Как настроить авторизацию с помощью протокола аутентификации Kerberos?

Данная инструкция описывает процесс единого входа (Single Sign-On, SSO) в ПО Biosmart-Studio v6 с использованием протокола Kerberos.

Kerberos позволяет пользователям, уже вошедшим в домен Active Directory (AD) автоматически получать доступ в ПО Biosmart-Studio v6 без повторного ввода логина и пароля. Это повышает удобство и безопасность, так как учетные данные не передаются и не хранятся в ПО Biosmart-Studio v6.

Как это работает?

При входе в Windows пользователь получает от контроллера домена (KDC) специальный билет. При запуске Biosmart-Studio этот билет предъявляется службе для автоматической проверки подлинности. Ключевым элементом этой связки является **Service Principal Name (SPN)** — уникальный идентификатор, который сообщает KDC, какой службе принадлежит запрос.

> Корректная регистрация SPN является обязательным условием для работы с протоколом Kerberos.

Настройка авторизации включает в себя три этапа:

1. Регистрация SPN в Active Directory.
2. Настройка службы Biosmart Server (для Windows) или создание keytab файла (для Astra Linux).
3. Активация и настройка Kerberos-авторизации в интерфейсе Biosmart-Studio.

Далее в статье подробно рассмотрены основные понятия и детальные инструкции для каждого этапа.

Основные понятия и определения:

Kerberos - это протокол взаимной аутентификации сервера и клиента при участии доверенной третьей стороны (KDC). Протокол обеспечивает защиту даже при условии прохождения пакетов по незащищенной сети, где они могут быть перехвачены, модифицированы и перенаправлены злоумышленником.

Realm - это домен аутентификации в инфраструктуре Kerberos, который управляется одним или несколькими KDC.

KDC (*Key Distribution Center или Центр распределения ключей)* - это контроллер домена, отвечающий за аутентификацию и распределение билетов.

SPN (*Service Principal Name)* - это уникальный идентификатор, который связывает сервер с учетной записью пользователя домена.

SSO (*Single Sign-On*) - это механизм аутентификации, позволяющий пользователю автоматически авторизовываться в в ПО Biosmart-Studio v6 без повторного ввода логина и пароля.

Регистрация SPN в Active Directory

Настройте SPN в соответствии с инструкцией для ПК с ОС Windows.

> Для регистрации SPN необходимы права администратора домена.

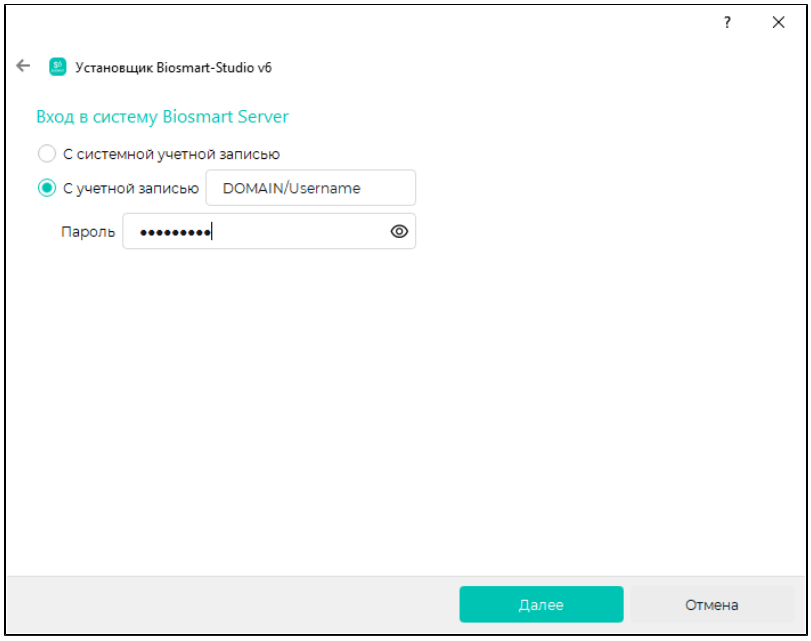
Начальная настройка

Для того, чтобы настроить авторизацию с помощью протокола аутентификации Kerberos, выполните настройку службы **Biosmart Server** для ПК с **ОС Windows** или создайте **keytab файл** для ПК с **ОС Astra Linux.**

Установите или обновите ПО Biosmart-Studio v6 в соответствии со статьей Установка ПО Biosmart-Studio v6 и статьей Обновление на ПК с ОС Windows.

