housekeeping
TLCom.exe	• Communicates with ACE/DCE/RFID using D-032 • Receives commands from PMS and passes them on to AppPMS • Communicates with Zigbee Gateways and Open-Card printers • Manages GSM modems
TLConcentrator.exe	• Used when Visionline is installed on a ZigBee server
TLMifare.exe	• Manages encoding of Mifare cards
TLPCSC.exe	• Communicates with PCSC (Gemplus and Omnikey) encoders
TLRFID.exe	• Manages USB connection to the RFID encoder
TLSRT32.exe	• Manages encoding using KDE encoder

10.1 Logging dropped packets
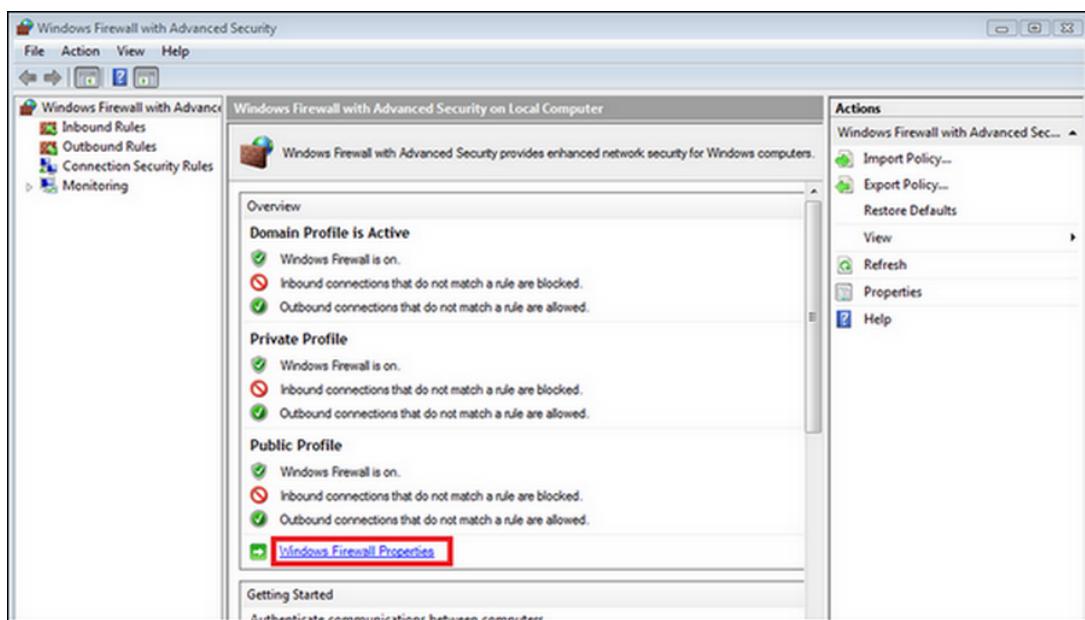
If Visionline cannot be run even though exceptions have been made for the concerned exe files, it is recommended to log what the firewall blocks according to below:

1. Go to **Control Panel/System and Security/Administrative Tools**.
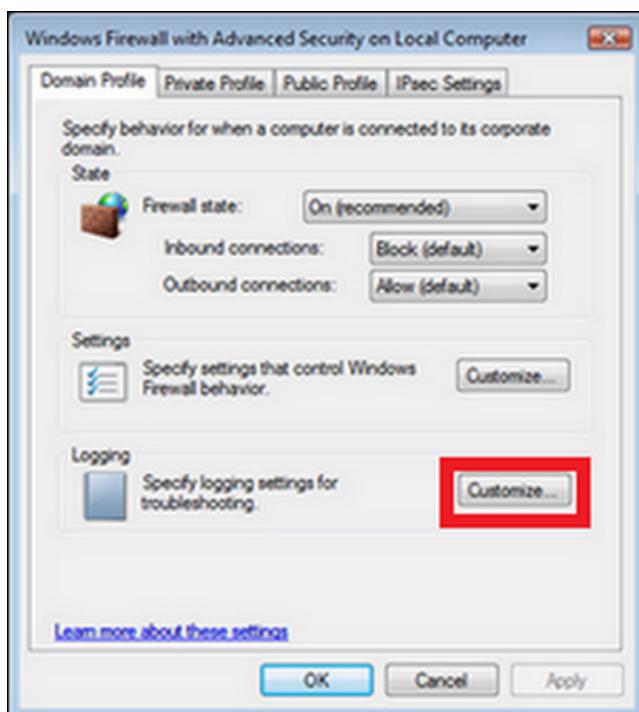
- Double click on **Windows Firewall with Advanced Security**.

