Credential Management V5.0

Including Mobile Access

en Software manual

Table of contents

1	**Introduction**	**5**
1.1	About Credential and Visitor Management	**5**
1.2	About Mobile Access	**5**
2	**Credential Management overview**	**6**
3	**Installing and uninstalling**	**8**
3.1	Software prerequisites	**8**
3.2	Hardware prerequisites	**9**
3.2.1	Setting up the Peripheral Devices add-on	**9**
3.3	Installing Credential Management	**10**
3.3.1	CredMgmt prerequisites	**10**
3.3.2	Installation procedure	**11**
3.4	Installing Mobile Access	**12**
3.4.1	Overview of installation, configuration, and use	**12**
3.4.2	Mobile Access hardware prerequisites	**13**
3.4.3	Mobile Access configuration prerequisites	**13**
3.4.4	Procedure for co-located installation	**14**
3.4.5	Procedure for distributed installation	**15**
3.5	Installing the Mobile Access apps	**18**
3.6	Certificates for secure communication	**18**
3.6.1	Certificates for the Firefox browser	**19**
3.6.2	Certificates for the Chrome browser	**20**
3.7	Repair installations of Mobile Access	**20**
3.8	Uninstalling the software	**21**
4	**Configuration**	**22**
4.1	Creating Credential Management users in the ACS	**22**
4.2	Logging on for configuration tasks	**22**
4.3	Using the Settings menu for configuration	**22**
4.3.1	Email templates	**23**
4.3.2	Preview mode	**24**
4.4	Customizing the UI	**24**
4.4.1	Setting options visible, invisible and mandatory	**24**
4.4.2	Customizing the company logo	**25**
4.5	Firewall settings	**25**
4.5.1	Programs and services as firewall exceptions	**26**
4.6	IT security	**28**
4.6.1	Hardware responsibilities	**28**
4.6.2	Software responsibilities	**28**
4.6.3	Secure handling of mobile credentials	**28**
4.7	Data privacy and protection at Bosch	**29**
5	**Operation**	**31**
5.1	Overview of user roles	**31**
5.2	Using the dashboard	**31**
5.3	Assigning physical credentials	**33**
5.4	Assigning mobile credentials	**33**
5.5	Deassigning credentials	**35**
5.6	Authorizing installers of mobile access readers	**35**
5.6.1	Resetting Mobile Access readers	**36**
5.7	Using the Mobile Access apps on mobile devices	**36**

5.7.1 Setting RSSI thresholds in the Setup Access app 37
Glossary 39

1 Introduction

1.1 About Credential and Visitor Management

Credential Management, hereafter referred to as CredMgmt, is a browser-based software tool that operates in tandem with a Bosch access control system or ACS. With a simple and intuitive user interface, it enables even relatively inexperienced operators to manage the access credentials of employees and external personnel. The credentials themselves can be either physical cards, or virtual cards sent to employees' mobile devices.

Credential management

In CredMgmt, ACS operators can manage both credentials and the employee records to whom the credentials belong.

Entity	Add	Modify	Delete	Assign/ Deassign
Physical credentials				Yes
Virtual "mobile" credentials (if Mobile Access is installed)	Yes		Yes	Yes
Authorizations				Yes
Cardholder records	Yes	Yes	Yes	

Visitor management

In VisMgmt ACS operators manage credentials, visitor records, and the visit records.

Entity	Add	Modify	Delete	Assign/ Deassign
Physical credentials				Yes
Virtual "mobile" credentials (if Mobile Access is installed)	Yes			Yes
Visitor records	Yes	Yes	Yes	
Visit records	Yes	Yes	Yes	

1.2 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.

2 Credential Management overview

The following illustrate possible topologies of credential management installations, both with and without Mobile Access. Each enclosing box represents a separate computer.

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.