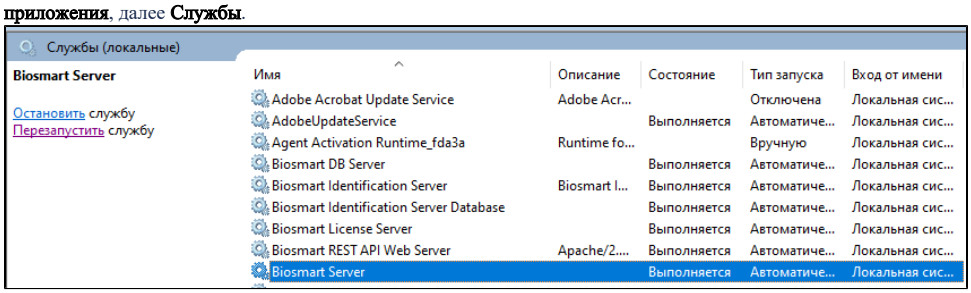
> Если ПО Biosmart-Studio v6 на вашем ПК установлено и обновлено, то пропустите первый пункт настройки.

1. В окне **Вход в систему Biosmart Server** выберите **С учетной записью** и введите название домена и имя учетной записи, укажите пароль от учетной записи.



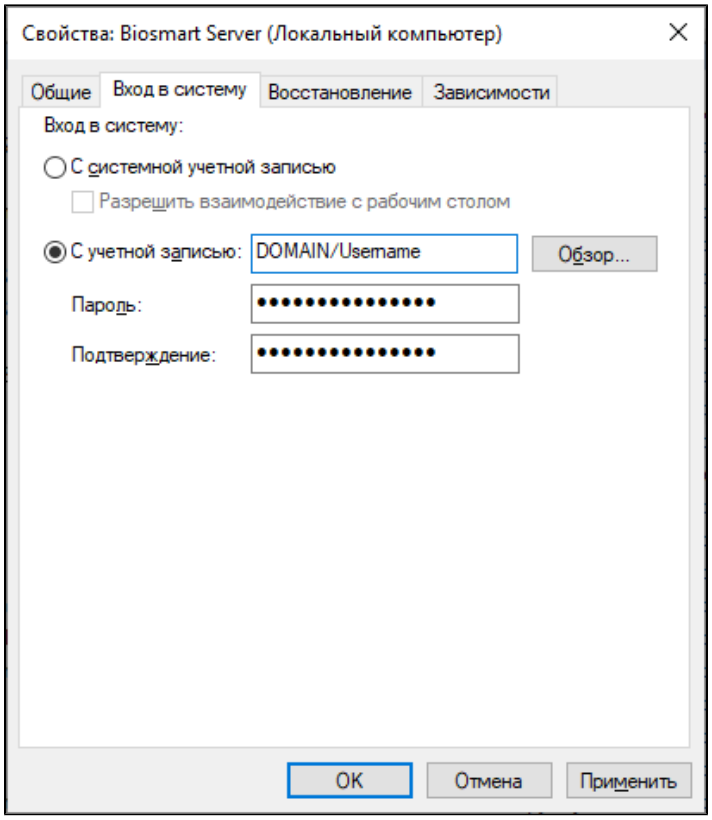
Завершите установку или обновление по инструкции.

2. Проверьте параметры учетной записи в **Службах**, для этого откройте окно **Управление компьютером**, выберите вкладку **Службы и приложения**, далее **Службы**.



