Visitor Management V5.5

C Mobile Access

ru Руководство пользователя

Содержание

1 Безопасность

Используйте последнюю версию программного обеспечения

Прежде чем впервые использовать устройство, убедитесь в том, что на нем установлена последняя версия программного обеспечения. Чтобы обеспечить постоянную работу, совместимость, эффективность и безопасность, регулярно обновляйте программное обеспечение в течение всего срока эксплуатации устройства. Следуйте инструкциям по обновлению программного обеспечения, приведенным в документации к продукту. Дополнительные сведения см. по ссылкам ниже:

- Общие сведения: https://www.boschsecurity.com/xc/en/support/product-security/
- Рекомендации по безопасности, представляющие собой список известных уязвимых мест и предлагаемых решений: https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html

Компания Bosch не несет ответственности за ущерб, вызванный эксплуатацией ее продукции с устаревшими программными компонентами.

2 Введение

2.1 О программе Bosch Visitor Management

Программное обеспечение Visitor Management, далее называемое VisMgmt, — это браузерное программное средство, которое работает совместно с системами управления доступом Bosch. Оно позволяет управлять посещениями объектов с контролируемым доступом, в том числе планированием посещений, персональными данными посетителей, связанными документами и контрактами, а также назначением временных учетных данных.
Пользовательский интерфейс настраивается, при этом любой пользователь может оперативно изменить язык интерфейса, не завершая сеанс.
Основные пользователи и сценарии использования:

Тип пользователя	Сценарии использования
Работник приемной	Регистрация новых посещений и посетителей Утверждение и отклонение посещений Добавление посетителей в черный список Назначение и отмена назначения карт посетителей Управление связанными документами Отслеживание количества посетителей на объекте
Посетитель	Самостоятельная и предварительная регистрация Создание и сопровождение профиля посетителя Подписание документов
Принимающая сторона	Управление расписаниями и списками посещений и посетителей Предварительная регистрация посещений
Администратор	Установка глобальных параметров Настройка поведения инструмента и его пользовательского интерфейса Дополнительно: Все варианты использования для работника приемной

2.2 О службе Mobile Access

Mobile Access — это средство управления доступом лиц с помощью виртуальных учетных данных, хранимых на мобильном устройстве, например на смартфоне. Управление виртуальными учетными данными осуществляется в основной системе управления доступом, или ACS.

- Операторы системы ACS генерируют и назначают виртуальные учетные данные, а также отправляют их пользователям с помощью взаимодействующих с ACS веб-приложений.
- Владельцы мобильных учетных данных взаимодействуют со считывателями контроля доступа по Bluetooth с помощью приложения Mobile Access на своих мобильных устройствах.
- Установщики систем Mobile Access настраивают считыватели контроля доступа по Bluetooth с помощью специального приложения настройки на своих мобильных устройствах.
- Система не хранит персональные данные на мобильных устройствах.

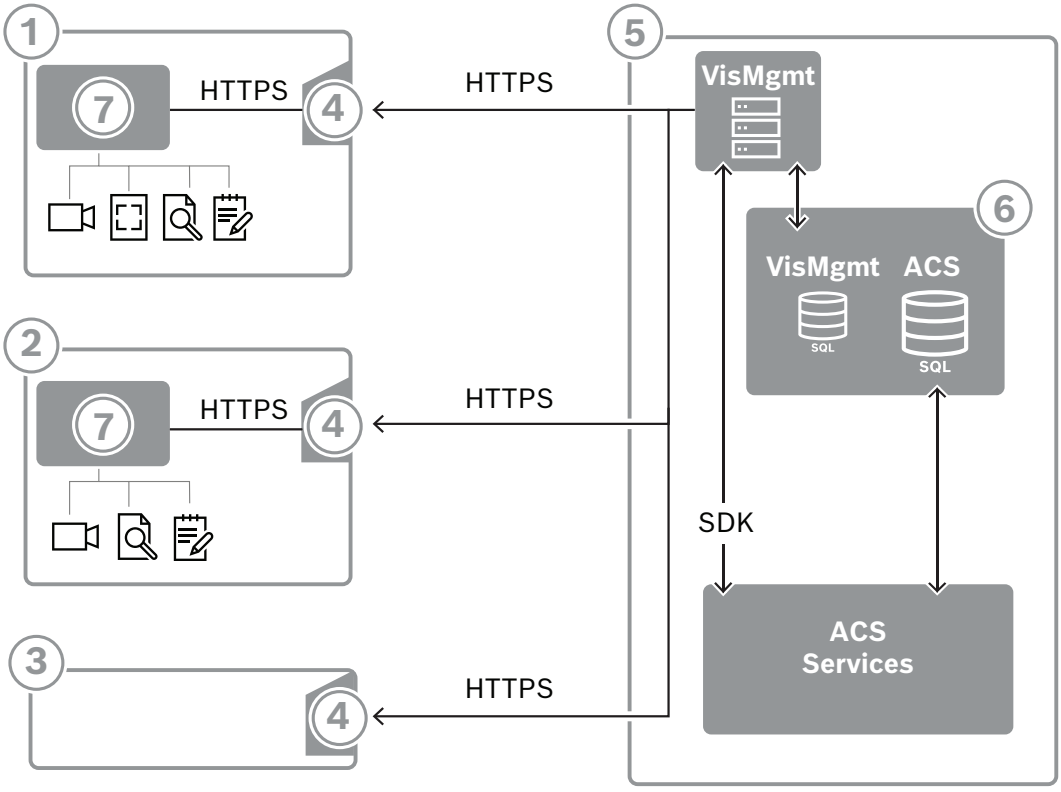
2.3 Целевая аудитория

- Установщики и администраторы Visitor Management
- Основные типы пользователей Visitor Management

2.4 Использование данного документа

- Воспользуйтесь функцией **Поиск** в средстве просмотра справки, чтобы найти необходимое содержимое.
- Разделы **Обзор системы, Установка** и **Конфигурация** преимущественно представляют интерес для системных администраторов.
- Раздел **Эксплуатация** в первую очередь представляет интерес для пользователей системы.

3 Обзор и топология системы



Метка	Описание
1	Рабочая станция **Receptionist (Работник ресепшена)**. Эта рабочая станция может иметь дополнительное периферийное оборудование, в частности, считыватель регистрации, веб-камеру и сканеры для подписей и документов.
2	Рабочая станция-киоск **Visitor (Посетитель)** с браузером в режиме киоска. Эта рабочая станция может иметь дополнительное периферийное оборудование, в частности, веб-камеру и сканеры для подписей и документов.
3	Рабочая станция **Host (Принимающий)** – это рабочая станция сотрудника, принимающего посетителя.
4	Поддерживает работу в браузере с сайтом VisMgmt
5	Сервер ACS (BIS или AMS)
6	Экземпляр базы данных сервера ACS (может находиться на отдельном компьютере).
7	Опциональная **Надстройка для периферийных устройств Bosch**, регулирует обмен данными между браузером и периферийным оборудованием.

Рекомендуемая топология системы включает сервер VisMgmt, расположенный на том же компьютере, что и основная система управления доступом, и его базу данных в том же экземпляре базы данных.

Надстройка для периферийных устройств Bosch устанавливается только на тех рабочих станциях, которым требуется доступ к периферийным устройствам.
Для рабочей станции принимающей стороны обычно требуется только доступ к серверу VisMgmt с помощью браузера.

4 Установка и удаление

4.1 Требования к оборудованию и программному обеспечению

Установите сервер VisMgmt на компьютер, на котором установлена основная система управления доступом. Действуют те же требования к программному и аппаратному обеспечению.
Если основная система управления доступом еще не установлена, установите ее перед установкой Visitor Management.
При первой установке или обновлении соблюдайте приведенный ниже порядок установки.

1. Основная система управления доступом — Access Management System.
2. Credential Management и/или Visitor Management.
3. Mobile Access.

Требования к серверу

Операционные системы	– Windows 11 Профессиональная и Корпоративная 23H2; – Windows Server 2019 (Version 1809) (64bit, Standard, Datacenter); – Windows Server 2022 (64-разрядная, выпуски Standard и Datacenter)
Системы управления базами данных	– MS SQL Server 2019 and later Всегда используйте тот же экземпляр базы данных, что и ACS (основная система управления доступом)
Минимальное разрешение монитора	Full HD 1920 x 1080
Поддерживаемые браузеры	Google Chrome, Mozilla Firefox, Microsoft Edge (на основе Chromium) Используйте самую новую версию браузера для операционной системы Windows .

Требования для надстройки периферийных устройств Bosch
Надстройка **периферийных устройств Bosch** — это программа, обрабатывающая электронную связь между браузером и периферийными устройствами, такими как считыватель регистрации, веб-камера, сканер подписи и сканер документов.
Клиентским компьютером является компьютер, физически подключенный к периферийному оборудованию. Он также запускает браузер, который подключается к серверу VisMgmt.
Несмотря на то, что периферийные устройства не являются обязательными для установки, их использование настоятельно рекомендуется, так как они значительно повышают эффективность процесса регистрации посетителей.

Требование	**Описание**
Минимальное разрешение монитора	Full HD 1920x1080

Требование	Описание
Поддерживаемые браузеры	Google Chrome, Mozilla Firefox, Microsoft Edge (Chromium based) Используйте самую новую версию браузера для операционной системы Windows.

4.1.1 Основная система управления доступом

Без службы Mobile Access

Если служба Mobile Access не требуется, система VisMgmt версии 5.5 может работать со следующими системами управления доступом Bosch:

– Access Management System (AMS) версии 5.5 и выше

Со службой Mobile Access

Если в качестве дополнительной лицензии выбрано Mobile Access, система VisMgmt версии 5.5 может работать со следующими системами управления доступом Bosch:

– Версии Access Management System (AMS) 5.5 (с расширением Mobile Access) и выше

Завершите и проверьте установку основной системы управления доступом по соответствующей инструкции по установке прежде, чем устанавливать VisMgmt.

4.1.2 Экземпляр базы данных для размещения базы данных Visitor Manager

При установке основной системы управления доступом создается экземпляр базы данных, который можно использовать для размещения базы данных VisMgmt, `dbVisitorManagement`.

Имя такого экземпляра по умолчанию зависит от сервера ACS

– Для AMS именем является `ACE`
– Для BIS ACE именем является `BIS_ACE`

4.1.3 Выделенный пользователь для доступа к локальной базе данных

Пользователь `VMUser` обращается к базе данных Visitor Manager от имени приложения VisMgmt.

Программа установки сервера VisMgmt создает пользователя Windows `VMUser` на сервере VisMgmt.

4.1.4 Выделенный пользователь для доступа к удаленной базе данных

При необходимости использовать для VisMgmt базы данных на удаленном сервере баз данных, создайте и настройте пользователя `VMUser` в Windows и на сервере SQL Server, как описано ниже.

ВНИМАНИЕ: не запускайте настройку VisMgmt до завершения этой операции.

1. На удаленном сервере баз данных создайте пользователя Windows со следующими параметрами:

– **Имя пользователя** (с учетом регистра): `VMUser`
– **Пароль**: настройте пароль в соответствии с политиками безопасности, применяемыми ко всем вашим компьютерам. Обратите внимание, что он потребуется для настройки VisMgmt.

- **Участник группы**: Administrators
- **При следующем входе в систему пользователь должен изменить пароль**: NO
- **Пользователь не может изменить пароль**: YES
- **Срок действия пароля не ограничен**: YES
- **Вход в качестве службы**: YES
- **Учетная запись отключена**: NO

(Добавить VMUser как данные для входа на удаленный сервер SQL Server)

1. Откройте центр SQL Management Studio
2. Подключитесь к удаленному экземпляру SQL
3. Перейдите в раздел **Security (Безопасность)** > **Login (Вход)**
4. Добавьте пользователя VMUser с ролью сервера sysadmin

Затем, когда вы запустите настройку VisMgmt на сервере VisMgmt, выберите опцию компьютера **удаленного сервера баз данных** и введите пароль, заданный выше для VMUser.

4.1.5 Выделенный пользователь в основной системе управления доступом

1. В основной системе управления доступом создайте пользователя с функцией **неограниченного использования API-интерфейса**.
   Подробная информация приведена в главе **Назначение профилей пользователей (операторов)** руководства оператора основной системы управления доступом.
2. При использовании BIS ACE войдите под этим пользователем в классический BIS клиент или Smart клиент чтобы задать пароль.
3. Запомните имя пользователя и пароль, поскольку они потребуются для мастеров установки VisMgmt.

4.2 Установка сервера

Не запускайте программу установки, пока не будут соблюдены все требования к программному обеспечению.
Если в корпоративной среде используется AMS, Visitor Management, Credential Management, Mobile Access, рекомендуется использовать сертификаты, выданные корпоративным ЦС (центром сертификации). Сертификаты необходимо получить перед установкой любой серверной системы. См. раздел *Использование пользовательских сертификатов* в руководстве по установке AMS.

4.2.1 Запуск программы установки сервера

1. На будущем сервере VisMgmt от имени администратора запустите BoschVisitorManagementServer.exe.
2. Нажмите кнопку **Далее**, чтобы принять пакет установки по умолчанию.
3. Если вы согласны с лицензионным соглашением конечного пользователя (EULA), примите его и нажмите **Далее**.
4. Выберите папку назначения для установки. Рекомендуется использовать папку по умолчанию.

– На экране **Конфигурация SQL-сервера** выполните следующие действия.

5. Выберите, следует ли создать базу данных на локальном экземпляре SQL-сервера, который находится в экземпляре базы данных на сервере VisMgmt, либо на удаленном компьютере сервера баз данных.

– **Примечание.** Если выбран удаленный сервер баз данных, программа установки запросит пароль `VMUser`, пользователя с правами администратора, созданного на удаленном сервере баз данных (см. раздел «Требования к программному обеспечению»).

6. Проверьте и, если необходимо, измените значения для следующих параметров:

Сервер SQL	Имя компьютера сервера базы данных
Экземпляр SQL	Имя экземпляра главной базы данных ACS. Именно здесь создается база данных посетителей. Для AMS именем является `ACE` Для BIS ACE именем является `BIS_ACE`
Имя пользователя SQL	Имя пользователя с правами администратора экземпляра. Как правило, это `sa`.
Пароль SQL	Пароль этого администратора.

7. Нажмите **Проверить подключение**, чтобы проверить возможность доступа к экземпляру базы данных с помощью указанных вами значений параметров. Если проверка не пройдена, убедитесь в правильности указанных параметры.
8. Нажмите кнопку **Далее**, чтобы продолжить.

– На экране **Конфигурация доступа к ACS** (где ACS означает основную систему управления доступом, AMS или ACE) выполните следующие действия.

9. Введите значения для следующих параметров:

Имя узла ACS	Имя компьютера, на котором работает система ACS
Имя пользователя ACS	Имя выделенного пользователя ACS с неограниченным доступом к использованию API. См. раздел «Требования к программному обеспечению».
Пароль ACS	Пароль данного выделенного пользователя ACS.

10. Нажмите кнопку **Далее**, чтобы продолжить.

– На экране **Конфигурация сервера идентификации** выполните следующие действия.

