ACE Visitor Management

en Installation / Configuration / Operation

Table of contents

1 Introduction

1.1 About Bosch Visitor Management

Bosch 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

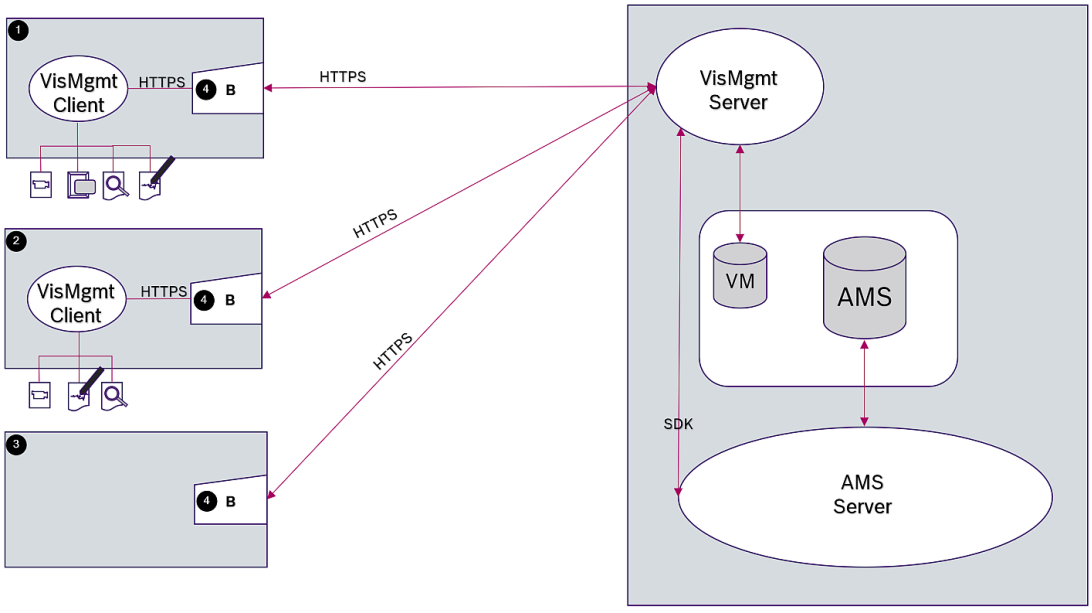
1.2 Intended audiences

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

1.3 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 **Reception** workstation, with enrollment reader and other peripheral hardware.
2	The **Visitor** kiosk workstation, with browser in kiosk mode and peripheral hardware.
3	The **Host** (the employee visited) workstation
4	Supported browser

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 VisMgmt client is installed 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

The server is the computer that runs the VisMgmt application.

Operating systems	Windows 10, Windows Server 2016
Database management systems	MS SQL Server 2017 and later
Supported browsers	Google Chrome, Mozilla Firefox, Microsoft Edge (Chromium based)
Minimum monitor resolution (for using the application UI)	Full HD 1920x1080

Client requirements

The client is the computer that runs the browser that connects to the VisMgmtserver, and also connects physically to the peripheral hardware: enrollment reader, web camera, signature scanner and document scanner.

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.

Supported browsers	Google Chrome, Mozilla Firefox, Microsoft Edge (Chromium based)
Minimum monitor resolution	Full HD 1920x1080

3.1.1 The main access control system

VisMgmt works with the following Bosch access control systems:

– Access Management System (AMS) versions 3.0.1 and later
– BIS Access Engine (ACE) versions 4.9 and later

Complete and verify the installation of the main access control system 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 VisMgmtdatabase, *dbVisitorManagement*.

The default name of this instance is *ace*.

Alternatively, during the installation of the VisMgmt server, you can create the VisMgmt database on a pre-existing database instance on the network, provided you have administrator access to that instance.

3.1.3 A dedicated user for local database access

The user *VMUser* accesses the Visitor Manager database on behalf of the VisMgmt application. By default, 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 your policies, and 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. Accept the End User License Agreement (EULA) 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. Enter values for the following parameters:

SQL server	The name of the database server computer
SQL instance	The name of the database instance where the visitor database is to be created
SQL user name	The name of an administrator user of the instance, typically *sa*
SQL password	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:

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

10. Click **Next** to continue

– On the **Identity server configuration** screen

11. Select **AMS identity server**
12. Enter the name of the ACE server followed immediately by the port number *:44333*
13. Click **Test connection** to test whether the identity server is reachable.
    Due to network timeouts you may need to click **Test connection** more than once.
14. Click **Next** for the summary screen, then click **Install** to start the installation of the VisMgmt server.
15. 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.

