

# Visitor Management V5.0.1

With Mobile Access



# Table of contents

<b>1</b>	<b>Introduction</b>	<b>5</b>
1.1	Functionality change log	5
1.2	About Bosch Visitor Management	5
1.3	About Mobile Access	6
1.4	Intended audiences	6
1.5	How to use this documentation	6
<b>2</b>	<b>System overview and topology</b>	<b>7</b>
<b>3</b>	<b>Installing and uninstalling</b>	<b>8</b>
3.1	Software and hardware requirements	8
3.1.1	The main access control system	8
3.1.2	A database instance to host the Visitor Manager database	9
3.1.3	A dedicated user for local database access	9
3.1.4	A dedicated user for remote database access	9
3.1.5	A dedicated user in the main access control system	9
3.2	Installing the Server	10
3.2.1	Running the server setup program	10
3.2.2	Appsettings JSON file	11
3.3	Setting up the VisMgmt client computer	11
3.3.1	Setting up the Peripheral Devices add-on	12
3.3.2	Certificates for secure communication	13
3.3.3	Appsettings JSON file	15
3.4	Verifying server installation	15
3.5	Installing Mobile Access	15
3.5.1	Overview of installation, configuration, and use	15
3.5.2	Mobile Access hardware prerequisites	16
3.5.3	Mobile Access configuration prerequisites	16
3.5.4	Procedure for co-located installation	17
3.5.5	Procedure for distributed installation	19
3.6	Installing the Mobile Access apps	21
3.7	Peripheral hardware	22
3.7.1	Registering peripheral hardware with the client computer	22
3.8	Repair installations of Mobile Access	23
3.9	Uninstalling the software	23
<b>4</b>	<b>Configuration</b>	<b>24</b>
4.1	Creating Visitor Management users in the ACS	24
4.2	Creating Visitor authorizations and profiles in the ACS	24
4.3	Setting up the Receptionist computer	25
4.4	Setting up a kiosk computer for Visitors	25
4.5	Logging on for configuration tasks	25
4.6	Using the Settings menu for configuration	26
4.6.1	Email templates	28
4.6.2	Preview mode	30
4.6.3	Document templates	30
4.7	Customizing the UI	30
4.7.1	Setting options visible, invisible and mandatory	30
4.7.2	Customizing kiosk mode	30
4.7.3	Customizing the company logo	31
4.8	Firewall settings	31

4.8.1	Programs and services as firewall exceptions	32
4.9	IT security	34
4.9.1	Hardware responsibilities	34
4.9.2	Software responsibilities	34
4.9.3	Secure handling of mobile credentials	34
4.10	Backing up the system	35
5	<b>Operation</b>	<b>36</b>
5.1	Overview of user roles	36
5.2	Using the dashboard	36
5.2.1	The visits table	36
5.2.2	Table columns and actions	37
5.3	Receptionist	39
5.3.1	Logging onto the Receptionist role	39
5.3.2	Searching and filtering visits	39
5.3.3	Registering visits	39
5.3.4	Approving and declining visits	40
5.3.5	Assigning physical credentials	41
5.3.6	Assigning mobile credentials	43
5.3.7	Deassigning credentials	44
5.3.8	Checking in and out without card	45
5.3.9	Adding, removing and exempting from the blacklist	46
5.3.10	Maintaining visitor profiles	46
5.3.11	Viewing visit records	47
5.4	Host	47
5.4.1	Logging onto the Host role	47
5.4.2	Searching and filtering	47
5.4.3	Registering visits	48
5.4.4	Copying visit appointments	48
5.5	Visitor	49
5.5.1	Introduction to Kiosk mode	49
5.5.2	Creating a visitor profile: Self check-in	49
5.6	Authorizing installers of mobile access readers	50
5.6.1	Resetting Mobile Access readers	51
5.7	Using the Mobile Access apps on mobile devices	51
5.7.1	Setting RSSI thresholds in the Setup Access app	51
	<b>Glossary</b>	<b>53</b>

# 1 Introduction

## 1.1 Functionality change log

VisMgmt version	Added functionality	AMS version	BIS version
1.0	n/a	3.0.1	4.9
1.0.1	Checking visitors in and out without cards Searching for the numbers of free cards Distinguishing between different hosts with the same name (Performance enhancement) Finer granularity of dialog refresh	4.0	4.9.1
5.0	Support for mail server Support for HID Omnikey readers Customizable company logos	5.0	tbd
5.0.1	Support for Mobile Access Pre-assigning mobile credentials	5.0.1	tbd

## 1.2 About Bosch Visitor Management

Visitor Management, hereafter referred to as VisMgmt is a browser-based software tool that operates in tandem with Bosch access control systems. It manages visits to an access-controlled site, including the scheduling of visits, the professional data of the visitor, associated documents and contracts, and the assignment of temporary credentials. The user interface is customizable, and any user may change its language on-the-fly without logging out.

The primary users and their use cases are:

User type	Use cases
Receptionist	Registering new visits and visitors Approving and declining visits Blacklisting visitors Assigning and deassigning visitor cards Managing associated documents Monitoring the number of visitors on site
Visitor	Self-registration and pre-registration Creating and maintaining a visitor profile Signing documents
Host	Managing schedules and lists of visits and visitors Pre-registering visits
Administrator	Making global settings Customizing the behavior of the tool and its user interface Plus: All the use cases of Receptionist

## 1.3 About Mobile Access

Mobile Access is access control of persons using virtual credentials stored on a mobile device such as the person's smartphone. The virtual credentials are maintained in the primary access control system or ACS .

- Operators of the ACS generate, assign and send these virtual credentials to persons via a cooperating web application such as Credential Management or Visitor Management.
- The holders of mobile credentials operate access control readers via Bluetooth from a mobile access app on their mobile devices.
- Installers of mobile access systems configure access control readers via Bluetooth from a special setup app on their mobile devices.
- The system stores no personal data on mobile devices.

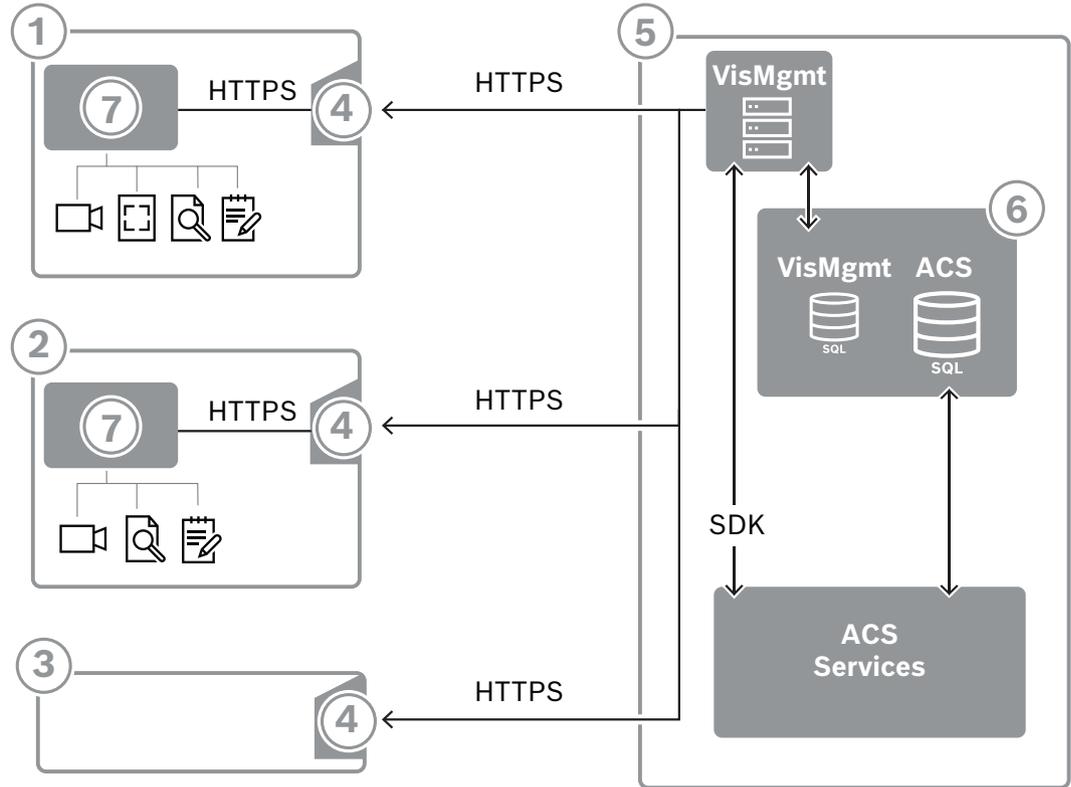
## 1.4 Intended audiences

- Installers and administrators of VisMgmt
- The main user types of VisMgmt

## 1.5 How to use this documentation

- Use the **Search** function in your help viewer to locate relevant content.
- The **system overview, installation** and **configuration** sections are primarily of interest to system administrators
- The **operation** sections are primarily of interest to system users.

## 2 System overview and topology



Label	Description
1	The <b>Receptionist</b> workstation. This workstation can have optional peripheral hardware, such as an enrollment reader, web camera, and scanners for signatures and documents.
2	The <b>Visitor</b> kiosk workstation, with supported browser in kiosk mode. This workstation can have optional peripheral hardware, such as a web camera and scanners for signatures and documents.
3	The <b>Host</b> workstation, that is, the workstation of the employee who receives the visitor.
4	Supported browser with the VisMgmt website
5	The ACS server (BIS or AMS)
6	The database instance of the ACS server (This can be on a separate computer).
7	The optional <b>Bosch Peripheral Device add-on</b> , which manages communication between the browser and peripheral hardware.

The recommended system topology has the VisMgmt server on the same computer as that of the main access control system, and its database on the same database instance.

The Bosch Peripheral Device add-on is installed only on those workstations that require access to peripheral devices.

The host workstation usually requires only browser access to the VisMgmt server.

## 3 Installing and uninstalling

### 3.1 Software and hardware requirements

Install VisMgmt server on the same computer as the main access control system: the same software and hardware requirements apply.

#### Server requirements

Operating systems	Windows 10, Windows Server 2016, Windows Server 2019
Database management systems	MS SQL Server 2019 and later Always use the same database instance as that of the ACS (the primary access control system)
Supported browsers	Google Chrome, Mozilla Firefox, Microsoft Edge (Chromium based) Use the most recent version of the browser for your Windows operating system.
Minimum monitor resolution (for using the application UI)	Full HD 1920x1080

#### Requirements for the Bosch Peripheral Devices add-on

The **Bosch Peripheral Devices add-on** is the program that handles the electronic communication between the browser and peripheral devices such as enrollment reader, web camera, signature scanner and document scanner.

The client computer is the computer that is physically connected to the peripheral hardware. It also runs the browser that connects to the VisMgmt server.

Although the peripheral devices are not strict requirements for installation, they are urgently recommended, as they greatly increase the efficiency of the visitor registration process.

Requirement	Description
Minimum monitor resolution	Full HD 1920x1080
Supported browsers	Google Chrome, Mozilla Firefox, Microsoft Edge (Chromium based) Use the most recent version of the browser for your Windows operating system.

#### 3.1.1 The main access control system

##### Without Mobile Access

If Mobile Access is not required VisMgmt version 5.0.1 works with the following Bosch access control systems:

- Access Management System (AMS) versions 5.0 and later

##### With Mobile Access

If Mobile Access is required VisMgmt version 5.0.1 works with the following Bosch access control systems:

- Access Management System (AMS) versions 5.0.1 (includes a Mobile Access extension) and later

Complete and verify the installation of the main access control system, according to its own installation guide, before proceeding with the installation of VisMgmt .

