

Credential Management V5.5

C Mobile Access

Содержание

1	Безопасность	5
2	Введение	6
2.1	О Credential Management и Visitor Management	6
2.2	О службе Mobile Access	6
3	Установка и удаление	8
3.1	Необходимое программное обеспечение	8
3.2	Необходимое оборудование	9
3.2.1	Настройка надстройки для периферийных устройств	9
3.3	Установка Credential Management	10
3.3.1	Требования для установки CredMgmt	10
3.3.2	Процесс установки	11
3.4	Установка службы Mobile Access	13
3.4.1	Обзор установки, настройки и использования	13
3.4.2	Аппаратные требования службы Mobile Access	14
3.4.3	Требования к конфигурации службы Mobile Access	14
3.4.4	Процедура совмещенной установки	15
3.4.5	Процедура распределенной установки	17
3.5	Сертификаты для защищенной связи	20
3.5.1	Сертификаты для браузера Firefox	21
3.5.2	Сертификаты для браузера Chrome	22
3.5.3	Установка приложений Mobile Access	22
3.6	Восстановление установки службы Mobile Access	23
3.7	Удаление программного обеспечения	23
4	Обзор Credential Management	25
5	Конфигурирование	27
5.1	Создание пользователей Credential Management в ACS	27
5.2	Вход в систему для выполнения задач конфигурирования	27
5.3	Конфигурация с помощью меню «Параметры»	28
5.3.1	Шаблоны электронной почты	29
5.3.2	Шаблоны документов	30
5.4	Настройка пользовательского интерфейса	30
5.4.1	Настройка отображаемых, невидимых и обязательных параметров	30
5.4.2	Настройка текстов пользовательского интерфейса для локализации	30
5.4.3	Настройка логотипа компании	31
5.5	Параметры брандмауэра	31
5.5.1	Программы и службы в исключениях брандмауэра	32
5.5.2	API Mobile Access	34
5.6	ИТ-безопасность	35
5.6.1	Ответственность за оборудование	35
5.6.2	Ответственность за ПО	35
5.6.3	Безопасная работа с мобильными учетными данными	36
5.7	Конфиденциальность и защита данных в компании Bosch	37
5.8	Авторизация с высоким уровнем безопасности	38
5.8.1	Принцип согласия двух лиц	38
5.8.2	Настройка авторизаций с высоким уровнем безопасности	38
6	Эксплуатация	40
6.1	Обзор ролей пользователей	40
6.2	Использование панели мониторинга	40

6.2.1	Обзор страницы сотрудника	42
6.3	Назначение авторизаций	43
6.4	Назначение физических учетных данных	45
6.5	Назначение мобильных учетных данных	45
6.6	Отмена назначения учетных данных	47
6.7	Авторизация установщиков считывателей мобильного доступа	48
6.7.1	Сброс настроек считывателей мобильного доступа	49
6.8	Использование приложений Mobile Access на мобильных устройствах	49
6.8.1	Настройка пороговых значений RSSI в приложении Setup Access	50
	Словарь	52

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 Credential Management и Visitor Management

Программа Credential Management, далее называемая CredMgmt, — это браузерное программное средство, которое работает совместно с системой управления доступом Bosch или ACS. Благодаря простому и интуитивно понятному интерфейсу, даже относительно неопытные пользователи смогут управлять учетными данными сотрудников и внешнего персонала. Учетные данные могут быть в форме физических карт либо мобильных учетных данных.

Система Credential Management

В CredMgmt операторы ACS могут управлять как учетными данными, так и записями сотрудников, которым они принадлежат.

Организация	Добавить	Изменить	Удалить	Назначить/ Отменить назначение
Физические средства идентификации				Да
Виртуальные мобильные учетные данные (если установлена программа Mobile Access)	Да		Да	Да
Авторизации				Да
Записи держателей карт	Да	Да	Да	

Управление посетителями

В ACS VisMgmt операторы управляют учетными данными, сведениями о посетителях и посещениях.

Организация	Добавить	Изменить	Удалить	Назначить/ Отменить назначение
Физические средства идентификации				Да
Виртуальные мобильные учетные данные (если установлена программа Mobile Access)	Да			Да
Сведения о посетителях	Да	Да	Да	
Сведения о посещениях	Да	Да	Да	

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.

3 Установка и удаление

3.1 Необходимое программное обеспечение

Сервер CredMgmt устанавливается на том же компьютере, что и ACS (основная система управления доступом). К программному обеспечению и оборудованию применяются те же требования.

Если основная система управления доступом еще не установлена, установите ее перед установкой Credential 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.

Программы установки CredMgmt и Mobile Access записаны на отдельные от ACS носители. Их можно загрузить из онлайн-каталогов продуктов Bosch.

Замечание!

Необходим постоянный корневой сертификат

Прежде чем перейти к установке по указаниям ниже, убедитесь, что ACS установлена и лицензирована в соответствии с руководством по ее установке. Это подразумевает наличие окончательного решения по корневому сертификату сервера ACS (самоподписанный или подписанный ЦС) и его постоянную работу. Чтобы изменить корневой сертификат сервера ACS впоследствии, необходимо перенастроить сертификаты на всех компьютерах и считывателях мобильного доступа, включенных в его систему управления доступом.