11. Введите URI соответствующего сервера удостоверений ACS:
    – AMS: `HTTPS://<ИмяСервераACS>:44333`
    – BIS: `HTTPS://<ИмяСервераACS>/BisIdServer`
12. Нажмите **Проверить подключение**, чтобы проверить возможность доступа к серверу идентификации.
13. Нажмите кнопку **Далее** для отображения сводных сведений, а затем нажмите **Установить**, чтобы начать процесс установки сервера VisMgmt.
14. После установки перезагрузите компьютер.

4.2.2 Файл JSON AppSettings

Несколько параметров конфигурации сервера VisMgmt хранятся в следующем файле `.JSON`:

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

Как правило, изменять значения по умолчанию не требуется, однако в разделе **Settings** (Параметры) этого файла может быть полезно настроить следующие параметры. При изменении параметров необходимо предварительно создать резервную копию файла. Резервная копия поможет быстро отменить изменения, если эти изменения приведут к несоответствующей работе.
Сохраните изменения и перезапустите службу Windows VisMgmt, чтобы измененные параметры вступили в силу. Имя службы — `Bosch Visitor Management`.

Имя параметра	Значение по умолчанию	Описание
`PageSizeNumberOfVisit`	`20`	Максимальное количество посещений, одновременно отображаемых на экране. При прокручивании пользователем на каждой новой странице отображается указанное количество записей, загруженное из базы данных.
`MaximumUploadFileSizeBytes`	`31457289`	Максимальное количество байтов, которое может содержаться в загруженном файле.
`StartoverTimeoutAskSeconds`	`300`	Количество секунд, которое приложение ожидает, если пользователь приостанавливает ввод регистрационной информации, а затем запрашивает учетные данные.
`StartoverTimeoutResetSeconds`	`60`	После запроса приложение ожидает в течение указанного количества секунд, а затем сбрасывает экран входа в систему.

4.3 Настройка компьютера клиента VisMgmt

Надстройка для периферийных устройств Bosch может быть установлена на компьютер с сервером, но обычно она устанавливается на клиентский компьютер в той же сети. В этом случае следует скопировать сертификат HTTPS с сервера ACS и установить его на клиентском компьютере. Инструкции см. в разделе *Сертификаты для защищенной связи, Страница 16* ниже.
Надстройка для периферийных устройств Bosch – это программное обеспечение для подключения периферийных устройств, таких как регистрационные считыватели и сканеры. Если такие устройства не требуются, например для пользователя host (принимающий), то для входа в систему и запуска приложения VisMgmt достаточно доступа к браузеру.

Поддерживаются следующие регистрационные считыватели и форматы карт.

	Код Bosch MIFARE DESFire EV1	MIFARE DESFire EV1 CSN	MIFARE Classic CSN	HID Prox 26 бит	iCLASS 26 бит	iCLASS 35 бит	iCLASS 37 бит	iCLASS 48 бит	EM 26 бит
LECTUS enroll ARD-EDMCV002-USB	X								
OMNIKEY 5427 CK		X	X	X	X	X	X	X	X

См.

– *Сертификаты для защищенной связи, Страница 16*

4.3.1 Настройка надстройки для периферийных устройств

Надстройка для периферийных устройств требуется только на клиентских компьютерах, подключаемых к регистрационным считывателями, сканерам и другим периферийным устройствам. Повторите описанную ниже процедуру на каждом клиентском компьютере, где это необходимо.

1. На выделенном клиентском компьютере от имени администратора запустите `BoschPeripheralDeviceAddon.exe` с установочного носителя.
   – Будут перечислены основные компоненты, т. е. программное обеспечение клиента и программное обеспечение для обычно используемого периферийных устройств. Рекомендуется установить все перечисленные компоненты, даже если в настоящее время оборудование недоступно.
2. Нажмите кнопку **Далее**, чтобы принять пакеты установки по умолчанию.
3. На экране **Конфигурация клиента** выполните следующие действия.

– **Каталог установки:** примите выбранное по умолчанию (рекомендуется) или измените по необходимости.
– **COM-порт:**
  – При использовании регистрационного считывателя LECTUS введите номер COM-порта, например `COM3`, к которому подключен регистрационный считыватель. Проверьте это значение в диспетчере устройств Windows.
  – При использовании считывателя HID OMNIKEY оставьте это поле пустым.
  – Камера, устройство SignoPad и сканер документов готовы к работе из коробки и не требуют настройки COM-порта. Когда в браузере появится окно с запросом разрешить подключение, нажмите **Разрешить**.
– **Адрес сервера** и **порт:**
  – Введите имена любых компьютеров с сервером (по умолчанию хотя бы имя основного компьютера с сервером ACS) и номера портов любых внутренних служб, которым необходима возможность управлять периферийными устройствами.
  Затем нажмите кнопку **Проверить подключение** и дождитесь подтверждения для каждого компьютера или службы.
  Нажмите **Добавить**, чтобы добавить дополнительные серверы.
  Нажмите **Удалить**, чтобы удалить серверы.

– Порты по умолчанию для стандартных серверных служб:
  5806 для CredMgmt
  5706 для VisMgmt

4. Нажмите **Далее** для получения сводки компонентов, которые будут установлены.
5. Нажмите **Установить**, чтобы начать установку.
6. Нажмите кнопку **Готово**, чтобы завершить установку.
7. После установки перезагрузите компьютер.

4.3.2 Сертификаты для защищенной связи

Для безопасного обмена данными между браузером на клиентском компьютере и сервером ACS скопируйте следующий сертификат с сервера ACS на клиентские компьютеры. Для установки воспользуйтесь учетной записью с правами администратора Windows.

Обычный путь к сертификату:

– <установочный диск>:
  `\Bosch Sicherheitssysteme\Access Management System\Certificates\Bosch Security System Internal CA - BISAMS.cer`

Примечание. После разворачивания сертификата перезапустите серверную часть Mobile Access или службу Bosch Credential Management и Visitor Management.

Обзор путей передачи сертификатов

Из → **В ↓**	**ACS**	Серверная часть **MA** Mobile Access	**DB** База данных	**S** Приложение настройки	**M** Приложение доступа владельца карты	**R** Считыватель
ACS	/	Передается мастером установки (с помощью инструмента сертификации)	/	/	/	/
Серверная часть **MA** Mobile Access	Передается мастером установки мобильного доступа	/	/	Передается при регистрации с помощью QR-кода Обновляется с помощью push-уведомления	Передается при регистрации с помощью QR-кода Обновляется с помощью push-уведомления	/

DB База данных	/	/	/	/	/	/
S Приложение настройки	/	Передается при регистрации с помощью QR-кода	/	/	/	/
M Приложение доступа владельца карты	/	Передается при регистрации с помощью QR-кода	/	/	/	/

4.3.2.1 Сертификаты для браузера Firefox

Можно пропустить этот раздел, если вы не используете браузер Firefox.

Браузер Firefox обрабатывает корневые сертификаты по-другому: Firefox не обращается к хранилищу сертификатов Windows для доверенных корневых сертификатов. Вместо этого каждый профиль браузера поддерживает собственное хранилище корневых сертификатов. Дополнительные сведения см. в https://support.mozilla.org/en-US/kb/setting-certificate-authorities-firefox
На этой веб-странице также содержатся инструкции по использованию хранилища сертификатов Windows для всех пользователей в браузере Firefox.
Кроме того, можно импортировать используемые по умолчанию сертификаты, как описано ниже. Примечание.

- Необходимо импортировать сертификаты для каждого пользователя и профиля браузера Firefox.
- Нижеописанный сертификат сервера представляет собой сертификат по умолчанию, созданный при установке. Если вы приобрели собственный сертификат у центра сертификации, то можете использовать его вместо этого сертификата.

Импорт сертификатов в хранилище сертификатов Firefox

Для доступа к серверу ACS из Firefox на клиентском компьютере можно импортировать следующий сертификат по умолчанию с сервера:

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

Также для BIS ACE можно загрузить сертификат через Интернет:

- `HTTP://`<Имя принимающего>/<Имя принимающего>`.cer`

Периферийные устройства: для доступа к подключенному периферийному устройству, такому как сканер документов или цифровой подписи, из Firefox на компьютере клиента можно использовать сертификат по умолчанию. Его можно найти на клиентском компьютере в следующем расположении:
<установочный диск>:`\Program Files (x86)\Bosch Sicherheitssysteme\Bosch Peripheral Device Addon\BoschAcePeripheralDeviceAddonHardware CA.cer`

Порядок действий (повторить для каждого сертификата и профиля Firefox):
Для установки необходимых сертификатов на компьютере клиента выполните следующие действия:

1. Найдите сертификат, который хотите установить.
2. Откройте браузер Firefox и введите `about:preferences` в адресную строку.
– Откроется страница параметров.
3. В поле **Найти в параметрах** введите `certificate`
– На странице появится кнопка **Просмотр сертификатов**.
4. Нажмите кнопку **Просмотр сертификатов**.
– Откроется диалоговое окно **Диспетчер сертификатов** с несколькими вкладками.
5. Перейдите на вкладку **Центры сертификации**.
6. Нажмите **Импорт**...
– Откроется диалоговое окно выбора сертификата.
7. Выберите сертификат, который вы находили на шаге 1, и нажмите **Открыть**.
– Откроется диалоговое окно **Загрузка сертификата**.
8. Выберите **Доверять данному ЦС для идентификации веб-сайтов** и нажмите **ОК**.
– Диалоговое окно **Загрузка сертификата** закроется.
9. В диалоговом окне **Диспетчер сертификатов** нажмите **ОК**.
– На этом процедура импорта сертификата завершена.

4.3.2.2 Сертификаты для браузера Chrome

Можно пропустить этот раздел, если вы не используете браузер Chrome.
См. примечания к выпуску вашей версии системы ACS, чтобы ознакомиться с изменениями в обработке сертификатов в браузере Chrome.
Установка сертификата в браузере Chrome для Microsoft Windows:

1. Скачайте файл сертификата.
2. Перейдите на страницу настроек браузера Chrome (`chrome://settings`) и щелкните **Дополнительно**.
3. В разделе **Конфиденциальность и безопасность** щелкните **Управление сертификатами**
4. На вкладке **Сертификаты** нажмите кнопку **Импорт**, чтобы начать установку сертификата:
– Отобразится мастер импорта сертификатов.
5. Выберите файл сертификата и завершите работу мастера.
6. Установленный сертификат появится на вкладке **Доверенные корневые центры сертификации**.

4.3.2.3 Установка приложений Mobile Access

Введение
Bosch предлагает следующие приложения для Mobile Access

– Bosch Mobile Access: приложение владельца карты для хранения виртуальных учетных данных и их передачи по Bluetooth на считыватели, настроенные для Mobile Access. Затем такой считыватель предоставляет или запрещает доступ в зависимости от того, есть ли в приложении действительные для него учетные данные.
– Bosch Setup Access: приложение установщика для сканирования и настройки считывателей по Bluetooth.

Уполномоченные операторы систем Visitor Management и Credential Management могут отправлять виртуальные учетные данные для приложений владельца карты и установщика.

Когда на мобильном устройстве запущено приложение и включен Bluetooth, устройство можно использовать в качестве физической карты. При этом не требуется давать какие-либо команды из приложения или даже разблокировать экран.

Замечание!
ВНИМАНИЕ: не запускайте приложения владельца карты и установщика одновременно Убедитесь, что никто не использует приложения установщика и владельца карты одновременно.

Процедура
Приложения Bosch Mobile Access можно просто скачать и установить из магазинов приложений Google и Apple. Их названия в магазинах приложений:
– Bosch Mobile Access
– Bosch Setup Access

4.3.3 Файл JSON AppSettings

Несколько параметров конфигурации клиентского компьютера VisMgmt хранятся в следующем файле `.JSON`:
<установочный диск>`:\Program Files (x86)\Bosch Sicherheitssysteme\Bosch Visitor Management\appsettings.json`
Как правило, изменять значения по умолчанию не требуется, однако в разделе **AppSettings** этого файла может быть полезно настроить следующие параметры. Сохраните изменения и перезапустите службу Windows VisMgmt, чтобы измененные параметры вступили в силу. Имя службы — `Bosch Ace Visitor Management Client`.

Имя параметра	Пример	Описание
`CorseOrigins`	`"https://my-vm-server:5706"`	Адрес и номер порта сервера управления посетителями.
`CardReaderPort`	`"com3"`	Номер COM-порта, к которому подключен регистрационный считыватель LECTUS. Для считывателей HID OMNIKEY этот параметр можно не заполнять.

4.4 Проверка установки сервера

На компьютере в той же сети, используя один из поддерживаемых браузеров, откройте следующий URL-адрес:
`https://`<Компьютер сервера VisMgmt>`:5706/main`
Если сервер работает, будет отображена страница входа в приложение.

4.5 Установка службы Mobile Access

Введение

Внутренняя служба Mobile Access обеспечивает возможность мобильного доступа для Credential Management и Visitor Management.

Убедитесь в том, что используется последняя версия основной системы управления доступом и сервера Mobile Access.

ПРИМЕЧАНИЕ. Если вы используете и CredMgmt, и VisMgmt, достаточно установить службу Mobile Access один раз.

- Ее можно установить на одном сервере с системой ACS (совмещенная установка) либо на отдельном сервере (распределенная установка).
- Ее можно установить для использования локальной или удаленной базы данных.

Доступность внутренней службы Mobile Access

Внутренняя служба Mobile Access должна быть постоянно доступна для мобильных устройств.

По соображениям безопасности очень нежелательно предоставлять мобильным устройствам сетевой доступ к серверу системы ACS. Поэтому рекомендуется использовать распределенную установку. Это позволит запускать серверную службу Mobile Access на более широкодоступном облачном сервере.

4.5.1 Обзор установки, настройки и использования

Для работы службы Mobile Access необходимо взаимодействие нескольких компонентов. Здесь перечислены общие этапы. Соответствующие предварительные требования и процедуры будут описаны в следующих разделах этой главы.

Установка сервера ACS

1. Система ACS устанавливается, лицензируется и работает с постоянным корневым сертификатом и совместимыми считывателями доступа. В ней определяются операторы с правами на управление службой Mobile Access.

Настройка службы Mobile Access

1. Системный администратор устанавливает в системе ACS одно из приложений, использующих службу Mobile Access: Credential Management или Visitor Management, либо оба приложения сразу.
2. Системный администратор устанавливает серверную службу Mobile Access.
3. Системный администратор активирует службу Mobile Access в установленных веб-приложениях.

Настройка считывателей

1. Системный администратор создает установщика (лицо с правами для настройки считывателей Mobile Access мобильного доступа) в приложении CredMgmt.
2. Установщик загружает приложение установщика (Setup Access) на мобильное устройство из обычного общедоступного магазина приложений.
3. Системный администратор отправляет приглашение назначенному установщику.
4. Установщик принимает приглашение в приложении установщика. Это приглашение дает установщику право настраивать считыватели доступа для использования службы Mobile Access.
5. Установщик настраивает считыватели с помощью приложения установщика.