2. In the **Windows Firewall with Advanced Security** window,
   click the link **Windows Firewall Properties**; see next page.
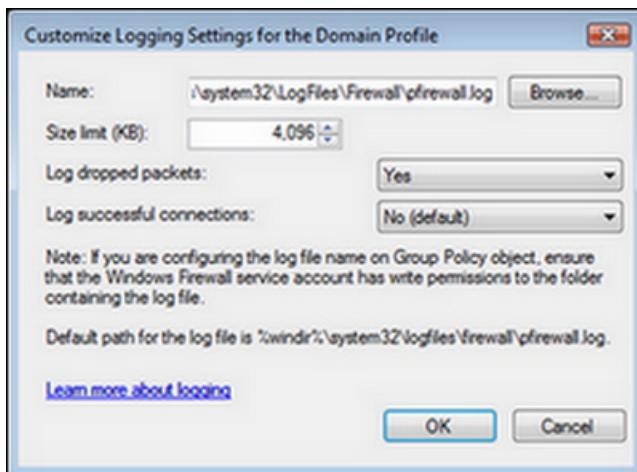
3. In the **Windows Firewall with Advanced Security on Local
   Computer** dialog, click **Customize** at 'Logging'.

4. Click **OK**.

5. In the **Customize Logging Settings for the Domain Profile**
dialog, change to **Yes** in the drop-down-menu at 'Log dropped packets'.

6. Click **OK**.

Note: To look at the log, open **pfirewall.log** which is located at **C:\Windows
\System32\LogFiles\Firewall\pfirewall.log**

11. Making firewall exceptions

As described in section 2.6, Visionline setup will automatically add exceptions
in Windows Firewall for some of the files in the installation folder, and also
for the DCOM command port 135. If 'Web server' is chosen during the installation,
there will automatically be an exception also for port 443. Note however
that the below items must manually be set up as firewall exceptions in
Windows Firewall:
- PMS
- service device hosts
- encoders
- ZigBee gateways
- other applicable devices

Note: The exceptions described in this chapter 11 can be added during the
Visionline installation or at any later occasion, when the devices etc are introduced
in the system.

Note: If any other firewall than Windows Firewall is used, all exceptions must
be made manually according to the procedure for the concerned firewall.
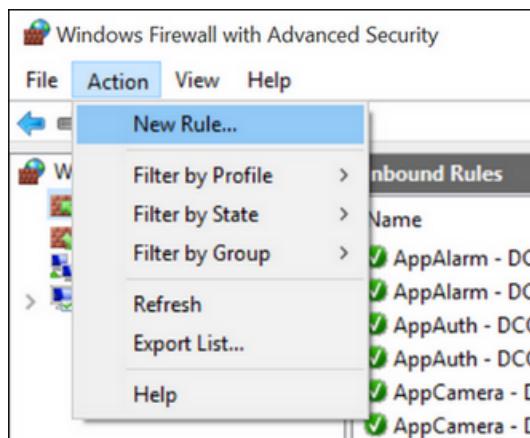
1. Go to **Start/Control Panel/Adminstrative tools**.