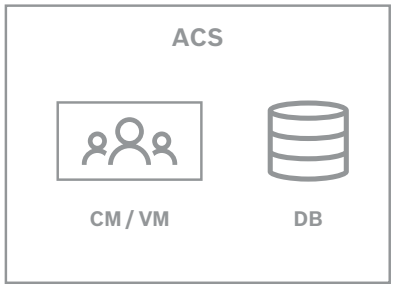
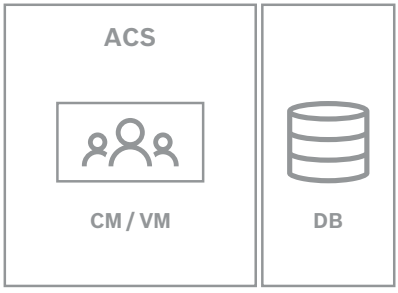
Credential Management, local DB	Credential Management, remote DB
	

Table 2.1: Credential Management topologies

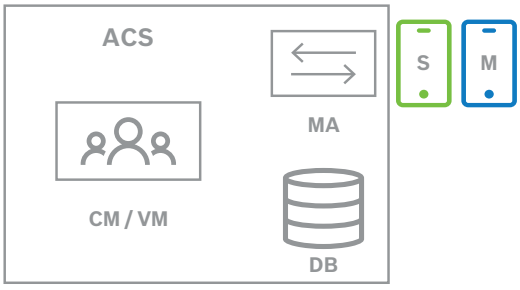
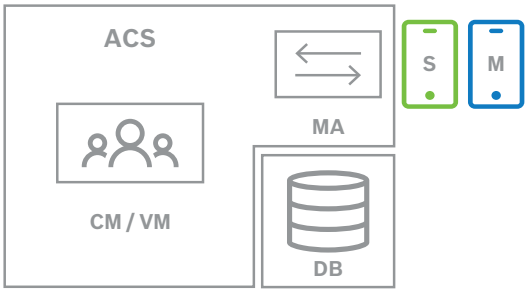
Mobile Access, co-located, local DB	Mobile Access, co-located, remote DB
	

Table 2.2: Mobile Access co-located topologies

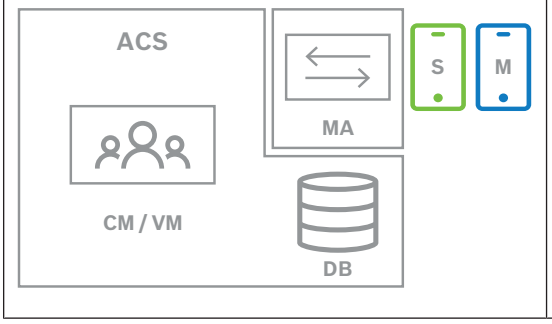
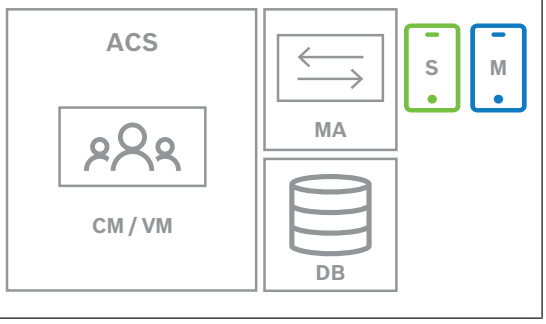
Mobile Access, distributed, local DB	Mobile Access, distributed, remote DB
	

Table 2.3: Mobile Access distributed topologies

Compatible versions of related software

The following table lists the versions of auxiliary software tools that are compatible with this version of the system.

Component	Version	Location
Access Management System (AMS)	5.0.1 (includes Mobile Access extension)	Download Store /Product Catalogue
Visitor Management (VisMgmt)	5.0.1 (includes Mobile Access extension)	Download Store /Product Catalogue

Notice!

Divisions

Credential Management, Visitor Management and Mobile Access do not support the "Divisions" feature of Bosch access control systems, where one (ACS) administers the access control of multiple independent tenants.

3 Installing and uninstalling

3.1 Software prerequisites

You install CredMgmt server on the same computer as the ACS (the primary access control system). The same software and hardware requirements apply.
The CredMgmt and Mobile Access setup programs have their own installation media, separate from the ACS. They are downloadable from Bosch online product catalogs.

Notice!
Necessity of a stable root certificate
Before proceeding with the installations below, make sure that the installation of the ACS is complete and licensed, according to its own installation guide. This includes a final decision on the root certificate of the ACS server (whether self-signed or CA-based) and its stable implementation. Post-hoc changes to the root certificate of the ACS server would require reconfiguration of certificates on all computers and mobile-access readers participating in its access control system.

Server requirements
The server is the computer that runs the ACS and the CredMgmt application.

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

Client requirements

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.

3.2 Hardware prerequisites

Enrollment readers

CredMgmt requires at least one enrollment reader to enroll physical cards. Enrollment readers are typically installed on client workstations. The client workstation communicates with peripheral hardware via a program called *BoschPeripheralDeviceAddon.exe*. Its installation of this program is described below.