Требования к серверу

Сервер – это компьютер, на котором работает ACS и приложение CredMgmt.

Операционные системы	<ul style="list-style-type: none"> – 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	<ul style="list-style-type: none"> – MS SQL Server 2019 and later <p>Всегда используйте тот же экземпляр базы данных, что и ACS (основная система управления доступом)</p>
Минимальное разрешение монитора	Full HD 1920 x 1080
Поддерживаемые браузеры	<p>Google Chrome, Mozilla Firefox, Microsoft Edge (на основе Chromium)</p> <p>Используйте самую новую версию браузера для операционной системы Windows</p> <p>.</p>

Требования к клиенту

Требование	Описание
Минимальное разрешение монитора	Full HD 1920x1080
Поддерживаемые браузеры	Google Chrome, Mozilla Firefox, Microsoft Edge (Chromium based) Используйте самую новую версию браузера для операционной системы Windows.

3.2 Необходимое оборудование

Регистрационные считыватели

Для регистрации физических карт системе CredMgmt нужен по крайней мере один регистрационный считыватель. Они обычно устанавливаются на рабочих станциях клиента. Рабочая станция клиента взаимодействует с периферийным оборудованием через программу под названием `BoschPeripheralDeviceAddon.exe`. Установка этой программы описана ниже.

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 СК		X	X	X	X	X	X	X	X

3.2.1 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.

3.3 Установка Credential Management

Введение

CredMgmt запускается как веб-приложение вместе с системой управления доступом Bosch (ACS). В следующих разделах описана установка серверного компонента, управляющего этим веб-приложением.

- Ее можно установить для использования локальной или удаленной базы данных. 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.

3.3.1 Требования для установки CredMgmt

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

Пользователь `CMUser` обращается к базе данных системы ACS от имени приложения CredMgmt.

Если CredMgmt будет использовать базу данных на удаленном сервере, используйте описанную ниже процедуру.

ВНИМАНИЕ: не запускайте настройку CredMgmt до завершения этой операции.

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>\CMUser
 - **Пароль**: настройте пароль в соответствии с политиками безопасности, применяемыми ко всем вашим компьютерам. Обратите внимание, что он потребуется для настройки CredMgmt.
 - **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 CMUser 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 CMUser
6. В области **Выберите страницу** выберите пункт **Роли на сервере**
7. Установите флажки public и dbcreator

Выделенный пользователь для локальной базы данных (только если используется локальная база данных)

Пользователь CMUser обращается к базе данных системы ACS от имени приложения CredMgmt.

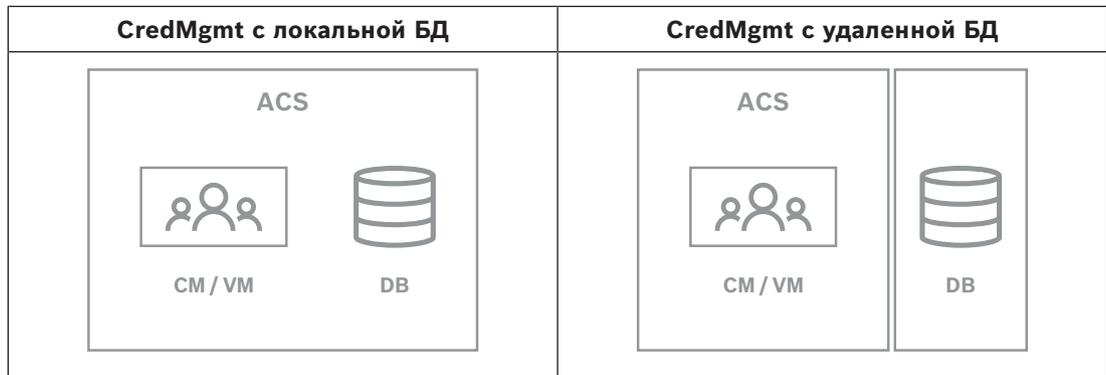
Если CredMgmt будет использовать локальную базу данных, создавать такого пользователя НЕ обязательно. Программа установки CredMgmt автоматически создает на сервере ACS пользователя Windows CMUser.

Выделенный пользователь в ACS

1. Создайте в ACS пользователя с **неограниченным доступом к использованию API**.
 - Путь к диалоговому окну в AMS: **Конфигурация > Операторы и рабочие станции > Права пользователя > вкладка Учетная запись пользователя > Управление правами доступа к API**.
Выберите Unlimited access из списка.
 - Путь к диалоговому окну в BIS: **Конфигурация Обзор > Администрирование > Операторы > выберите оператора > вкладка Права доступа к API ACE**.
Выберите Unlimited access.
 - Подробные инструкции см. в разделе **Назначение профилей пользователей (операторов)** в руководстве оператора ACS.
2. Запомните имя пользователя и пароль, поскольку они потребуются для мастеров установки веб-приложений.