### 3.1.2 A database instance to host the Visitor Manager database

The installation of the main access control system creates a database instance which you can use to host the VisMgmt database, *dbVisitorManagement*.

The default name of this instance varies, depending on the ACS

- For AMS the name is *ACE*
- For BIS ACE the name is *BIS\_ACE*

### 3.1.3 A dedicated user for local database access

The user *VMUser* accesses the Visitor Manager database on behalf of the VisMgmt application. The VisMgmt server installation program creates a Windows user *VMUser* on the VisMgmt server.

### 3.1.4 A dedicated user for remote database access

If VisMgmt is to use a database on a remote database server, create and configure the *VMUser* user in Windows and on the SQL Server as described below.

IMPORTANT: Do not run the VisMgmt setup before completing this procedure.

1. On the remote database server create a Windows user with the following settings:
  - **Username** (case sensitive): *VMUser*
  - **Password**: Set the password according to the security policies that apply to all your computers. Note it carefully as it will be required for the VisMgmt setup.
  - **Member of group**: *Administrators*
  - **User must change password at next logon**: *NO*
  - **User cannot change password**: *YES*
  - **Password never expires**: *YES*
  - **Logon as a service**: *YES*
  - **Account is disabled**: *NO*

(Add *VMUser* as a login to remote the SQL Server)

1. Open SQL Management Studio
2. Connect to the remote SQL instance
3. Go to **Security > Login**
4. Add the user *VMUser* with server role *sysadmin*

Later, when you execute the VisMgmt setup on the VisMgmt server, you will select the option for **remote database server** computer and enter the password that you defined above for *VMUser*.

### 3.1.5 A dedicated user in the main access control system

1. In the main access control system, create a user that has the feature **unlimited API usage**.  
For detailed instructions, see the chapter **Assigning user (operator) profiles** in the operator manual of the main access control system.
2. Note the username and password carefully, because the VisMgmt installation wizards will require them.

## 3.2 Installing the Server

Do not start the setup program until you have provided all the software requirements.

### 3.2.1 Running the server setup program

1. On the intended VisMgmt server, as Administrator, run `BoschVisitorManagementServer.exe`.
2. Click **Next** to accept the default installation package.
3. If you agree with the End User License Agreement (EULA), accept it and click **Next**.
4. Select the destination folder for the installation. The default folder is recommended.
  - On the **SQL Server configuration** screen
5. Select whether you wish to create the database on the local SQL server instance, that is on the database instance on the VisMgmt server, or on a remote database server computer.
  - **Note:** If you choose a remote database server, the setup program prompts for the password of `VMUser`, the administrator user that you set up on the remote database server (see section Software requirements).
6. Check and, if necessary, modify the values for the following parameters:

<b>SQL server</b>	The name of the database server computer
<b>SQL instance</b>	The name of the instance of the main ACS database. This is where the visitor database is created. For AMS the name is <code>ACE</code> For BIS ACE the name is <code>BIS_ACE</code>
<b>SQL user name</b>	The name of an administrator user of the instance, typically <code>sa</code>
<b>SQL password</b>	The password of this administrator user.

7. Click **Test connection** to test whether the database instance can be reached using the parameter values that you have entered. If the test fails, re-check the parameters.
8. Click **Next** to continue
  - On the **ACS access configuration** screen (where ACS refers to the main access control system, AMS or ACE)
9. Enter values for the following parameters:

<b>ACS host name</b>	The name of the computer where the ACS is running
<b>ACS user name</b>	The name of the dedicated user of the ACS, with unlimited API usage. See section Software requirements.
<b>ACS password</b>	The password of this dedicated ACS user.

10. Click **Next** to continue
  - On the **Identity server configuration** screen
11. Enter the URI of the corresponding ACS identity server:
  - AMS: `HTTPS://<NameOfACSserver>:44333`
  - BIS: `HTTPS://<NameOfACSserver>/BisIdServer`
12. Click **Test connection** to test whether the identity server is reachable.
13. Click **Next** for the summary screen, then click **Install** to start the installation of the VisMgmt server.
14. After installation, reboot the computer.

### 3.2.2 Appsettings JSON file

A number of configuration parameters for the VisMgmt server are stored in the following .JSON file:

```
<installation drive>:\Program Files (x86)\Bosch Sicherheitssysteme\
Bosch Visitor Management\appsettings.json
```

It is generally not necessary to change the default values, but it may be beneficial to adjust the following parameters in the **Settings** section of the file. If you do adjust parameters, make a backup copy of the file first. The backup will help you revert changes quickly if your changes cause a malfunction.

Save your changes and restart the VisMgmt Windows service to put the changed parameters into effect. The name of the service is *Bosch Visitor Management*.

Parameter name	Default value	Description
<i>PageSizeNumberOfVisit</i>	20	The maximum number visit records that appear on the screen at one time. As the user scrolls, each new page is filled with this number of records, loaded from the database.
<i>MaximumUploadFileSizeBytes</i>	31457289	The maximum number of bytes that an uploaded file may contain.
<i>StartoverTimeoutAskSeconds</i>	300	The application waits this number of seconds if the user pauses during the input of login information, then it prompts for input.
<i>StartoverTimeoutResetSeconds</i>	60	After prompting, the application waits this number of seconds before resetting the login screen.

### 3.3 Setting up the VisMgmt client computer

The Bosch Peripheral Devices add-on can be installed on the server computer, but is usually installed on a client computer in the same network. If so, copy the HTTPS certificate from ACS server and install it on the client computer also. See *Certificates for secure communication, page 13* below for instructions.

The Bosch Peripheral Devices add-on is the connecting software for devices such as enrollment readers and scanners. If such devices are not required, for example for the host user, then browser access is enough to log in and run the VisMgmt application.

The following enrollment readers and card formats are supported.

	MIFARE DESfire Ev1 Bosch Code	MIFARE DESfire Ev1 CSN	MIFARE Classic CSN	iCLAS S 26 bit	iCLAS S 35 bit	iCLAS S 37 bit	iCLAS S 48 bit	HID Prox 26 bit	EM 26 bit
LECTUS enroll ARD- EDMCV0 02-USB	X								
OMNIKEY 5427 CK		X	X	X	X	X	X	X	X

**Refer to**

- *Certificates for secure communication, page 13*

**3.3.1****Setting up the Peripheral Devices add-on**

The Peripheral Devices add-on is required only on those client computers that connect to enrollment readers, scanners or other peripheral devices. Repeat the procedure below on each client computer that has this requirement.

- On the intended client computer, as Administrator, run *BoschPeripheralDeviceAddon.exe* from the installation medium.
  - The core components are listed, that is, the client software and the software for the usual peripheral devices. We recommend that you install all the listed components, even if you do not currently have the hardware available.
- Click **Next** to accept the default installation packages.
- On the **Client configuration** screen
  - **Installation directory:** Accept the default (recommended), or change as required.
  - **COM port:**
    - If using a LECTUS enroll reader, enter the number of the COM port, for example *COM3*, to which the enrollment reader is connected. Verify this value in the Windows device manager.
    - If using an HID OMNIKEY reader, leave this field blank.
    - The camera, Signopad and document scanner are "plug-and-play" and require no COM port. Click **Allow** when the browser prompts for permission to connect.
  - **Server address and Port:**
    - Enter the name of any server computers, by default at least the primary ACS server computer, and the port numbers for any backend services that need to control the peripheral devices.  
In each case, click **Test Connection** and await confirmation.  
Click **Add** to add further servers.  
Click **Delete** to remove servers.
    - The default ports for the usual backend services are:  
*5806* for CredMgmt  
*5706* for VisMgmt
- Click **Next** for a summary of the components to be installed.
- Click **Install** to start the installation.
- Click **Finish** to finish the installation.

7. After installation, reboot the computer.

### 3.3.2 Certificates for secure communication

For secure communication between the browser on the client machine and the ACS server, copy the following certificate from the ACS server to the client computers. Use an account with Windows administrator rights to install it.

The usual path to the certificate is:

- <installation drive> :  
`\Bosch Sicherheitssysteme\Access Management System\Certificates\Bosch Security System Internal CA - BISAMS.cer`

#### Overview of certificate transfers

To → From ↓	ACS	MA Mobile Access backend	DB Data- base	S Setup app	M Cardholder access app	R Reader
ACS	/	Transferred by setup wizard (by means of cert tool)	/	/	/	/
MA Mobile Access backend	Transferred by MA setup wizard	/	/	Transferred by QR code enrollment  Updated via push notification	Transferred by QR code enrollment  Updated via push notification	/
DB Database	/	/	/	/	/	/
S Setup app	/	Transferred by QR code enrollment	/	/	/	/
M Cardholder access app	/	Transferred by QR code enrollment	/	/	/	/

#### 3.3.2.1 Certificates for the Firefox browser

You may ignore this section if you are not using the Firefox browser.

The Firefox browser handles root certificates differently: Firefox does not consult the Windows certificate store for trusted root certificates. Instead, each browser profile maintains its own root certificate store. For more details, refer to <https://support.mozilla.org/en-US/kb/setting-certificate-authorities-firefox>

This webpage also offers instructions for forcing Firefox to use the Windows certificate store for all users.

Alternatively, you can import the default certificates as described below. Note:

- You must import the certificates for each user and Firefox profile.
- The server certificate described below is the default certificate created by the installation. If you have purchased your own certificate from a Certificate Authority, then you can use that instead.

### Importing certificates into the Firefox certificate store

To access the ACS server from Firefox on the client computer, you can import the following default certificate from the server:

- <installation drive> :  
`\Bosch Sicherheitssysteme\Access Management System\Certificates\Bosch Security System Internal CA - BISAMS.cer`

Or, for BIS ACE, you can also download the certificate through the web:

- `HTTP://<Hostname>/<Hostname>.cer`

**Peripheral devices:** To access a connected peripheral device, such as a document or signature scanner, from Firefox on the client computer, you can use the default certificate. You can find it on the client computer at the following location:

<installation drive>:\Program Files (x86)\Bosch Sicherheitssysteme\  
Bosch Peripheral Device Addon\BoschAcePeripheralDeviceAddonHardware CA.cer

### Procedure (repeat for each certificate and Firefox profile):

Use the following procedure on the client computer to install the certificates you require:

1. Locate the certificate that you want to install.
2. Open Firefox browser and type `about:preferences` in the address bar.
  - An options page opens.
3. In the **Find in Options** field, type `certificate`
  - The **View Certificates** button appears on the page.
4. Click the **View Certificates** button.
  - The **Certificate Manager** dialog opens with several tabs
5. Select the **Authorities** tab.
6. Click **Import...**
  - A certificate selector dialog opens.
7. Select the certificate you located in step 1, and click **Open**.
  - The **Downloading Certificate** dialog opens.
8. Select **Trust this CA to identify websites** and click **OK**.
  - The **Downloading Certificate** dialog closes
9. In the **Certificate Manager** dialog, click **OK**.
  - The certificate import procedure is finished.

### 3.3.2.2

#### Certificates for the Chrome browser

You may ignore this section if you are not using the Chrome browser.

Please consult the release notes of your ACS for changes to certificate handling in the Chrome browser.

### 3.3.3 Appsettings JSON file

A number of configuration parameters for the VisMgmt client computer are stored in the following `.JSON` file:

```
<installation drive>:\Program Files (x86)\Bosch Sicherheitssysteme\
Bosch Visitor Management\appsettings.json
```

It is generally not necessary to change the default values, but it may be beneficial to adjust the following parameters in the **AppSettings** section of the file.

Save your changes and restart the VisMgmt Windows service to put the changed parameters into effect. The name of the service is *Bosch Ace Visitor Management Client*

Parameter name	Example	Description
<code>CorseOrigins</code>	<code>"https://my-vm-server:5706"</code>	The address and port number of the Visitor Management server.
<code>CardReaderPort</code>	<code>"com3"</code>	The COM port number to which a LECTUS enrollment reader is connected. For HID OMNIKEY readers this parameter can be blank.