The following enrollment readers and card formats are supported.

	MIFARE DESfire Ev1 Bosch Code	MIFARE DESfire Ev1 CSN	MIFARE Classic CSN	iCLASS 26 bit	iCLASS 35 bit	iCLASS 37 bit	iCLASS 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

3.2.1 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.

1. 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.
2. Click **Next** to accept the default installation packages.
3. 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

4. Click **Next** for a summary of the components to be installed.
5. Click **Install** to start the installation.
6. Click **Finish** to finish the installation.
7. After installation, reboot the computer.

3.3 Installing Credential Management

Introduction

CredMgmt runs as a web application in tandem with a Bosch access control system (ACS). The following sections describe the installation of the backend component that drives this web application.

– You can install it to use either a local or a remote database.

3.3.1 CredMgmt prerequisites

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

The user *CMUser* accesses the ACS database on behalf of the CredMgmt.application.
If CredMgmt is to use a database on a remote database server, use the procedure below.
IMPORTANT: Do not run the CredMgmt setup before completing this 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>*CMUser*
– **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 CredMgmt 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 *CMUser* 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 *CMUser*
6. In the **Select a page** pane, select **Server roles**
7. Select the check boxes *public* and *dbcreator*

Dedicated user for the local database (only if you are using a local database)

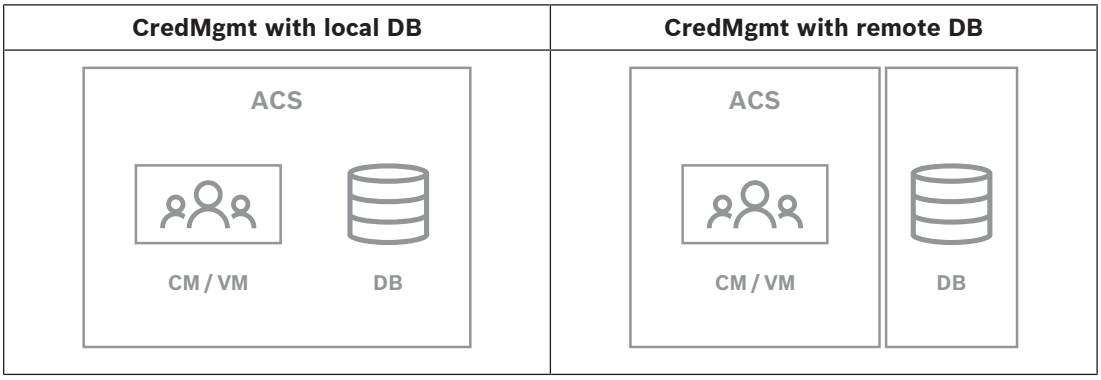
The user *CMUser* accesses the ACS database on behalf of the CredMgmt.application.
You do NOT need to create this user if CredMgmt is to use a local database, because the CredMgmt setup program creates a Windows user *CMUser* on the ACS server automatically.

A dedicated user in the ACS

1. In the ACS, create a user that has the feature **unlimited API usage**.

– Dialog path in AMS: **Configuration** > **Operators and Workstations** > **User rights** > tab: **User account** > **API Access rights control.**
Pick *Unlimited access* from the list.
– For more detailed instructions, see the chapter **Assigning user (operator) profiles** in the operator manual of the ACS.
2. Note the username and password carefully, because the web application's installation wizard will require them.

3.3.2 Installation procedure



Procedure

1. On the ACS server, run *BoschCredentialManagementServer.exe* as Administrator.
– The installation program opens
2. On the **Core components** screen, select *Bosch Credential Management* and click **Next**
3. 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.
4. Browse and select a destination folder for the installation, or accept the default (recommended), click **Next**
5. 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**
6. On the **ACS access configuration** screen:
– Enter the hostname of the ACS server.
– Enter the name of an ACS user with unlimited API usage (see Prerequisites above).
– Enter the ACS password for this ACS user and confirm it.
7. 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 CredMgmt is selected and click **Install**
10. When the installation is complete, start CredMgmt with the following URL:
https:// <NameOfACSserver>*:5806*

3.4 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.

3.4.1 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.