3.3.2

Процесс установки



Процедура

1. На сервере ACS запустите `BoschCredentialManagementServer.exe` от имени администратора.
 - Откроется программа установки
2. На экране **Основные компоненты** выберите `Bosch Credential Management` и нажмите **Далее**
3. Внимательно прочитайте лицензионное соглашение с конечным пользователем (EULA) и нажмите **Принять**, если согласны с его условиями. Установку можно будет продолжить только в таком случае.
4. Выберите целевую папку для установки или используйте папку по умолчанию (рекомендуется). Нажмите **Далее**
5. 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**
6. На экране **Конфигурация доступа к ACS** выполните описанные ниже действия.
 - Введите имя хоста для сервера ACS.
 - Введите имя пользователя ACS с неограниченным доступом к использованию API (см. требования выше).
 - Введите пароль ACS для этого пользователя ACS и подтвердите его.
7. 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** подтвердите выбор CredMgmt и нажмите кнопку **Установка**
10. После завершения установки запустите CredMgmt, используя следующий URL-адрес:
`https:// <NameOfACSserver>:5806`

3.4 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.

3.4.1

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.

3.4.2

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 В и W обозначают цвет: черный или белый
- Буква О обозначает OSDP
- Буква К означает наличие клавиатуры
- Буква М обозначает поддержку службы Mobile Access

3.4.3

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.

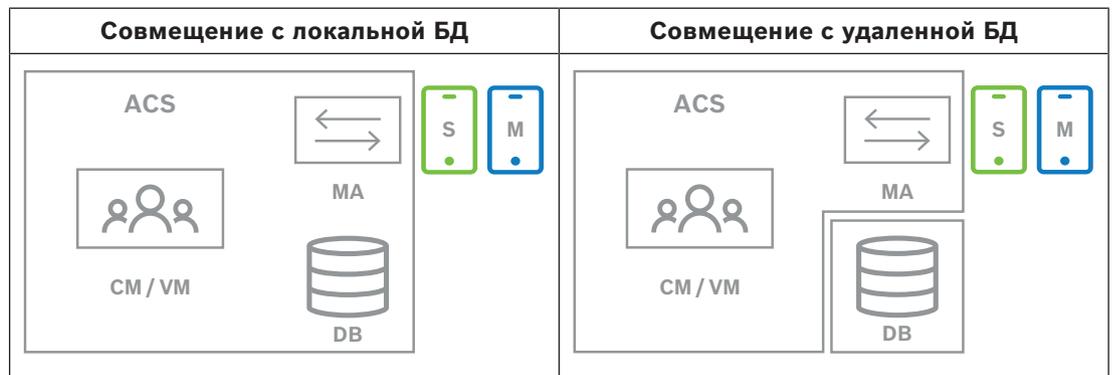
3.4.4

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**.



Клaviша	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.

Клавиша	Значение
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.

3.4.5

Процедура распределенной установки

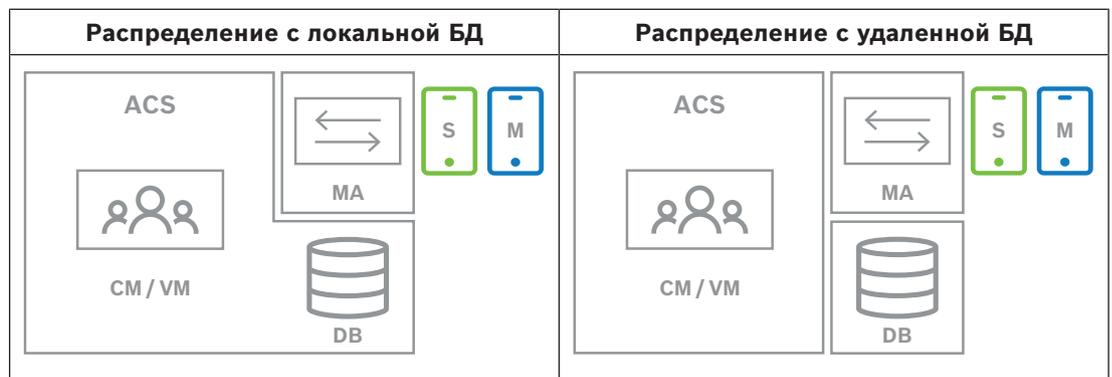
Совмещенная установка подразумевает, что внутренняя служба Mobile Access запускается на том же сервере, что и система ACS.

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.

3.5

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	/	/	/	/

3.5.1 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.

3.5.2

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**.

3.5.3

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

3.6

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.

3.7

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.

4 Обзор Credential Management

Ниже показаны возможные топологии установки системы Credential Management, как с программой Mobile Access, так и без нее. Каждая рамка представляет собой отдельный компьютер.

Клaviшa	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.