## 3.4 Verifying server installation

From a computer in the same network, using one of the supported browsers, open the following URL:

```
https://<VisMgmt server computer>:5706/main
```

If the server is running, it displays the application login page.

## 3.5 Installing Mobile Access

### Introduction

The Bosch Mobile Access backend service provides mobile access functionality for both Credential Management and Visitor Management.

**NOTE:** If you are using both CredMgmt and VisMgmt then you need install Mobile Access only once.

- You can install it on the same server as the ACS (co-located installation), or on a separate server (distributed installation).
- You can install it to use either a local or a remote database.

### Reachability of the Mobile Access backend service

The Mobile Access backend service must be continuously reachable for the mobile devices. For security reasons it is very unlikely that mobile devices will have network access to an ACS server. Therefore, distributed installation is recommended. This allows you to run the mobile access backend service on a more widely available "cloud" server.

### 3.5.1 Overview of installation, configuration, and use

Mobile Access requires several components to work in concert. We list the overall stages here, and describe their respective prerequisites and procedures in the following sections of this chapter:

### Setting up the ACS server

1. An ACS is installed, licensed and running, with a permanent root certificate and compatible access readers. Operators are defined in it with authorizations to manage Mobile Access.

### Setting up Mobile Access

1. A system administrator installs one or both of the web applications that use Mobile Access, either Credential Management or Visitor Management on the ACS.
2. A system administrator installs the Mobile Access backend.
3. A system administrator activates Mobile Access in those web applications that are installed.

### Setting up the readers

1. A system administrator creates an installer (a person authorized to configure Mobile Access readers) in the CredMgmt application.
2. The installer downloads the installer app ("Setup Access") to his mobile device from the device's usual public app store.
3. A system administrator sends an invitation to the designated installer.
4. The installer accepts the invitation in the installer app. This invitation authorizes the installer to configure access readers for Mobile Access.
5. The installer configures the readers by use of the installer app.

### Using Mobile Access

1. Credential holders who are eligible to use mobile access download the credential holder app ("Mobile Access") to their mobile devices from the device's usual public app store.
2. CredMgmt and/or VisMgmt operators send mobile credentials by QR-code or email to the eligible credential holders.
3. The credential holders read the QR-code or Email in their credential holder ("Mobile Access") app. This enables their mobile device to function as a physical credential when the app is running.

## 3.5.2

### Mobile Access hardware prerequisites

Mobile Access requires access readers with a BLE module. The following Bosch readers are suitable:

- ARD-SELECT -BOM, -WOM, -BOKM, -WOKM
- B and W signify the color, black or white
  - O signifies OSDP
  - K signifies the presence of a keypad
  - M signifies suitability for Mobile Access

## 3.5.3

### Mobile Access configuration prerequisites

#### Dedicated user for a remote database (if you are using a remote database)

If Mobile Access is to use a database on a remote database server, then create and configure an administrator user named *MAUser* on that remote server, both in Windows and on the SQL Server. During the setup described below, select the option for remote database server and enter the password that you defined for *MAUser*.

IMPORTANT: Do not run the Mobile Access setup before completing this procedure.

#### Procedure

1. On the remote database server, create a domain Windows user in the same domain as the ACS . Use the following settings:
  - **Username** (the username itself is case sensitive): <ACS-Domain>\MAUser
  - **Password**: Set the password according to the security policies that apply to all your computers. Note it carefully as it will be required for the Mobile Access setup.
  - **User must change password at next logon**: NO
  - **User cannot change password**: YES
  - **Password never expires**: YES
  - **Logon as a service**: YES
  - **Account is disabled**: NO

Then add MAUser as a login to remote the SQL Server as follows:

1. Open SQL Management Studio
2. Connect to the remote SQL instance
3. Go to **Security > Login**
4. In the **Select a page** pane, select **General**
5. Select user MAUser
6. In the **Select a page** pane, select **Server roles**
7. Select the check boxes *public* and *dbcreator*

**A dedicated user for the local database (if you are using a local database)**

The user MAUser accesses the ACS database on behalf of the Mobile Access.application. You do NOT need to create this user if you are using a local database. The Mobile Access setup program creates a Windows user MAUser on the ACS server automatically.

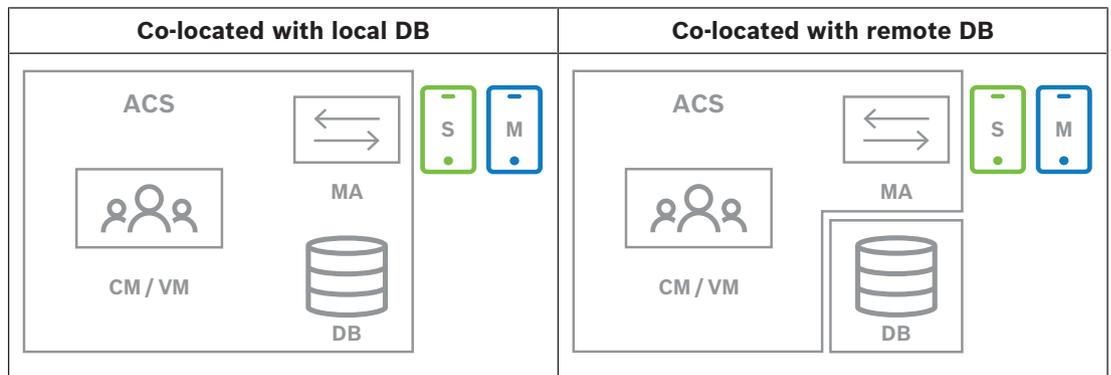
**3.5.4**

**Procedure for co-located installation**

**Co-located installation** means that the Mobile Access Backend service runs on the same server.as the ACS.

**Distributed installation** means that the Mobile Access Backend service runs on a different server, for example a "cloud server".

For the distributed option, consult the next section **Procedure for distributed installation.**



Key	Meaning
ACS	The primary access control system, AMS or BIS-ACE
CM/VM	Backend for the web application: Credential Management or Visitor Management
DB	Main ACS database
MA	Mobile Access backend

Key	Meaning
S	"Setup Access" installer app for mobile devices of system installers and configurers
M	"Mobile Access" access app for mobile devices of normal credential holders.

### Procedure

1. On the ACS server, which for co-located installations is also the Mobile Access server, run *BoschMobileAccessBackend.exe* as Administrator
  - The setup program opens
2. On the **Location** screen select the type of setup: **Co-located**
3. On the **Components** screen, verify that *Bosch Mobile Access* is selected, and click **Next**
4. On the **EULA** screen, read carefully and click **Accept** if you wish to accept the End User License Agreement (EULA). The installation can only proceed if you do this.
5. On the **Installation directory** screen:
  - Browse and select a destination folder for the installation, or accept the default (recommended)
  - Enter your company name as it is to be displayed in the mobile app and in HTML email templates
  - Click **Next**
6. On the **Certificate** screen
  - Enter the host name where the Mobile Access Backend is to run
  - If desired, or if the network provides no hostname resolution, enter the IP address of that host
  - Click **Next**
7. On the **SQL Server** screen, select one of two alternatives for the location of the database. The configurations are slightly different. Choose one alternative for the next step:
  - ALTERNATIVE 1 **Local database** option:
    - The setup program finds local database and preselects it.
    - Enter SQL password for an admin user (default is *sa*)
    - Click **Test Connection**
    - Click **Next**
  - ALTERNATIVE 2 **Remote database** option
    - Enter name of SQL server that is on the network
    - Enter the name of the SQL instance
    - Enter SQL password for an admin user (the default is *sa*)
    - Click **Test Connection**
    - Check the username and enter the password of the Windows and SQL administrator user that you created for remote database usage (see Prerequisites above)
    - Click **Next**
8. On the **Identity server configuration** screen
  - The default identity server (preselected) is the primary ACS server with port *44333*  
*https://<NameOfACSserver>:44333*
  - Click **Test Connection**
  - If the test fails, re-check the availability of the Identity server.
  - Click **Next**
9. On the **Core Components** screen, confirm that **Bosch Mobile Access** is selected and click **Install**
  - The installation wizard completes

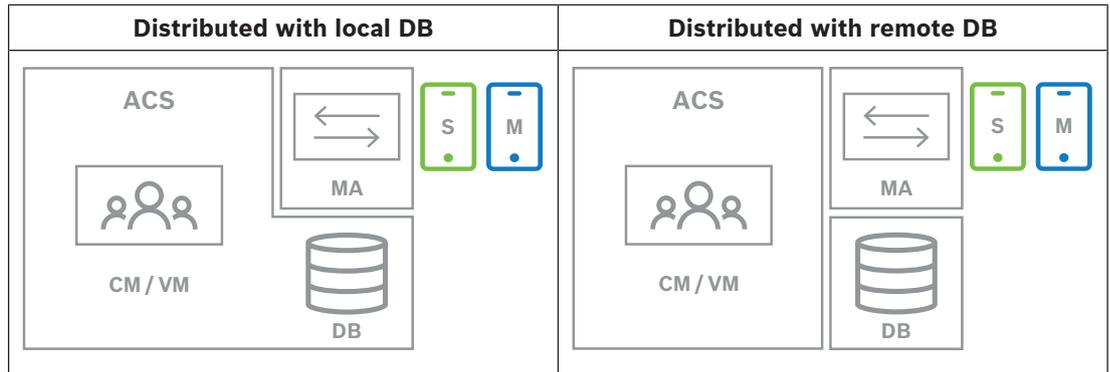
10. Click **Next**
11. On the **Core Components** screen, verify that the installation completed successfully, and click **Finish**
12. In the Windows *Services* application, verify that the service *Bosch Mobile Access* is running.

### 3.5.5 Procedure for distributed installation

**Co-located installation** means that the Mobile Access Backend service runs on the same server as the ACS.

**Distributed installation** means that the Mobile Access Backend service runs on a different server, for example a "cloud server".

For the co-located option, consult the previous section **Procedure for co-located installation**.



Key	Meaning
ACS	The primary access control system, AMS or BIS-ACE
CM/VM	Backend for the web application: Credential Management or Visitor Management
DB	Main ACS database
MA	Mobile Access backend
S	"Setup Access" installer app for mobile devices of system installers and configurers
M	"Mobile Access" access app for mobile devices of normal credential holders.

**Procedure**

1. On the Mobile Access Backend server, run *BoschMobileAccessBackend.exe* as Administrator
  - The setup program opens
2. On the **Location** screen select the type of setup: **Distributed**
3. On the **Host** screen, select **Mobile Access Backend** and click **Next**
  - Note: the **ACS** option will be used later in this procedure, when we install mobile access on the ACS server.
4. On the **Components** screen, verify that **Bosch Mobile Access** is selected, and click **Next**
5. On the **EULA** screen, read carefully and click **Accept** if you wish to accept the End User License Agreement (EULA). The installation can only proceed if you do this.
6. On the **Installation directory** screen:
  - Browse and select a destination folder for the installation, or accept the default (recommended)

- Enter your company name as it is to be displayed in the mobile app and in HTML email templates
- Click **Next**
- 7. On the **SQL Server** screen, select one of two alternatives for the location of the database. The configurations are slightly different. Choose one alternative for the next step:
  - ALTERNATIVE 1 **Local database** option:
    - The setup program finds local database and preselects it.
    - Enter SQL password for an admin user (default is *sa*)
    - Click **Test Connection**
    - Click **Next**
  - ALTERNATIVE 2 **Remote database** option
    - Enter name of SQL server that is on the network
    - Enter the name of the SQL instance
    - Enter SQL password for an admin user (the default is *sa*)
    - Click **Test Connection**
    - Check the username and enter the password of the Windows and SQL administrator user that you created for remote database usage (see Prerequisites above)
    - Click **Next**

*At this point in the Distributed installation, you must switch to the computer where the ACS server is running and configure mobile access there, so that it can later communicate with the mobile access backend on the local computer.*

*After you have done the steps indicated there, the setup program will guide you back to the local server to confirm and proceed.*

1. On the ACS server computer, run *BoschMobileAccessBackend.exe* as Administrator
  - The setup program opens
2. On the **Location** screen select the type of setup: **Distributed**
3. On the **Host** screen, select **ACS** and click **Next**
4. On the **Companion wizard** screen, read the explanatory text and click **Next**
5. On the **Certificate** screen
  - Enter the host name where the Mobile Access Backend is to run
  - If desired, or if the network provides no hostname resolution, enter the IP address of that host
  - Click **Next**
6. On the **Identity server configuration** screen
  - The default identity server (preselected) is the primary ACS server with port *44333*  
*https://<NameOfACSserver>:44333*
  - Click **Test Connection**
  - If the test fails, re-check the availability of the Identity server.
  - Click **Next**
7. On the **Create file** screen
 

Here we create a configuration file in a password-protected ZIP file, make it available to the Mobile Access Backend.