Откройте свойства службы **Biosmart Server** с помощью двойного нажатия на службу.
Перейдите на вкладку **Вход в систему** и проверьте, что выбран параметр входа в систему **С учетной записью** и имя учетной записи и пароль установлены.

> Если ПО Biosmart-Studio v6 на вашем ПК установлено и обновлено, то на вкладке **Вход в систему** выберите параметр входа в систему **С учетной записью.** Введите имя учетной записи и пароль.
>
> Сохраните изменения, нажав на кнопку **ОК.**



1. Установите или обновите ПО Biosmart-Studio v6 в соответствии со статьей Установка на ПК с ОС Astra Linux и статьей Обновление на ПК с ОС Astra Linux.
   Для авторизации с помощью Kerberos при установке создайте keytab файл с помощью команды:

   ```
   sudo ./bss-install.sh --kerberos

   sudo ./bss-install.sh --kerberos --krbuser=UPN --krbpassword=password
   ```

   При вводе второй команды параметры пользователя будут взяты из командной строки.

2. Если ПО Biosmart-Studio v6 уже установлено, то для авторизации с помощью Kerberos во время обновления серверной части ПО Biosmart-Studio v6 создайте keytab файл с помощью команды:

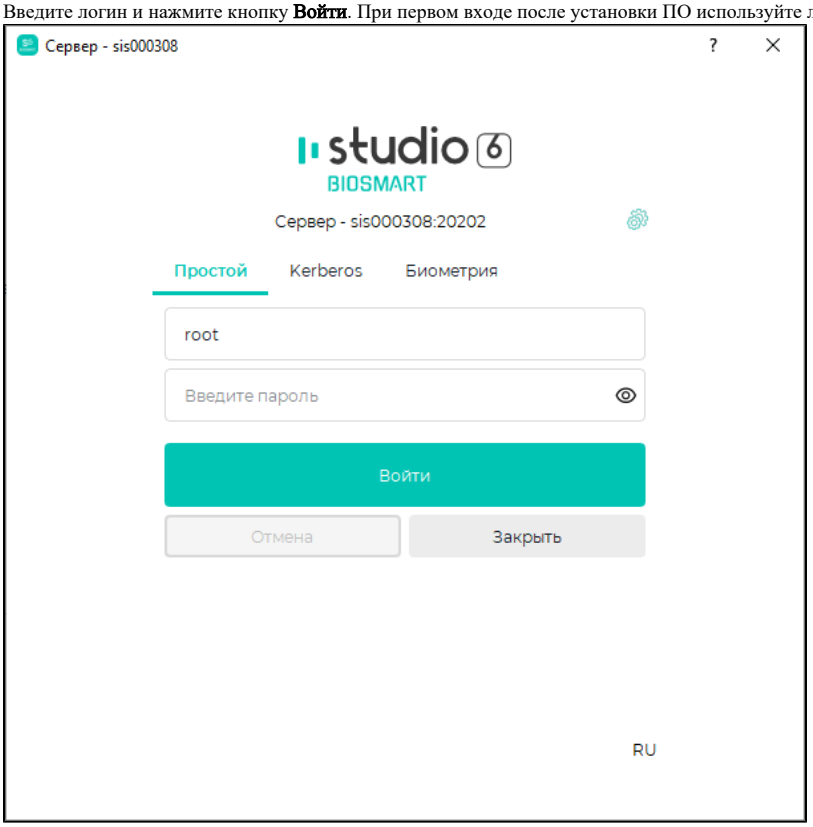
   ```
   sudo ./bss-update.sh --kerberos

   sudo ./bss-update.sh --kerberos --krbuser=UPN --krbpassword=password
   ```

   При вводе второй команды параметры пользователя будут взяты из командной строки.

