Building Technologies

Mobile Access 5.0
Credential Management 5.0
Visitor Management 5.0.1

Release notes

This document is intended to familiarize you with your new product version as quickly as possible

Version	Description
1	2023-02-28 Release of Mobile Access 5.0
2	
3	
4	

General note on documentation
Although every effort is made to keep translations as up-to-date as possible, late changes to the software may be documented only in English, and their translations available only after release of the product, or in the next version. In case of discrepancies, the English-language documentation should be regarded as more up-to-date.

Table of contents

2 11

1 Installation Notes

3 11

1.1 Visitor Management

1.1.1 Supported browser versions

These are the software requirements for the browser-based client of Visitor Management:

Browser software	Either one of: • Google Chrome, version 110 or higher • Microsoft Edge, version 110 or higher • Mozilla Firefox, version 109.01 or higher

1.2 Credential Management

1.2.1 Supported browser versions

These are the software requirements for the browser-based client of Visitor Management:

Browser software	Either one of: • Google Chrome, version 110 or higher • Microsoft Edge, version 110 or higher • Mozilla Firefox, version 109.01 or higher

1.3 Mobile Access

1.3.1 Avoid changing root certificate of AMS - #405888

Modifying the root certificate of the AMS should be the last resort to solve a technical problem and only be performed after careful consideration of the side-effects.

As described in the user documentation, the root certificate is distributed also to the readers during the enrollment phase. Moreover, the certificate of the Identity Server is derived from the root certificate, which in turn is checked when CredMgmt or VisMgmt talks to the Mobile Access backend.

In general, make sure that you keep backup copies of the certificates that you create, and their respective private keys.

1.3.2 App Stores

4 11

Both apps – Mobile Access and Setup Access – can be downloaded from the public app stores of both Apple and Google. The links are as follows:

	Apple App Store	Google Play Store
Mobile Access	https://apps.apple.com/de/app/bosch-mobile-access/id1580526947	https://play.google.com/store/apps/details?id=com.bosch.access.mobileaccess&gl=DE
Setup Access	https://apps.apple.com/de/app/bosch-setup-access/id1580527238	https://play.google.com/store/apps/details?id=com.bosch.access.readerconfig&gl=DE

1.3.3 Procedure to reset a BLE Reader Configuration

The following LECTUS Select variants support Bluetooth Low Energy (BLE):

F.01U.389.847	ARD-SELECT-BOM	Reader, OSDP, BLE, black
F.01U.389.848	ARD-SELECT-WOM	Reader, OSDP, BLE, white
F.01U.389.851	ARD-SELECT-BOKM	Reader, OSDP, keypad, BLE, black
F.01U.389.852	ARD-SELECT-WOKM	Reader, OSDP, keypad, BLE, white

LECTUS Select readers with Bluetooth modules offer two ways to remove a configuration from the device.

Option 1:
Prerequisite: Physical access to the reader

- Disconnect the reader from the power supply.
- On the back, set all DIP switches to zero.
- Reconnect the reader to the power supply and wait 1 minute (reader blinks in different colors).
- The reader beeps when the reset is complete.
- Disconnect the reader from the power supply.
- On the back, reset the DIP switches to the desired bus address.
- Reconnect the reader to the power supply

Note: This option also resets the OSDP key, which is used to encrypt the communication between reader and controller. Therefore, you must pair a newly reset reader with the AMC2 controller. For instructions, consult the configuration help of the primary access control system: **Creating entrances > Secure communication with OSDP**

Option 2:
Prerequisite: Installer certificate for configuring to this reader

- Open the Setup Access app.
- Wait for the reader to appear and select the device.
- Tap button “Reset” at the end of the page.

Note: this is not a factory reset, as it does not restore the original firmware version. It is nevertheless a way to remove any customer specific settings from the device.

You can set the firmware to factory default using the Setup Access App.

1.3.4 Procedure to restore a BLE Reader after an interrupted update process

If the upload of firmware to a reader is interrupted, the reader may fail to appear in the installer app. This is a rare case as the transmission takes only 10-20 seconds, and there is a warning against disrupting the upload in any way.

Cause: The new firmware was transferred only partially. The reader detects this incomplete state and stays in the so called **DFU mode**. It is essentially waiting for an upload of firmware, and therefore is not visible in the Setup Access app.

In this case, use the mobile app nRF Connect (Apple AppStore) from Nordic Semiconductor.

- Download the nRF Connect app from App store
- Open the app nRF Connect app

- Search for the reader and click **Connect** (the reader is shown as “INtacs Reader”)
- Open the **DFU** tab
- Click **Open Document Picker** and choose the firmware that you wanted to upload initially to the reader
- Click **Start** and wait for the successful upload
- Close the nRF Connect App and check with the Setup Access app if the reader is again visible.

1.4 Certificate Tool

The Certificate tool has been adapted to support Mobile Access. For further details, consult the AMS release notes.

2 New features

2.1 Credential Management

This is a new product.

2.2 Mobile Access

This is a new product.

3 Resolved issues

3.1 Visitor Management

3.1.1 Updated API calls to Mobile Access

Mobile Access requires the updated Visitor Management Version 5.0.1.

Some URLs in the Mobile Access backend’s REST-API have been harmonized with other Bosch APIs.

3.2 Credential Management

No issues. This is a new product.

3.3 Mobile Access

No issues. This is a new product.

3.4 Certificate Tool

No issues.

4 Known limitations

7 11

4.1 Visitor Management

4.1.1 After installing the certificate of external email server VisitorManagementServer Service needs to be restarted - #391881

Sometimes the network connection to external mail servers requires installation of additional certificates in the Windows Certificate store. Visitor Management service must be restarted for this change to take effect.