  - **User password:** Enter a password for the ZIP file
  - **Configuration file:** Enter or browse to a folder in which to place the ZIP file. Note that this folder should be accessible to the computer where the Mobile Access Backend is running. If not, you must transfer the ZIP file to that computer by other means.
  - Click **Create configuration file**

- Click **Next**
- 8. On the **Switch machine** screen  
The installation steps on the ACS server are now complete.
- Click **Confirm** to end the procedure

*At this point in the Distributed installation, you return to the setup program on the mobile access backend computer.*

1. Return to the setup program *BoschMobileAccessBackend.exe* on the Bosch Mobile Access server computer.
2. On the **Switch machine** page
  - select the check box labeled **I have already completed the required steps on the ACS machine**
  - Click **Next**
3. On the **Upload file** screen
  - **Upload configuration file:** Select the configuration file that you created on the ACS server
  - **Password verification:** Enter the password that you set for the ZIP file on the ACS server
  - When you have entered the correct password, you can click **Next** to read the configuration file
4. On the **Core Components** screen, confirm that **Bosch Mobile Access** is selected and click **Install**
  - The installation wizard completes
5. Click **Next**
6. On the **Core Components** screen, verify that the installation completed successfully, and click **Finish**
7. In the Windows *Services* application, verify that the service *Bosch Mobile Access* is running.

## 3.6 Installing the Mobile Access apps

### Introduction

Bosch provides the following apps for mobile access

- Bosch Mobile Access: A cardholder app to store virtual credentials and transmit them via Bluetooth to those readers that are configured for mobile access. Such a reader then grants or denies access depending on whether one of the app's stored credentials is valid for it.
- Bosch Setup Access: An installer app for scanning and configuring the readers via Bluetooth.

Authorized operators of Visitor Management and Credential Management can send virtual credentials for both cardholder and installer apps.

As long as the cardholder app is running and Bluetooth is activated on the mobile device, you can use it as if it were a physical card. There is no need to give commands from the app or even to unlock the screen.



### Notice!

**IMPORTANT:** Do not operate the cardholder and installer apps simultaneously  
Make sure that nobody uses the installer app when the cardholder app is in use, and vice versa.

**Procedure**

The Bosch mobile access apps can be downloaded from Google and Apple app stores and installed in the usual way. Their names in the app stores are:

- Bosch Mobile Access
- Bosch Setup Access

### 3.7 Peripheral hardware

The following peripheral USB devices have been tested and approved for use with VisMgmt and CredMgmt at the time of writing. For a continually updated list of compatible devices, consult the datasheet of the main access control system.

Card enrollment reader	LECTUS enroll ARD-EDMCV002-USB, HID OMNIKEY 5427 CK
Scanner for ID documents	ARH Combo, ARH Osmond
Signature scanner	signotec LITE, signotec Omega

Follow the manufacturer's instructions to connect these devices to your client computers.

**Enrollment readers**

The following enrollment readers and card formats are supported.

	MIFARE DESfire Ev1 Bosch Code	MIFARE DESfire Ev1 CSN	MIFARE Classic CSN	iCLAS S 26 bit	iCLAS S 35 bit	iCLAS S 37 bit	iCLAS S 48 bit	HID Prox 26 bit	EM 26 bit
LECTUS enroll ARD-EDMCV002-USB	X								
OMNIKEY 5427 CK		X	X	X	X	X	X	X	X

#### 3.7.1 Registering peripheral hardware with the client computer

To register peripheral hardware with the VisMgmt client computer, run the Bosch Peripheral Devices setup program, *BoschPeripheralDeviceAddon.exe*, on the client. For instructions see *Setting up the Peripheral Devices add-on, page 12*.

**Refer to**

- *Setting up the Peripheral Devices add-on, page 12*

## 3.8 Repair installations of Mobile Access

### Introduction

In order to update the binaries, or to recreate the Mobile Access certificate, you can run the installer of the current or a later version of Mobile Access, over an existing installation:

### Procedure

1. On the Mobile Access backend server, run the new version of *BoschMobileAccessBackend.exe* as Administrator.
  - Note that for co-located installations the Mobile Access backend server is the same as the ACS server.
2. Follow the setup wizard, making the same settings as in the original installation.
  - To re-create the certificate, on the **Certificates** screen select the radio button **Re-create certificate**.
3. After the setup program has completed, start a fresh logon session on each web application that is using Mobile Access (CredMgmt or VisMgmt or both).
  - The web application will be using the new binaries.
  - If you selected **Re-create certificate**, any further invitations that you send to Mobile Access users and installers will be based on the new Mobile Access certificate.

## 3.9 Uninstalling the software

To uninstall the software from the server or client:

1. With Windows administrator rights, start the Windows program **Add or remove programs**.
2. Select the program (server or client) and click **Uninstall**.
3. (For visitor management, and on the server only) Select whether you want to remove the visitor management database as well as the program.
  - **Note:** The database contains records of all the visits that were registered while the program was in use. You may wish to archive the database or transfer it to another installation.
4. Select whether you want to remove the log files.
5. Complete the uninstallation in the usual way.
6. (Recommended) Reboot the computer to ensure complete modification of the Windows registry.

## 4 Configuration

### 4.1 Creating Visitor Management users in the ACS

#### Introduction

Every Administrator, Receptionist or Host user of VisMgmt must be a cardholder with a separate Operator definition in the ACS, that is, the main access control system.

These Operator definitions contain special VisMgmt rights in the form of **User profiles**. See the online help in your ACS for detailed information and instructions regarding **User profiles**.

- You must define a separate Operator for each cardholder who works in Visitor management. You cannot assign multiple cardholders to the same Operator.



#### Notice!

IT security and user accounts

In accordance with best practices for IT security, we recommend that each Receptionist, Host and Administrator user work under his own Windows account.

#### Creating User profiles for Visitor management

1. Log onto the main access control system with administrator privileges.
2. Create one or more user (operator) profiles for VisMgmt users.

Dialog path:

3. Assign one of the following user rights to these profiles.
  - Administrator: *Visitor Management > Administrator*
  - Host: *Visitor Management > Host*
  - Receptionist: *Visitor Management > Receptionist*

When you have created the user profiles that you require for the various VisMgmt roles (Administrator, Receptionist, Host), you can assign each profile to multiple Operators.

#### Assigning User profiles to ACS operators and cardholders

Dialog path:

1. Add a new operator type (Click  or , depending on the ACS) and give it a name that clearly relates to one of the VisMgmt roles (Administrator, Host or Receptionist).
2. On the tab **General operator settings**, select *Operator ACE* from the Authorization list.
3. On the tab **ACE operator settings**, use the arrow buttons to assign the **ACE user profile** that you created above.
 

Deassign the default profile *UP-Administrator*, except in the unlikely case that the cardholder requires general administrator rights in the ACS.
4. Still on the tab **ACE operator settings**, use the **Assign person** pane to find the cardholder in the system who is to have the VisMgmt role.
5. Click **Assign person** to complete the assignment to the selected cardholder.
  - You must define a separate Operator for each cardholder who works in Visitor management. You cannot assign multiple cardholders to the same Operator.

### 4.2 Creating Visitor authorizations and profiles in the ACS

#### Introduction

The receptionist or administrator of the VisMgmt system selects for each new visitor a **Visitor type**. This visitor type is based on a predefined **Person type** called **Visitor** in the main access control system (ACS), or on a subtype of **Visitor** that the administrators of the ACS have created.

These administrators must also configure the Person type **Visitor** and its subtypes in the ACS with access profiles. The access profiles allow these person types to operate real doors on the site.

### 4.3 Setting up the Receptionist computer

The receptionist's computer runs the **Bosch Peripheral Devices** add-on, which allows it physical connections to peripheral devices for reading cards, scanning ID documents and scanning signatures.

Connect all required peripheral devices before installing the client software.

Make sure that the computer and its peripheral devices are adequately protected from unauthorized access.

### 4.4 Setting up a kiosk computer for Visitors

#### Introduction

Visitors typically register their visits, and create their own profiles, at a computer that is freely accessible in the reception area of the access-controlled site. For security reasons, the computer's web browser runs in kiosk mode, which allows access only to VisMgmt, and not to multiple tabs, browser settings, or the computer's operating system. All the supported browsers offer kiosk mode, but its exact configuration depends on the browser.

The kiosk computer runs the **Bosch Peripheral Devices** add-on, which allows it physical connections to peripheral devices for scanning ID documents and signatures.

- The URL for kiosk mode is `https://<My_VisMgmt_server>:5706`

#### Configuring browsers for kiosk mode

The following links describe the configuration of kiosk mode for browsers supported by VisMgmt

	Instructions for setting up kiosk mode
<b>Chrome</b>	<a href="https://support.google.com/chrome/a/answer/9273974">https://support.google.com/chrome/a/answer/9273974</a>
<b>Firefox</b>	<a href="https://support.mozilla.org/en-US/kb/firefox-enterprise-kiosk-mode">https://support.mozilla.org/en-US/kb/firefox-enterprise-kiosk-mode</a>
<b>Edge</b>	<a href="https://docs.microsoft.com/en-us/deployedge/microsoft-edge-configure-kiosk-mode">https://docs.microsoft.com/en-us/deployedge/microsoft-edge-configure-kiosk-mode</a>



#### Notice!

For security reasons, always disable the browser option for saving passwords automatically.

### 4.5 Logging on for configuration tasks

For configuration and administration tasks, use a computer that is physically protected from unauthorized access.

1. In your browser, enter the HTTPS address of the VisMgmt server followed by a colon and the port number (default 5706)  
`https://<My_VisMgmt_server>:5706/main`  
 The **Login** screen appears
2. Log on as a VisMgmt **Administrator** user.