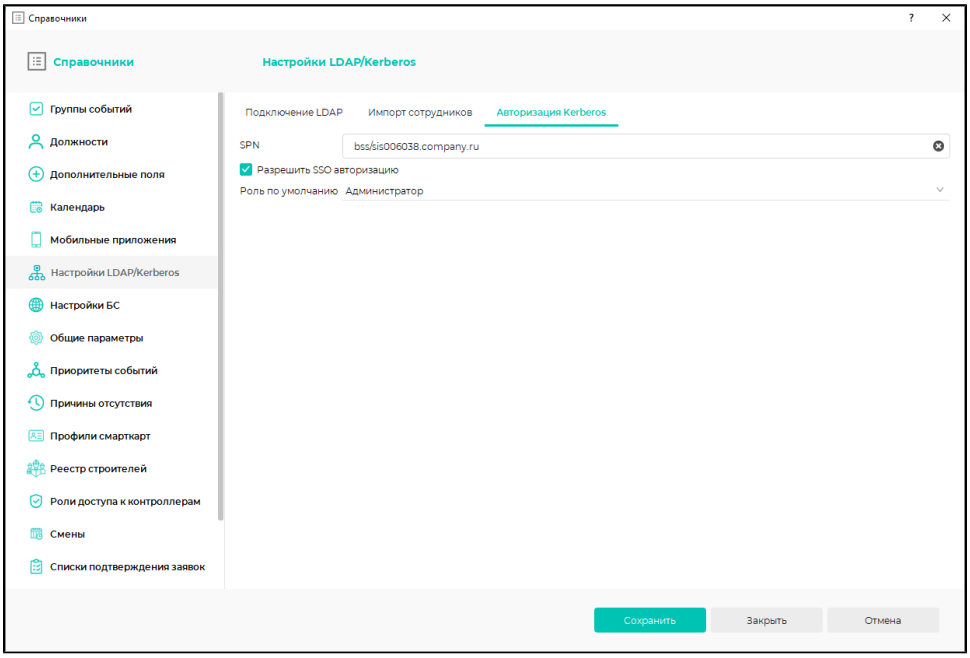
Настройка входа в ПО Biosmart-Studio v6

1. Запустите ПО Biosmart-Studio v6. Появится окно авторизации пользователей.
   Введите логин и нажмите кнопку **Войти**. При первом входе после установки ПО используйте логин **root**, пароль пустой.



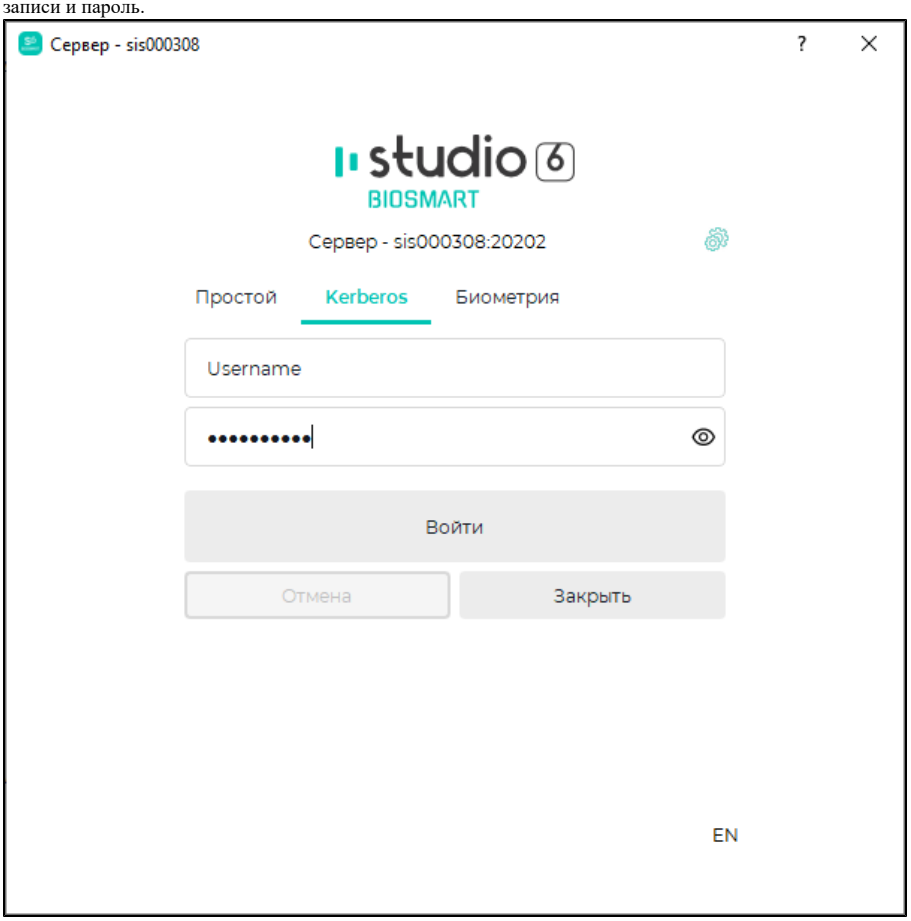
2. После авторизации, в ПО Biosmart-Studio v6 перейдите в раздел **Справочники → Настройки LDAP/Kerberos → Авторизация Kerberos.**
   Введите ранее зарегистрированный SPN.
   Выберите **Роль по умолчанию** для пользователя, который будет использовать ПО Biosmart-Studio v6.