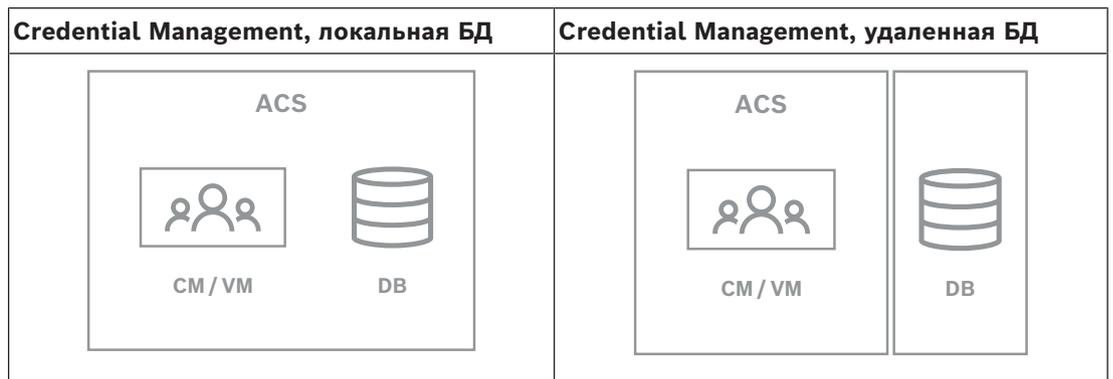


Таблица 4.1: Топологии Credential Management

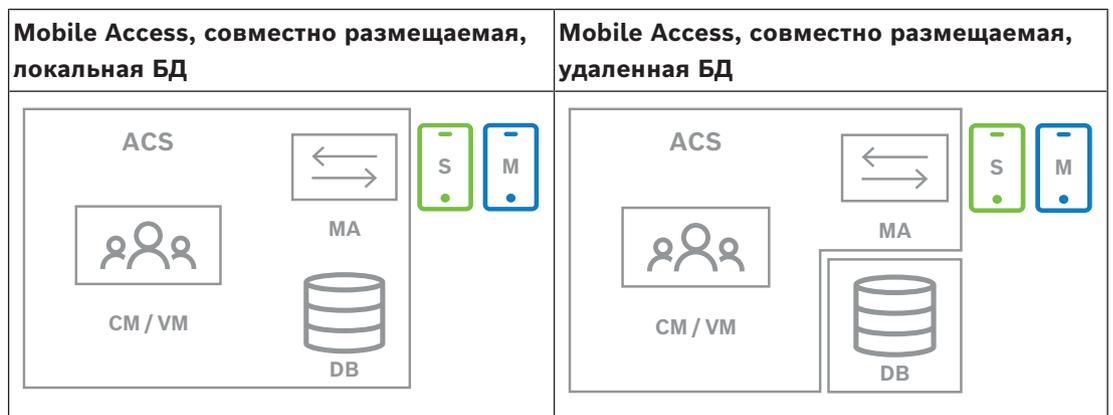


Таблица 4.2: Совместно размещаемые топологии Mobile Access

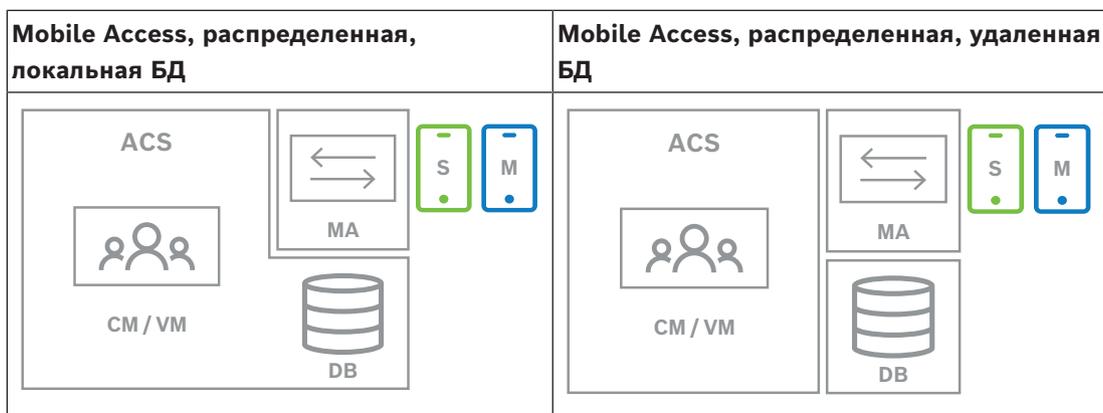


Таблица 4.3: Распределенные топологии Mobile Access

Совместимые версии вспомогательного программного обеспечения

В таблице ниже перечислены версии вспомогательных программных средств, совместимых с этой версией системы.

Компонент	Версия	Местоположение
Access Management System (AMS)	5.5 (с расширением Mobile Access)	Магазин загрузок/каталог продуктов
Visitor Management (VisMgmt)	5.5 (с расширением Mobile Access)	Магазин загрузок/каталог продуктов



Замечание!

Подразделения (разделы)

Credential Management, Visitor Management и Mobile Access не поддерживают функцию «Подразделения» в системах управления доступом Bosch, при которой один пользователь (ACS) управляет доступом нескольких независимых арендаторов.

5 Конфигурирование

5.1 Создание пользователей Credential Management в ACS

В ACS (ACE или AMS) каждый пользователь Credential Management должен быть держателем карты с отдельным определением оператора.

Эти определения операторов содержат специальные права CredMgmt, представленные в виде **Профилей пользователей**.

Необходимо определить отдельного оператора для каждого держателя карты, работающего в CredMgmt. Одному оператору нельзя назначить несколько картодержателей.