2. Double click on 'Windows firewall with advanced security'.
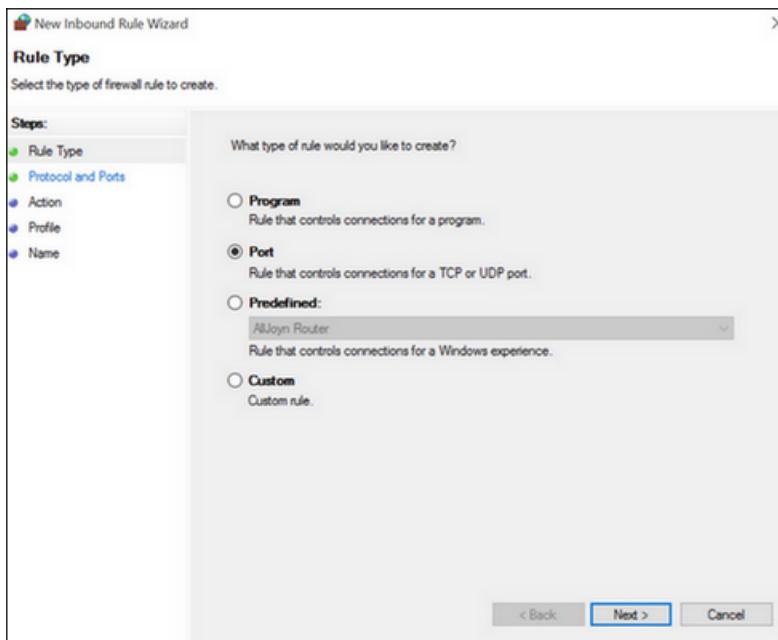
3. Click 'Inbound rules' in the left pane of the **Windows firewall with advanced security** window.
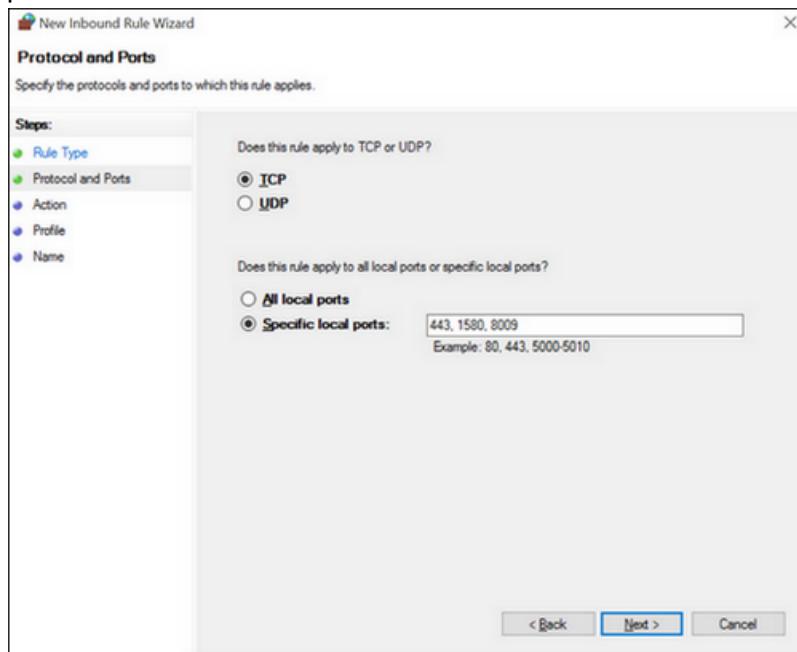
4. Go to the menu **Action** and choose **New rule**.
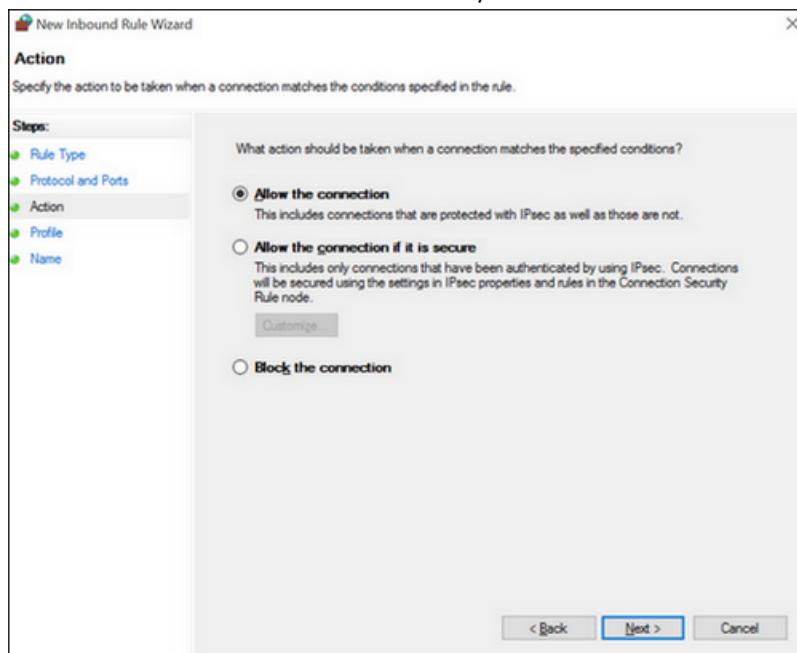
5. In the **Rule Type** dialog which is shown, mark the radio button **Port** and click **Next**.
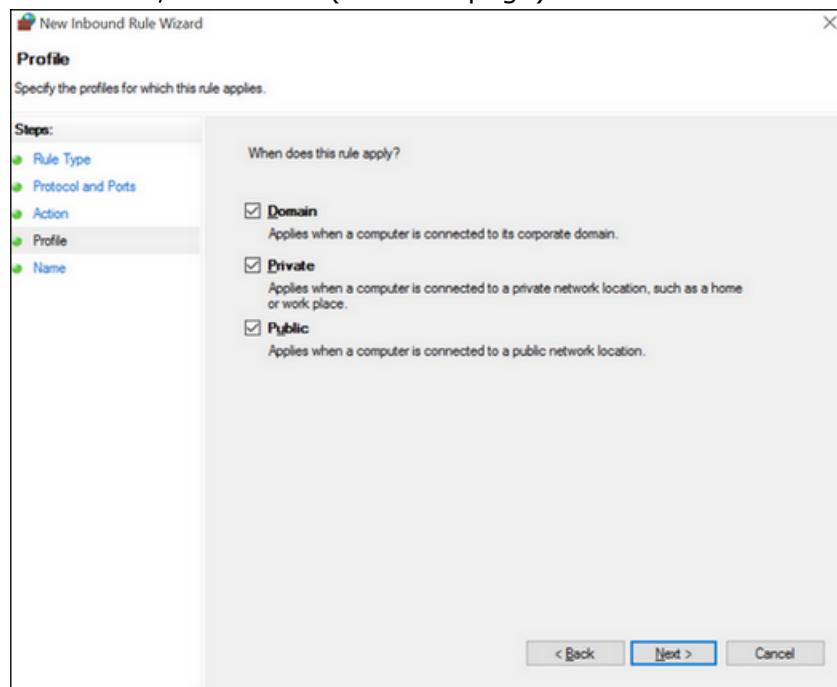
6. In the **Protocol and Ports** dialog which is shown (see next page), make sure that the radio buttons **TCP** and **Specific local ports** are marked. In the field at Specific local ports, enter the concerned TCP ports with comma in between. Click **Next**.