> **Роль по умолчанию** применяется только для новых пользователей ПО Biosmart-Studio v6. Если пользователь добавлен в домен AD, но не создан в ПО Biosmart-Studio v6, то при первой авторизации будет автоматически создан пользователь с выбранной ролью по умолчанию.



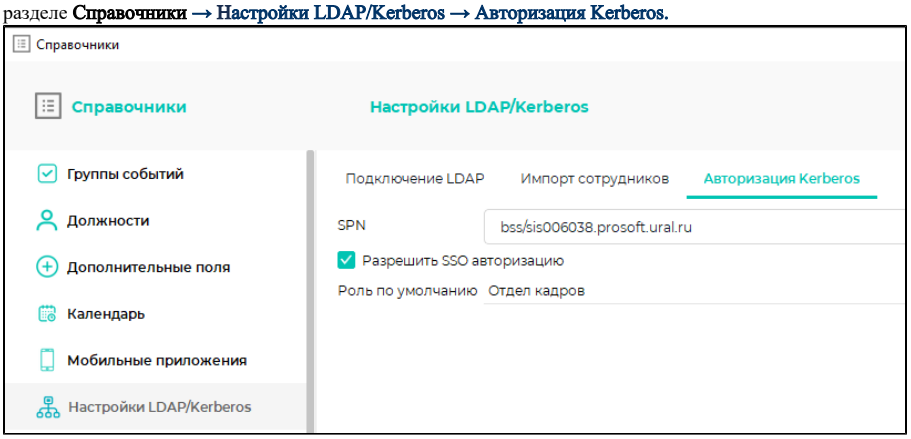
Сохраните изменения, нажав на кнопку **Сохранить и завершите работу с ПО Biosmart-Studio v6.**

3. Для входа в ПО Biosmart-Studio v6 с помощью Kerberos запустите ПО Biosmart-Studio v6, перейдите на вкладку Kerberos и введите имя учетной записи и пароль.