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
PageSizeNumberOfVisit	*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.
MaximumUploadFileSizeBytes	*31457289*	The maximum number of bytes that an uploaded file may contain.
StartoverTimeoutAskSeconds	*300*	The application waits this number of seconds if the user pauses during the input of login information, then it prompts for input.
StartoverTimeoutResetSeconds	*60*	After prompting, the application waits this number of seconds before resetting the login screen.

3.3 Installing the Client

The VisMgmt client can be installed on the server computer, but is usually installed on a separate computer in the same network. If so, copy the HTTPS certificate from the ACE server and install it on the separate computer also. See *Certificates for secure communication, page 11* below for instructions.
The client setup program installs connecting software for peripheral 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 application.

Refer to
– *Certificates for secure communication, page 11*

3.3.1 Running the client setup program

1. On the intended VisMgmt client, as Administrator, run *BoschVisitorManagementClient.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.
– On the **Client configuration** screen
3. Enter the name of the VisMgmt server, and the port number given on the screen (default value *5706*).
4. 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.
5. Click **Next** for a summary of the components to be installed.
6. Click **Install** to start the installation.
7. Click **Finish** to finish the installation.
8. After installation, reboot the computer.

3.3.2 Certificates for secure communication

For secure communication between the VisMgmt client or server computer and the main access control system, copy the following certificate from the ACE server to the VisMgmt computers. Use an account with Windows administrator rights to install it.
The usual path to the certificate is:

– For BIS ACE: *<installation drive>:\Inetpub\wwwroot\<Hostname>.cer*

3.3.3 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 VisMgmt 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

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

– For BIS ACE: *<installation drive>:\Inetpub\wwwroot\<Hostname>.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 VisMgmt client, you can use the default certificate. You can find it on the client at the following location:
C:\Program Files (x86)\Bosch Sicherheitssysteme
\Bosch Visitor Management Client\BoschAceVisitorManagementHardware CA.cer

Procedure (repeat for each certificate and Firefox profile):
Use the following procedure on the VisMgmt 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.

3.3.4 Appsettings JSON file

A number of configuration parameters for the VisMgmt client 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
CorseOrigins	*"https://my-vm-server:5706"*	The address and port number of the Visitor Management server.
CardReaderPort	*"com3"*	The COM port number to which the enrollment reader is connected.

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 Peripheral hardware

The following peripheral USB devices have been tested and approved for use with Bosch Visitor Management 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 5000 MD
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 VisMgmt client computers. The client setup program installs the necessary connecting software for communication with VisMgmt

3.5.1 Registering peripheral hardware with the client application.

To register peripheral hardware with the VisMgmt client, run the client setup program on the client. For instructions see *Running the client setup program, page 10*.

Refer to

– *Running the client setup program, page 10*

3.6 Uninstalling the software

To uninstall VisMgmt from the VisMgmt server or client:

1. With Windows administrator rights, start the Windows program **Add or remove programs**.
2. Select the **Bosch Visitor Management** program (server or client) and click **Uninstall**.
3. (For 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 VisMgmt installation.

4. Select whether you want to remove the VisMgmt 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**.

– 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:

– Configuration Browser > **Administration** > **ACE User profiles**

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.

Assiging User profiles to ACS operators and cardholders

Dialog path:

– Configuration Browser > **Administration** > **Operators**

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 VisMgmt **client** software, 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 VisMgmt **client** software, 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
Chrome	https://support.google.com/chrome/a/answer/9273974
Firefox	https://support.mozilla.org/en-US/kb/firefox-enterprise-kiosk-mode
Edge	https://docs.microsoft.com/en-us/deployedge/microsoft-edge-configure-kiosk-mode

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:

General settings	– **Retention period (days)**: This setting governs the handling of visit 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 visit records are retained indefinitely. – **Document storage mode**: Select whether documents are to be stored as paper or digital files. – **Maximum number of visitors** allowed on the site at one time. Default value is *100*. Set *0* to deactivate the visitor counters on the dashboard completely. – **Document expiry period (days)**: 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 *365* – **Document expiry warning period (days)**: 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. – Select or clear the check boxes that govern whether the Bosch **Supergraphic** and the **Bosch logo** appear in the dialogs. – 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.
Receptionist	– This settings screen contains 2 check boxes for each of the data fields in the receptionist's visitor registration dialogs.