Использование службы Mobile Access

1. Владельцы учетных данных, которые имеют право использовать приложение Mobile Access, загружают приложение для владельцев учетных данных (Mobile Access) на свои мобильные устройства из обычного общедоступного магазина приложений.
2. Операторы CredMgmt и/или VisMgmt с помощью QR-кода или по электронной почте предоставляют мобильные учетные данные владельцам учетных данных с соответствующими правами.
3. Владельцы учетных данных считывают QR-код или открывают электронное письмо в своем приложении для владельцев учетных данных (Mobile Access). Это позволяет использовать мобильное устройство в качестве физического средства идентификации, когда приложение запущено.

4.5.2 Аппаратные требования службы Mobile Access

Для использования службы Mobile Access необходимы считыватели доступа с модулем BLE. Подходят следующие считыватели Bosch:

ARD-SELECT -BOM, -WOM, -BOKM, -WOKM

- Буквы B и W обозначают цвет: черный или белый
- Буква O обозначает OSDP
- Буква K означает наличие клавиатуры
- Буква M обозначает поддержку службы Mobile Access

4.5.3 Требования к конфигурации службы Mobile Access

Выделенный пользователь для удаленной базы данных (если используется удаленная база данных)

Если служба Mobile Access будет использовать базу данных на удаленном сервере базы данных, то создайте и настройте пользователя с правами администратора с именем `MAUser` на этом удаленном сервере как в Windows, так и в системе SQL Server. Во время выполнения описанных ниже настроек выберите вариант для удаленного сервера базы данных и введите пароль, установленный для `MAUser`.

ВНИМАНИЕ: не запускайте настройку Mobile Access до завершения этой операции.

Процедура

1. На удаленном сервере базы данных создайте пользователя домена Windows в том же домене, что и ACS. Используйте следующие настройки:

- **Имя пользователя** (имя пользователя с учетом регистра): <ACS-Domain>\`MAUser`
- **Пароль**: настройте пароль в соответствии с политиками безопасности, применяемыми ко всем вашим компьютерам. Обратите внимание, что он потребуется для настройки Mobile Access.
- **При следующем входе в систему пользователь должен изменить пароль**: `NO`
- **Пользователь не может изменить пароль**: `YES`
- **Срок действия пароля не ограничен**: `YES`
- **Вход в качестве службы**: `YES`
- **Учетная запись отключена**: `NO`

Затем добавьте `MAUser` в качестве логина для удаленного сервера SQL как описано ниже:

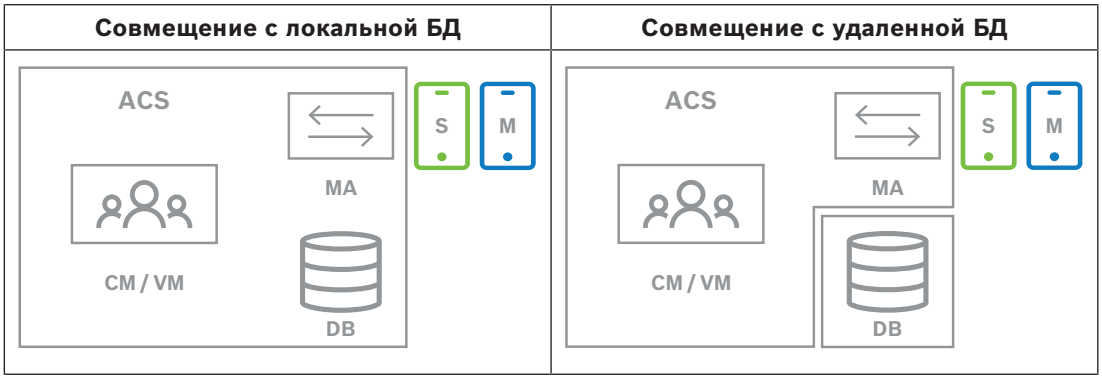
1. Откройте центр SQL Management Studio
2. Подключитесь к удаленному экземпляру SQL
3. Перейдите в раздел **Security (Безопасность)** > **Login (Вход)**
4. В области **Выберите страницу** выберите пункт **Общие**
5. Выберите пользователя `MAUser`

6. В области **Выберите страницу** выберите пункт **Роли на сервере**
7. Установите флажки `public` и `dbcreator`

Выделенный пользователь для локальной базы данных (если используется локальная база данных)
Пользователь `MAUser` обращается к базе данных системы ACS от имени приложения Mobile Access.
НЕ нужно создавать этого пользователя, если используется локальная база данных. Программа установки Mobile Access автоматически создает пользователя `MAUser` на сервере ACS.

4.5.4 Процедура совмещенной установки

Совмещенная установка подразумевает, что внутренняя служба Mobile Access запускается на том же сервере, что и система ACS.
Распределенная установка подразумевает, что внутренняя служба Mobile Access запускается на другом сервере, например в облаке.
Подробнее о распределенной установке см. в следующем разделе **Процедура распределенной установки**.



Клавиша	Значение
ACS	Основная система управления доступом: AMS или BIS-ACE
CM/VM	Серверная часть веб-приложения: Credential Management или Visitor Management
DB	Основная база данных ACS
MA	Серверная часть Mobile Access
S	Приложение установщика Setup Access для мобильных устройств системных установщиков и конфигураторов.
M	Приложение доступа Mobile Access для мобильных устройств обычных владельцев учетных данных.

Процедура

1. На сервере системы ACS, который в случае совмещенной установки также является сервером службы Mobile Access, запустите файл `BoschMobileAccessBackend.exe` от имени администратора
– Откроется программа установки
2. На экране **Местоположение** выберите тип установки **Совмещенная**

3. На экране **Компоненты** убедитесь, что выбран вариант `Bosch Mobile Access`, а затем нажмите кнопку **Далее**
4. Внимательно прочитайте информацию на экране **EULA** и нажмите **Принять**, если вы принимаете условия лицензионного соглашения с конечным пользователем (EULA). Установку можно будет продолжить только в таком случае.
5. На экране **Каталог установки**:

– Выберите целевую папку для установки или используйте папку, выбранную по умолчанию (рекомендуется)
– Введите название компании, которое будет отображаться в мобильном приложении и в HTML-шаблонах электронных писем
– Нажмите кнопку **Далее**

6. На экране **Сертификат**

– Введите имя узла, на котором будет запускаться серверная часть службы Mobile Access
– При желании или если сеть не поддерживает разрешение имени узла, введите IP-адрес узла.
– Нажмите кнопку **Далее**

7. На экране **SQL Server** выберите один из двух вариантов расположения базы данных. Настройки немного отличаются. Выберите один из вариантов для следующего этапа:

– ВАРИАНТ 1. Опция **Локальная база данных**:
  – Программа установки находит локальную базу данных и выбирает ее.
  – Введите пароль администратора SQL (по умолчанию `sa`)
  – Нажмите **Проверить подключение**
  – Нажмите кнопку **Далее**
– ВАРИАНТ 2. Опция **Удаленная база данных**
  – Введите имя находящегося в сети сервера SQL
  – Введите имя экземпляра SQL
  – Введите пароль администратора SQL (по умолчанию `sa`)
  – Нажмите **Проверить подключение**
  – Проверьте имя пользователя и введите пароль администратора Windows и SQL, который вы создали для удаленного использования базы данных (см. раздел «Предварительные требования» выше)
  – Нажмите кнопку **Далее**

8. На экране **Конфигурация сервера идентификации** выполните следующие действия.

– Сервером удостоверений по умолчанию (предварительно выбранным) является основной сервер ACS с портом `44333` `https://`<NameOfACSserver>`:44333`
– Нажмите **Проверить подключение**
– Если проверка не прошла, проверьте доступность сервера удостоверений еще раз.
– Нажмите кнопку **Далее**

9. На экране **Основные компоненты** убедитесь, что выбран вариант **Bosch Mobile Access**, и нажмите кнопку **Установить**

– Работа мастера установки завершена

10. Нажмите кнопку **Далее**
11. На экране **Основные компоненты** убедитесь, что установка успешно завершена, и нажмите кнопку **Завершить**
12. В приложении Windows `Services` убедитесь, что служба `Bosch Mobile Access` запущена.

4.5.5 Процедура распределенной установки

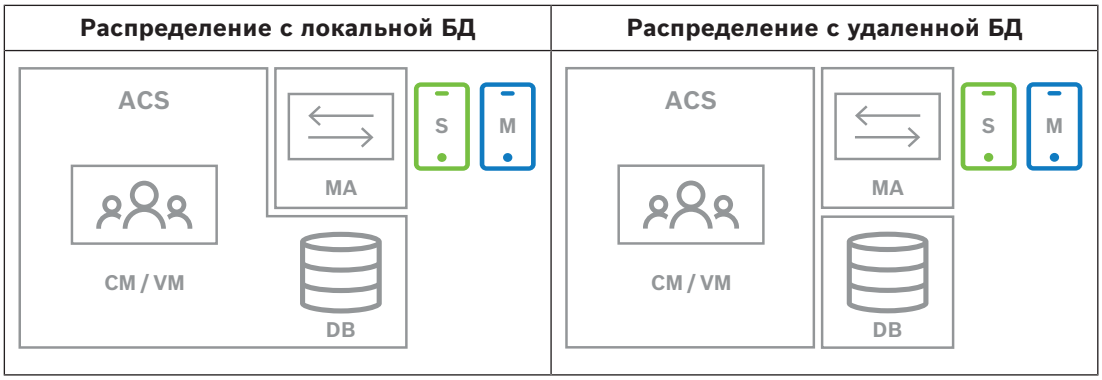
Совмещенная установка подразумевает, что внутренняя служба Mobile Access запускается на том же сервере, что и система ACS.

Распределенная установка подразумевает, что внутренняя служба Mobile Access запускается на другом сервере, например в облаке.

Подробнее о совмещенной установке см. в предыдущем разделе **Процедура совмещенной установки**.

Прежде чем запустить установку Mobile Access или во время обновления системы на распределенном внутреннем сервере Mobile Access необходимо выполнить перечисленные ниже требования. В совместно размещенной среде это не обязательно.

– Перед запуском программы установки Mobile Access установите **серверный пакет ASP.NET Core 8.0 Runtime (v8.0.2)** на распределенном внутреннем сервере Mobile Access.
– Чтобы загрузить необходимый серверный пакет, перейдите по ссылке: https://dotnet.microsoft.com/en-us/download/dotnet/thank-you/runtime-aspnetcore-8.0.2-windows-hosting-bundle-installer.



Клавиша	Значение
ACS	Основная система управления доступом: AMS или BIS-ACE
CM/VM	Серверная часть веб-приложения: Credential Management или Visitor Management
DB	Основная база данных ACS
MA	Серверная часть Mobile Access
S	Приложение установщика Setup Access для мобильных устройств системных установщиков и конфигураторов.
M	Приложение доступа Mobile Access для мобильных устройств обычных владельцев учетных данных.

Процедура

Убедитесь в том, что вы используете последнюю версию основной системы управления доступом.

1. На внутреннем сервере службы Mobile Access запустите файл `BoschMobileAccessBackend.exe` от имени администратора
– Откроется программа установки
2. На экране **Местоположение** выберите тип установки **Распределенная**
3. На экране **Узел** выберите серверную часть **Mobile Access** и нажмите кнопку **Далее**

– Примечание. Вариант **ACS** будет впоследствии использоваться в этой процедуре при установке службы Mobile Access на сервер системы ACS.
4. На экране **Компоненты** убедитесь, что выбран вариант **Bosch Mobile Access**, а затем нажмите кнопку **Далее**
5. Внимательно прочитайте информацию на экране **EULA** и нажмите **Принять**, если вы принимаете условия лицензионного соглашения с конечным пользователем (EULA). Установку можно будет продолжить только в таком случае.
6. На экране **Каталог установки**:
– Выберите целевую папку для установки или используйте папку, выбранную по умолчанию (рекомендуется)
– Введите название компании, которое будет отображаться в мобильном приложении и в HTML-шаблонах электронных писем
– Нажмите кнопку **Далее**
7. На экране **SQL Server** выберите один из двух вариантов расположения базы данных. Настройки немного отличаются. Выберите один из вариантов для следующего этапа:
– ВАРИАНТ 1. Опция **Локальная база данных**:
  – Программа установки находит локальную базу данных и выбирает ее.
  – Введите пароль администратора SQL (по умолчанию `sa`)
  – Нажмите **Проверить подключение**
  – Нажмите кнопку **Далее**
– ВАРИАНТ 2. Опция **Удаленная база данных**
  – Введите имя находящегося в сети сервера SQL
  – Введите имя экземпляра SQL
  – Введите пароль администратора SQL (по умолчанию `sa`)
  – Нажмите **Проверить подключение**
  – Проверьте имя пользователя и введите пароль администратора Windows и SQL, который вы создали для удаленного использования базы данных (см. раздел «Предварительные требования» выше)
  – Нажмите кнопку **Далее**

На этом этапе распределенной установки нужно переключиться на компьютер, на котором запущен сервер ACS, и настроить там службу Mobile Access, *чтобы впоследствии он мог взаимодействовать с серверной частью службы* Mobile Access *на локальном компьютере. После выполнения указанных там действий программа установки вернет вас на локальный сервер для подтверждения и продолжения работы.*

1. На компьютере с сервером ACS запустите файл `BoschMobileAccessBackend.exe` от имени администратора
– Откроется программа установки
2. На экране **Местоположение** выберите тип установки **Распределенная**
3. На экране **Узел** выберите **ACS** и нажмите кнопку **Далее**
4. На экране **Мастер-компаньон** прочитайте пояснительный текст и нажмите кнопку **Далее**
5. На экране **Сертификат**
– Введите имя узла, на котором будет запускаться серверная часть службы Mobile Access
– При желании или если сеть не поддерживает разрешение имени узла, введите IP-адрес узла.
– Нажмите кнопку **Далее**

6. На экране **Конфигурация сервера идентификации** выполните следующие действия.
– Сервером удостоверений по умолчанию (предварительно выбранным) является основной сервер ACS с портом `44333` `https://`<NameOfACSserver>`:44333`
– Нажмите **Проверить подключение**
– Если проверка не прошла, проверьте доступность сервера удостоверений еще раз.
– Нажмите кнопку **Далее**
7. На экране **Создать файл**
Здесь мы создаем файл конфигурации в защищенном паролем ZIP-файле и делаем его доступным для серверной части службы Mobile Access.
– **Пароль пользователя**: введите пароль для ZIP-файла
– **Файл конфигурации**: найдите папку, в которую будет помещен ZIP-файл, или введите путь к ней. Обратите внимание, что эта папка должна быть доступна для компьютера, на котором запущена серверная часть службы Mobile Access. Если это не так, перенесите ZIP-файл на этот компьютер другим способом.
– Нажмите **Создать файл конфигурации**
– Нажмите кнопку **Далее**
8. На экране **Переключить компьютер**
Действия по установке на сервере службы ACS завершены.
– Нажмите кнопку **Подтвердить**, чтобы завершить процедуру

На этом этапе распределенной установки вам нужно вернуться в программу установки на компьютере, на котором запущена серверная часть службы Mobile Access.