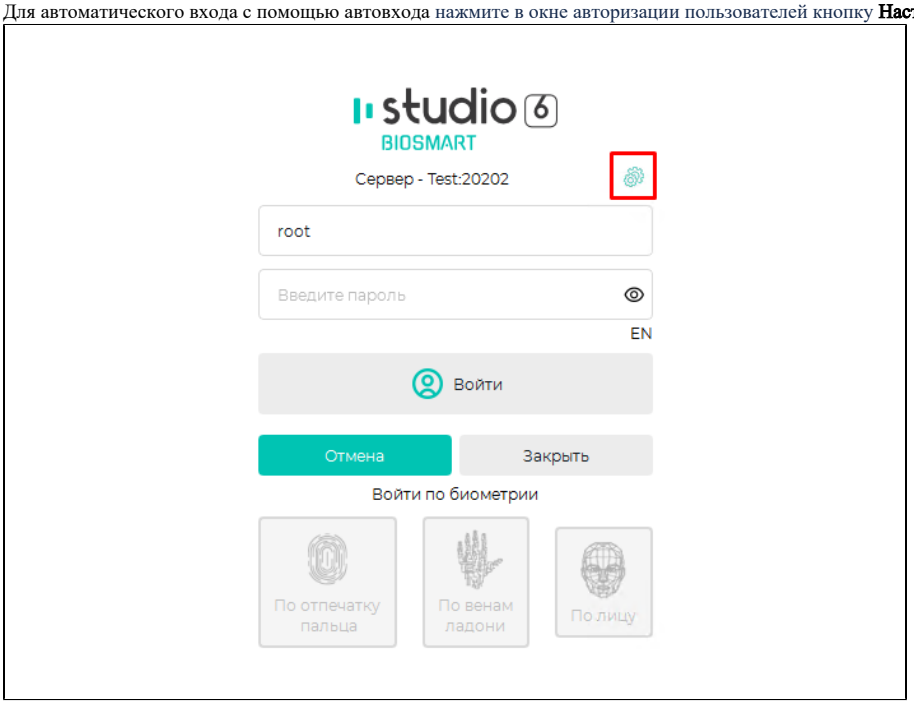


> Имя учетной записи можно вводить в формате Username или Username@realm.
>
> При использовании короткого формата Username для входа в ПО Biosmart-Studio v6 будет использоваться текущий домен.
>
> При первом входе в ПО Biosmart-Studio v6 с помощью Kerberos необходимо вводить логин и пароль пользователя.

4. При использовании протокола аутентификации Kerberos можно настроить автоматический вход в ПО Biosmart-Studio v6.
   Настроить автоматических вход можно двумя способами:
   - с помощью SSO авторизации (используется учетная запись пользователя, авторизованного в AD, для входа в ПО Biosmart-Studio v6 необходимо нажать кнопку **Войти**);
   - с помощью автовхода (используется SSO авторизация, при открытии ПО Biosmart-Studio v6).
5. Для автоматического входа в систему без ввода имени пользователи и пароля поставьте отметку в чекбоксе **Разрешить SSO авторизацию** в разделе **Справочники → Настройки LDAP/Kerberos → Авторизация Kerberos.**