3. Click  to open the **Settings** menu.

## 4.6 Using the Settings menu for configuration

The **Settings** menu contains subsections that let you perform the following configuration steps:

<b>General settings</b>	<ul style="list-style-type: none"> <li>– <b>Retention period (days):</b> This setting governs the handling of visit records. <ul style="list-style-type: none"> <li>– When the period elapses for the first time, the application anonymizes the record.</li> <li>– When the period elapses for the second time, the application deletes the record.</li> </ul> <p>Default value is <i>365</i>.</p> <p>Set <i>0</i> to deactivate the retention period completely. In this case visit records are retained indefinitely.</p> </li> <li>– <b>Document storage mode:</b> Select whether documents are to be stored as paper or digital files.</li> <li>– <b>Maximum number of visitors</b> allowed on the site at one time. Default value is <i>100</i>. Set <i>0</i> to deactivate the visitor counters on the dashboard completely.</li> <li>– <b>Document expiry period (days):</b> Enter how long uploaded documents, such as non-disclosure agreements (NDA) and Terms of Use, are to remain valid. The period applies to both paper and digital files. After this period, the documents are marked as expired in the visitor's profile (clock icon with a red dot). Default value is <i>365</i></li> <li>– <b>Document expiry warning period (days):</b> Enter the length of the warning period before the expiry date. During this warning period, documents are marked in the visitor's profile (clock icon with an orange dot). Before the warning period the clock icon has a green dot.</li> <li>– <b>Logo:</b> Select or clear the check boxes that govern whether the dialogs display a customized logo or the default logo; and whether to display the Bosch <b>supergraphic</b>. <ul style="list-style-type: none"> <li>– For criteria for customized logo files see: <i>Customizing the company logo, page 31</i></li> </ul> </li> <li>– Click <b>Preview</b> to show the dialog page as it would appear with these settings. See the next section for more details on Preview mode.</li> <li>– <b>Languages:</b> Select which languages are to be available in the user interface, along with their preferred <b>date</b> and <b>time</b> formats.</li> <li>– <b>Mail server</b> Enter the IP address, port number and account details of your email server, in order to enable the sending of emails from the application.</li> </ul>
-------------------------	---

	<ul style="list-style-type: none"> <li>- <b>Email templates</b> Several HTML email templates are provided, which you typically customize to your own requirements. For details, see the separate section <b>Email templates</b> below.</li> <li>- <b>Mobile Access</b> Select the <b>Mobile Access</b> check box to activate Mobile Access.  <b>Connection:</b> Enter the address of the mobile access server (registration service address). <code>https://&lt;MyMobileAccessBackendServer&gt;:5700</code> Use an (FQDN) for &lt;MyMobileAccessBackendServer&gt; in multi-domain environments.  <b>Note:</b> to use an IP address instead of an FQDN you must enter that IP address, under <b>Certificate creation</b>, when you run the setup wizard for the Mobile Access Backend.  <b>Installer onboarding:</b> Select the information that you require from installers, so that they can configure mobile access readers using the Bosch Setup Access.  Log off the web application and log on again in order to use the Mobile Access feature immediately.</li> </ul>
<b>Receptionist</b>	<ul style="list-style-type: none"> <li>- This settings screen contains 2 check boxes for each of the data fields in the receptionist's visitor registration dialogs.             <ul style="list-style-type: none"> <li>- Clear or select the first check box to govern whether the data field is <b>visible</b> at all the registration dialogs.</li> <li>- Clear or select the second check box (marked with an asterisk) to govern whether the data field is <b>mandatory</b>.</li> </ul> </li> <li>- Customize the default header texts in the data-collection dialogs. For more details, see <i>Customizing the UI, page 30</i> below.</li> </ul> <p><b>Special option: Enable check-in/check-out without card</b> If visitors have close escorts, or are restricted to public spaces, individual cards for visitors may be unnecessary. For such cases there exists the option of checking visitors in and out without cards. For security reasons this option is disabled by default. Select the check box to enable it:</p> <ul style="list-style-type: none"> <li>- <b>Note:</b> if the option is enabled then any <b>Visitor</b> who self-registers at the kiosk computer automatically approves and checks in their own visit at the same moment.</li> <li>- See the <b>Operation</b> chapter <i>Checking in and out without card, page 45</i> of this document for details on how a <b>Receptionist</b> user processes visitors without cards.</li> </ul>
<b>Host</b>	The settings for the <b>Host</b> and <b>Visitor</b> users remain read-only until you have edited and saved the settings for <b>Receptionist</b> .
<b>Visitor</b>	Fields that you mark as not visible in the <b>Receptionist</b> settings are automatically set not visible for <b>Host</b> and <b>Visitor</b> . After that, the configuration procedure is identical.

**Refer to**

- *Assigning physical credentials, page 41*
- *Customizing the UI, page 30*

**4.6.1****Email templates**

Several HTML email templates are provided, which you typically customize to your own company requirements. For each template, you can store mail addresses for CC, BCC and a test receiver, to whom you can send a test email immediately. When you download a template for editing, it is copied to the default downloads folder of your browser.

- *MobileAccess.html* An invitation for a cardholder to use smartphone-based credentials.
- *SetupAccess.html* An invitation for an installer to configure readers for mobile access.
- *VisitorInvite.html* An invitation for someone to visit your site, with the option to append an iCalendar file to the email.
- *InformHostAboutCheckin.html* An email to inform the host that a visitor has arrived.

**Placeholders for use in email templates**

The email templates provide several text placeholders for including database fields in the text. These placeholders are described in the following tables, according to the templates where they can be used.

**Mobile Access**

Email that is sent to a cardholder (for Mobile Access app) when mobile access is granted to them

Placeholder	Description
{{Title}}	person's title (Mr. Ms. Dr. etc.)
{{FirstName}}	person's first name
{{LastName}}	person's surname
{{CompanyName}}	person's company
{{QrcodeLink}}	QR-code corresponding to the link that offers the cardholder mobile access via the app
{{InviteLink}}	link that offers the cardholder mobile access via the app

**Setup Access**

Email that is sent to a mobile access installer (for the Setup Access app) when mobile access is granted to them for setting up readers

Placeholder	Description
{{Title}}	installer's title (Mr. Ms. Dr. etc.)
{{FirstName}}	installer's first name
{{LastName}}	installer's surname
{{CompanyName}}	installer's company
{{QrcodeLink}}	QR-code corresponding to the link that offers the installer mobile access for setting up readers via the Setup Access app

Placeholder	Description
{{InviteLink}}	link that offers the installer mobile access for setting up readers via the Setup Access app

**Visitor invitation**

Email that is sent to the visitor when a visit is created or edited.

Placeholder	Description
{{VisitorID}}	visitor's ID code, as generated by the VisMgmt application
{{Title}}	visitor's title (Mr. Ms. Dr. etc.)
{{FirstName}}	visitor's first name
{{LastName}}	visitor's surname
{{CompanyName}}	visitor's company
{{HostFirstName}}	host's first name
{{HostLastName}}	host's surname
{{ExpArrivalDate}}	planned date of visit

**Visitor Arrived**

Email that is sent to the host when the receptionist approves the visit

Placeholder	Description
{{VisitorID}}	visitor's ID code, as generated by the VisMgmt application
{{Title}}	visitor's title (Mr. Ms. Dr. etc.)
{{FirstName}}	visitor's first name
{{LastName}}	visitor's surname
{{CompanyName}}	visitor's company
{{HostFirstName}}	host's first name
{{HostLastName}}	host's surname
{{ExpArrivalDate}}	planned date of visit
{{ArrivalDate}}	actual date of visit

**Visitor Pass**

Document that can be printed out and given to a visitor. This could contain a map of the building or a checklist.

Placeholder	Description
{{VisitorID}}	visitor's ID code, as generated by the VisMgmt application
{{Title}}	visitor's title (Mr. Ms. Dr. etc.)
{{FirstName}}	visitor's first name

Placeholder	Description
{{LastName}}	visitor's surname
{{CompanyName}}	visitor's company
{{HostFirstName}}	host's first name
{{HostLastName}}	host's surname
{{ExpArrivalDate}}	planned date of visit
{{ArrivalDate}}	actual date of visit

## 4.6.2

### Preview mode

Certain sets of options provide a **Preview** button that activates preview mode, to let you to see the dialogs as they would appear when those options are set.

In preview mode, the following conditions apply:

- A banner appears at the top of the dashboard.

 **Preview mode. Any changes will not be applied. Close preview-mode or change role** 

- Changes made in the dashboard or menus are **not** saved.
- Click **Close preview mode** within the banner to close preview mode
- Use the **Change role** list within the banner to preview the appearance of the interface for the different user types.

## 4.6.3

### Document templates

For the various documents and emails, you can download templates, and upload customized versions of those templates, in the dialog **Dashboard > Settings > General**.

## 4.7

### Customizing the UI

Customize the user interface in the **Dashboard > Settings** dialogs,

## 4.7.1

### Setting options visible, invisible and mandatory

Select which data fields will be visible in the dialogs, and which of those data are mandatory.

Example:

<input checked="" type="checkbox"/>	①	<input checked="" type="checkbox"/> *
<input checked="" type="checkbox"/>	②	<input type="checkbox"/> *
<input type="checkbox"/>	③	<input type="checkbox"/> *

- (1) is visible and mandatory,
- (2) is visible but not mandatory
- (3) is not visible.

## 4.7.2

### Customizing kiosk mode

If your site lacks one or more peripheral hardware devices, for example a document scanner, you can customize the visitor's self-registration process in kiosk mode by clearing the check boxes for the corresponding registration steps.

### 4.7.3 Customizing the company logo

Graphic files that you upload for your company logo must meet the following criteria:

Supported formats	PNG, JPEG, JPG
Exact width (pixels)	125
Exact height (pixels)	63
Max. size (MB)	1

## 4.8 Firewall settings

Add auxiliary applications to the firewall configuration of server and client computers:

1. Start the Windows Firewall click Start > **Control Panel** > **Windows-Firewall**
2. Select **Advanced settings**
3. Select **Inbound Rules**
4. In the **Actions** pane, select **New Rule...**
5. In the **Rule Type** dialog, select **Port** and click **Next >**
6. On the next page, select **TCP and Specific local ports**
7. Allow communication through the following ports:
  - On the server computer or computers
    - <server name> : 44333 - used by the AMS Identity server
    - <server name> : 5706 - used by the VisMgmt server
    - <server name> : 5806 - used by the CredMgmt server
    - <server name> : 5700 - used by the Mobile Access backend server
  - On client computers
    - localhost:5707 - used by the Bosch Peripheral Device add-on

### Port usage within the system

Server Outgoing	Port Out	Server Incoming	Port In	Protocol	Comments
VisMgmt, or CredMgmt	*	Mobile Access backend	5700	HTTPS	Commands from the web application to create and/or delete mobile credentials
Mobile devices from Internet	*	Mobile Access backend	5700	HTTPS	Mobile devices receive mobile credentials via the internet
Mobile Access Backend	*	Google Firebase (Internet)	*	HTTPS	Mobile devices receive push notifications, please refer to Google Firebase documentation about firewalls settings  <a href="https://firebase.google.com/docs/cloud-messaging/concept-options">https://firebase.google.com/docs/cloud-messaging/concept-options</a>

Server Outgoing	Port Out	Server Incoming	Port In	Protocol	Comments
Client computer of the VisMgmt user	*	VisMgmt backend	5706	HTTPS	Commands from the VisMgmt client computer to the VisMgmt backend
Client computer of the CredMgmt user	*	CredMgmt backend	5806	HTTPS	Commands from the CredMgmt client computer to the CredMgmt backend
Admin computer	*	Mobile Access backend	3389	Remote Desktop (RDP)	For security reasons, you should allow administrator access to the Mobile Access backend computer only temporarily.

**Notice!**

Note that Mobile Access and the ACS have no direct connection, neither inbound nor outbound.