См. онлайн-справку в ACS для получения подробной информации и инструкций относительно **Профилей пользователей**.

В AMS необходимо создать пользователей Credential Management:

Путь к диалоговому окну

Конфигурация > Операторы и рабочие станции > Профили пользователей

Процедура

1. Щелкните , чтобы создать новый профиль
 2. Введите имя профиля в поле **Имя профиля** (обязательно)
 3. Введите описание профиля в поле **Описание** (необязательно, но рекомендуется)
 4. Нажмите  или **Применить**, чтобы сохранить изменения
 5. Выберите функцию в соответствии с типом профиля:
 - В области списка выберите функции (первый столбец) и возможности в составе этой функции (**Выполнить**, **Изменить**, **Добавить**, **Удалить**), которые должны быть доступны этому профилю. Дважды щелкните их, чтобы изменить значение параметра на Yes.
 - Кроме того, необходимо убедиться, что для всех функций, которые должны быть недоступны, задано значение No.
 6. Нажмите  или **Применить**, чтобы сохранить изменения
- Дополнительные сведения о ролях пользователя для Credential Management см. в разделе *Обзор ролей пользователей*.

5.2 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 CredMgmt с двоеточием и номером порта (по умолчанию — 5806)
`https://<My_CredMgmt_server>:5806`
Появится экран **Вход в систему**
2. Выполните вход в качестве пользователя CredMgmt с правами **администратора**.
3. Нажмите значок , чтобы открыть меню **Параметры**.

5.3 Конфигурация с помощью меню «Параметры»

<p>Общие</p>	<ul style="list-style-type: none"> – Срок хранения (в днях). Управляет обработкой записей о лицах. <ul style="list-style-type: none"> – 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. – Логотип. Установите или снимите флажок, чтобы задать отображение в диалоговых окнах пользовательского логотипа или логотипа по умолчанию. <ul style="list-style-type: none"> – Требования для файлов настраиваемых логотипов см. здесь: <i>Настройка логотипа компании, Страница 31</i> – Графика. Установите или снимите флажок, который определяет, отображается ли в диалоговых окнах графика Bosch. – 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 <code>VisitorManagerServer</code>. – 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). <code>https://<MyMobileAccessBackendServer>:5700</code> 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.

5.3.1

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 (СС, ВСС и Test), которым можно мгновенно отправить тестовое электронное сообщение. После загрузки из меню **Настройки** шаблоны сохраняются в папке «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.

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.)

Заполнитель	Описание
{{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

5.3.2 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.**

5.4 Настройка пользовательского интерфейса

Пользовательский интерфейс можно настроить в диалоговых окнах панели управления > **Настройки.**

5.4.1 Настройка отображаемых, невидимых и обязательных параметров

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

Пример:

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

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

5.4.2 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>
```

Localization text	Locale
General information	EN ▾

5.4.3 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

5.5 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 **Порти** 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 (*)
 - На клиентских компьютерах
 <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

Исходящий сервер	Исход. порт	Входящий сервер	Вход. порт	Протокол	Комментарии
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
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.

5.5.1

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
acs.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
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

Сервис	Расположение файла
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]\
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]\

5.5.2 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 трафик 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 окончательный 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.

5.6 ИТ-безопасность

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

5.6.1 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.

5.6.2 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.

5.6.3

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.

5.7 Конфиденциальность и защита данных в компании Bosch

Введение

Согласно действующим нормативным требованиям мы гарантируем конфиденциальность, защиту персональных данных и безопасность коммерческой информации во всех бизнес-процессах. Мы придерживаемся соответствующих стандартов, учитывающих новейшие достижения и соответствующие угрозы, в технической и организационной сфере и уделяем особое внимание защите от несанкционированного доступа и потери данных. При разработке продуктов Bosch и новых бизнес-моделей мы гарантируем выполнение правовых требований, регулирующих защиту данных и информационную безопасность, уже на ранних стадиях. Помимо отдела соблюдения нормативных требований и юридического отдела, по вопросам надлежащей обработки данных можно обратиться к сотруднику службы безопасности данных.

Обработка персональных данных в приложении Mobile Access и серверной системе Mobile Access

- Категории персональных данных
 - Приложения Mobile Access содержат персональные данные. Это информация о номере карты, которую прикладывают к считывателю для получения доступа. Доступ к актуальным данным реальных людей можно получить только с использованием дополнительных программ AMS, ACE или Visitor Management.
 - Во время регистрации установщика в меню **Настройки** персональные данные не сохраняются. Однако дополнительно могут сохраняться некоторые сведения о пользователе, например адреса электронной почты.
 - Внутренний сервер приложения Mobile Access сохраняет персональную информацию для управления учетными данными.
- Передача данных
 - Сведения об учетных записях передаются между сервером, приложением Mobile Access и системой Visitor Management для контроля доступа с помощью считывателей.
- Ведение журналов данных
 - В приложении Mobile Access ведутся технические журналы. Такие журналы хранятся локально на мобильном устройстве. При необходимости их можно отправить третьим лицам, например в службу технической поддержки.
 - На сервере также ведутся технические журналы. Данные хранятся локально в серверной системе.
 - По умолчанию сервер не удаляет файлы журнала автоматически. Однако автоматическое удаление можно настроить в зависимости от оставшегося объема памяти или по расписанию.

Как мы обеспечиваем защиту данных при использовании наших продуктов?

Системы управления доступом Bosch управляют правами доступа пользователей. Чтобы защитить их, компания Bosch принимает меры по внедрению требований Общего регламента защиты данных (GDPR) в процесс разработки продуктов и следует принципу конфиденциальности по умолчанию.

- Используются современные методы шифрования.
- Сведения об учетных записях псевдонимизированы.
- Пользователю приложения не нужно вводить персональные данные, чтобы получить виртуальные учетные данные через QR-код или по почте.

- Сведения об учетных записях можно удалить из приложений Mobile Access, из основных систем управления доступом, а также вспомогательных приложений, таких как Visitor Management и Credential Management.
- Операторы основных систем управления доступом и вспомогательных приложений могут в любое время заблокировать учетные данные.
- Данные телеметрии анонимизированы по умолчанию.
- Файлы журналов не передаются с мобильных устройств третьим сторонам, например в службу технической поддержки, без активного согласия пользователя и выполнения определенных действий.
- Автоматическое удаление файлов журналов по расписанию настраивается в основной системе управления доступом.
- Компания Bosch не требует регистрации в магазине приложений или приложении. Магазин приложений не передает персональные данные компании Bosch.
- Для работы приложения требуется Bluetooth. Пользователь должен включить эту функцию вручную по запросу приложения.

Другие вопросы

Дополнительные сведения о конфиденциальности данных см. в примечании о конфиденциальности данных в приложении Mobile Access. Вы также можете обратиться к группе разработчиков компании Bosch.

5.8 Авторизация с высоким уровнем безопасности

5.8.1 Принцип согласия двух лиц

В версии AMS 5.5 и выше можно включить принцип согласия двух лиц. Эта функция обеспечивает безопасность при назначении авторизаций. Для этого в процесс добавлено утверждающее лицо. В Credential Management оператор может назначить пользователю одну или несколько авторизаций. При назначении обычной авторизации она сразу же назначается пользователю. Если используется принцип согласия двух лиц, запрос на авторизацию сначала отправляется другому оператору, который имеет право утвердить или отклонить его. Эта функция позволяет избежать ошибочных назначений, поэтому ее можно использовать для защиты сфер с повышенной безопасностью. Это значит, что некоторые авторизации можно назначить сотруднику только при согласии двух операторов (отправитель запроса и утверждающий).

5.8.2 Настройка авторизаций с высоким уровнем безопасности

Чтобы включить принцип согласия двух лиц, необходимо выполнить описанные ниже требования.

- Система AMS должна быть обновлена до последней версии.
- Включить функцию может администратор AMS.

Создание авторизации для доступа с использованием принципа согласия двух лиц

В основной системе управления доступом:

Путь к диалоговому окну