3.4.2 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

3.4.3 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*

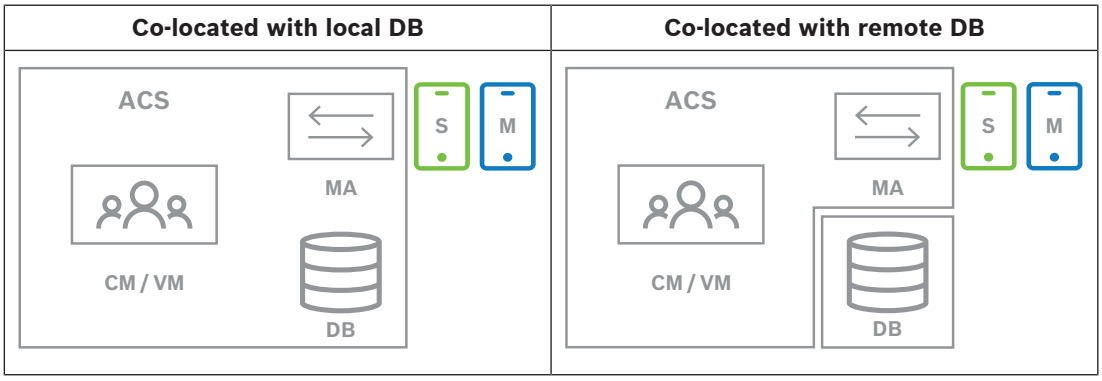
Then add *MAUser* as a login to remote the SQL Server as follows:

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.

3.4.4 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
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

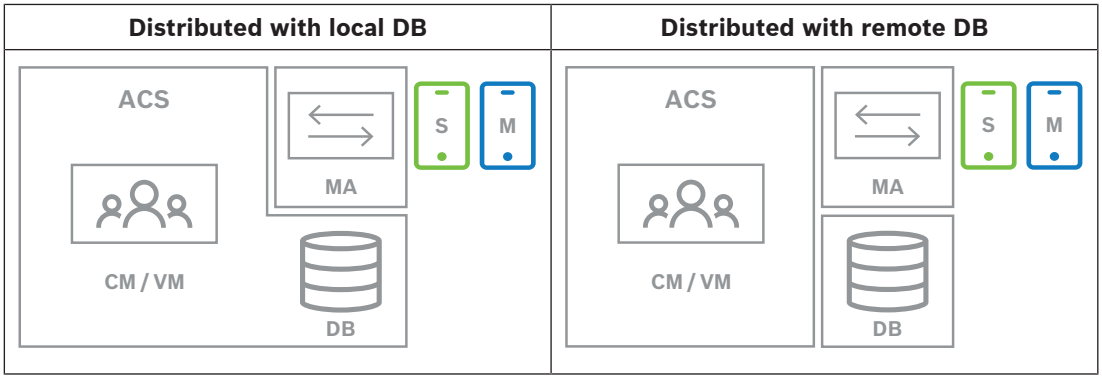
10. Click **Next**
11. On the **Core Components** screen, verify that the installation completed successfully, and click **Finish**
12. In the Windows *Services* application, verify that the service *Bosch Mobile Access* is running.

3.4.5 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.

3.5 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

3.6 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	/	/	/	/

3.6.1 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.

3.6.2 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.

3.7 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.

3.8 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 Credential Management users in the ACS

For AMS, every user of CredMgmtmust be a cardholder with a separate Operator definition.

These Operator definitions contain special CredMgmt 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 CredMgmt. You cannot assign multiple cardholders to the same Operator.

4.2 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 CredMgmt server followed by a colon and the port number (default *5806*)
   https://<My_CredMgmt_server>*:5806*
   The **Login** screen appears
2. Log on as a CredMgmt **Administrator** user.
3. Click to open the **Settings** menu.

4.3 Using the Settings menu for configuration

General	– **Retention period (days)**: This setting governs the handling of person records. – When the period elapses for the first time, the application anonymizes the record. – When the period elapses for the second time, the application deletes the record. Default value is *365*. Set 0 to deactivate the retention period completely. In this case, records are retained indefinitely. – **Logo**: Select or clear to check box that governs whether the dialogs display a customized logo or the default logo. – For criteria for customized logo files see: *Customizing the company logo, page 25* – **Supergraphic:** Select or clear to check box that governs whether the dialogs display the Bosch supergraphic. – Click **Preview** to show the dialog page as it would appear with these settings. See the next section for more details on Preview mode. – **Languages**: Select which languages are to be available in the user interface, along with their preferred **date** and **time** formats. – **Mail server** Enter the IP address, port number and account details of your email server, in order to enable the sending of emails from the application.