	– Clear or select the first check box to govern whether the data field is **visible** at all the registration dialogs. – Clear or select the second check box (marked with an asterisk) to govern whether the data field is **mandatory**. – Customize the default header texts in the data-collection dialogs. For more details, see *Customizing the UI, page 17* below.
Host **Visitor**	The settings for the **Host** and **Visitor** users remain read-only until you have edited and saved the settings for **Receptionist**. Fields that you mark as not visible in the **Receptionist** settings are automatically set not visible for **Host** and **Visitor**. After that, the configuration procedure is identical.

Refer to

– *Customizing the UI, page 17*

4.6.1 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
– Use the **Change role** list within the banner to preview the appearance of the interface for the different user types: **Receptionist**, **Host**, **Visitor**.

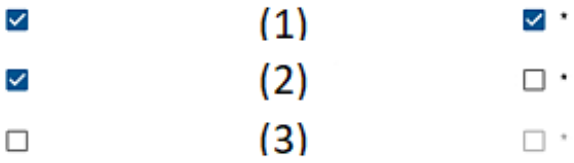
4.6.2 Customizing the UI

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

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.

Customizing UI texts for localization

You can easily customize the texts of the user interface on a per-language basis.

By default, **localization text** contains the standard headers for blocks of data fields in the data collection dialogs.

To customize these headers to local requirements:

1. Select a UI language from the list.

2. Overwrite the texts in the text box.
   You may use HTML tags for simple formatting, for example:
   *this text will appear bold *
   italics
   <u>underline</u>

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.

4.6.3 Document templates
Upload templates for various documents in the **Dashboard** > **Settings > General** dialog.

4.7 Firewall settings

Add Visitor Management 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:

– Server

[Server name]:44333 - used by the AMS Identity Server

[Server name]:5706 - used by the VisMgmt Server

– Client

localhost:5707 - used by the VisMgmt Client

4.8 Network security

The security of an organization’s access control systems 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 basically responsible for at least the following:

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.
- 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.

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 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**
<current count> */ <total capacity>*	*<current count>* */ <total capacity>*	*<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 16*.

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 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

The horizontal tool bar has the following functions:

Label	Function
1 N **entries**	The total number N of visits (each visit is a row in the table).
2 **Search**	Search for arbitrary text among the visits in the table
3	Show the visits that were added most recently to the table.
4	Open a dialog for selecting filter criteria
5	Reset the table to its default view, and revert all filters.
6 **Deassign card**	Open a dialog for deassigning assigned cards using a connected enrollment reader.
7	Open a dialog for creating a new visit entry in the table

5.2.2 Table columns and actions

Columns

Column	Value	Description
Status	Visit expected Visit approved Visit declined Card assigned Card expired	An icon reflecting the status of the visit

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

Actions

Icon	Function
	**Approve** 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 *Adding, removing and exempting from the blacklist, page 25*
	**Decline** the visit. This button is deactivated after the visitor has checked in, that is, when they already have a card.
	**Assign** one or more cards to the visitor
	**Edit** the visit event and/or the visitors credentials

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 29*.

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 12* 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 the name of the employee visited under **Host**.
  - Note that you can select only cardholders of the main access control system.
- 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.
- 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 12*

5.3.4 Approving and declining visitors

It is necessary to approve a visit before you can assign cards to a visitor. 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:

- **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 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.

5.3.6 Assigning and deassigning cards

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 visitors, page 24*
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 visitor, 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.
4. 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 

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 **Current visit** 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 have not yet been assigned.
   – Click  next to a card number to assign that card to the current visitor.
   – Repeat the last step to assign further cards, if desired.

5. Click **Save** to save the current visit with the card assignments.
6.

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 **Current visit** 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 

5.3.7 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.

5.3.8 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
	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 VisMgmt **client** software, 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.

Bosch Access Systems GmbH
Charlottenburger Allee 50
52068 Aachen
Germany
www.boschsecurity.com

202106241438