**4.8.1****Programs and services as firewall exceptions**

You can also configure the firewall by adding programs and services as exceptions

1. Start the Windows Firewall UI, select **Start > Settings > Control Panel > Windows-Firewall**.
2. Select tab **Allow an app or Feature through Windows Firewall**.
3. Select **Allow another app** (if greyed-out, enable button by selecting **Change settings**).
4. You can add the following programs:

**Programs**

The default install path is *C:\Program Files (x86)\Bosch Sicherheitssysteme\*

Program	File Location
acsp.exe	[Install-path]\AccessEngine\AC\BIN
ACTA-3.exe	[Install-path]\AccessEngine\AC\BIN
BioVerify.exe	[Install-path]\AccessEngine\AC\BIN
Bioidentify.exe	[Install-path]\AccessEngine\AC\BIN
Bosch.Ace.CredentialManagement.exe	[Install-path]\Bosch Credential Management
Bosch.Access.MobileAccessBackend.exe	[Install-path]\Bosch Mobile Access
Bosch.Ace.VisitorManagement.exe	[Install-path]\Bosch Visitor Management
CalTa-3.exe	[Install-path]\AccessEngine\AC\BIN
CDTA-1.exe	[Install-path]\AccessEngine\AC\BIN
EMDP.exe	[Install-path]\AccessEngine\AC\BIN

Program	File Location
KCKemas.exe	[Install-path]\AccessEngine\AC\BIN
KCS.exe	[Install-path]\AccessEngine\AC\BIN
Loggifier-2.exe	[Install-path]\AccessEngine\AC\BIN
PictureServer.exe	[Install-path]\AccessEngine\AC\BIN
ReplServer.exe	[Install-path]\AccessEngine\AC\BIN
reps.exe	[Install-path]\AccessEngine\AC\BIN
TAccExc.exe	[Install-path]\AccessEngine\AC\BIN
EMAILSP.exe	[Install-path]\AccessEngine\AC\BIN
master-3.exe	[Install-path]\AccessEngine\AC\BIN
querySrv-2.exe	[Install-path]\AccessEngine\AC\BIN
webSrv-1.exe	[Install-path]\AccessEngine\AC\BIN
LicenseGateway.exe	[Install-path]\AccessEngine\ AC\BIN\net6.0
DMS.exe	[install-path]\AccessEngine\MAC\BIN
lac.exe	[install-path]\AccessEngine\MAC\BIN

### Services

The default install path is *C:*

*\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System*

Service	File Location
Bosch.States.Api	[install-path]\States API
Bosch.Map.Api	[install-path]\Map API
Bosch.MapView.Api	[install-path]\Map View API
Bosch.Events.Api	[install-path]\Events API
Bosch.Alarms.Api	[install-path]\Alarms API
Bosch.Ace.IdentityServer	[install-path]\Identity Server
Bosch.Ace.Api	[install-path]\Access API
Bosch.DialogManager.Api	[install-path]\Dialog Manager API
Bosch.Intrusion.Api	[install-path]\Intrusion API
Bosch Ace Visitor Management	[VM-install-path]\
Bosch Ace Visitor Management Client	[VM-client-install-path]\
Bosch.OSS-SO	[install-path]\OSS-SO
Bosch.OSS-SO.Configurator	[install-path]\OSS-SO.Configurator
Bosch.Access.ProductApi.Api	[install-path]\ProductApi

## 4.9 IT security

The security of an organization's access control system is a critical part of its infrastructure. Bosch advises strict adherence to the IT-security guidelines prescribed for the country of installation.

The organization that operates the access control system is responsible for at least the following:

### 4.9.1 Hardware responsibilities

- The prevention of unauthorized physical access to network components, such as RJ45 connections.
  - Attackers need physical access in order to carry out man-in-the-middle attacks.
- The prevention of unauthorized physical access to the AMC2 controller hardware.
- Use of a dedicated network for access control.
  - Attackers can gain access via other devices within the same network.
- The use of secure credentials such as **DESFire** with Bosch code and multi-factor authentication with biometry.
- The prompt enrollment, via the **Setup Access** app, of mobile access readers with BLE (Bluetooth Low Energy) modules. Unenrolled, powered-on readers are vulnerable to hijacking by third parties. To remedy such hijacking, consult the reader's installation manual for instruction on how to reset factory defaults.
- Providing a failover mechanism and a backup power supply for the access control system.
- The tracking and disabling of credentials claimed to have been lost or misplaced.
- The proper decommissioning of hardware that is no longer in use, in particular its reset to factory defaults, and the deletion of personal data and security information.

### 4.9.2 Software responsibilities

- The proper maintenance, update and functioning of the access control network's firewall.
- The monitoring of alarms that indicate when hardware components, such as card readers or AMC2 controllers, go offline.
  - These alarms may indicate an attempt to swap hardware components.
- The monitoring of tamper-detection alarms triggered by electric contacts in access control hardware, for example, controllers, readers and cabinets.
- The limiting of UDP broadcasts within the dedicated network.
- Updates, especially security updates and patches, to the access control software.
- Updates, especially security updates and patches, to the hardware's firmware.
  - Note that even recently delivered hardware may require a firmware update. See the hardware manual for instructions.
  - Bosch assumes no liability for damages caused by products put into operation with outdated firmware.
- The use of OSDPV2 secure-channel communication.
- The use of strong password phrases.
- The enforcement of the *Principle of least privilege* to ensure that individual users have access only to those resources that they require for their legitimate purpose.

### 4.9.3 Secure handling of mobile credentials

- Do not leave unconfigured Mobile-Access readers unguarded.
  - An attacker could hijack the reader for a different ACS. This would require a costly factory reset.

- If a mobile device carrying mobile credentials is lost or stolen, treat that device as a lost card: block or delete all its mobile credentials as soon as possible.
- For high-security environments, Bosch recommends two-factor authentication. This requires the credential holder to unlock the mobile device before using it as a credential.
- Mobile credentials are not restored when a phone is restored from a backup. If a mobile-credential holder receives a new mobile device, you must resend all current invitations.
- An attacker could use a communication jammer to block communication with mobile-access readers. Employees whose access to areas is essential should carry physical credentials as a backup.
  - As backup for Mobile Access, use only physical cards with a secure encoding (such as Bosch code).
- Protect the Mobile Access server against unauthorized physical access. Bosch recommends additional measures such as, for example, BitLocker disk encryption.
- Protect the Mobile Access server against Denial-of-Service (DoS) attacks. It must be part of a secure network environment that provides protections such as a rate-limiter.
- Treat installer invitation QR-codes as administrator credentials. A stolen installer phone, with active installer credentials, could enable an attacker to reconfigure Mobile-Access readers maliciously.
  - Send invitations to installers just in time for the reader setup, and make sure that they delete those credentials as soon as the setup is completed.
  - Use the "Scan QR-codes from screen" function in preference to emailed invitations. Make sure that the intended installer loads the credential immediately.

## 4.10 Backing up the system

VisMgmt is an auxiliary web application for a main access control system. Consult the documentation for the main access control system regarding the backup of system databases.

## 5 Operation

### 5.1 Overview of user roles

User type	Use cases
Receptionist	Registering new visits and visitors Approving and declining visits Blacklisting visitors Assigning and deassigning visitor cards Managing associated documents Monitoring the number of visitors on site
Visitor	Self-registration and pre-registration Creating and maintaining a visitor profile Signing documents
Host	Managing schedules and lists of visits and visitors Pre-registering visits
Administrator	Making global settings Customizing the behavior of the tool and its user interface Plus: All the use cases of Receptionist

### 5.2 Using the dashboard

The dashboard is the home screen - a central dialog that leads to all other dialogs.

#### Overview and quick filters

The top of the dashboard contains a quick overview of the day's visits. This enables the user easily to monitor the number of visitors on site.

Visitors expected today: _%	Visitors checked in: _%	Visitors still to check out today	Visitors overdue for check-out
<current count> / <total capacity>	<current count> / <total capacity>	<current count>	<current count>

Click any of the headers to filter the visits table according to the meaning of the header. For example, click **Visitors checked in** to see only those visitors to whom a card is assigned. The value for <total capacity> is a configuration setting, made by the system administrator. See *Using the Settings menu for configuration, page 26*.

#### 5.2.1 The visits table

Each row in the table represents an appointment for a visit.

- You can sort the table by any of its columns by clicking the column header.
- You can select individual visits, or several visits at once, by using the keyboard-mouse idioms:
  - Ctrl-click for multiple selection of individual lines.
  - Ctrl-click on an already selected line to remove it from the selection.
  - Shift-click for multiple selection of contiguous lines
- You can add new visits to the table
- You can process visits and visitor details by clicking the action buttons
  - Approve visit

- Decline visit
- Assign cards to the visitor
- Edit visit and visitor details
- You can export the currently filtered lines to a *.CSV* or *.XLSX* file.

The horizontal tool bar has the following functions:



Label	Function
<b>1</b> N entries	The total number N of visits (each visit is a row in the table).
<b>2</b> Search	Search for arbitrary text among the visits in the table
<b>3</b> 	Show the visits that were added most recently to the table.
<b>4</b> 	Open a dialog for selecting filter criteria
<b>5</b> 	Reset the table to its default view, and revert all filters.
<b>6</b> Deassign card	Open a dialog for deassigning assigned cards using a connected enrollment reader.
<b>7</b> 	Open a dialog for creating a new visit entry in the table
...	Click the ellipsis symbol for a menu to export the currently filtered visits, and also documents, to various file formats, for example <i>.CSV</i> and <i>.XLSX</i> Note that for reasons of data security, you can only export if your client is running in a secured HTTPS connection, with a certificate.

## 5.2.2 Table columns and actions

### Columns

Column	Value	Description
Status	 Visit expected	An icon reflecting the status of the visit

Column	Value	Description
	 Visit approved  Visit declined  Card assigned  Card expired  Visit ended (Visitor no longer holds cards, and has left the premises)	
<b>Name</b>	Visitor's name as a hyperlink	Click the hyperlink to view the details of the visitor and their current visit.
<b>Exp. arrival</b>	Date and time	The expected date and time of the visitor's arrival
<b>Exp. departure</b>	Date and time	The expected date and time of the visitor's departure
<b>Checked in</b>	Date and time	The date and time of the assignment of the first card to the visitor.
<b>Checked out</b>	Date and time	The date and time of the deassignment of the last card from the visitor.
<b>Card numbers</b>	Numeric	The numbers of the cards assigned to this visitor.
<b>Actions</b>	Icons	See separate table below

**Actions**

Icon	Function
	<b>Approve</b> the visit. NOTE: It is not possible to assign a card to visitors on the blacklist. First remove the visitor from the blacklist, or exempt them temporarily. See <i>Adding, removing and exempting from the blacklist, page 46</i>
	<b>Decline</b> the visit. This button is deactivated after the visitor has checked in, that is, when they already have a card.

Icon	Function
	<p><b>Assign</b> one or more cards to the visitor</p>
	<p><b>Edit</b> the visit event and/or the visitors credentials</p>

## 5.3 Receptionist

### 5.3.1 Logging onto the Receptionist role

1. In your browser, open `https://<My_VisMgmt_server>:5706/main/` for the login screen.
2. Enter the username of an account with the required rights for your role.  
Consult your system administrator if you do not have an account.
3. Enter the password.
4. Click **Login**.

### 5.3.2 Searching and filtering visits

On the VisMgmt dashboard, in the toolbar above the visits table.

#### Search

To search names and hosts, enter alphanumeric text in the search box, and press Return.

#### Filtering

- To see the visits that are closest to the current time, click **Latest**
- To construct a complex filter from visit status, dates of check-in and check-out, and card numbers, click **Filter**.
  - Enter the desired filter criteria in the popup dialog
  - Click **Apply**  
The system reduces the visits table to only those visit appointments that meet the filter criteria.
- To delete all filter criteria click **Reset**

### 5.3.3 Registering visits

#### Introduction

A receptionist has two basic scenarios for registering visits:

- **A:** When a visitor uses the visitor kiosk to create their own visitor ID and upload documents, the receptionist needs only complete any required information and signatures that are still missing, and assign a card to the visitor.
- **B:** When a visitor bypasses the visitor kiosk and approaches the reception desk directly, the receptionist can register the visit from scratch: collect the required information, collect signatures for required documents, and assign a card to the visitor.

Scenario **A** is a subset of scenario **B**, so the complete scenario **B** is described here. The use of kiosk mode by a visitor is described in its own section. See *Introduction to Kiosk mode, page 49*.