	– **Email templates** Several HTML email templates are provided, which you typically customize to your own requirements. For details, see the separate section **Email templates** below. – **Mobile Access** Select the **Mobile Access** check box to activate Mobile Access. **Connection**: Enter the address of the mobile access server (registration service address). *https://*<MyMobileAccessBackendServer>*:5700* Use an (FQDN) for <MyMobileAccessBackendServer> in multi-domain environments. **Note:** to use an IP address instead of an FQDN you must enter that IP address, under **Certificate creation**, when you run the setup wizard for the Mobile Access Backend. **Installer onboarding:** 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.

4.3.1 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.
After you download them from the **Settings** menu, the templates are stored in 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.

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

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

4.3.2 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.

– Changes made in the dashboard or menus are **not** saved.

– Click **Close preview mode** within the banner to close preview mode

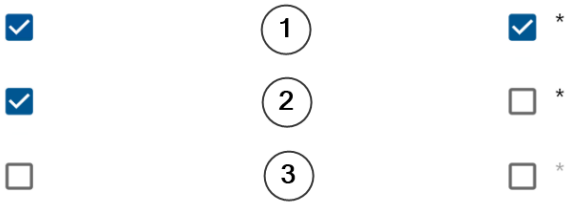
4.4 Customizing the UI

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

4.4.1 Setting options visible, invisible and mandatory

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

Example:



– (1) is visible and mandatory,

– (2) is visible but not mandatory

– (3) is not visible.

4.4.2 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

4.5 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 https://firebase.google.com/docs/cloud-messaging/concept-options

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 CreMgmt 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.

4.5.1 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

4.6 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:

4.6.1 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.

4.6.2 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.

4.6.3 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.

4.7 Data privacy and protection at Bosch

Introduction

In all business processes and in compliance with the applicable statutory requirements , we ensure that privacy is safeguarded, personal data is protected, and business information is kept secure. Technically and organizationally, and especially with regard to protection against unauthorized access and loss, we apply an appropriate standard that reflects the state of the art and takes account of the associated risks. When developing Bosch products and new business models, we ensure that the legal requirements governing data protection and information security are taken into account at an early stage.

Processing person-related data in the Mobile Access app and in the Mobile Access backend system

- Categories of personal data
  - The Mobile Access apps contain person-relatable data. This is the card-number information that is used to gain access at readers. Access to the actual data of real persons is only possible through the additional use of the AMS or Visitor Management programs.
  - The Installer registration procedure in the **Settings** menu does not need to store personal data. Nevertheless, some user information, such as email addresses, may be stored optionally.
  - The backend server for the Mobile Access app stores person-related data for credential management.
- Data transfer
  - Credential information is transferred between the backend system, the Mobile Access app and the Visitor Management system to control access at the readers.
- Logging of data

- The Mobile Access app keeps technical logs. These logs are stored locally on the mobile device and can be sent to third parties, such as technical support, if required.
- The backend server also keeps technical logs. The data are stored locally on the server system.
- By default, the backend server does not delete log files automatically. Nevertheless, automatic deletion can be configured based on remaining storage capacity or on a time schedule.

What have we done to make the product data protection friendly?

Bosch access control systems manage access rights for persons. To protect these persons, Bosch takes measures to integrate the requirements of the GDPR directly into product development, following a "privacy by design" approach.

- State-of-the-art encryption is used.
- Credential information is pseudonymized.
- The user of the app is not required to enter personal information in order to receive virtual credentials via QR-Code or mail.
- The deletion of credential information is possible from the Mobile Access apps, from the primary access control systems, and from auxiliary applications such as Visitor and Credential management.
- Credentials can be blocked by operators of the primary access control systems and auxiliary applications at any time.
- Telemetry data is anonymized by design.
- Log files are not transferred from mobile devices to other parties, such as technical support, without the user's active consent and cooperation.
- The scheduled automatic deletion of log files is configurable in the primary access control system.
- Bosch requires no registration in the app store or app. The app store forwards no personal data to Bosch.
- The app requires Bluetooth in order to function, but requests and requires the user to activate Bluetooth manually.

Further questions

For further information regarding data privacy, consult the data privacy notice in the Mobile Access app, or contact your Bosch project team.