4.1.2 PNG file format for picture not supported - #395279

The file format PNG for user photographs is not supported in Visitor Management. Please use JPEG instead.

4.1.3 No support for Divisions - #401908

Visitor Management (VM) does not support AMS Divisions (“Tenants”). Do not use the Visitor Management product together with an AMS system where Divisions have been configured.

4.1.4 Do not delete SDK user - #403324

The SDK User, which you create when installing Visitor Management, may appear on the dashboard. Do not delete this user, as that will impact the communication between Visitor Management and the AMS.

4.1.5 Language switch not immediately applied to pulldown menus - #408602

When switching the language of the web user interface the language switch is not applied to items of pulldown menus. This happens for instance in the settings menu.
Workaround: Select the desired language and reload the full page in the browser.

4.1.6 Omnikey Reader not recognized when using Firefox browser - #408837

The fault occurs when a Peripheral Device (PD) certificate is missing from the internal Firefox certificate store.
Workaround:

1. Open the "Certificate Manager" tool from windows (on the machine where the PD tool has been installed)
2. Open "**Trusted Root Certification Authorities**

3. Select the PD certification called `BoschAcePeripheralDeviceAddonHardware CA`
4. Right click and export this certificate as "`DER encoded binary X.509 (.CER)`")
5. Start Firefox and open Firefox settings
6. Import the above certificate into the internal Firefox certification store.
7. Restart Firefox.

4.1.7 Expected departure is not synchronized to Visitor Management. - #410593

Visitor Management overrides the “authorized until” date for credential holders when the user edits any detail of a visit

4.2 Credential Management

4.2.1 Database becomes inconsistent after restoring Credential Management - #409651

Workaround: Deinstall CM with the option “**Deinstall Database**”, install AMS Backup, Install CM again. Note: The synch process may take considerable time.

4.2.2 No support for Divisions - #401908

Credential Management (CM) does not support AMS Divisions (“Tenants”). Do not use the Credential Management product together with an AMS system where Divisions have been configured.

4.2.3 Omnikey Reader not recognized when using Firefox browser - #408837

The fault occurs when a Peripheral Device (PD) certificate is missing from the internal Firefox certificate store.

Workaround:

1. Open the "Certificate Manager" tool from windows (on the machine where the PD tool has been installed)
2. Open "**Trusted Root Certification Authorities**
3. Select the PD certification called `BoschAcePeripheralDeviceAddonHardware CA`
4. Right click and export this certificate as "`DER encoded binary X.509 (.CER)`")
5. Start Firefox and open Firefox settings
6. Import the above certificate into the internal Firefox certification store.

7. Restart Firefox.

4.2.4 Language switch not applied for pulldown menu entries - #408602

When switching the language of the web user interface the language switch is not applied to items of pulldown menus. This happens for instance in the settings menu.
Workaround: Select the desired language and reload the full page in the browser.

4.2.5 Do not delete SDK user - #403324

The SDK User, which you create when installing Credential Management, may appear on the dashboard. Do not delete this user, as that will impact the communication between Visitor Management and the AMS.

4.2.6 PNG file format for picture not supported - #395279

The file format PNG for user photographs is not supported in Credential Management. Please use JPEG instead.

4.2.7 After installing certificate of external email server CredentialManagementServer Service needs to be restarted - #391881

Sometimes the network connection to external mail servers requires installation of additional certificates in the Windows Certificate store. Credential Management service must be restarted so that this change takes effect.

4.2.8 Slow synchronization with AMS - #409658

The synchronization of employee data between AMS and Credential Management is slow when the number of persons is large (> several thousands). We have observed that syncing 50,000 persons may take 2 hours.

4.2.9 The blocking of persons in AMS is not synched to Credential Management - #410363

The blocking of a person in AMS is not translated to a blacklisting in Credential Management.

4.3 Mobile Access

10 11

4.3.1 Mobile Access is not covered by the AMS Backup and Restore tool - #402572 #408255

Mobile Access is not covered by the AMS Backup and Restore tool. Please use SQL Server integrated solution for backup and restore, e.g. the SQL Management Studio. Please also export certificates and private keys from the Windows certificate store. If they are required, please also back up the log files.

4.3.2 Some files are not removed by uninstallation - #399789, #399787

After successful uninstallation of the Mobile Access backend, some files are not deleted:

- `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Identity Server\appsettings.Extension.MobileAccessBackend`
- `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Certificates\Config\config.Extension.MobileAccessBackendStandalone`

Please remove the files manually.

4.3.3 Certificates are not removed by uninstallation - #399787

After successful uninstallation of the Mobile Access backend, the Windows Certificate store still contains the backend's certificates and private keys. This is by design so that important security data is not deleted accidentally. Please export the data and delete it manually if desired.

4.3.4 User not deleted after uninstallation - #399315

After successful uninstallation of the Mobile Access there remains a Windows user "MAUser". This is the user that runs the backend service.
Workaround: Remove the user manually after uninstallation.

4.3.5 Modified settings do not appear immediately- #339260

In Visitor Management, changes to stored documents, such as an NDA, are not propagated immediately to clients already running in kiosk mode.
Workaround: Close the tab where the kiosk mode is open and restart it.

4.3.6 Deleting the content of the text fields when reconfiguring a mail server - #405888

11 11

The settings dialog for configuring a mail server cannot delete the contents of multiple text fields simultaneously.
Workaround: Click **Save** after deleting each individual text field.

4.3.7 Operating systems of mobile devices may halt backgrounded apps

The Mobile Access app can run in background to open doors as the user approaches them. However, the operating system (iOS or Android) may decide to stop backgrounded apps that have not been used for a long time. This behavior is outside of the control of the app.
Workaround: Check that the app is still running in the background, and if not, restart it manually.