#### Procedure

On the VisMgmt dashboard, in the toolbar above the visits table.

1. Click  to add a visit appointment to the visits table.

2. On the **Personal Data** dialog, enter the data that your site requires from visitors. Mandatory fields are marked with an asterisk (\*). You can enter data manually, but more quickly and accurately through a document scanner, if available at the receptionist's workstation. See *Peripheral hardware, page 22* for details on the supported peripheral devices.
  - **General information**
    - Locate and load an entire visitor profile created on a previous visit. To locate profiles click the  (search) icon, located at the **Last name\*** field. When a visitor profile is created, it receives a unique alphanumeric code that the visitor should carefully save, in order to accelerate the registration process for future visits.
    - Else, enter data by hand.
  - **ID photos**
    - **Upload** a photo from the file system.
    - **Capture** photos of the visitor from a connected web camera.
  - **Identity documents**
    - Click **Scan document** to read data from a document scanner (if available) and automatically complete the relevant data fields in the dialog.
    - Else, enter text by hand, if your system does not have a document scanner.
  - **Legal documents**
    - Load the documents that the visitor signed electronically at the kiosk.
    - If your system does not have a visitor kiosk, print out and file (with the visitor's signature) the required PDF documents stored on the file system.
3. Click **Next** to proceed to the **Visits** dialog.
4. On the **Visits** dialog, in the **Current visit** pane, enter the data that your site requires. Mandatory fields are marked with an asterisk (\*).
  - Select a **Visitor type**. This is either **Visitor** (default) or a customized subclass of **Visitor**, defined as a **Person type** in the main access control system.
  - Select under **Host** the name of the employee to be visited.
    - Note that you can select only cardholders of the main access control system.
    - A tooltip displays the person's email address as an aid to identification.
  - If the visitor requires an escort through the premises, select the name of the escorting employee under **Escort**.
    - Note that you can select only cardholders of the main access control system.
    - A tooltip displays the person's email address as an aid to identification.
  - If the visitor requires extra time to pass through a door, select the checkbox **Extended door opening time**
5. Click **Save**. Note that you will not be able to save the data until you have completed all mandatory fields.

**Refer to**

- *Peripheral hardware, page 22*

**5.3.4****Approving and declining visits****Background: approving physical cards**

You must approve a visit before you can assign cards to a visitor.

### Background: approving mobile credentials

You can create and share a mobile credential on the day of the visit, similarly to assigning a physical card.

- **Note:** The mobile credential will not work until you approve the visit.
- Alternatively,* you can create the mobile credential and share it in advance. When the visitor arrives at reception, approve the visit, as described below, to finally activate the credential.
- **Note:** The mobile credential will not work until you approve the visit.
  - If you have set an expected departure time for the visit, then that time will apply.
  - If you have not set an expected departure time, a default number of hours (8) will apply. Administrators can change this default in the **Settings** menu.

### Procedures for approving and declining

There are two places to approve or decline a visit:

- in the visits table on the dashboard
- in the visit editor

#### In the visits table on the dashboard:

- **Approve:** In the visits table, select a line from the table and click . After a confirmation popup, the icon turns gray to show that the visit is approved.

- **Decline:** In the visits table, select a line from the table and click . After a confirmation popup the **Approve** icon is restored to blue, to show that the visit still needs to be approved.

#### In the visit editor:

1. On the dashboard, in the visits table, select a line from the table and click  to edit the visit.
2. On the **Personal Data** dialog, click **Next**.
3. On the **Visits** dialog, click the **Approve** or the **Decline** button.
4. Confirm your action in the popup window.

## 5.3.5 Assigning physical credentials

### Introduction

Assign a visitor card to every visitor whom you allow onto the premises. You can assign multiple cards to a single visitor if required.

- The **Checked-in** time of a visit is the time of the assignment of the first card.
- The **Checked-out** time of a visit is the time of the deassignment of the last card that is still assigned to the visitor.

The receptionist can assign and deassign cards easily from the dashboard, if an enrollment card reader is connected to the receptionist's computer.

Nevertheless the visit editor provides a way of assigning card numbers, if no such reader is available.



### Notice!

Blacklisted persons cannot receive cards

It is not possible to assign cards to visitors who are on the blacklist. Remove the visitor from the blacklist, or create a temporary exemption for the visitor, before attempting to assign a card.

### Assigning a card from the dashboard (requires an enrollment reader)

1. Have a physical visitor card ready to present to the enrollment reader.
2. In the visits table, approve the visit. See *Approving and declining visits*, page 40



3. Select the row of the visit and click
4. Follow the instructions in the popup for use of the enrollment reader.

### Deassigning a card from the dashboard (requires an enrollment reader)

1. Collect the physical card from the cardholder, and have it ready to present to the enrollment reader.



2. In the toolbar click **Deassign card**.
3. Follow the instructions in the popup for use of the enrollment reader.

### Assigning a card in the visit editor



1. On the dashboard, in the visits table, select a row in the table and click to edit that visit.
2. On the **Personal data** dialog, click **Next**
3. On the **Visits** dialog, if the visit has not yet been approved, click **Approve**.
4. If you have an enrollment reader connected, click **Read card** and follow the instructions in the popup for use of the enrollment reader.
  - Otherwise click **Show free cards** to display a list of the visitor cards that are still available.
 

Alternatively, if you have unsorted physical cards with printed numbers, select any card and use the **Search** tool to find its number quickly in the list.
  - Click  next to a card number to assign that card to the current visitor.
  - Repeat the last steps to assign further cards, if required.
5. Click **Save** to save the current visit with the card assignments.

### Deassigning a card in the visit editor



1. On the dashboard, in the visits table, select a row in the table and click to edit that visit.
2. On the **Personal data** dialog, click **Next**

3. On the **Visits** dialog, in the Visitor cards pane, click  next to the card that you want to deassign, and confirm your action in the popup window. Repeat this step until you have deassigned all the cards that you want to deassign.
4. Click **Save** to save the current visit with the card assignments.
5. When you deassign the last card assigned to the visitor, the system records this date and time as the check-out time of the visitor.



In the visits table, the status of this visit record becomes \_\_\_\_\_

#### Refer to

- *Using the Settings menu for configuration, page 26*
- *Registering visits, page 39*
- *Approving and declining visits, page 40*

## 5.3.6

### Assigning mobile credentials

#### Prerequisites

- Mobile Access is installed and configured on your system.
  - For instructions, see the relevant section in the installation chapter of this document.
- The receiving person has installed the Mobile Access App, and it is running on their smart device.
  - For instructions, see the relevant section in the installation chapter of this document.

#### Procedure in the dashboard

1. Select the row of the person to receive mobile credentials



2. On the selected row, click
3. Select one of the large icons for the options:
  - **QR code**
  - or
  - **Invitation mail**
4. If you select the **QR code option**:
  - The system displays a QR code
  - The person scans the QR code with the Mobile Access app on their mobile device
  - In order for the credential to work, you must **approve** the visit. For instructions, see the section *Approving and declining visits, page 40*
  - The mobile device functions like a physical access card, as long as the app is running
5. If you select the **Invitation mail** option:
  - By default, the program selects the email address defined for the selected person. Enter an alternative email address if required
  - The system sends an email to the selected address
  - The person takes delivery of the email on their mobile device, which is running the mobile access app
  - The person opens link in the email

- In order for the credential to work, you must **approve** the visit.  
For instructions, see the section *Approving and declining visits, page 40*
- The mobile device functions like a physical access card, as long as the app is running

#### Procedure in the edit dialogs

1. Select the row of the person to receive mobile credentials



2. On the selected row, click
  - The edit dialog opens
3. In VisMgmt, click **Next** to proceed to the **Visit details** screen
4. Click the button **Add mobile access**
5. Select one of the large icons for the options:
  - **QR code**
  - or
  - **Invitation mail**
6. If you select the **QR code option**:
  - The system displays a QR code
  - The person scans the QR code with the Mobile Access app on their mobile device
  - In order for the credential to work, you must **approve** the visit.  
For instructions, see the section *Approving and declining visits, page 40*
  - The mobile device functions like a physical access card, as long as the app is running
7. If you select the **Invitation mail option**:
  - By default, the program selects the email address defined for the selected person. Enter an alternative email address if required
  - The system sends an email to the selected address
  - The person takes delivery of the email on their mobile device, which is running the mobile access app
  - The person opens link in the email
  - In order for the credential to work, you must **approve** the visit.  
For instructions, see the section *Approving and declining visits, page 40*
  - The mobile device functions like a physical access card, as long as the app is running

#### Refer to

- *Installing Mobile Access, page 15*
- *Installing the Mobile Access apps, page 21*

### 5.3.7

#### Deassigning credentials

##### Deassigning a card from the dashboard (requires an enrollment reader)

1. Collect the physical card from the cardholder, and have it ready to present to the enrollment reader.



2. In the toolbar click **Deassign card**.
3. Follow the instructions in the popup for use of the enrollment reader.

### Deassigning a card in the credentials editor



1. On the dashboard, in the main table, select a row in the table and click  to edit that cardholder.
2. On the editing dialog, in the **Employee cards** column, click  next to the card that you want to deassign, and confirm your action in the popup window.  
Repeat this step until you have deassigned all the cards that you want to deassign.
3. Click **Save** to save the current visit with the card assignments.

## 5.3.8 Checking in and out without card

### Introduction

If visitors have close escorts, or are restricted to public spaces, then individual cards for visitors may be unnecessary. For such cases there exists the option of checking visitors in and out without cards. For security reasons this option is disabled by default.

### Prerequisite.

Your system administrator has enabled the special option **Check-in/check-out without card** in the dialog **Settings > Receptionist > Visits**. See the configuration chapter *Using the Settings menu for configuration, page 26* for instructions.

### Process

When the option is enabled the following occur:

- Any visitor who self-registers at the kiosk computer automatically approves the visit and checks in at the same time.
- The system sets the check-in date and time to the moment of registration.
- The toggle button **Check-in/out without card** appears in the visit editor and the dashboard for the same visit.

### Procedure: Checking a visitor in without card

If a visitor cannot register himself at the kiosk, but is to check in without a card:

1. register the visit manually, as described in the chapter *Registering visits, page 39*



2. On the dashboard, in the visits table, click the visitor's name in the table or click  to edit that visit.
3. On the **Personal data** dialog, click **Next**
4. On the **Visits** dialog, in the **Visitor cards** pane, click **Check-in without card**

### Procedure: Checking a visitor out without card

If a visitor without card leaves the premises:



1. On the dashboard, in the visits table, click the visitor's name in the table or click  to edit that visit.
2. On the **Personal data** dialog, click **Next**
3. On the **Visits** dialog, in the **Visitor cards** pane, click **Check-out without card**

**Refer to**

- *Registering visits, page 39*

**5.3.9**

**Adding, removing and exempting from the blacklist**

Visitors that are not welcome on site can be put on a blacklist. As long as a visitor is on the blacklist, you cannot assign a card to that person. You may remove the visitor from the blacklist at any time, or grant a temporary exemption, in order to assign a card.

**Blacklisting**



1. On the dashboard, in the visits table, select a line from the table and click  to edit a visit.
  2. On the **Personal Data** dialog, click **Blacklist**.
  3. In the popup window, confirm that you really want to blacklist this person.
  4. In the next popup window, enter a reason for blacklisting, and confirm.
- A banner **Blacklisted** appears in the visit editor,



- Two buttons appear under the banner: one for removing the visitor from the blacklist, and one for granting a temporary exemption.
- In the visits table the name of every blacklisted visitor appears with a warning triangle.