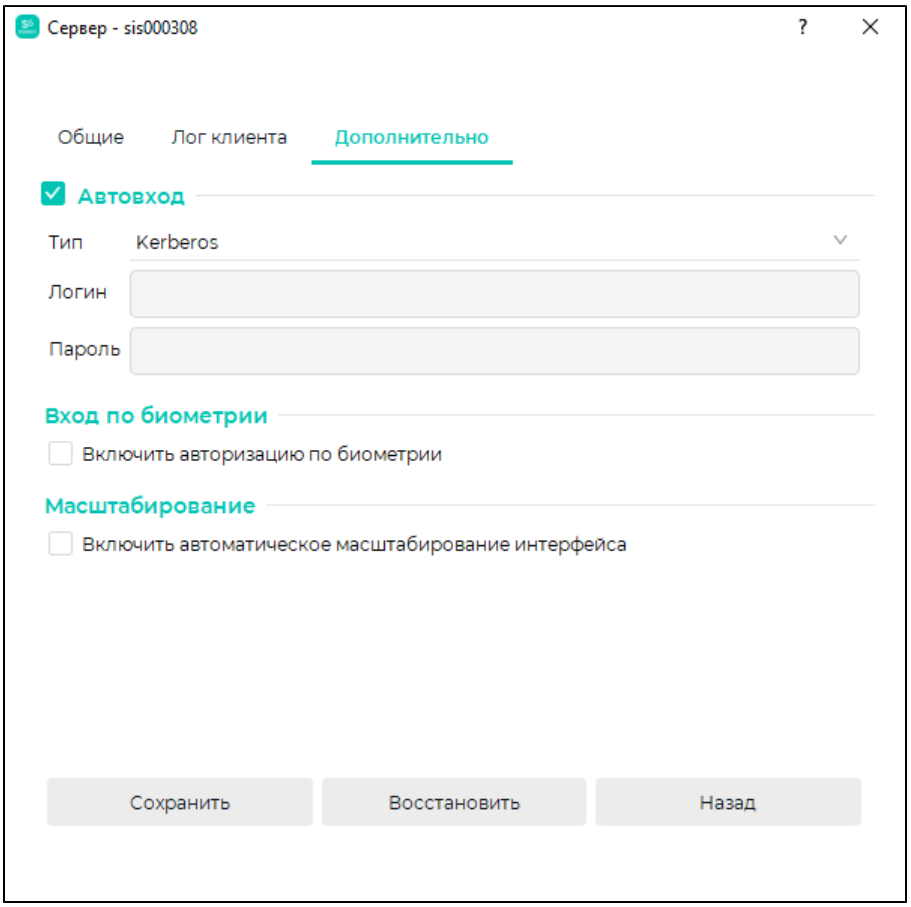


6. Для автоматического входа с помощью автовхода нажмите в окне авторизации пользователей кнопку **Настройки**.

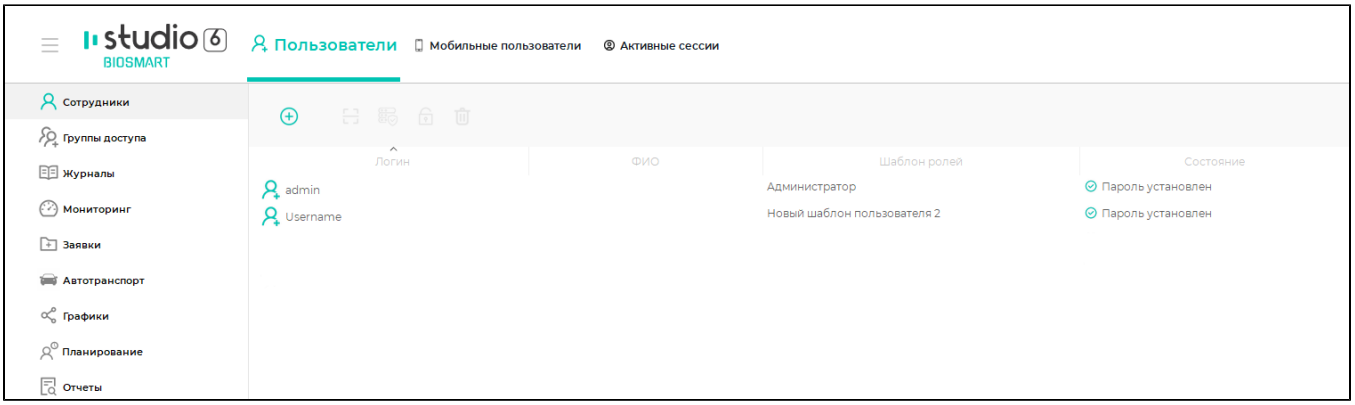


7. Перейдите на вкладку **Дополнительно**, установите флаг **Автовход** и выберите тип автовхода **Kerberos**.

> Автовход с использованием Kerberos работает только в связке с SSO-авторизацией. Это необходимо для безопасной работы, чтобы не хранить пароли в открытом виде.



После авторизации в помощью Kerberos в ПО Biosmart-Studio v6 создается пользователь с ролью, указанной на вкладке **Авторизация Kerberos,** если пользователь не был создан ранее.



При необходимости можно отредактировать роль пользователя в разделе Редактирование свойств пользователя.

Связанные статьи:

- Установка на ПК с ОС Windows
- Установка на ПК с ОС Astra Linux
- Настройки LDAP/Kerberos