5 Operation

5.1 Overview of user roles

The capabilities of the users of Credential Management are determined by their User Profiles in the ACS . See *Creating Credential Management users in the ACS, page 22* for more details. There are two basic types of user:

User type	Use cases
Operator	Assigning and deassigning physical access cards, and virtual credentials for mobile access
Administrator	Making global settings Customizing the behavior of the tool and its user interface plus All the use cases of Operator

Refer to

– *Creating Credential Management users in the ACS, page 22*

5.2 Using the dashboard

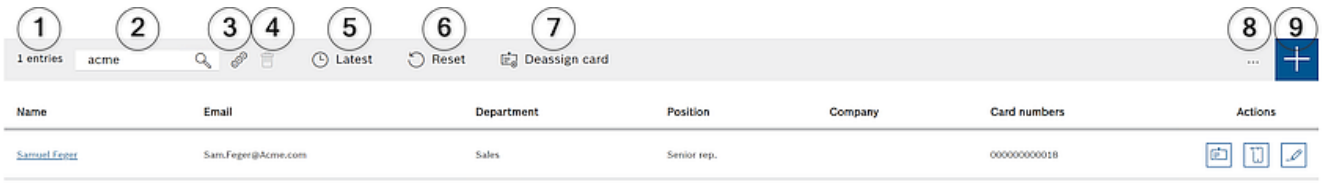
The dashboard is the home screen - a central dialog that leads to all other dialogs.

General use of the personnel table

Each row in the table represents a person. These are internal or external staff members who require credentials to access the premises.

– You can sort the table by any of its columns by clicking the column header.
– You can select individual persons, or several persons 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 persons to the table
– You can assign and deassign credentials by clicking the action buttons
  – Assign a physical credential
  – Assign a virtual credential (for mobile access)
  – Edit details for the person
– You can export the currently filtered lines to a `.CSV` or `.XLSX` file.

The functions of the dashboard



Label	Function
(1) N **entries**	The total number N of persons (each person is a row in the table).

Label	Function
(2) **Search**	Search for arbitrary text among the persons in the table
(3)	Select all the items in the list
(4) **Delete**	Deletes the selected items
(5) **Latest**	Show the persons that were added most recently to the table.
(6) **Reset**	Reset the table to its default view, and revert all filters.
(7) **Deassign card**	Open a dialog for deassigning assigned cards using a connected enrollment reader.
(8) **...**	Click the ellipsis symbol for a menu to export the currently filtered persons, and also documents, to various file formats, for example *.CSV* and *.XLSX* Note that for reasons of data security, you can only export if your client is running in a secured HTTPS connection, with a certificate.
(9)	Open a dialog for creating a new entry in the table

The columns of the dashboard

Column	Description
Name	Click the hyperlink to view the details of the person.
Email	
Department	
Position	
Company	
Card numbers	The numbers of the cards assigned to this person.
Actions	See separate table below

Actions to perform on personnel records in the dashboard table

Icon	Actions
	Assign one or more physical cards to the person
	Assign a virtual credential to the person for mobile access
	Edit the person's personnel details. Changes are propagated to the ACS. Changes made in the ACS are propagated to the CredMgmt application.

5.3 Assigning physical credentials

Prerequisites

It is highly recommended to assign fresh credentials to new personnel, using a fresh card, a card printer and an enrollment reader.

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

1. Have a physical access card ready to present to the enrollment reader.
2. Select the row of the person and click
3. Follow the instructions in the popup for use of the enrollment reader.

Assigning a card in the credentials editor (requires an enrollment reader)

1. On the dashboard, in the persons table, select a person and click to edit that person's credentials.
2. Click **Read card** and follow the instructions in the popup for use of the enrollment reader.

– Repeat the last steps to assign further cards, if required.

3. Click **Save** to save the current person with the card assignments.

5.4 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
– 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
– 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. Click the button **Add mobile access**
4. Select one of the large icons for the options:
– **QR code**
or
– **Invitation mail**
5. 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
– The mobile device functions like a physical access card, as long as the app is running
6. 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
– The mobile device functions like a physical access card, as long as the app is running

Refer to

– *Installing Mobile Access, page 12*
– *Installing the Mobile Access apps, page 18*

5.5 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.

5.6 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).

GDPR

The General Data Protection Regulation (GDPR) is a privacy and security law that was made by the European Union (EU), and came into effect in 2018, It imposes obligations on organizations anywhere that collect data related to people in the EU.

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
© Bosch Security Systems B.V., 2023

Building solutions for a better life.

202302201310