For example:

**Removing and exempting**

1. On the dashboard, in the visits table, select a line from the table where the visitor is marked as blacklisted, and click  to edit the visit.
2. On the **Personal Data** dialog, click one of the following:
  - **Remove** to remove the visitor permanently from the blacklist.
  - **Exempt** to keep the visitor on the blacklist but allow the assignment of a card for this visit only.
3. Confirm your action in the popup window.

**5.3.10**

**Maintaining visitor profiles**

The system keeps visitor profiles until the visitors themselves, receptionists or administrators delete them.

After a retention period defined in the system settings (default value 12 months) the system deletes records of the visit.

When a visitor or receptionist creates a new visitor profile, the profile receives a unique alphanumeric code. Visitors can log in with this code at the visitor kiosk, and so gain access to maintain their own profiles.



**Notice!**

Protect visitor IDs

Protect visitor IDs carefully from unauthorized access, as they provide access to personal data.

**5.3.11 Viewing visit records**



1. On the dashboard, in the visits table, select a row in the table and click  to edit that visit.
2. On the **Personal Data** dialog, click **Next**
3. On the **Current visit** dialog, click **Show all visits**  
The **Current visit** dialog shows a list of previous visits.

**5.4 Host**

Hosts are employees who receive visits. They can register their own appointments, and browse the system for details of visitors and records of their visits: past, present and future.

**5.4.1 Logging onto the Host role**

1. In your browser, open `https://<My_VisMgmt_server>:5706/main/` for the login screen.
2. Enter the username of an account with the required rights for your role.  
Consult your system administrator if you do not have an account.
3. Enter the password.
4. Click **Login**.

**5.4.2 Searching and filtering**



The toolbar for the Host dashboard contains the following functions:

Label	Function
 N entries	The total number N of visits (each visit is a row in the table).
 Search	Search for arbitrary text among the visits in the table
	Show the visits that were added most recently to the table.
	Open a dialog for selecting filter criteria

Label	Function
	Reset the table to its default view, and revert all filters.
	Open a dialog for creating a new visit entry in the table

### Search

To search names and hosts, enter alphanumeric text in the search box, and press Return.

### Filtering

- To see the visits that are closest to the current time, click **Latest**
- To construct a complex filter from visit status, dates of check-in and check-out, and card numbers, click **Filter**.
  - Enter the desired filter criteria in the popup dialog
  - Click **Apply**  
The system reduces the visits table to only those visit appointments that meet the filter criteria.
- To delete all filter criteria click **Reset**

## 5.4.3

### Registering visits

To register a visit appointment from a first-time visitor:

On the VisMgmt dashboard, in the toolbar above the visits table.



1. Click  to add a row to the visits table
2. On the **Personal Data** dialog, in the **General information** section, enter the personal data that your site requires from visitors.
3. In the **Visit details** section, enter the required details, typically the expected arrival and departure times, plus a reason for the visit.
4. Click **Save** to save the visit appointment.  
The visit appears on the dashboard as a line in the visits table.

## 5.4.4

### Copying visit appointments

To schedule a further appointment with the same visitor

1. On the VisMgmt dashboard, find an existing appointment with the same visitor in the visits table.



2. Click the smaller  icon at the end of the row.
3. On the **Personal Data** dialog, in the **Visit details** section, enter the required details, typically the expected arrival and departure times, plus a reason for the visit.
4. Click **Save** to save the visit appointment.  
The visit appears on the dashboard as a line in the visits table.

## 5.5 Visitor

Visitors can use the system in kiosk mode on the premises to create their own visitor profiles, and sign required documents before proceeding to reception to collect their visitor cards.

### 5.5.1 Introduction to Kiosk mode

Visitors typically register their visits, and create their own profiles, at a computer that is freely accessible in the reception area of the access-controlled site. For security reasons, the computer's web browser runs in kiosk mode, which allows access only to VisMgmt, and not to multiple tabs, browser settings, or the computer's operating system. All the supported browsers offer kiosk mode, but its exact configuration depends on the browser.

The kiosk computer runs the **Bosch Peripheral Devices** add-on, which allows it physical connections to peripheral devices for scanning ID documents and signatures.

- The URL for kiosk mode is `https://<My_VisMgmt_server>:5706`
- By contrast, the URL for logging on as Administrator, Receptionist or Host is `https://<My_VisMgmt_server>:5706/main/`

### 5.5.2 Creating a visitor profile: Self check-in

#### First time visitors

Note that the exact procedure depends on what peripheral devices, such as document and signature scanners, and photo cameras, are available to the kiosk computer.

1. At the welcome screen on the kiosk computer, click **Continue without visitor ID**.
2. On the next screen, click **Self check-in**.
3. On the next screen, select **Scan document**.
4. Follow the instructions on screen for site-specific requirements, such as:
  - scanning ID documents,
  - signing any other legal documents required,
  - capturing a photograph.
5. The system displays the collected information for you to correct and complete.
6. The system asks whether you require special access authorizations, and communicates this to the reception desk, if required.
7. At the end of the check-in process, the screen displays a unique visitor ID.  
Take this ID to the reception desk to receive your visitor card.



#### Notice!

Your unique visitor ID

Carefully note your visitor ID, and protect it from unauthorized use. It gives access to your visitor profile. You can use it to log on at the kiosk computer and so expedite your next check-in.

#### Repeat visitors

1. Log on at the kiosk with your unique visitor ID.
2. The system displays the collected information for you to correct and complete, if required.
3. Proceed to the reception desk to collect your visitor card.

## 5.6 Authorizing installers of mobile access readers

### Introduction

The installers of mobile access readers use the Bosch Setup Access for scanning and configuring the readers via BLE .

Authorized operators of **Credential Management** and **Visitor Management** send virtual credentials to the installer app, to authorize the installer. This section describes that procedure.

### Prerequisites

- Mobile Access is installed and configured on your system.
  - For instructions, see the relevant section in the installation chapter of this document.
- Make sure that the installer who is receiving the authorization has installed the Bosch Setup Access, and it is running on their smart device.
  - For instructions, see the relevant section in the installation chapter of this document.

### Procedure

1. In the main menu, click  to open the **Installer onboarding** dialog.
2. Click **Add** to add an installer to the list, or  to delete an existing installer
  - The **Add installer** pop-up window appears.
3. In the **Add installer** pop-up window, enter the details you require, for example:
  - Personal names, company name, email address, phone number
- Note: you can click  to modify the details for a selected installer at a later date
4. Click **Next**
5. Select one of the large icons for the options:
  - **QR code**
  - or
  - **Invitation mail**
6. If you select the **QR code option**:
  - The system displays a QR code
  - The person scans the QR code with the Mobile Access app on their mobile device
  - This completes the registration process of the installer
  - It enables the mobile device to scan for mobile access readers and configure them by BLE, as long as the app is running
7. If you select the **Invitation mail** option:
  - By default, the program selects the email address defined for the selected person. Enter an alternative email address if required
  - The system sends an email to the selected address
  - The person takes delivery of the email on their mobile device, which is running the Bosch Setup Access
  - The person opens link in the email
  - This completes the registration process of the installer
  - It enables the mobile device to scan for mobile access readers and configure them by BLE, as long as the app is running

### Resending invitations

1. On the installer onboarding dialog, select the desired installer



2. Click  on the same line, to resend the authorization to the selected installer by QR code or email.

**NOTE:** You can only resend the authorization if the installer has not yet activated it.

## 5.6.1

### Resetting Mobile Access readers

It may become necessary to reset access readers to factory defaults to enable their re-configuration.

For instance, if an installer needs to reconfigure Mobile Access readers that have already been configured for a different site, then those readers will require a reset.

Consult the LECTUS select reader's manual for a description of how to reset the reader, using its DIP switches.

## 5.7

### Using the Mobile Access apps on mobile devices

**NOTE:** Use of the Bosch Mobile Access apps is described in detail for their respective users in separate **Quick User Guides**. These documents are available from the Bosch online product catalog.

#### Introduction

Bosch provides the following apps for mobile access

- Bosch Mobile Access: A cardholder app to store virtual credentials and transmit them via Bluetooth to those readers that are configured for mobile access. Such a reader then grants or denies access depending on whether one of the app's stored credentials is valid for it.
- Bosch Setup Access: An installer app for scanning and configuring the readers via Bluetooth.

Authorized operators of Visitor Management and Credential Management can send virtual credentials for both cardholder and installer apps.



#### Notice!

**IMPORTANT:** Do not operate the cardholder and installer apps simultaneously

Make sure that nobody uses the installer app when the cardholder app is in use, and vice versa.

## 5.7.1

### Setting RSSI thresholds in the Setup Access app

#### Introduction

RSSI threshold and BLE range can be considered roughly equivalent concepts in the context of Bosch Mobile Access.

Mobile access devices transmit BLE signals to nearby readers. An important part of reader configuration is the setting of an RSSI threshold for each reader. This threshold is the minimum BLE signal strength, measured in dBm, that the reader (R) is to accept as a request to enter. The reader is to ignore all weaker BLE signals.



RSSI values can vary greatly depending on many factors, including the type of transmitting device, battery-level, and the material and thickness of nearby walls. There is no linear relation between the RSSI value and distance between transmitter and receiver.

For this reason, the Setup Access app provides a tool to measure the reader's RSSI from the current position of the mobile device. The procedure below describes how to use this tool.

When you have found a suitable threshold value for the BLE range, use the Setup Access app to store that value in the reader configuration.

#### Procedure

Configure the **BLE range** using one of the following options, A or B:

**A:** Using RSSI values reflected by the reader

1. Position yourself before the reader, at the point where you expect the mobile credential user to be.
2. Tap **Check and use current range**
  - A pop-up message will appear. Tap **OK**
3. An RSSI value will appear.
  - Recommended: Repeat this step a few times from the same position, to get an impression of the degree of variance in perceived signal strength.
4. When you have found a suitable threshold value, tap **Save**.

**B:** Setting the RSSI threshold manually

1. Enter a value in the RSSI threshold.  
See the table of typical thresholds below
2. Tap **Save**

#### Typical threshold values (approximate only):

Expected distance from mobile device to reader	Suggested RSSI threshold
Near (5 cm - 10 cm)	-30 ... -40 dBm
Medium (0,5m - 2m)	-50 ... -60 dBm
Far (> 2m)	-70 ... -90 dBm



#### Notice!

RSSI values can vary greatly depending on many factors, including the type of transmitting device, battery-level, and the material and thickness of nearby walls.

---

# Glossary

## ACS

---

generic term for a Bosch Access Control System, for example, AMS (Access Management System) or ACE (BIS Access Engine).

## BLE

---

Bluetooth Low Energy is a wireless network technology that provides a similar communication range to Bluetooth, but with lower energy consumption..

## FQDN

---

A fully qualified domain name is a network domain name that expresses its absolute location in the hierarchy of the Domain Name System (DNS).

## host

---

in the context of visitor management, the host is the visitee, that is, the person who receives the visitor.

## kiosk mode

---

A highly restricted mode of browser usage that typically allows access only to a single web application, and not to browser settings, multiple tabs or the computer's operating system.

## Mobile Access

---

access control of persons using virtual credentials stored on a mobile device, such the person's smartphone.

## OSDP

---

Open Supervised Device Protocol is an access control communications standard, introduced in 2011 by the Security Industry Association (SIA). It offers advantages over older protocols in the areas of encryption, biometrics, ease of use, and interoperability.

## RSSI

---

the Received Signal Strength Indicator (RSSI) is the signal strength perceived by a receiving device, measured in dBm. Mobile devices typically display RSSI by a signal-strength bar graphic.





**Bosch Security Systems B.V.**

Torenallee 49

5617 BA Eindhoven

Netherlands

**[www.boschsecurity.com](http://www.boschsecurity.com)**

© Bosch Security Systems B.V., 2023

**Building solutions for a better life.**

202302171342