1. Вернитесь в программу установки `BoschMobileAccessBackend.exe` на компьютере с сервером службы Bosch Mobile Access.
2. На странице **Переключить компьютер**
– установите флажок **Я уже выполнил(а) необходимые действия на компьютере ACS**
– Нажмите кнопку **Далее**
3. На экране **Загрузить файл**
– **Загрузка файла конфигурации:** выберите файл конфигурации, созданный на сервере ACS
– **Проверка пароля:** введите пароль, заданный для ZIP-файла на сервере ACS
– После ввода правильного пароля можно нажать кнопку **Далее** для чтения файла конфигурации
4. На экране **Основные компоненты** убедитесь, что выбран вариант **Bosch Mobile Access**, и нажмите кнопку **Установить**
– Работа мастера установки завершена
5. Нажмите кнопку **Далее**
6. На экране **Основные компоненты** убедитесь, что установка успешно завершена, и нажмите кнопку **Завершить**
7. В приложении Windows `Services` убедитесь, что служба `Bosch Mobile Access` запущена.

4.6 Установка приложений Mobile Access

Введение
Bosch предлагает следующие приложения для Mobile Access

– Bosch Mobile Access: приложение владельца карты для хранения виртуальных учетных данных и их передачи по Bluetooth на считыватели, настроенные для Mobile Access. Затем такой считыватель предоставляет или запрещает доступ в зависимости от того, есть ли в приложении действительные для него учетные данные.
– Bosch Setup Access: приложение установщика для сканирования и настройки считывателей по Bluetooth.

Уполномоченные операторы систем Visitor Management и Credential Management могут отправлять виртуальные учетные данные для приложений владельца карты и установщика.

Когда на мобильном устройстве запущено приложение и включен Bluetooth, устройство можно использовать в качестве физической карты. При этом не требуется давать какие-либо команды из приложения или даже разблокировать экран.

Замечание!
ВНИМАНИЕ: не запускайте приложения владельца карты и установщика одновременно Убедитесь, что никто не использует приложения установщика и владельца карты одновременно.

Процедура
Приложения Bosch Mobile Access можно просто скачать и установить из магазинов приложений Google и Apple. Их названия в магазинах приложений:
– Bosch Mobile Access
– Bosch Setup Access

4.7 Периферийное оборудование

Следующие периферийные USB-устройства были протестированы и одобрены для использования с системами VisMgmt и CredMgmt на момент подготовки документа. Постоянно обновляемый список совместимых устройств см. в кратком описании основной системы управления доступом.

Регистрационный считыватель карт	LECTUS enroll ARD-EDMCV002-USB, HID OMNIKEY 5427 CK
Сканер для удостоверений личности	ARH Combo, ARH Osmond
Сканер подписей	signotec LITE, signotec Omega

Для подключения этих устройств к клиентским компьютерам следуйте инструкциям производителей.

Регистрационные считыватели
Поддерживаются следующие регистрационные считыватели и форматы карт.

	Код Bosch MIFARE DESFire EV1	MIFARE DESFire EV1 CSN	MIFARE Classic CSN	HID Prox 26 бит	iCLASS 26 бит	iCLASS 35 бит	iCLASS 37 бит	iCLASS 48 бит	EM 26 бит
LECTUS enroll ARD-EDMCV002-USB	X								
OMNIKEY 5427 CK		X	X	X	X	X	X	X	X

4.7.1 Регистрация периферийного оборудования в клиентском компьютере.

Чтобы зарегистрировать периферийное оборудование на клиентском компьютере VisMgmt, запустите с клиента программу настройки периферийных устройств Bosch, `BoschPeripheralDeviceAddon.exe`. Инструкции см. в разделе *Настройка надстройки для периферийных устройств, Страница 15*.

См.

– *Настройка надстройки для периферийных устройств, Страница 15*

4.8 Восстановление установки службы Mobile Access

Введение

Чтобы обновить двоичные файлы или создать сертификат Mobile Access повторно, можно запустить программу установки имеющейся или более новой версии Mobile Access, не удаляя уже установленную службу:

Процедура

1. На внутреннем сервере службы Mobile Access запустите новую версию файла `BoschMobileAccessBackend.exe` от имени администратора.

– Помните, что в случае совмещенной установки внутренним сервером службы Mobile Access является сервер системы ACS.

2. Следуйте указаниям в мастере установки и выберите те же настройки, что и при первоначальной установке.

– Чтобы заново создать сертификат, на экране **Сертификаты** нажмите переключатель **Создать сертификат заново**.

3. После завершения установки перезапустите сервер.
4. Заново войдите в систему в каждом веб-приложении, использующем службу Mobile Access (в CredMgmt, VisMgmt или обоих приложениях).

– Веб-приложение будет использовать новые двоичные файлы.

– Если вы включили переключатель **Создать сертификат заново**, все последующие приглашения, отправляемые пользователям и установщикам службы Mobile Access, будут использовать новый сертификат Mobile Access.

4.9 Удаление программного обеспечения

Чтобы удалить программу с сервера или клиента:

1. Запустите приложение Windows **Установка и удаление программ** с правами администратора.
2. Выберите программу (сервер или клиент) и нажмите кнопку **Удалить**.
3. Только для Visitor Management и только на сервере: укажите, следует ли удалить вместе с программой базу данных управления посетителями.

– **Примечание**. База данных содержит записи о всех посетителях, зарегистрированных на протяжении использования программы. Возможно, нужно заархивировать базу данных или перенести ее на другую систему.

4. Укажите, нужно ли удалить файлы журнала.
5. Завершите удаление обычным образом.
6. Рекомендуется: перезагрузите компьютер для внесения изменений в реестр Windows.

Примечание. При необходимости после удаления сервера Mobile Access удалите вручную следующие остаточные файлы конфигурации:

– **MAUser** — этот пользователь остается после удаления. Администратор должен удалить его вручную.
– **Сертификаты** — чтобы вручную удалить все сертификаты, установленные при установке Mobile Access, используйте меню *Управление сертификатами компьютера*.
– **Конфигурация идентификации для Mobile Access** — файл *appsettings.Extension.MobileAccessBackend* остается после удаления сервера. Удалите его вручную.

5 Конфигурирование

5.1 Создание пользователей Visitor Management в ACS

Введение

У каждого пользователя VisMgmt с правами администратора, работника приемной или принимающего должен быть картодержатель с отдельным определением оператора в ACS, т.е. в основной системе управления доступом.

Эти определения операторов содержат специальные права VisMgmt, представленные в виде **Профилей пользователей**. См. онлайн-справку в ACS для получения подробной информации и инструкций относительно **Профилей пользователей**.

– Необходимо определить отдельного оператора для каждого держателя карты, который работает в системе управления посетителями. Одному оператору нельзя назначить несколько держателей карт.

Замечание!

ИТ-безопасность и учетные записи пользователей

Согласно практических рекомендаций по обеспечению ИТ-безопасности, каждый пользователь с правами работника приемной, принимающего и администратора должен работать под своей учетной записью Windows.

Создание профилей пользователей для управления посетителями

1. Выполните вход в основную систему управления доступом с правами администратора.
2. Создайте один или несколько профилей пользователя (оператора) для пользователей VisMgmt.
   Путь к диалоговому окну:

– **Конфигурация > Операторы и рабочие станции** > **Профили пользователей**
– Конфигуратор > **Administration** (Администрирование) > **ACE User profiles** (Профили пользователей ACE)

3. Назначьте этим профилям одни из следующих прав пользователя.

– Администратор: `Visitor Management > Administrator`
– Принимающая сторона: `Visitor Management > Host`
– Работник приемной: `Visitor Management > Receptionist`

После создания профилей пользователей, необходимых для различных ролей VisMgmt (администратор, работник приемной, принимающая сторона), можно назначить для каждого профиля несколько операторов.

Назначение профилей пользователей операторам и владельцам карт ACS

Путь к диалоговому окну:

– **Конфигурация** > **Операторы и рабочие станции** > **Права пользователей**
– BIS Конфигуратор > **Администрирование** > **Операторы**

1. Добавьте новый тип оператора (щелкните  или  , в зависимости от ACS) и присвойте ему имя, четко связанное с одной из ролей VisMgmt (администратор, работник приемной или принимающая сторона).
2. На вкладке **Общие параметры оператора** выберите `Operator ACE` в списке авторизаций.

3. На вкладке **Параметры оператора ACE** с помощью кнопок со стрелками назначьте созданный ранее **профиль пользователя ACE**.
   Отмените назначение профиля по умолчанию `UP-Administrator`, за исключением случая, когда держателю карты требуются общие права администратора в ACS.
4. На той же вкладке **Параметры оператора ACE** воспользуйтесь панелью **Назначить лицо** для поиска в системе держателя карты, которому необходимо назначить роль VisMgmt.
5. Щелкните **Назначить лицо** для завершения назначения роли для выбранного держателя карты.

– Необходимо определить отдельного оператора для каждого держателя карты, который работает в системе управления посетителями. Одному оператору нельзя назначить несколько держателей карт.

5.2 Создание авторизаций и профилей посетителей в системе контроля доступа

Введение

Работник приемной или администратор системы VisMgmt выбирает **тип** для каждого нового посетителя. Тип посетителя основан на предварительно настроенном в основной системе управления доступом (СКД) **типе персонала**, называемом **Посетитель**, или на подтипе **Посетитель**, созданном администратором системы СКД.
Администратор также должен настроить тип **Посетитель**, его подтипы в СКД и профили доступа. Профили доступа позволяют этим типам лиц открывать двери на объекте.

5.3 Настройка компьютера работника приемной

На компьютере работника ресепшена запускается надстройка для **периферийных устройств Bosch**, которая обеспечивает физическое подключение периферийных устройств для считывания карт, сканирование идентификационных документов и сканирование подписей.
Перед установкой клиентского программного обеспечения подключите все необходимые периферийные устройства.
Убедитесь, что компьютер и его периферийные устройства достаточно защищены от несанкционированного доступа.

5.4 Настройка компьютера-киоска для посетителей

Введение

Посетители обычно регистрируют свои посещения и создают собственные профили на компьютере, который находится в свободном доступе в зоне приемной объекта с контролируемым доступом. В целях безопасности веб-браузер компьютера работает в режиме киоска, который предоставляет доступ только к VisMgmt, не позволяя открыть несколько вкладок, параметры браузера и получить доступ к операционной системе компьютера. Все поддерживаемые браузеры предлагают режим киоска, но точная конфигурация зависит от браузера.
На компьютере-киоске запускается надстройка для **периферийных устройств Bosch**, которая обеспечивает физическое подключение периферийных устройств для сканирования идентификационных документов и подписей.

– URL-адрес для режима киоска — `https://`<My_VisMgmt_server>`:5706`

Настройка режима киоска в браузерах

Следующие ссылки описывают настройку режима киоска в браузерах, поддерживаемых VisMgmt

	Инструкции по настройке режима киоска
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

Замечание!
В целях безопасности всегда отключайте автоматическое сохранение паролей в браузере.

5.5 Вход в систему для выполнения задач конфигурирования

Для выполнения задач конфигурации и администрирования следует использовать компьютер, который физически защищен от несанкционированного доступа.

1. Введите в браузере HTTPS-адрес сервера VisMgmt с двоеточием и номером порта (по умолчанию — `5706`)
   `https://`<My_VisMgmt_server>`:5706/main`
   Появится экран **Вход в систему**
2. Выполните вход в качестве пользователя VisMgmt с правами **администратора**.
3. Нажмите значок  , чтобы открыть меню **Параметры**.

5.6 Конфигурация с помощью меню «Параметры»

Меню **Параметры** содержит подразделы, позволяющие выполнить следующие действия по настройке.

Основные параметры	– **Срок хранения (в днях)**. Управляет обработкой записей о посещениях.
	  – При первом истечении периода приложение анонимизирует запись.
	  – При втором истечении периода приложение удаляет запись. Значение по умолчанию — `365`.
	  Для отключения периода хранения установите значение 0. В таком случае записи будут храниться бессрочно.
	– **Режим хранения документов**. Укажите, как хранить документы: в бумажном или цифровом виде.
	– **Максимально допустимое количество посетителей**, которые могут находиться на объекте одновременно.
	Значение по умолчанию — `100`.
	Установите значение `0` для полного отключения счетчиков посетителей на панели мониторинга.

- **Срок действия документов (в днях)**. Введите срок, в течение которого загружаемые документы (например соглашения о неразглашении (NDA) и условия использования) остаются действительными. Этот срок распространяется как на бумажные, так и на цифровые версии документов.
  По истечении срока документы помечаются в профиле посетителя как просроченные (значок часов с красной точкой).
  Значение по умолчанию — `365`.
- **Период предупреждения об истечении срока действия документов (в днях)**. Укажите продолжительность периода предупреждения об истечения срока действия документов.
  В течение периода предупреждения документы с истекающим сроком действия будут помечены в профиле пользователя значком часов с оранжевой точкой. До наступления периода предупреждения отображается значок часов с зеленой точкой.
- **Логотип.** Установите или снимите флажки, которые определяют, какой логотип отображается в диалоговых окнах: стандартный или настраиваемый, а также отображается ли **графика** Bosch.
  - Требования для файлов настраиваемых логотипов см. здесь: *Настройка логотипа компании, Страница 38*
- Нажмите кнопку **Предварительный просмотр**, чтобы открыть страницу диалогового окна в том виде, в котором она будет отображаться с учетом выбранных параметров. Подробные сведения о режиме предварительного просмотра см. в следующем разделе.
- **Языки**.
  Выберите языки, которые будут доступны в пользовательском интерфейсе, а также предпочтительный формат **даты** и **времени**.
- **Почтовый сервер**
  Введите IP-адрес, номер порта и сведения об учетной записи для почтового сервера, чтобы разрешить отправку электронной почты из приложения. Если для внешнего почтового сервера требуется дополнительный сертификат SSL/TSL, импортируйте его в компьютер, на котором запущен сервер мобильного доступа. После импорта перезапустите `VisitorManagerServer`.
- **Шаблоны электронной почты**
  Доступно несколько шаблонов HTML-сообщений, которые обычно настраиваются под индивидуальные потребности. Подробные сведения см. в специальном разделе **«шаблоны электронной почты»** ниже.
- **Mobile Access**
  Установите флажок **Mobile Access**, чтобы активировать службу Mobile Access.

  Подключение. Введите адрес сервера службы Mobile Access (адрес службы регистрации).
  `https://`<MyMobileAccessBackendServer>`:5700`
  Для <MyMobileAccessBackendServer> в средах с несколькими

	доменами используйте имя домена (FQDN). **Примечание.** Чтобы использовать вместо FQDN IP-адрес, необходимо ввести этот IP-адрес в диалоговом окне **Создание сертификата** при запуске мастера установки серверной части службы Mobile Access. **Регистрация установщиков.** Выберите информацию, которую должны предоставить установщики для получения доступа к настройке считывателей мобильного доступа с помощью Bosch Setup Access. Выйдите из веб-приложения и снова войдите в него, чтобы сразу начать пользоваться функцией мобильного доступа Mobile Access.

Работник приемной	– Этот экран настроек содержит два флажка для каждого поля данных в диалоговых окнах регистрации посетителей сотрудника приемной.
	  – Снимите или установите первый флажок, чтобы указать, является ли поле данных **видимым** во всех диалоговых окнах регистрации.
	  – Снимите или установите второй флажок (отмечен звездочкой), чтобы указать, является ли поле данных **обязательным** для заполнения.
	– Настройте текст заголовка по умолчанию в диалоговых окнах сбора данных.
	Более подробные сведения см. в разделе *Настройка пользовательского интерфейса, Страница 38* ниже.