Главное меню AMS > **Системные данные** > **Авторизации**

1. Очистите поля ввода, нажав кнопку **Создать**  на панели инструментов.

Кроме того, можно нажать **Копировать** , чтобы создать новую авторизацию на основе существующей.

2. Введите уникальное имя авторизации
3. (Необязательно) Введите описание
4. (Необязательно) Выберите временную модель, которая будет управлять этой авторизацией
5. Выберите из списка **Предел неактивности** (необязательно).
6. Назначьте хотя бы один **Вход** (обязательно).
7. Установите флажок **Требуется утверждение** (этот параметр включает принцип согласия двух лиц).
8. Нажмите «Сохранить»  для сохранения авторизации.

Замечание!

Рекомендации по безопасности



Эту функцию можно использовать только для Credential Management. В AMS администраторы должны назначить и правильно настроить профили пользователей для операторов, чтобы диалоговые окна были недоступны для них. Так обычные операторы не смогут назначать авторизации с высоким уровнем безопасности без согласия двух лиц.

Дополнительные сведения см. в последней версии руководства по *конфигурации и эксплуатации Access Management System*.

6 Эксплуатация

6.1 Обзор ролей пользователей

Возможности пользователей Credential Management зависят от их профиля в ACS.

Тип пользователя	Сценарии использования
Администратор	Установка глобальных параметров Настройка поведения инструмента и его пользовательского интерфейса плюс Все варианты использования для операторов
Оператор	Назначение и отмена назначения физических карт доступа, а также виртуальных учетных данных для мобильного доступа
Принцип согласия двух лиц: отправитель запроса	Запрос авторизации с высоким уровнем безопасности
Принцип согласия двух лиц: утверждающий	Одобрение или отклонение назначения авторизации с высоким уровнем безопасности Удаление обычных авторизаций

См.

- *Создание пользователей Credential Management в ACS, Страница 27*

6.2 Использование панели мониторинга

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

Общее использование таблицы персонала

Каждая строка в таблице обозначает сотрудника. Это внутренний или внешний персонал, для которого необходимо назначить учетные данные для входа на территорию.

- Можно выбрать отдельных или сразу несколько сотрудников 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 новых сотрудников
- Можно назначать и отменять назначение учетных данных с помощью кнопок действия
 - Можно назначать физические средства идентификации
 - Можно назначать виртуальные учетные данные (для мобильного доступа)
 - Можно редактировать сведения о пользователе
- 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.

Функции панели управления



Метка	Функция
(1) Кол-во проходов	Общее число пользователей N (каждый пользователь соответствует строке в таблице).
(2) Поиск	Поиск сотрудников в таблице по произвольному тексту
(3)	Выберите все элементы списка
(4) Удалить	Удаление выбранных элементов
(5) Последние	Отображение списка сотрудников, которые были недавно добавлены в таблицу.
(6) Сброс	Возврат представления таблицы по умолчанию и отмена всех фильтров.
(7) Отмена назначенной карты	Открытие диалогового окна для отмены назначенной карты с помощью подключенного регистрационного считывателя.
(8) . . .	Щелкните значок с многоточием для вызова меню, чтобы экспортировать данные сотрудников и 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.
(9)	Чтобы создать нового сотрудника, откройте диалоговое окно

Столбцы панели управления

Столбец	Описание
Название	Нажмите ссылку для просмотра сведений о сотруднике.
Эл. почта	
Отдел	
Расположение	
Компания	
Номера карт	Номера карт, назначенных данному сотруднику.
Действия	См. отдельную таблицу ниже

Действия с записями сотрудников в таблице на панели управления

Значок	Действия
	Назначение сотруднику одной или нескольких физических карт
	Назначение сотруднику виртуальных учетных данных для мобильного доступа
	Редактирование персональных данных сотрудника. Изменения вносятся также в ACS. Изменения, внесенные в ACS, сохраняются также в приложении CredMgmt.

6.2.1**Обзор страницы сотрудника**

Нажмите имя нужного сотрудника. Откроется диалоговое окно с персональными данными. В полях диалогового окна отображаются и доступны для редактирования основные сведения о сотруднике. Однако основные персональные данные постоянно отображаются в левой части окна.

Сведения о записях в черном списке (при наличии) отображаются в нижней части столбца с основной персональной информацией.

Совет. В поле **Должность** можно вводить любой текст, кроме вариантов в раскрывающемся списке.

В этом диалоговом окне также есть три вкладки с отдельным представлением:

Сведения, Учетные данные, Авторизации.

Если сотрудник заблокирован, в Credential Management появится оранжевое уведомление с примечанием **В черном списке**. Здесь также отображается причина и оператор, добавивший сотрудника в черный список.

Администратор и оператор с соответствующими правами могут заблокировать сотрудника, нажав на кнопку **Черный список**.

– Откроется окно с предупреждением

1. Нажмите **Да**

2. В мастере **Причина** укажите причину > **Сохранить** > **ОК**

Обратите внимание, что у внесенного в черный список сотрудника сохраняются назначенные авторизации. Однако он не может войти/открыть дверь.

Чтобы удалить сотрудника из черного списка, просто нажмите кнопку **X Удалить из черного списка**.

Правильно настройте права пользователя. Дополнительные сведения о правах пользователей см. в руководстве по *конфигурации и эксплуатации Access Management System*.

Подробнее

На этой вкладке можно вводить персональные данные. Они не обязательно постоянно отображаются.

PIN

На вкладке **Сведения** можно просмотреть и изменить PIN-коды (для подтверждения)¹ держателя карты. При изменении PIN-кода можно указать срок его действия.

Примечание. Во время изменения PIN-кода или его настроек необходимо повторно ввести его для подтверждения.

Если для учетных данных выбранного сотрудника отображается один или несколько случаев блокировки по **PIN-коду**, в нижней части столбца с основной персональной информацией появится уведомление. Когда оператор нажимает на это уведомление, открывается вкладка **Учетные данные**, в которой отображаются дополнительные сведения о блокировке по **PIN-коду**.

Примечание. Если на вкладке отображается ошибка проверки, до решения проблемы будет невозможно перейти на другую страницу.

¹Credential Management поддерживает только стандартный PIN-код. Идентификационные И отдельные PIN-коды IDS/постановки на охрану не поддерживаются.

Дополнительные сведения о **PIN-кодах** см. в руководстве по *конфигурации и эксплуатации Access Management System*.

ID карты

