Вопросы и ответы (FAQ)

Документация на ПО и устройства BIOSMART

Документацию на устройства и программное обеспечение можно найти на нашем сайте в разделе Техподдержка.

Видеоинструкции по работе и настройке устройств и ПО доступны на следующих платформах:

- RUTUBE
- VK Видео
- YouTube

Техническая поддержка работает по будням с 7:00 до 16:00 по московскому времени, и связаться с ней вы можете следующими способами:

- По телефону: 8 804 700 25 46, доб.2 (бесплатно по РФ).
- Через технический портал (нажмите кнопку «Получить консультацию»): https://bio-smart.ru/support.
- По почте: bot@bio-smart.ru.

Интеграции с ЕБС, КБС и РС г. Москва

Если в логах серверной части ПО Biosmart-Studio v6 появляется ошибка:

```
[2026-06-17 12:15:47.250] [1:1] I:
BSHttpServer::sendResponse:248 - send response
1 status: 408 body: {
    "error_message": "Timeout waiting for
message from Apache Kafka",
    "status": "error"
}
```

то возможная причина – изменение схемы авторизации Kafka со стороны ДИТ, в том числе переход на авторизацию через **SASL**.

Для восстановления работы выполните следующие действия:

1. Обновите ПО Biosmart-Studio до версии 6.4.10. Скачать по можно на нашем **сайте**.
2. Запустите ПО Biosmart-Studio v6 и перейдите в раздел **Справ очники**.
3. Выберите в разделе **Профили БС** созданный профиль для РС г. Москва.
4. Перейдите на вкладку **Подключение Kafka** и установите метку в чекбоске **Авторизация SASL**.
5. В поле **Bootstrap servers** введите последовательно адреса 10.2 3.66.85-91 и порты 31050-31056 для подключения.

   Адреса и порты вводите в формате:

   ```
   http://10.23.66.85:31050,10.23.66.85:
   31051,10.23.66.85:31052,10.23.66.85:
   31053,10.23.66.85:31054
   ```

   и далее.

Если остались вопросы, то более подробная инструкция расположена в **статье**.

Лицензии ПО Biosmart-Studio v6

Лицензионный ключ — это уникальный код, который подтверждает ваше право на использование программного обеспечения. Он нужен для активации программы и разблокировки ее функций.

Лицензионные ключи ПО Biosmart-Studio v6 предоставляются в **аппар атном** или **программном** виде.

1. Аппаратный ключ - это USB-флэш-накопитель (USB 2.0) с предустановленным ключом активации лицензии.
   - Преимущества: не зависит от изменений параметров ПК, можно использовать на разных ПК (достаточно перенести USB-накопитель). Работает, даже если нет доступа в Интернет.
   - Недостатки: USB-накопитель может потеряться или сломаться, ограниченное применение на виртуальных машинах.
2. Программный ключ - это электронный код для активации и аутентификации программного обеспечения. Передается в электронном виде через Интернет.
   - Преимущества: не требует USB-порт, невозможно потерять или сломать. Нет ограничений для применения в виртуальных средах.
   - Недостатки: повторная активация при изменении параметров ПК, переустановке системы или переносе сервера на другой ПК,

SSL-сертификат — это цифровой паспорт сайта. Его основная задача — активировать протокол SSL (Secure Sockets Layer), который создаёт зашифрованное соединение между веб-сервером и веб-браузером.

В ПО Biosmart-Studio v6 SSL-сертификат обеспечивает работу защищённого сетевого подключения между клиентом и сервером BioSmart

SSL-сертификат предназначен для защиты соединения и сохранности конфиденциальных данных, будь то персональные данные пользователей или информация об уровнях доступа.

Для активации аппаратного лицензионного ключа на ПК с ОС Windows, установите драйверы (если ранее не были установлены) и вставьте USB ключ в компьютер. Скачать драйверы можно на нашем **с айте**.