	Особая функция: разрешить регистрацию прибытия/убытия без карты Личные карты не являются обязательными для посетителей, которые идут с индивидуальным сопровождением или ограничиваются общественными местами. Для таких случаев предусмотрена возможность контроля посетителей без карт. В целях безопасности эта функция по умолчанию отключена. Чтобы включить ее, установите флажок: – **Примечание:** если эта функция включена, то любой **посетитель**, который самостоятельно регистрируется на компьютере в режиме киоска, автоматически получает разрешение и одновременно регистрирует вход. – См. главу **Эксплуатация** *Проверка входа и выхода посетителей без карт, Страница 56* этого документа, где детально описано, как пользователь с правами **работника приемной** может обрабатывать пользователей без карт.
Принимающая сторона	Параметры для пользователей **Принимающая сторона** и **Посетитель** доступны только для чтения до тех пор, пока не будут изменены и сохранены параметры для пользователя **Сотрудник приемной**.
Посетитель	

	Поля, отмеченные как невидимые в настройках пользователя **Работник приемной**, автоматически задаются как невидимые для пользователей **Принимающая сторона** и **Посетитель**. Далее процедура конфигурации идентична предыдущей.

См.
- *Назначение физических учетных данных, Страница 52*
- *Настройка пользовательского интерфейса, Страница 38*

5.6.1 Шаблоны электронной почты

Доступно несколько шаблонов HTML-сообщений, которые обычно настраиваются под индивидуальные потребности компании. Каждый шаблон позволяет сохранять адреса электронной почты для получателей в копии / скрытой копии / пробной рассылке (CC, BCC и Test), которым можно мгновенно отправить тестовое электронное сообщение. При загрузке шаблона для редактирования он копируется в папку «Загрузки» браузера по умолчанию.

- `MobileAccess.html` Приглашение для владельца карты для использования идентификаторов на базе смартфона.
- `SetupAccess.html` Приглашение для установщика для настройки считывателей для Mobile Access.
- `VisitorInvite.html` Приглашение посетить ваш сайт с возможностью вложения файла iCalendar в сообщение электронной почты.
- `InformHostAboutCheckin.html` Электронное уведомление принимающего о прибытии посетителя.

Заполнители для использования в шаблонах электронной почты

Шаблоны электронной почты содержат несколько заполнителей для включения в текст полей базы данных. Эти заполнители описаны в следующих таблицах с учетом шаблонов, в которых их можно использовать.

Служба Mobile Access

Сообщение владельцу карты (для приложения Mobile Access) после предоставления мобильного доступа

Заполнитель	Описание
`{{Title}}`	обращение к лицу (г-н, г-жа, д-р и т. д.)
`{{FirstName}}`	имя лица
`{{LastName}}`	фамилия лица
`{{CompanyName}}`	компания лица
`{{QrcodeLink}}`	QR-код, который соответствует ссылке, предоставляющей владельцу карты мобильный доступ через приложение
`{{InviteLink}}`	ссылка, предоставляющая владельцу карты мобильный доступ через приложение

Setup Access (Настройка доступа)
Сообщение установщику Mobile Access (для приложения Setup Access) при предоставлении им мобильного доступа для настройки считывателей.

Заполнитель	Описание
{{Title}}	обращение к установщику (г-н, г-жа, д-р и т. д.)
{{FirstName}}	имя установщика
{{LastName}}	фамилия установщика
{{CompanyName}}	компания установщика
{{QrcodeLink}}	QR-код, который соответствует ссылке, предоставляющей установщику мобильный доступ для настройки считывателей через приложение Setup Access
{{InviteLink}}	ссылка, предоставляющая установщику мобильный доступ для настройки считывателей через приложение Setup Access

Приглашение посетителя
Электронное письмо, которое отправляется посетителю при создании или редактировании посещения.

Заполнитель	Описание
{{VisitorID}}	Идентификатор посетителя, созданный приложением VisMgmt
{{Title}}	обращение к посетителю (г-н, г-жа, д-р и т. д.)
{{FirstName}}	имя посетителя
{{LastName}}	фамилия посетителя
{{CompanyName}}	компания посетителя
{{HostFirstName}}	имя принимающего
{{HostLastName}}	фамилия принимающего
{{ExpArrivalDate}}	плановая дата посещения

Посетитель прибыл
Электронное письмо, отправляемое принимающему лицу, когда работник приемной утверждает посещение

Заполнитель	Описание
{{VisitorID}}	Идентификатор посетителя, созданный приложением VisMgmt
{{Title}}	обращение к посетителю (г-н, г-жа, д-р и т. д.)
{{FirstName}}	имя посетителя
{{LastName}}	фамилия посетителя

Заполнитель	Описание
{{CompanyName}}	компания посетителя
{{HostFirstName}}	имя принимающего
{{HostLastName}}	фамилия принимающего
{{ExpArrivalDate}}	плановая дата посещения
{{ArrivalDate}}	фактическая дата посещения

Пропуск посетителя

Документ, который можно распечатать и предоставить посетителю. Он может включать карту здания или контрольный список.

Заполнитель	Описание
{{VisitorID}}	Идентификатор посетителя, созданный приложением VisMgmt
{{Title}}	обращение к посетителю (г-н, г-жа, д-р и т. д.)
{{FirstName}}	имя посетителя
{{LastName}}	фамилия посетителя
{{CompanyName}}	компания посетителя
{{HostFirstName}}	имя принимающего
{{HostLastName}}	фамилия принимающего
{{ExpArrivalDate}}	плановая дата посещения
{{ArrivalDate}}	фактическая дата посещения

5.6.2 Режим предварительного просмотра

Определенные наборы параметров имеют кнопку **Предварительный просмотр**, которая активирует режим предварительного просмотра, позволяющего просматривать диалоговые окна в том виде, в котором они будут отображаться при выборе этих параметров.

В режиме предварительного просмотра действуют следующие условия:

– В верхней части панели мониторинга отображается баннер.

– Изменения, внесенные в панели мониторинга или в меню, **не** сохраняются.
– Нажмите **Закрыть режим предварительного просмотра** в области баннера, чтобы закрыть режим предварительного просмотра.
– Используйте список **Изменить роль** в области баннера, чтобы просмотреть внешний вид интерфейса для различных типов пользователей.

5.6.3 Шаблоны документов

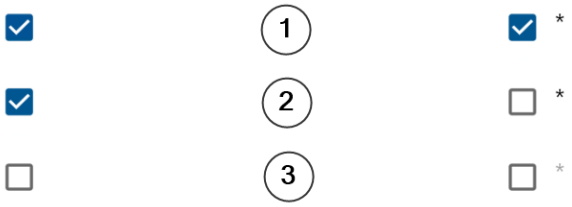
Вы можете скачивать шаблоны различных документов и электронных писем, а также загружать отредактированные версии этих шаблонов с помощью диалогового окна **Панель мониторинга** > **Параметры > Основные**.

5.7 Настройка пользовательского интерфейса

Пользовательский интерфейс можно настроить в диалоговых окнах **Панель мониторинга** > **Параметры**.

5.7.1 Настройка отображаемых, невидимых и обязательных параметров

Выберите поля данных, которые будут отображаться в диалоговых окнах, и укажите, какие из этих данных являются обязательными.
Пример:



- Поле (1) является видимым и обязательным.
- Поле (2) является видимым, но необязательным.
- Поле (3) является невидимым.

5.7.2 Настройка текстов пользовательского интерфейса для локализации

Тексты пользовательского интерфейса можно легко настроить для определенного языка. По умолчанию **текст локализации** содержит стандартные заголовки для блоков полей данных в диалоговых окнах сбора данных.
Чтобы настроить заголовки в соответствии с местными требованиями, выполните следующие действия.

1. Выберите язык пользовательского интерфейса из списка.
2. Перепишите текст в текстовом поле.
   Допускается использование HTML-тегов для простого форматирования, например:
   ```
   <b>this text will appear bold </b>
   <i>italics</i>
   <u>underline</u>
   ```

5.7.3 Настройка режима киоска

Если на объекте нет одного или нескольких периферийных устройств, например сканера документов, можно настроить процесс самостоятельной регистрации посетителя в режиме киоска, сняв флажки соответствующих шагов регистрации.

5.7.4 Настройка логотипа компании

Графические файлы, загружаемые в качестве логотипа компании, должны соответствовать следующим требованиям:

Поддерживаемые форматы	PNG, JPEG, JPG

Точная ширина (пиксели)	125
Точная высота (пиксели)	63
Макс. размер (МБ)	1

5.8 Параметры брандмауэра

Добавьте вспомогательные приложения в конфигурацию брандмауэра на серверном и клиентском компьютерах.

1. Запустите брандмауэр Windows, нажав кнопку «Пуск» и выбрав **Панель управления** > **Брандмауэр Windows**.
2. Выберите **Дополнительные настройки**.
3. Выберите **Правила для входящих подключений**.
4. На панели **Действия** выберите пункт **Новое правило...**
5. В диалоговом окне **Тип правила** выберите **Порт**и нажмите кнопку **Далее >**.
6. На следующей странице выберите **TCP и конкретные локальные порты**
7. Разрешить связь через следующие порты:

– На компьютере или компьютерах с сервером

<имя сервера>:44333 — используется сервером удостоверений AMS **(*)**

<имя сервера>:5706 — используется сервером VisMgmt

<имя сервера>:5806 — используется сервером CredMgmt

<имя сервера>:5701 — используется сервером Mobile Access

– На клиентских компьютерах

localhost:5707 – используется надстройкой для периферийных устройств Bosch

(*) Мы используем серверы идентификации AMS и BIS, как описано в соответствующих руководствах по их установке.

Использование портов в системе

Исходящий сервер	**Исход. порт**	**Входящий сервер**	**Вход. порт**	**Протокол**	**Комментарии**
VisMgmt или CredMgmt	*	Серверная часть Mobile Access	5701	HTTPS	Команды из веб-приложения для создания и/или удаления мобильных учетных данных
Мобильные устройства в Интернете	*	Серверная часть Mobile Access	5701	HTTPS	Мобильные устройства получают мобильные учетные данные через Интернет
Серверная часть Mobile Access	*	Google Firebase (Интернет)	*	HTTPS	Мобильные устройства получают push-уведомления (см. раздел о настройках брандмауэра в документации по Google Firebase) https://firebase.google.com/docs/cloud-messaging/concept-options

Исходящий сервер	Исход. порт	Входящий сервер	Вход. порт	Протокол	Комментарии
Клиентский компьютер пользователя VisMgmt	*	Серверная часть VisMgmt	5706	HTTPS	Команды с клиентского компьютера VisMgmt в серверную часть VisMgmt
Клиентский компьютер пользователя CredMgmt	*	Серверная часть CredMgmt	5806	HTTPS	Команды с клиентского компьютера CredMgmt в серверную часть CredMgmt
Компьютер администратора	*	Серверная часть Mobile Access	3389	Удаленный рабочий стол (RDP)	По соображениям безопасности администратору необходимо предоставить лишь временный доступ к компьютеру, на котором запущена серверная часть службы Mobile Access.

Замечание!
Обратите внимание, что служба Mobile Access и система ACS не поддерживают ни входящего, ни исходящего прямого подключения.

5.8.1 Программы и службы в исключениях брандмауэра

Вы можете настроить брандмауэр, добавив программы и службы в исключения

1. Запустите интерфейс брандмауэра Windows, нажав **Пуск > Настройки > Панель управления > Брандмауэр Windows**.
2. Выберите вкладку **Разрешение взаимодействия с приложением или компонентом в брандмауэре Windows**.
3. Выберите **Разрешить другое приложение** (если эта кнопка не активна, активируйте ее, щелкнув **Изменить настройки**.
4. Можно добавить в исключения следующие программы:

Программы

Путь установки по умолчанию — `C:\Program Files (x86)\Bosch Sicherheitssysteme\`

Программа	Расположение файла
acsp.exe	[Путь установки]\AccessEngine**AC**\BIN
ACTA-3.exe	[Путь установки]\AccessEngine**AC**\BIN
BioVerify.exe	[Путь установки]\AccessEngine**AC**\BIN
BioIdentify.exe	[Путь установки]\AccessEngine**AC**\BIN
Bosch.Ace.CredentialManagement.exe	[Путь установки]\Bosch Credential Management

Программа	Расположение файла
Bosch.Access.MobileAccessBackend.exe	[Путь установки]\Bosch Mobile Access
Bosch.Ace.VisitorManagement.exe	[Путь установки]\Bosch Visitor Management
CalTa-3.exe	[Путь установки]\AccessEngine**AC**\BIN
CDTA-1.exe	[Путь установки]\AccessEngine**AC**\BIN
EMDP.exe	[Путь установки]\AccessEngine**AC**\BIN
KCKemas.exe	[Путь установки]\AccessEngine**AC**\BIN
KCS.exe	[Путь установки]\AccessEngine**AC**\BIN
Loggifier-2.exe	[Путь установки]\AccessEngine**AC**\BIN
PictureServer.exe	[Путь установки]\AccessEngine**AC**\BIN
ReplServer.exe	[Путь установки]\AccessEngine**AC**\BIN
reps.exe	[Путь установки]\AccessEngine**AC**\BIN
TAccExc.exe	[Путь установки]\AccessEngine**AC**\BIN
EMAILSP.exe	[Путь установки]\AccessEngine**AC**\BIN
master-3.exe	[Путь установки]\AccessEngine**AC**\BIN
querySrv-2.exe	[Путь установки]\AccessEngine**AC**\BIN
webSrv-1.exe	[Путь установки]\AccessEngine**AC**\BIN
LicenseGateway.exe	[Путь установки]\AccessEngine**AC**\BIN
DMS.exe	[путь установки]\AccessEngine**MAC**\BIN
lac.exe	[путь установки]\AccessEngine**MAC**\BIN

Сервис

Путь установки по умолчанию — `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System`

Сервис	Расположение файла
Bosch.States.Api	[путь установки]\States API
Bosch.Map.Api	[путь установки]\Map API
Bosch.MapView.Api	[путь установки]\Map View API
Bosch.Events.Api	[путь установки]\Events API
Bosch.Alarms.Api	[путь установки]\Alarms API
Bosch.Ace.IdentityServer	[путь установки]\Identity Server
Bosch.Ace.Api	[путь установки]\Access API
Bosch.DialogManager.Api	[путь установки]\Dialog Manager API
Bosch.Intrusion.Api	[путь установки]\Intrusion API
Bosch Ace Visitor Management	[путь установки VM]\
Клиент Bosch Ace Visitor Management	[путь установки клиента VM]\

Сервис	Расположение файла
Bosch.OSS-SO	[путь установки]\OSS-SO
Bosch.OSS-SO.Configurator	[путь установки]\OSS-SO.Configurator
Bosch.Access.ProductApi.Api	[путь установки]\ProductApi
Bosch.MUM	[MUM-install-path]\

5.8.2 API Mobile Access

В версии Mobile Access 5.2 и выше, Credential Management 5.2 и выше и Visitor Management 5.2 и выше API сервера Mobile Access был разделен на передний и обратный канал. Передний канал предназначен для взаимодействия с мобильными телефонами, а обратный — с Credential Management и/или Visitor Management.
Это позволяет настроить правила брандмауэра и маршруты, чтобы регламентировать сетевой траффик и повысить информационную безопасность. Из-за разделения API используются два разных номера портов. Для мобильных телефонов предусмотрен порт 5700, а Credential Management и Visitor Management обращаются к порту 5701.
В Credential Management и Visitor Management предусмотрены отдельные настройки для URL-адресов переднего и обратного канала. В интерфейсе пользователя они называются «Адрес службы администрирования» (обратный канал) и «Адрес службы регистрации» (передний канал).
Для адреса службы администрирования (обратный канал) по умолчанию назначен порт 5701. В пользовательском правиле брандмауэра этот порт настраивается только для взаимодействия с компьютером, на котором запущен сервер Credential Management и/или Visitor Management. В большинстве случаев это сервер AMS.
Для адреса службы регистрации (передний канал) по умолчанию назначен порт 5700. В пользовательском правиле брандмауэра для этого порта должна быть настроена возможность доступа из приложений Mobile Access. Во многих случаях этот оконечный пункт будет открыт для доступа извне. Однако это сильно зависит от сценария использования клиента.
Если клиент обновляет более раннюю версию AMS до последней, необходимо настроить параметры Credential Management и Visitor Management. Этот параметр доступен на странице настроек для пользователей с ролью администратора Visitor Management и Credential Management.
Обратный канал должен быть защищен и закрыт для доступа через общедоступное интернет-соединение или любую несанкционированную сеть.