На этой вкладке можно назначить физическую карту с помощью кнопки **Считать карту** или мобильные учетные данные с помощью кнопки **Добавить мобильный доступ**.

Дополнительные сведения см. в разделах *Назначение мобильных учетных данных* и *Назначение физических средств идентификации*.

Примечание. Если на значке на экране телефона появляется оранжевая точка, учетные данные уже содержатся в мобильном телефоне, но ожидают подтверждения от сервера мобильного доступа. После его получения точка становится зеленой.

Авторизации

На этой вкладке можно просмотреть все назначенные авторизации и изменять их.

Дополнительные сведения см. в разделе *Назначение авторизаций на странице сведений о сотруднике*.

Примечание. При нажатии кнопки **Сохранить и закрыть** на любой вкладке этого диалогового окна вы будете перенаправлены в диалоговое окно **панели управления**.

6.3

Назначение авторизаций

Назначение авторизаций на странице сведений о сотруднике

– В диалоговом окне панели управления появится список сотрудников.

1. Нажмите имя сотрудника.

– Откроется диалоговое окно со сведениями о нем.

1. Выберите вкладку **Авторизации** в правом верхнем углу окна.
2. Чтобы назначить новую авторизацию, нажмите **Изменить авторизации**
Появляется мастер со списком авторизаций. Все авторизации предварительно сконфигурированы в Access Management System. После этого выберите авторизации, которые нужно назначить.



1. Нажмите кнопку  > **Подтвердить** > **Сохранить**.

Примечание. Авторизации с высоким уровнем безопасности, то есть со включенной функцией согласия двух лиц, отображаются с .

Откроется диалоговое окно панели управления. Если назначена обычная авторизация, можно проверить, была ли она действительно назначена. Для этого снова нажмите имя сотрудника и перейдите на вкладку **Авторизации**.

Если назначена авторизация с согласия двух лиц, результат проверки будет другим. Авторизация не будет активна сразу после сохранения, а будет отображаться только отправка запроса. В столбцах **Авторизации** и **Действия** можно просмотреть отправителя запроса на авторизацию.

Для авторизаций с согласием двух лиц на вкладке **Авторизации** отображается, были ли они утверждены или отклонены. Наведите курсор на имя авторизации, чтобы узнать имя отправителя, дату и время запроса. Появится всплывающая подсказка.

В зависимости от типа авторизации, роли и прав пользователя могут отображаться следующие кнопки **Действия**:

Запрос

Отозвать — отмена неутвержденного запроса на назначение авторизации.

Утвердить — утверждение запроса на назначение авторизации от другого оператора.

Отклонить — отклонение запроса на назначение авторизации от другого оператора.

Удалить — удаление назначенной авторизации. Это относится к обычным авторизациям и авторизациям с высоким уровнем безопасности.

Примечание. Действия выполняются только после нажатия на кнопку действия. Всегда нажимайте **Сохранить**.

Дополнительные сведения см. в разделе *Обзор ролей пользователей*.

В AMS необходимо правильно настроить **профили пользователей** с учетом прав при использовании принципа согласия двух лиц.

- Администратор
- Оператор
- Принцип согласия двух лиц: отправитель запроса
- Принцип согласия двух лиц: утверждающий

Дополнительные сведения о настройке **профилей пользователей** см. в последней версии *руководства по конфигурации и эксплуатации Access Management System*.

Запросы на авторизацию, ожидающие рассмотрения

Оператор с правом утверждения или отправки запросов и администратор могут просматривать в меню **запросы на авторизацию**. В этом диалоговом окне показаны все **запросы на авторизацию, ожидающие рассмотрения**. Они отображаются в одном представлении, без необходимости просматривать каждого сотрудника по отдельности. В этом диалоговом окне оператор с правом утверждения может утверждать авторизации, а администратор может отзываться их. Оператор, отправивший запрос, может только просматривать авторизации, ожидающие рассмотрения. Оператор без прав утверждения и отправки запросов не может просматривать это диалоговое окно.

Примечание. Действия выполняются только после нажатия на кнопку действия. Нажмите кнопку действия. После этого она станет серой. Затем нажмите **Сохранить**.

6.4 Назначение физических учетных данных

Предварительные требования

Настоятельно рекомендуется назначать новым сотрудникам новые учетные данные с использованием новой карты, принтера для карт и регистрационного считывателя.

Назначение карты (требуется регистрационный считыватель)

Процедура

Карту можно назначить, нажав непосредственно на значок панели управления или на странице сотрудника.

На **панели управления**:

1. Приготовьте физическую карту доступа, чтобы приложить ее к регистрационному считывателю.



2. Выберите строку сотрудника и щелкните значок
3. Следуйте инструкциям во всплывающем окне для использования регистрационного считывателя.

На странице сотрудника:

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

Назначение карты в редакторе учетных данных (требуется регистрационный считыватель)



1. На панели управления выберите сотрудника в таблице и нажмите  , чтобы редактировать его учетные данные.
2. Нажмите **Считать карту** и следуйте инструкциям по использованию регистрационного считывателя во всплывающем окне.
 - При необходимости назначить и другие карты повторите последнее действие.
3. Нажмите **Сохранить**, чтобы сохранить текущего сотрудника с назначенной картой.

6.5 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
- 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
- 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
 - 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
 - Когда приложение запущено, мобильное устройство действует аналогично физической карте доступа

См.

- *Установка службы Mobile Access, Страница 13*
- *Установка приложений Mobile Access, Страница 22*

6.6

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.

6.7

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.

6.7.1

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.

6.8

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.

6.8.1**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).

GDPR

Общий регламент защиты данных (GDPR) — это закон Европейского союза (ЕС) о конфиденциальности и безопасности данных, который вступил в силу в 2018 г. Он устанавливает обязательства для всех организаций в ЕС, осуществляющих сбор персональных данных.

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.

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

© Bosch Security Systems B.V., 2024

Решения в сфере управления зданиями для улучшения качества жизни

202405132120