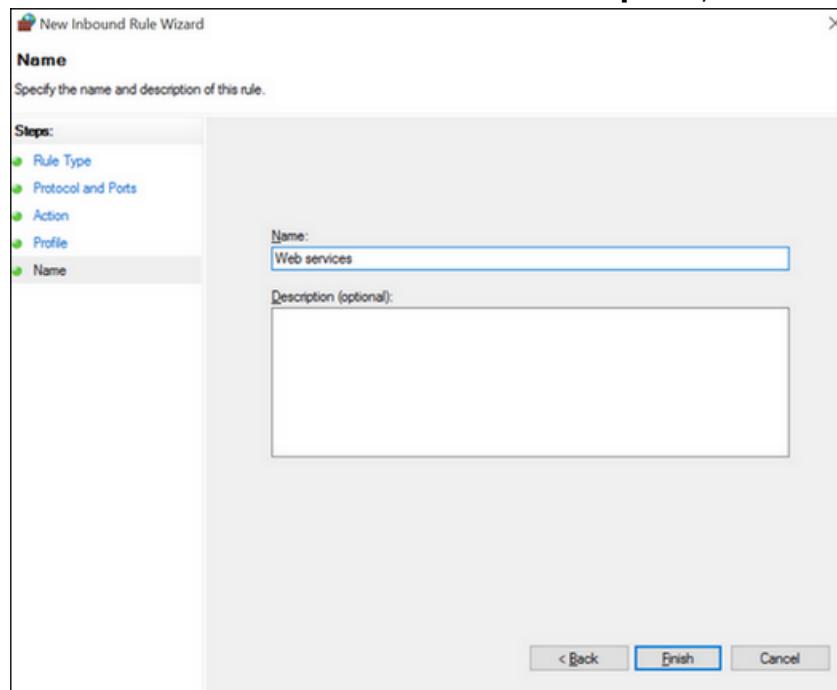
7. In the **Action** dialog which is shown, make sure that the radio button **Allow the connection** is marked; click **Next**.

8. In the **Profile** dialog which is shown, let all three checkboxes be marked; click **Next** (see next page).

9. In the **Name** dialog which is shown, enter an applicable **Name** for the new rule and if desired also a **Description**; click **Finish**.

The ASSA ABLOY Group is the global leader in access solutions. Every day we help people feel safe, secure and experience a more open world.

ASSA ABLOY
Global Solutions