5.9 IT-безопасность

Безопасность системы управления доступом организации является важной частью ее инфраструктуры. Компания Bosch рекомендует строго соблюдать рекомендации по обеспечению IT-безопасности, предписанные для страны установки инструмента. Организация, использующая систему управления доступом, несет ответственность за следующее:

5.9.1 Ответственность за оборудование

– Предотвращение несанкционированного физического доступа к компонентам сети, таких как подключения RJ45.

  - Злоумышленникам необходим физический доступ для выполнения атак типа «атака посередине».
- Предотвращение несанкционированного физического доступа к аппаратному обеспечению контроллера AMC2.
- Использование выделенной сети для управления доступом.
  - Злоумышленники могут получить доступ через другие устройства в той же сети.
- Использование защищенных идентификаторов, таких как **DESFire** с кодом Bosch и многофакторной проверкой подлинности с биометрическими данными.
- Регистрация запросов с помощью приложения **Setup Access** и считывателей мобильного доступа с модулями BLE (Bluetooth с низким энергопотреблением). Незарегистрированные включенные считыватели уязвимы для взлома третьими лицами. Информацию по устранению подобных взломов путем сброса настроек до заводских см. в руководстве по установке считывающих устройств.
- Предоставление механизма отработки отказа и резервного источника питания для системы управления доступом.
- Отслеживание и отключение учетных данных, которые были утеряны.
- Надлежащее списание оборудования, которое больше не используется, в частности, сброс до заводских настроек и удаление персональных данных и информации о безопасности.

5.9.2 Ответственность за ПО

- Надлежащее обслуживание, обновление и обеспечение работы брандмауэра сети управления доступом.
- Мониторинг сигналов тревоги, указывающих на отключение аппаратных компонентов, таких как считыватели карт или контроллеры AMC2.
  - Эти сигналы могут означать попытку подмены аппаратных компонентов оборудования.
- Мониторинг сигналов вскрытия, вызванных электрическими контактами оборудования управления доступом, например контроллерами, считывателями и ключницами.
- Ограничение широковещательной передачи UDP в выделенной сети.
- Обновления, особенно обновления безопасности и исправления для программного обеспечения управления доступом.
- Обновления, в особенности обновления системы безопасности и исправления для микропрограмм оборудования.
  - Обратите внимание, что даже недавно поставленное оборудование может требовать обновления микропрограммного обеспечения. Инструкции см. в руководстве по оборудованию.
  - Компания Bosch не несет ответственности за ущерб, нанесенный в результате эксплуатации оборудования с устаревшими микропрограммами.
- Использование защищенного канала OSDPv2.
- Использование надежных паролей.
- Применение *Принципа минимальных полномочий* для предоставления доступа отдельных пользователей только к тем ресурсам, которые требуются им для их законных целей.
- Чтобы обычные операторы не могли назначать авторизации с высоким уровнем безопасности без получения согласия двух лиц, важно правильно назначить и настроить профили пользователей.

5.9.3 Безопасная работа с мобильными учетными данными

- Не оставляйте ненастроенные считыватели мобильного доступа без охраны.
  - Злоумышленник может использовать такой считыватель для взлома другой системы ACS. В результате потребуется затратный сброс до заводских настроек.
- Если мобильное устройство с мобильными учетными данными потеряно или украдено, необходимо предпринять те же действия, что и в случае потери карты: как можно быстрее заблокировать устройство или удалить с него все мобильные учетные данные.
- Для областей, где требуется высокий уровень безопасности, компания Bosch рекомендует использовать двухфакторную проверку подлинности. В таком случае владельцу учетных данных придется разблокировать мобильное устройство, прежде чем использовать его для идентификации.
- Мобильные учетные данные не восстанавливаются при восстановлении данных телефона из резервной копии. Если владелец мобильных учетных данных начинает использовать новое мобильное устройство, необходимо повторно отправить ему все имеющиеся приглашения.
- Злоумышленник может использовать глушитель связи для блокирования связи со считывателями мобильного доступа. Сотрудники, которым крайне необходим доступ в определенные зоны, должны иметь при себе физические средства идентификации в качестве запасного варианта.
  - В качестве запасного варианта вместо службы Mobile Access используйте только физические карты с надежным шифрованием (таким как шифрование Bosch).
- Защищайте сервер службы Mobile Access от несанкционированного физического доступа. Компания Bosch рекомендует использовать дополнительные меры, такие как шифрование диска BitLocker.
- Защищайте сервер службы Mobile Access от атак типа «отказ в обслуживании» (DoS). Сервер должен находиться в безопасной сетевой среде с такими средствами защиты, как ограничитель скорости.
- Обращайтесь с QR-кодами для приглашения установщика как с учетными данными администратора. Украденный телефон установщика с активными учетными данными позволит злоумышленнику перенастроить считыватели мобильного доступа в своих преступных целях.
  - Отправляйте приглашения установщикам непосредственно перед настройкой считывателей и следите за тем, чтобы они удаляли учетные данные сразу после завершения настройки.
  - По возможности лучше использовать функцию «Сканировать QR-коды с экрана», а не приглашения по электронной почте. Убедитесь, что назначенный установщик сразу же загружает учетные данные.

5.10 Создание резервной копии системы

VisMgmt представляет собой дополнительное веб-приложение для основной системы управления доступом. Для получения информации о резервном копировании системных баз данных см. документацию основной системы управления доступом.

6 Эксплуатация

6.1 Обзор ролей пользователей

Тип пользователя	Сценарии использования
Работник приемной	Регистрация новых посещений и посетителей Утверждение и отклонение посещений Добавление посетителей в черный список Назначение и отмена назначения карт посетителей Управление связанными документами Отслеживание количества посетителей на объекте
Посетитель	Самостоятельная и предварительная регистрация Создание и сопровождение профиля посетителя Подписание документов
Принимающая сторона	Управление расписаниями и списками посещений и посетителей Предварительная регистрация посещений
Администратор	Установка глобальных параметров Настройка поведения инструмента и его пользовательского интерфейса Дополнительно: Все варианты использования для работника приемной

6.2 Использование панели мониторинга

Панель мониторинга является главным экраном, центральным диалоговым окном, позволяющим перейти ко всем остальным диалоговым окнам.

Обзор и быстрые фильтры

Верхняя часть панели мониторинга содержит краткий обзор посещений за день. Это позволяет пользователям с легкостью отслеживать количество посетителей на объекте.

Ожидаемое сегодня число посетителей: _%	**Зарегистрированные посетители: _%**	**Посетители, выход которых сегодня пока не зарегистрирован**	**Посетители с истекшим временем регистрации выхода**
`<current count> / <total capacity>`	`<current count> / <total capacity>`	`<current count>`	`<current count>`

Щелкните любой из заголовков, чтобы отфильтровать таблицу посещений в соответствии со смыслом заголовка. Например, щелкните заголовок **Зарегистрированные посетители**, чтобы просмотреть только тех посетителей, которым назначена карта. Значение `<total capacity>` — это параметр конфигурации, настраиваемый администратором системы. См *Конфигурация с помощью меню «Параметры», Страница 32*.

6.2.1 Обзор страницы сотрудника

На панели управления нажмите имя нужного человека. Откроется диалоговое окно с персональными данными. Открываются данные. Поля персональных данных на странице сотрудника разделены на четыре раздела:

– Фото документа, удостоверяющего личность

- Документ, удостоверяющий личность
- Общие сведения
- документы

6.2.2 Таблица посещений

Каждая строка в таблице представляет собой назначенное посещение.

- Таблицу можно отсортировать по любому из столбцов, щелкнув заголовок столбца.
- Можно выбрать отдельных посетителей или сразу несколько посетителей с помощью стандартных инструментов мыши и клавиатуры:
  - Чтобы выбрать несколько отдельных строк, выделите их, удерживая клавишу Ctrl.
  - Чтобы удалить уже выделенную строку из списка выбранных, нажмите на нее, удерживая клавишу Shift.
  - Чтобы выделить несколько соседних строк, выделите их, удерживая клавишу Shift.
- В таблицу можно добавить новые посещения
- Обрабатывать посещения и сведения о посетителях можно, нажимая на кнопки действий
  - Утвердить посещение
  - Отклонить посещение
  - Назначить посетителю карты
  - Изменить сведения о посещении и посетителе
- Все данные можно экспортировать в файл .CSV или .XLSX. Если нужны только определенные данные, воспользуйтесь фильтрами. Невозможно экспортировать нужные данные, просто выбрав их. В файл .CSV или .XLSX можно экспортировать только отфильтрованные строки.

На горизонтальной панели инструментов предусмотрены следующие функции:

Метка	Функция
1 Кол-во **проходов**	Общее число посещений (N); каждое посещение — строка в таблице.
2 **Поиск**	Поиск произвольного текста по посещениям в таблице
3	Отображение списка посещений, которые были недавно добавлены в таблицу.
4	Открытие диалогового окна для выбора критериев фильтра
5	Возврат представления таблицы по умолчанию и отмена всех фильтров.

Метка	Функция
6 **Отмена назначенной карты**	Открытие диалогового окна для отмены назначенной карты с помощью подключенного регистрационного считывателя.
7 	Открытие диалогового окна для создания новой записи о посещении в таблице.
. . .	Щелкните значок с многоточием для вызова меню, чтобы экспортировать текущие фильтрованные визиты, а также документы в файлы различных форматов, например `CSV` или `.XLSX` Обратите внимание, что для обеспечения безопасности данных экспорт можно выполнить, только если клиент работает через защищенное соединение HTTPS с сертификатом.

6.2.3 Столбцы и действия в таблице

Столбцы

Столбец	Значение	Описание
Состояние	 Посещение ожидается  Посещение утверждено  Посещение отклонена  Карта назначена  Срок действия карты истек	Значок, отражающий состояние посещения

Столбец	Значение	Описание
	 Посещение завершено (посетитель больше не владеет картами и покинул территорию объекта)	
Имя	Имя посетителя с гиперссылкой	Щелкните гиперссылку, чтобы просмотреть сведения о посетителе и текущем посещении.
Ожидаемое прибытие	Дата и время	Ожидаемые дата и время прибытия посетителя
Ожидаемое убытие	Дата и время	Ожидаемые дата и время убытия посетителя
Зарегистрировано прибытие	Дата и время	Дата и время назначения посетителю первой карты.
Зарегистрировано убытие	Дата и время	Дата и время отмены назначения посетителю последней карты.
Номера карт	Числовое значение	Номера карт, назначенных данному посетителю.
Действия	Значки	См. отдельную таблицу ниже

Действия

Значок	Функция
	**Утвердить** посещение. ПРИМЕЧАНИЕ. Невозможно назначить карту посетителям, включенным в черный список. Сначала удалите посетителей из черного списка или временно исключите их. См. раздел *Черный список: добавление, удаление и исключение, Страница 57*.
	**Отклонить** посещение. Эта кнопка активируется после регистрации прибытия посетителя, т. е. после получения им карты.
	**Назначить** посетителю одну или несколько карт
	**Изменить** событие посещения и учетные данные посетителей

6.3 Работник приемной

6.3.1 Авторизация пользователя в роли «Работник приемной»

1. Для входа в систему откройте `https://< My_VisMgmt_server>:5706/main/` в браузере.
2. Введите имя пользователя учетной записи с необходимыми правами для вашей роли.
   Обратитесь к администратору системы, если у вас нет учетной записи.
3. Введите пароль.
4. Нажмите **Войти**.

6.3.2 Поиск и фильтрация посещений

На панели мониторинга VisMgmt над таблицей посещений.

Поиск

Для поиска по именам и принимающим сторонам, введите буквенно-цифровой запрос в поле поиска и нажмите клавишу «ВВОД».

Фильтрация

- Для просмотра ближайших к текущему времени посещений нажмите кнопку **Последние**.
- Для создания сложного фильтра на основе статуса посещения, даты прибытия и убытия, а также номеров карт нажмите кнопку **Фильтр**.
  - Во всплывающем диалоговом окне укажите требуемые критерии фильтрации.
  - Нажмите **Применить**.
    Система отобразит в таблице посещений только те встречи, которые соответствуют критериям фильтрации.
- Чтобы удалить все критерии, нажмите кнопку **Сбросить**.

6.3.3 Регистрация посещений

Введение

У работника приемной есть два базовых сценария регистрации посетителей:

- **А.** Если посетитель использует киоск для создания собственных идентификаторов посетителей и загрузки документов, сотруднику приемной достаточно лишь добавить недостающие сведения и подписи и назначить карту посетителю.
- **Б.** Если посетитель не использует киоск и обращается напрямую к сотруднику приемной, последний может зарегистрировать посещение с нуля: собрать необходимые сведения, получить подписи для необходимых документов и назначить карту посетителю.

Сценарий **А** частично входит в сценарий **Б**, поэтому здесь описан полный сценарий **Б**. Использование режима киоска посетителями описывается в отдельном разделе. См. раздел *Общие сведения о режиме киоска, Страница 60*.

Процедура

На панели мониторинга VisMgmt над таблицей посещений.

1. Нажмите значок  , чтобы добавить назначенное посещение в таблицу посещений.
2. В диалоговом окне **Персональные данные** введите данные, которые требуется указывать для посетителей вашего объекта. Обязательные поля помечены звездочкой (*).

Можно вводить данные вручную, но быстрее и точнее выполнить ввод можно с помощью сканера документов, если он доступен на рабочей станции работника приемной. Подробные сведения о поддерживаемых периферийных устройствах см. в разделе *Периферийное оборудование, Страница 27*.