Для активации аппаратного лицензионного ключа на ПК с ОС Astra Linux, вставьте USB ключ в компьютер и ПО Biosmart-Studio v6 будет готово к работе.

Если остались вопросы, то более подробная инструкция расположена в **статье**.

1. Запустите ПО Biosmart-Studio v6 и в окне **Проверка лицензии** нажмите кнопку **Удаленное обновление ключа Biosmart-Studio v6.**
2. Выберите действие **Начать новую операцию обновления ключа.**
3. Следуйте подсказкам программы.
4. Если процесс обновления был прерван после отправки запроса на активацию, повторно перейдите в окно **Активация ключа** и выберите действие **Продолжить операцию обновления ключа, инициированную во время предыдущего сеанса.**
5. Следуйте подсказкам программы.

Подробные инструкции по установке и активации программного лицензионного ключа смотрите в статье.

Для активации лицензий Demo или Light в ПО Biosmart-Studio v6 в окне **Проверка лицензии** сгенерируйте код активации для соответствующей лицензии и отправьте его на почту **KeyLicense@bio-smart.ru**.

Более подробная инструкция в статье.

Обновление и установка ПО Biosmart-Studio v6

Программное обеспечение можно скачать на нашем официальном сайте в разделе Техподдержка.

Поддерживаются следующие типы операционных систем:

- Windows,
- Astra Linux не ниже 1.7,
- Ubuntu не ниже 24.04 LTS.

Если при попытке обновления ПО Biosmart-Studio v6 всплывает информационное окно:

Истек период обновлений
или
Ошибка при обновлении ПО - Обновление невозможно: истек период обновлений

Это может означать что у вас закончился срок подписки на обновления ПО.

Проверить срок действия подписки на обновление можно по инструкции в статье.

Для продления подписки обратитесь в отдел в отдел продаж по электронной почте sale@bio-smart.ru, по телефону 8 (804)-700-25-46 или у наших партнеров.

Возможно, у вас закончились лимиты по вашей текущей лицензии. Проверить лимиты можно по инструкции в статье.

Если лимиты закончились, лицензию можно расширить, обратившись в отдел продаж по электронной почте sale@bio-smart.ru, по телефону 8 (804)-700-25-46 или у наших партнеров.

Да, установка сервера и клиентского рабочего места возможна на различных ОС. При установке убедитесь, что на клиентских рабочих местах и сервере установлено ПО одинаковой версии.

Да, перенести сервер с одной операционной системы на другую возможно, для этого:

- Создайте резервную копию БД на ОС, с которой хотите перенести сервер Biosmart, например ОС Windows.
- Перенесите резервную копию БД на другую ОС, например ОС Astra Linux SE 1.8.
- Восстановите резервную копию БД на выбранной ОС (Astra Linux SE 1.8).

Подробную инструкцию по переносу сервера смотри в статье.

Если при установке ПО Biosmart-Studio v6 возникает ошибка, это значит что попытка установки ПО уже была ранее.

Для решения данной проблемы:

1. Деинсталлируйте ПО Biosmart-Studio v6.

Работа с ПО Biosmart-Studio v6

1. В ПО Biosmart-Studio v6 в разделе **Группы доступа** создайте группы доступа. Как создавать и редактировать группы доступа рассказали в статье.
2. Назначьте группы доступа сотрудникам. Как назначать группы доступа сотрудникам рассказали в статье.
3. Выберите группы доступа, контроллер (терминал), на который нужно загрузить сотрудников, и нажмите **Сохранить** .

Полностью удалить сотрудника из ПО Biosmart-Studio v6можно двумя способами: с помощью периодического задания и вручную.

Для полного удаления сотрудника с помощью периодического задания:

1. Запустите ПО Biosmart Admin, перейдите на вкладку **Периодические задания** и выберите задание **Удаление уволенных сотрудников.**
2. В **Параметрах задания** укажите периодичность удаления сотрудников после увольнения.

Для удаления сотрудника вручную:

1. Запустите ПО Biosmart-Studio v6 и перейдите в раздел **Сотрудники**.
2. На вкладке **Уволенные сотрудники** выберите уволенного сотрудника и нажмите на кнопку **Удалить**.

Как увольнять и удалять сотрудников в ручную рассказали в статье.

Для исключения получения несанкционированного доступа к ПО Biosmart-Studio инструкция по сбросу пароля отправляется по запросу. Для восстановления пароля пользователя root:

1. Создайте обращение на портале технической поддержки.
2. К обращению прикрепите скан письма о восстановлении пароля на официальном бланке организации с подписью руководителя.
3. Дождитесь инструкции по сбросу пароля.

Для отображения в окне наблюдения дополнительной информации о сотруднике нажмите на строку Выбрать дополнительные параметры сотрудника и выберите нужные параметры.

Более подробная инструкция в статье.

Для передачи данных между серверной и клиентской частью ПО, сервером БД, сервером лицензий используется протокол TCP/IP.

Для передачи данных между контроллером BioSmart, сервером BioSmart и СИ BioSmart используются протоколы TCP/IP и UDP.

Про порты, используемые ПО и устройствами Biosmart, рассказали в статье.

Изменить IP-адреса контроллера или терминала можно, когда связь между ПО Biosmart-Studio v6 и настраиваемым контроллером /терминалом установлена.

2. Перейдите в каталог *C:\ProgramData* и удалите папки **bsdb** и **BioSmart**.
3. Перейдите в окно **Управление компьютером**, выберите вкладку **Службы и приложения**, далее **Службы**. Если там остались службы **Biosmart Server** и **Biosmart DB Server**, то удалите их с помощью командной строки(с правами администратора):

```
sc delete "Biosmart Server"
sc delete "Biosmart DB Server"
```

4. Перейдите в каталог *C:\Program Files* и удалите папки **BioSmart** и **Biosmart Studio 6**.
5. При необходимости перезагрузите компьютер.
6. Установите ПО Biosmart-Studio v6 по инструкции в статье для ПК с ОС Windows или статье для ПК с ОС Astra Linux.

Если после восстановлении БД более ранней версии ПО Biosmart-Studio v6:

---

*при входе в ПО Biosmart-Studio v6, возникает ошибка **Сервер не инициализирован***

или

*при попытке просмотра раздела **Журналы** возникает окно **Ошибка обновления журналов***

это значит, что структура более ранней версии ПО Biosmart-Studio v6 отличается от структуры актуальной версии ПО Biosmart-Studio v6.

Для корректной работы, запустите инсталлятор актуальной версии ПО Biosmart-Studio v6 и выполните обновление.

IP-адрес любого контроллера или терминала Biosmart по умолчанию 172.25.110.71 (за исключением контроллеров, входящих в состав накладки на турникет TTR-04 и T-83M, их IP-адреса 172.25.110.71 и 172.25.110.72).

Установите связь между ПО Biosmart-Studio v6 и настраиваемым контроллером или терминалом, для этого:

1. Перейдите на портал с технической документацией.
2. В меню выберите руководство на контроллер или терминал, для которого необходимо изменить IP-адрес.
3. Перейдите в раздел **Быстрый старт** и следуйте инструкции.

Для установки связи между ПО Biosmart-Studio v6 и контроллером или терминалом, подключенным в сети за роутером при отсутствии VPN, на роутере с белым IP-адресом предварительно организуйте переадресацию порта 20002 на локальный IP-адрес контроллера или терминала в настройках роутера. При необходимости работы с веб-интерфейсом контроллера или терминала, организуйте также переадресацию порта 8082.

Белый IP-адрес - это уникальный публичный адрес в сети Интернет.