- **Общие сведения**
  - Найдите и загрузите полный профиль посетителя, созданный при предыдущем посещении. Для поиска профиля нажмите значок  (Поиск), расположенный в поле **Фамилия***.
    При создании профиля посетитель получает уникальный буквенно-цифровой код, который необходимо хранить, чтобы ускорить процесс регистрации во время последующих посещений.
  - В противном случае введите данные вручную.
- **Идентификационные фотографии**
  - **Загрузите** фотографию из файловой системы.
  - **Сделайте фото** посетителя с помощью подключенной веб-камеры.
- **Идентификационные документы**
  - Нажмите **Сканировать документ**, чтобы считать данные с помощью сканера документов (при наличии) и автоматически заполнить соответствующие поля данных в этом диалоговом окне.
  - Если в вашей системе нет сканера документов, данные можно ввести вручную.
- **Юридические документы**
  - Загрузите документы, которые посетитель подписал в электронном виде с помощью киоска.
  - Если в вашей система не предусмотрен киоск для посетителей, распечатайте и загрузите необходимые PDF-документы (с подписью посетителя), хранящиеся в файловой системе.

3. Нажмите **Далее** для перехода к диалоговому окну **Посещения**.
4. В диалоговом окне **Посещения** на панели **Текущее посещение** введите данные, необходимые для вашего объекта. Обязательные поля помечены звездочкой (*).

- Выберите **Тип посетителя**.
  Это может быть **Посетитель** (по умолчанию) или настраиваемый подкласс **Посетителя**, определяемый как **Тип лица** в основной системе управления доступом.
- Выберите имя сотрудника, которого планируете посетить, в поле **Host (Принимающий)**.
  - Выбрать можно только держателей карт основной системы управления доступом.
  - Всплывающая подсказка отобразит адрес электронной почты этого лица для дополнительной идентификации.
- Если посетителю требуется сопровождение по территории объекта, выберите имя сопровождающего сотрудника в поле **Сопровождающий**.
  - Выбрать можно только держателей карт основной системы управления доступом.
  - Всплывающая подсказка отобразит адрес электронной почты этого лица для дополнительной идентификации.
- Если посетителю требуется дополнительное время для прохода через дверь, установите флажок **Расширенное время открытия двери**.

5. Нажмите кнопку **Сохранить**.
   Обратите внимание, что сохранить данные невозможно, пока не будут заполнены все обязательные поля.

См.
– *Периферийное оборудование, Страница 27*

6.3.4 Утверждение и отклонение посещений

Примечание: утверждение физических карт
Необходимо утвердить посещение, прежде чем можно будет назначить карты посетителю.

Примечание: утверждение мобильных учетных данных
Мобильные учетные данные можно создать и предоставить в день посещения аналогично назначению физической карты.
– **Примечание.** Мобильные учетные данные будут недействительными до утверждения посещения.

Кроме того, можно создать мобильные учетные данные и предоставить их заранее. Когда посетитель приходит в приемную, утвердите посещение, как описано ниже, чтобы активировать учетные данные.
– **Примечание.** Мобильные учетные данные будут недействительными до утверждения посещения.
– Если установлено предполагаемое время окончания посещения, это время будет применено.
– Если время окончания посещения не задано, будет применено количество часов по умолчанию (8). Администраторы могут изменить это значение по умолчанию в меню **Настройки**.

Процедуры утверждения и отклонения
Утвердить или отклонить посещения можно в двух местах:
– в таблице посещений на панели мониторинга
– в редакторе посещения

В таблице посещений на панели мониторинга:

– **Утвердить**: выберите строку в таблице посещений и щелкните значок  .
  После появления всплывающего окна подтверждения значок становится серым, показывая, что посещение утверждено.

– **Отклонить**: выберите строку в таблице посещений и щелкните значок  .
  После появления всплывающего окна подтверждения значок **Утвердить** снова становится синим, показывая, что данное посещение по-прежнему ожидает утверждения.

В редакторе посещения:

1. В таблице посещений на панели мониторинга выберите строку и щелкните значок  для редактирования посещения.
2. В диалоговом окне **Персональные данные** нажмите кнопку **Далее**.
3. В диалоговом окне **Посещения** нажмите кнопку **Утвердить** или **Отклонить**.
4. Подтвердите действие во всплывающем окне.

6.3.5 Назначение физических учетных данных

Введение

Назначьте карту посетителя каждому посетителю, которому разрешен вход на территорию данного объекта. При необходимости можно назначить несколько карт одному посетителю.

- Время **Регистрации прибытия** посещения — это время назначения первой карты.
- Время **Регистрации убытия** посещения — это время отмены назначения последней карты, назначенной посетителю.

Работник приемной может назначать карты и отменять их назначение на панели мониторинга, если к компьютеру работника приемной подключен считыватель регистрационных карт.

Тем не менее, если считыватель карт отсутствует, редактор посещений позволяет назначать номера карт.

Замечание!

Лица, занесенные в черный список, не могут получать карты

Карты нельзя назначить посетителям, которые находятся в черном списке. Перед попыткой назначить карту удалите посетителя из черного списка или создайте для него временное исключение.

Назначение карты на панели мониторинга (требуется регистрационный считыватель)

1. Приготовьте физическую карту посетителя, чтобы приложить ее к регистрационному считывателю.
2. Утвердите посещение в таблице посещений. См. раздел *Утверждение и отклонение посещений, Страница 51*.
3. Выберите строку посещения и щелкните значок 
4. Следуйте инструкциям во всплывающем окне для использования регистрационного считывателя.

Отмена назначения карты на панели мониторинга (требуется регистрационный считыватель)

1. Получите от владельца карты физическую карту и приготовьтесь приложить ее к регистрационному считывателю.
2. На панели инструментов щелкните **Отменить назначение карты**. 

3. Следуйте инструкциям во всплывающем окне для использования регистрационного считывателя.

Назначение карты в редакторе посещений

1. В таблице посещений на панели мониторинга выберите строку и щелкните значок  для редактирования этого посещения.
2. В диалоговом окне **Персональные данные** нажмите кнопку **Далее**
3. Если посещение еще не утверждено, нажмите кнопку **Утвердить** в диалоговом окне **Посещения**.
4. При наличии подключенного регистрационного считывателя нажмите кнопку **Считать карту** и следуйте инструкциям во всплывающем окне для использования регистрационного считывателя.

– В противном случае для просмотра списка доступных карт посетителей нажмите **Показать доступные карты**.
  При наличии несортированных физических карт с печатными номерами можно также выбрать любую карту и быстро найти ее номер в списке с помощью инструмента **поиска**.

– Щелкните значок  рядом с номером карты, чтобы назначить эту карту текущему посетителю.
– При необходимости назначить и другие карты повторите последнее действие.

5. Нажмите **Сохранить**, чтобы сохранить текущее посещение с назначенными картами.

Отмена назначения карты в редакторе посещений

1. В таблице посещений на панели мониторинга выберите строку и щелкните значок  для редактирования этого посещения.
2. В диалоговом окне **Персональные данные** нажмите кнопку **Далее**
3. В диалоговом окне **Посещения** на панели «Карты посетителей» щелкните значок  рядом с картой, назначение которой требуется отменить, и подтвердите действие во всплывающем окне.
  Повторяйте это действие до тех пор, пока не будет отменено назначение всех необходимых карт.
4. Нажмите **Сохранить**, чтобы сохранить текущее посещение с назначенными картами.
5. При отмене назначения последней карты, назначенной посетителю, система записывает эту дату и время в качестве времени регистрации убытия посетителя.

  В таблице посещений состояние этой записи меняется на  .

См.

– *Конфигурация с помощью меню «Параметры», Страница 32*
– *Регистрация посещений, Страница 49*

– *Утверждение и отклонение посещений, Страница 51*

6.3.6 Назначение мобильных учетных данных

Предварительные требования

– В системе установлена и настроена служба Mobile Access.
  – Инструкции см. в соответствующем разделе главы «Установка» данного документа.
– На смарт-устройстве принимающего лица установлено и запущено приложение Mobile Access.
  – Инструкции см. в соответствующем разделе главы «Установка» данного документа.

Процедура

Мобильные учетные данные можно назначить, нажав непосредственно на значок панели управления или на странице сотрудника.

На **панели управления:**

1. Выберите строку лица, которому нужно предоставить мобильные учетные данные
2. В выбранной строке щелкните значок 

На странице сотрудника:

1. На **панели управления** выберите имя нужного сотрудника. Откроется страница с его данными.
2. Выберите вкладку **Учетные данные** > **Добавить мобильный доступ.**

Выполните описанные ниже действия.

1. Выберите вариант с помощью одного из крупных значков:

– **QR-код**
  или
– **письмо с приглашением**

2. Если выбран **вариант с QR-кодом**:

– Система отображает QR-код
– Пользователь сканирует QR-код с помощью приложения Mobile Access на мобильном устройстве
– Чтобы активировать учетные данные, нужно **утвердить** посещение.
  Инструкции см. в разделе *Утверждение и отклонение посещений, Страница 51*
– Когда приложение запущено, мобильное устройство действует аналогично физической карте доступа

3. Если выбран **вариант письма с приглашением**:

– По умолчанию программа выбирает адрес электронной почты, указанный для выбранного лица. При необходимости введите другой адрес электронной почты
– Система отправляет электронное письмо на выбранный адрес
– Лицо получает электронное письмо на свое мобильное устройство, на котором установлено приложение Mobile Access
– Лицо открывает ссылку в электронном письме
– Чтобы активировать учетные данные, нужно **утвердить** посещение.
  Инструкции см. в разделе *Утверждение и отклонение посещений, Страница 51*
– Когда приложение запущено, мобильное устройство действует аналогично физической карте доступа

Процедура в диалоговых окнах редактирования

1. Выберите строку лица, которому нужно предоставить мобильные учетные данные

2. В выбранной строке щелкните значок 
– Откроется диалоговое окно редактирования
3. В VisMgmt нажмите кнопку **Далее**, чтобы перейти на экран **Сведения о посещении**
4. Нажмите кнопку **Добавить Mobile Access**
5. Выберите вариант с помощью одного из крупных значков:
– **QR-код**
или
– **письмо с приглашением**
6. Если выбран **вариант с QR-кодом**:
– Система отображает QR-код
– Пользователь сканирует QR-код с помощью приложения Mobile Access на мобильном устройстве
– Чтобы активировать учетные данные, нужно **утвердить** посещение.
Инструкции см. в разделе *Утверждение и отклонение посещений, Страница 51*
– Когда приложение запущено, мобильное устройство действует аналогично физической карте доступа
7. Если выбран **вариант письма с приглашением**:
– По умолчанию программа выбирает адрес электронной почты, указанный для выбранного лица. При необходимости введите другой адрес электронной почты
– Система отправляет электронное письмо на выбранный адрес
– Лицо получает электронное письмо на свое мобильное устройство, на котором установлено приложение Mobile Access
– Лицо открывает ссылку в электронном письме
– Чтобы активировать учетные данные, нужно **утвердить** посещение.
Инструкции см. в разделе *Утверждение и отклонение посещений, Страница 51*
– Когда приложение запущено, мобильное устройство действует аналогично физической карте доступа

См.
– *Установка службы Mobile Access, Страница 20*
– *Установка приложений Mobile Access, Страница 18*

6.3.7 Отмена назначения учетных данных

Отмена назначения карты на панели мониторинга (требуется регистрационный считыватель)

1. Получите от владельца карты физическую карту и приготовьтесь приложить ее к регистрационному считывателю.
2. На панели инструментов щелкните **Отменить назначение карты**. 
3. Следуйте инструкциям во всплывающем окне для использования регистрационного считывателя.

Отмена назначения карты в редакторе учетных данных

1. В таблице посещений на панели мониторинга выберите строку и щелкните значок  для редактирования этого владельца карты.
2. В диалоговом окне редактирования в столбце **Карты сотрудников** щелкните значок  рядом с картой, назначение которой требуется отменить, и подтвердите действие во всплывающем окне.
   Повторяйте это действие до тех пор, пока не будет отменено назначение всех необходимых карт.
3. Нажмите **Сохранить**, чтобы сохранить текущее посещение с назначенными картами.

6.3.8 Проверка входа и выхода посетителей без карт

Введение

Личные карты необязательны для посетителей, которые идут с индивидуальным сопровождением или ограничиваются общественными местами. Для таких случаев предусмотрена возможность контроля посетителей без карт. В целях безопасности эта функция по умолчанию отключена.

Предварительное требование.

Системный администратор включил функцию **регистрации прибытия/убытия без карты** в диалоговом окне **Настройки** > **Работник ресепшена > Посещения**. См. инструкции в главе по конфигурации *Конфигурация с помощью меню «Параметры», Страница 32*.

Процесс

Если эта функция включена, то происходит следующее:

– Любой посетитель, самостоятельно регистрирующийся на компьютере-киоске, автоматически подтверждает посещение и одновременно регистрирует вход.
– Система выставляет дату и время входа на момент регистрации.
– Кнопка **Регистрация прибытия/убытия без карты** появляется в редакторе посещений и на панели мониторинга соответствующего визита.

Порядок действий: Регистрация входа посетителя без карты

Если не может зарегистрировать себя в киоске, но ему нужно зарегистрировать вход без карты:

1. зарегистрируйте посещение вручную, как описано в главе *Регистрация посещений, Страница 49*
2. Щелкните имя посетителя в таблице посещений на панели мониторинга или щелкните  , чтобы отредактировать посещение.
3. В диалоговом окне **Персональные данные** нажмите кнопку **Далее**
4. В диалоговом окне **Посещения**, в области **Карты посетителей**, нажмите **Регистрация входа без карты**

Порядок действий: Регистрация выхода посетителя без карты

Если посетитель без карты покидает помещение:

1. Щелкните имя посетителя в таблице посещений на панели мониторинга или щелкните  , чтобы отредактировать посещение.
2. В диалоговом окне **Персональные данные** нажмите кнопку **Далее**
3. В диалоговом окне **Посещения**, в области **Карты посетителей**, нажмите **Регистрация выхода без карты**

См.

– *Регистрация посещений, Страница 49*

6.3.9 Черный список: добавление, удаление и исключение

Посетителей, присутствие которых на объекте нежелательно, можно поместить в черный список. Пока посетитель находится в черном списке, ему нельзя назначить карту. Посетителя можно в любое время удалить или временно исключить из черного списка, чтобы назначить ему карту.

Добавление в черный список

1. В таблице посещений на панели мониторинга выберите строку и щелкните значок  для редактирования посещения.
2. В диалоговом окне **Персональные данные** нажмите кнопку **Черный список**.
3. Во всплывающем окне подтвердите, что этот пользователя действительно необходимо внести в черный список.
4. В следующем всплывающем окне введите причину и подтвердите добавление в черный список.

– В редакторе посещения будет отображен баннер **В черном списке**:

.

– Под баннером появятся две кнопки: одна — для удаления, а другая — для временного исключения посетителя из черного списка.
– В таблице посещения имя каждого из занесенных в черный список посетителей отображается с треугольным знаком предупреждения. Пример: 

Удаление и исключение

1. В таблице посещений на панели мониторинга выберите строку, в которой посетитель отмечен как включенный в черный список, и щелкните значок  , чтобы отредактировать посещение.
2. В диалоговом окне **Персональные данные** нажмите одну из следующих кнопок:

– **Удалить**, чтобы навсегда удалить посетителя из черного списка.
– **Исключить**, чтобы оставить посетителя в черном списке, но разрешить назначение карты только для данного посещения.