Для проверки IP-адреса:

- *В веб-интерфейсе в настройках роутера посмотрите IP-адрес, выданный провайдером.*
- *На сайте-определителе (например 2ip.ru или myip.ru) сравните IP-адреса в настройках роутера и на сайте.*
- *Если IP-адреса совпадают, то IP-адрес белый.*

Если при добавлении нового контроллера в статусе состояния подключения отображается **Нет связи**, измените IP-адрес контроллера.

IP-адрес любого контроллера Biosmart по умолчанию 172.25.110.71 (за исключением контроллеров, входящих в состав накладки на турникет TTR-04 и T-83M, их IP-адреса 172.25.110.71 и 172.25.110.72).

Установите связь между ПО Biosmart-Studio v6 и настраиваемым контроллером, для этого:

1. Перейдите на портал с технической документацией.
2. В меню выберите руководство на контроллер, для которого необходимо изменить IP-адрес.
3. Перейдите в раздел **Быстрый старт** и следуйте инструкции.

Средства криптографической защиты информации (СКЗИ)

СКЗИ используется для защиты биометрических персональных данных при их обработке и передаче.

СКЗИ помогает снизить риски, связанные с основными угрозами:

- **нарушение целостности данных;**
  Например, подмена или удаление биометрических данных.
- **нарушение конфиденциальности данных.**
  Например, несанкционированный доступ к биометрическим персональным данным или их компроментация.

Таким образом, СКЗИ необходимо для защиты биометрических данных от изменения, удаления, перехвата и несанкционированного доступа.

Классы СКЗИ зависят от выбранной биометрической системы, схемы взаимодействия и архитектуры объекта.

Для поддерживаемых биометрических систем используются следующие варианты:

- **Коммерческая биометрическая система (КБС) Pridex**

При работе с КБС Pridex на терминале BioSmart Quasar 7 используется СКЗИ класса КС1. На сервере Biosmart организуется СКЗИ класса КС3. В качестве СКЗИ используется ViPNet Client 5. ПО устанавливается на терминал и на сервер Biosmart.

СКЗИ класса КС1 применяется:

- Для взаимодействия терминала с КБС при отправке запроса на идентификацию.
- Для взаимодействия терминала с ПО Biosmart Studio v6.

Для взаимодействия сервера Biosmart с КБС применяется СКЗИ класса КС3.

- **КБС Face 2**

При работе с КБС Face 2 используется КриптоПро CSP версии 5.0 R4 КС1. Взаимодействие с КБС выполняется по ГОСТ TLS с подписью запросов.

Для работы используется утилита KbsCrypt. Утилита управляет КриптоПро CSP при установлении ГОСТ TLS-соединения и подписании запросов.

СКЗИ устанавливается:

- На терминал.
- На сервер Biosmart.

Лицензия на KbsCrypt приобретается отдельно

- **Региональный сегмент единой биометрической системы**

Для регионального сегмента ЕБС используется схема, аналогичная КБС Pridex. На терминале используется СКЗИ класса КС1. Для межсетевого взаимодействия со стороны сервера Biosmart организуется СКЗИ класса КС3.

- **Единая биометрическая система (ЕБС)**

При работе с ЕБС по транзакционной модели на терминалы устанавливается КриптоПро CSP версии 5.0 R4 КС1. Взаимодействие терминала с КБС выполняется по ГОСТ TLS с подписью запросов. Для подписи запросов используется сервис BSCrypt. По принципу работы он аналогичен KbsCrypt и управляет КриптоПро CSP при установлении ГОСТ TLS-соединения и подписании запросов. Взаимодействие терминала с контролируемой зоной, в которой размещается Biosmart Studio, также выполняется по ГОСТ TLS.

На границе контролируемой зоны устанавливается ПАК, терминирующий ГОСТ TLS, например N-Gate.

Необходимость установки СКЗИ на сервер Biosmart Studio зависит от конкретного проекта и архитектуры объекта.

С поддерживаемыми биометрическими системами могут использоваться следующие версии СКЗИ:

- Для терминала:
  КриптоПро CSP версии 5.0 R4 КС1 или **ViPNet Client 5**.