3. Подтвердите действие во всплывающем окне.

6.3.10 Хранение профилей посетителей

Система хранит профили посетителей до тех пор, пока сами посетители или администраторы их не удалят.
По истечении срока хранения, определенного в настройках системы (значение по умолчанию — 12 месяцев), система удаляет записи о посещении.
Когда посетитель или работник приемной создает новый профиль посетителя, этот профиль получает уникальный буквенно-цифровой код. Посетители могут войти в систему с этим кодом с помощью киоска посетителя и, следовательно, получить доступ для сохранения своих собственных профилей.

Замечание!
Защита идентификаторов посетителей
Следует защищать идентификаторы посетителей от несанкционированного доступа, так как они обеспечивают доступ к персональным данным.

6.3.11 Просмотр записей о посещениях

1. В таблице посещений на панели мониторинга выберите строку и щелкните значок  для редактирования этого посещения.
2. В диалоговом окне **Персональные данные** нажмите кнопку **Далее**.
3. В диалоговом окне **Текущее посещение** нажмите кнопку **Показать все посещения**.
   В диалоговом окне **Текущее посещение** отображается список предыдущих посещений.

6.4 Принимающая сторона

Принимающая сторона — это сотрудник, который принимает посетителя. Сотрудники могут регистрировать свои собственные встречи и просматривать в системе подробные сведения о посетителях и их прошлых, текущих и будущих посещениях.

6.4.1 Авторизация пользователя в роли «Принимающая сторона»

1. Для входа в систему откройте `https://`< My_VisMgmt_server>`:5706/main/` в браузере.
2. Введите имя пользователя учетной записи с необходимыми правами для вашей роли.
   Обратитесь к администратору системы, если у вас нет учетной записи.
3. Введите пароль.
4. Нажмите **Войти**.

6.4.2 Поиск и фильтрация

Панель инструментов на панели мониторинга принимающей стороны содержит следующие функции:

Метка	Функция
1 Кол-во **проходов**	Общее число посещений (N); каждое посещение — строка в таблице.
2 **Поиск**	Поиск произвольного текста по посещениям в таблице
3	Отображение списка посещений, которые были недавно добавлены в таблицу.
4	Открытие диалогового окна для выбора критериев фильтра
5	Возврат представления таблицы по умолчанию и отмена всех фильтров.
6	Открытие диалогового окна для создания новой записи о посещении в таблице.

Поиск

Для поиска по именам и принимающим сторонам, введите буквенно-цифровой запрос в поле поиска и нажмите клавишу «ВВОД».

Фильтрация

- Для просмотра ближайших к текущему времени посещений нажмите кнопку **Последние**.
- Для создания сложного фильтра на основе статуса посещения, даты прибытия и убытия, а также номеров карт нажмите кнопку **Фильтр**.
  - Во всплывающем диалоговом окне укажите требуемые критерии фильтрации.
  - Нажмите **Применить**.
    Система отобразит в таблице посещений только те встречи, которые соответствуют критериям фильтрации.
- Чтобы удалить все критерии, нажмите кнопку **Сбросить**.

6.4.3 Регистрация посещений

Чтобы добавить назначенное посещение посетителя, приходящего на объект впервые, выполните следующие действия:

На панели мониторинга VisMgmt над таблицей посещений.

1. Щелкните значок  , чтобы добавить строку в таблицу посещений.
2. В разделе **Общие сведения** диалогового окна **Персональные данные** введите персональные данные, которые требуется указывать о посетителях вашего объекта.

3. Укажите необходимые сведения в разделе **Сведения о посещении**. Как правило, это ожидаемое время прибытия и убытия, а также цель посещения.
4. Нажмите кнопку **Сохранить**, чтобы сохранить назначенное посещение.
   Посещение появится на панели мониторинга в виде строки в таблице посещений.

6.4.4 Копирование назначенных посещений

Чтобы назначить еще одно посещение для того же посетителя, выполните следующие действия:

1. Найдите в таблице посещений на панели мониторинга VisMgmt существующую встречу с тем же посетителем.
2. Щелкните значок меньшего размера  в конце строки.
3. В разделе **Сведения о посещении** диалогового окна **Персональные данные** укажите необходимые сведения. Как правило, это ожидаемое время прибытия и убытия, а также цель посещения.
4. Нажмите кнопку **Сохранить**, чтобы сохранить назначенное посещение.
   Посещение появится на панели мониторинга в виде строки в таблице посещений.

6.5 Посетитель

Посетители могут использовать систему на территории объекта в режиме киоска для создания собственных профилей посетителей и подписания необходимых документов перед получением карты посетителя у работника приемной.

6.5.1 Общие сведения о режиме киоска

Посетители обычно регистрируют свои посещения и создают собственные профили на компьютере, который находится в свободном доступе в зоне приемной объекта с контролируемым доступом. В целях безопасности веб-браузер компьютера работает в режиме киоска, который предоставляет доступ только к VisMgmt, не позволяя открыть несколько вкладок, параметры браузера и получить доступ к операционной системе компьютера. Все поддерживаемые браузеры предлагают режим киоска, но точная конфигурация зависит от браузера.

На компьютере-киоске запускается надстройка для **периферийных устройств Bosch**, которая обеспечивает физическое подключение периферийных устройств для сканирования идентификационных документов и подписей.

- URL-адрес для режима киоска — `https://`<My_VisMgmt_server>`:5706`
- URL-адрес для входа в систему в роли администратора, работника приемной или принимающей стороны `https://`<My_VisMgmt_server>`:5706/main/`

6.5.2 Создание профиля посетителя: самостоятельная регистрация прибытия

Новые посетители

Обратите внимание, что точная процедура зависит от того, какие периферийные устройства (сканеры документов и подписей, фотоаппараты) подключены к компьютеру в режиме киоска.

1. На экране приветствия компьютера в режиме киоска нажмите **Продолжить без идентификатора посетителя**.

2. На следующем экране нажмите **Самостоятельная регистрация**.
3. На следующем экране выберите **Сканировать документ**.
4. Следуйте инструкциям на экране выполнения требований, действующих на объекте, таких как:

– сканирование идентифицирующих документов;
– подписание обязательных юридических документов;
– фотографирование.

5. Система отображает собранные сведения для исправления и завершения процесса.
6. Система запрашивает, требуется ли вам разрешение на особый доступ, и сообщает об этом работнику приемной в случае необходимости.
7. В конце процесса регистрации на экране отображается уникальный идентификатор посетителя.
   Сообщите этот идентификационный номер работнику приемной, чтобы получить карту посетителя.

Замечание!
Уникальный идентификатор посетителя
Бережно храните идентификатор посетителя и защищайте его от несанкционированного использования. Он предоставляет доступ к вашему профилю посетителя.
Идентификатор можно использовать для входа в систему на компьютере в режиме киоска, чтобы ускорить регистрацию посещения в дальнейшем.

Повторные посетители

1. Авторизуйтесь компьютере в режиме киоска, используя свой уникальный идентификатор посетителя.
2. Система отображает собранные сведения для исправления и завершения процесса в случае необходимости.
3. Обратитесь к работнику приемной для получения карты посетителя.

6.6 Авторизация установщиков считывателей мобильного доступа

Введение

Установщики считывателей мобильного доступа используют Bosch Setup Access для сканирования и настройки считывателей по BLE.
Уполномоченные операторы систем **Credential Management** и **Visitor Management** отправляют виртуальные учетные данные в приложение установщика для авторизации установщика. В этом разделе описана данная процедура.

Предварительные требования

– В системе установлена и настроена служба Mobile Access.
  – Инструкции см. в соответствующем разделе главы «Установка» данного документа.
– Убедитесь, что установщик, которому нужно авторизоваться, установил и запустил приложение Bosch Setup Access на своем смарт-устройстве.
  – Инструкции см. в соответствующем разделе главы «Установка» данного документа.

Процедура

1. В главном меню щелкните  , чтобы открыть диалоговое окно **Регистрация установщиков**.

2. Нажмите кнопку **Добавить**, чтобы добавить установщика в список или  , чтобы удалить существующего установщика

– Откроется всплывающее окно **Добавить установщика**.

3. Во всплывающем окне **Добавить установщика** введите нужные сведения, например:

– Имя и фамилию, название компании, адрес электронной почты, номер телефона

– Примечание. Позже можно будет нажать значок  , чтобы изменить сведения о выбранном установщике

4. Нажмите кнопку **Далее**

5. Выберите вариант с помощью одного из крупных значков:

– **QR-код**
или
– **письмо с приглашением**

6. Если выбран **вариант с QR-кодом**:

– Система отображает QR-код
– Пользователь сканирует QR-код с помощью приложения Mobile Access на мобильном устройстве
– Процесс регистрации установщика завершен
– Это позволит сканировать считыватели мобильного доступа с помощью мобильного устройства и настраивать их по BLE, пока приложение запущено

7. Если выбран **вариант письма с приглашением**:

– По умолчанию программа выбирает адрес электронной почты, указанный для выбранного лица. При необходимости введите другой адрес электронной почты
– Система отправляет электронное письмо на выбранный адрес
– Лицо получает электронное письмо на свое мобильное устройство, на котором установлено приложение Bosch Setup Access
– Лицо открывает ссылку в электронном письме
– Процесс регистрации установщика завершен
– Это позволит сканировать считыватели мобильного доступа с помощью мобильного устройства и настраивать их по BLE, пока приложение запущено

Повторная отправка приглашений

1. Выберите нужного установщика в диалоговом окне регистрации установщика

2. Нажмите значок  в той же строке, чтобы повторно отправить выбранному установщику приглашение для авторизации с помощью QR-кода или электронного письма.

ПРИМЕЧАНИЕ. Отправить приглашение для авторизации повторно можно лишь в том случае, если установщик еще не активировал его.

6.6.1 Сброс настроек считывателей мобильного доступа

Может возникнуть необходимость сбросить настройки считывателей доступа до заводских параметров по умолчанию, чтобы настроить их повторно.
Например, если установщику нужно будет перенастроить считыватели, уже настроенные для использования на другом объекте, их настройки придется сбросить.
Информацию по сбросу настроек считывателей с помощью DIP-переключателей см. в руководстве по эксплуатации считывателя LECTUS select.

6.7 Использование приложений Mobile Access на мобильных устройствах

ПРИМЕЧАНИЕ. Использование приложений Bosch Mobile Access для соответствующих пользователей подробно описано в отдельных **кратких руководствах пользователя**. Эти документы доступны в онлайн-каталоге продуктов Bosch.

Введение

Bosch предлагает следующие приложения для Mobile Access

- Bosch Mobile Access: приложение владельца карты для хранения виртуальных учетных данных и их передачи по Bluetooth на считыватели, настроенные для Mobile Access. Затем такой считыватель предоставляет или запрещает доступ в зависимости от того, есть ли в приложении действительные для него учетные данные.
- Bosch Setup Access: приложение установщика для сканирования и настройки считывателей по Bluetooth.

Уполномоченные операторы систем Visitor Management и Credential Management могут отправлять виртуальные учетные данные для приложений владельца карты и установщика.

Замечание!
ВНИМАНИЕ: не запускайте приложения владельца карты и установщика одновременно
Убедитесь, что никто не использует приложения установщика и владельца карты одновременно.

6.7.1 Настройка пороговых значений RSSI в приложении Setup Access

Введение

В контексте приложения Bosch Mobile Access пороговое значение RSSI и зону действия BLE можно считать практически тождественными понятиями.
Устройства мобильного доступа передают сигналы BLE на считыватели поблизости.
Установка порогового значения RSSI — важный этап настройки считывателя. Это пороговое значение отражает минимальный уровень сигнала BLE, измеряемый в дБм, который считыватель (R) должен принять в качестве запроса на вход. Более слабые сигналы BLE игнорируются считывателем.

Значения RSSI могут сильно отличаться в зависимости от многих факторов, включая тип передающего устройства, уровень заряда батареи, а также материал и толщину близлежащих стен. Не существует линейной зависимости между значением RSSI и расстоянием между передатчиком и приемником.
Поэтому приложение Setup Access предоставляет инструмент для измерения RSSI считывателя, исходя из текущего положения мобильного устройства. Ниже описана процедура использования этого инструмента.
Когда найдете подходящее пороговое значение зоны действия BLE, используйте приложение Setup Access, чтобы сохранить это значение в конфигурации считывателя.

Процедура

Настройте **зону действия BLE** с помощью одного из следующих вариантов, А или Б:

А. Использование определяемых считывателем значений RSSI

1. Встаньте перед считывателем в таком месте, где, как вы предполагаете, будут находиться пользователи мобильных учетных данных.
2. Нажмите кнопку **Проверить и использовать текущую зону действия**

– Появится всплывающее сообщение. Нажмите кнопку **ОК**

3. Отобразится значение RSSI.

– Рекомендуется повторить этот шаг несколько раз, стоя в одном и том же месте, чтобы определить степень вариативности уровня принимаемого сигнала.

4. Когда найдете подходящее пороговое значение, нажмите кнопку **Сохранить**.

Б. Установка порогового значения RSSI вручную

1. Введите пороговое значение RSSI.
   См. таблицу типичных пороговых значений ниже
2. Нажмите кнопку **Сохранить**

Типичные пороговые значения (приблизительные):

Ожидаемое расстояние от мобильного устройства до считывателя	Рекомендуемое пороговое значение RSSI
Близко (5–10 см)	-30...-40 дБм
Средне (0,5–2 м)	-50...-60 дБм
Далеко (> 2 м)	-70...-90 дБм

Замечание!
Значения RSSI могут сильно отличаться в зависимости от многих факторов, включая тип передающего устройства, уровень заряда батареи, а также материал и толщину близлежащих стен.

Глоссарий

ACS

Общий термин для системы управления доступом Bosch, например AMS (Access Management System) или ACE (BIS Access Engine).

BLE

Bluetooth с низким энергопотреблением — беспроводная сетевая технология, которая обеспечивает такую же зону действия, что и обычный Bluetooth, но с меньшим потреблением энергии.

FQDN

Полное доменное имя — это сетевое доменное имя, которое выражает свое абсолютное местоположение в иерархии системы доменных имен (DNS).

OSDP

Открытый двунаправленный контролируемый протокол устройств — это стандарт связи с контролем доступа, представленный в 2011 году Ассоциацией индустрии безопасности (SIA). Он превосходит старые протоколы в области шифрования и биометрии, а также простоты использования и совместимости.

RSSI

Показатель уровня принимаемого сигнала (RSSI) — это измеряемый в дБм показатель силы сигнала, принимаемого устройством. Мобильные устройства обычно отображают RSSI в виде гистограммы уровня сигнала.

принимающая сторона

в контексте управления посетителями принимающей стороной называется лицо, принимающее посетителя.

режим киоска

Режим использования браузера со строгими ограничениями, который обычно допускает доступ только к одному веб-приложению, не позволяя открыть параметры браузера, несколько вкладок или получить доступ к операционной системе компьютера.

Служба Mobile Access

Средство управления доступом лиц с помощью виртуальных учетных данных, хранимых на мобильном устройстве, например на смартфоне.

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Нидерланды
www.boschsecurity.com

Решения в сфере управления зданиями для улучшения качества жизни

202405131938