- Для сервера Biosmart:
  КриптоПро CSP версии 5.0 R4 КС1, **КриптоПро CSP версии 5.0 R4 КС3**, **ViPNet Client 5** или **ViPNet Client 4**.
- Дополнительно, в зависимости от выбранной биометрической системы и проекта, могут использоваться: **KbsCrypt** или **BSCrypt**.

> Конкретный состав СКЗИ определяется выбранной биометрической системой, требованиями заказчика и архитектурой объекта.

Мы используем СКЗИ от КриптоПро, потому что их продукты сертифицированы ФСБ России и подходят для защиты биометрических персональных данных.

Продукты КриптоПро поддерживают инструменты, необходимые для обеспечения:

- Защищенного соединения по ГОСТ TSL.
- Электронной подписи запросов.
- Управления сертификатами.
- Настройки криптографической защиты.

Использование этих инструментов проверено на системе Biosmart Linux, установленной на терминалах BioSmart Quasar 7.

Кроме того, решения КриптоПро широко применяются в инфраструктуре наших клиентов. Поэтому их использование упрощает внедрение системы на объектах, где уже используется данное ПО или совместимое программно-аппаратное оборудование.

На терминале BioSmart Quasar 7 устанавливается **КриптоПро CSP версии 5.0 R4**.

В составе системы используются следующие утилиты КриптоПро:

- **Stunnel** – используется для организации защитного соединения по ГОСТ TSL.
- **Csptest** – используется для работы с электронной подписью.
- **Certmgr** – используется для управления сертификатами.
- **Cpconfig** – используется для настройки СКЗИ.

Для каждого устройства приобретается отдельная лицензия на одно рабочее место согласно условиям поставщика СКЗИ.

Например, могут потребоваться следующие лицензии:

- Для ViPNet Client 5:
  Передача права на использование ПО ViPNet Client 5 for Linux.
- Для КриптоПро CSP 5.0:
  Лицензия на право использования СКЗИ «КриптоПро CSP» версии 5.0 на одном рабочем месте.
- Для KbsCrypt:
  Лицензия приобретается отдельно у Face 2.

> Для организации СКЗИ класса КС3 может потребоваться дополнительное программное обеспечение и оборудование. Состав таких компонентов определяется проектом и архитектурой системы.

Для использования СКЗИ необходимо приобрести лицензию и выполнить настройку.

СКЗИ устанавливается на терминал на производстве, но для его использования требуется:

1. Установить лицензионный ключ.

2. Выпустить и установить необходимые сертификаты.
3. Настроить защищенное соединение и подпись запросов.

Для КриптоПро настройка, как правило, включает выпуск и установку сертификатов подписи и сертификатов ГОСТ TSL.

Для ViPNet Client настройка включает выпуск и установку дистрибутивов и ключей.

СКЗИ устанавливается на устройствах и серверах, которые участвуют в защищенном обмене данными.

На терминалах BioSmart Quasar 7 СКЗИ устанавливается на производстве. После этого для начала работы необходимо установить ключи и выполнить настройку сертификатов.

Необходимость установки СКЗИ на сервере зависит от выбранной биометрической системы, схемы подключения и архитектуры конкретного объекта.

Как происходит управление сертификатами?

Сертификаты загружаются на терминал через веб-интерфейс.

Для загрузки сертификатов:

- Перейдите в веб-интерфейс терминала.
- Откройте раздел СКЗИ.
- Загрузите сертификаты в настройках соответствующего криптографического программного обеспечения.

Версию установленного СКЗИ можно посмотреть в веб-интерфейсе терминала.

Для проверки версии:

1. Перейдите в веб-интерфейс терминала.
2. Откройте раздел СКЗИ.
3. Перейдите на вкладку соответствующего программного обеспечения.
4. Проверьте отображаемую версию СКЗИ.
5. По указанной версии можно определить, используется ли сертифицированный экземпляр СКЗИ.