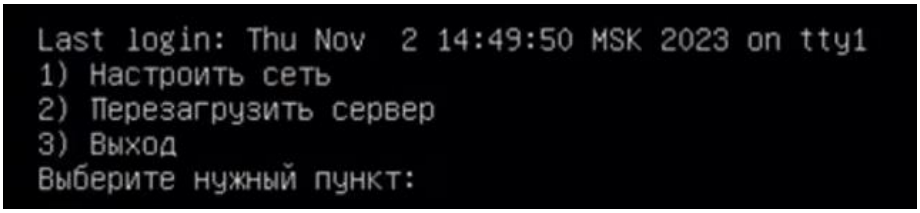
Инструкция по установке и настройке

Разворачиваем ВМ во внутреннем факторе из образа, который предоставили.

Через консоль подключаемся к ВМ вводим логин и пароль.

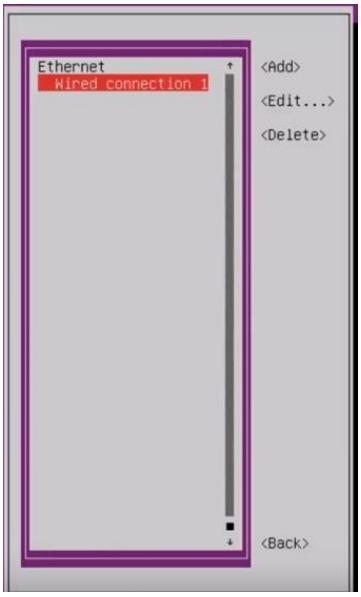
Настройка сети.

Для удобства создано меню, где необходимо ввести «1» для настройки.

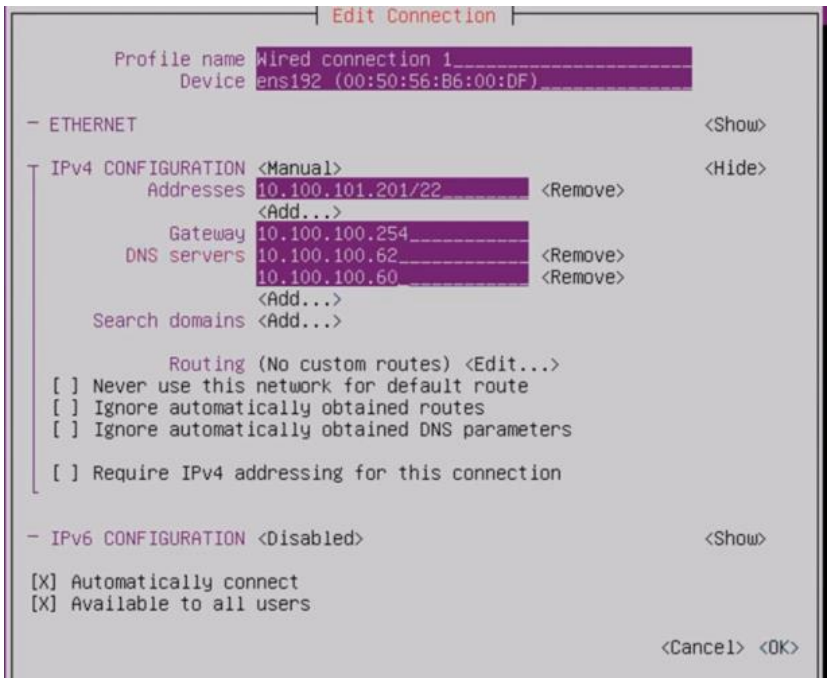


Выбираем редактирование

Выбираем нужную сеть

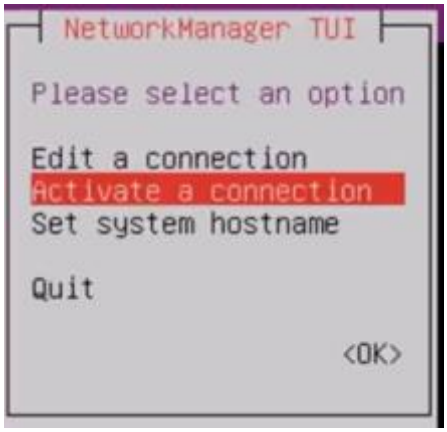


Вводим IP адрес, Gateway и dns сервера. Есть возможность ввести в домен (Search domain), но это не обязательно.

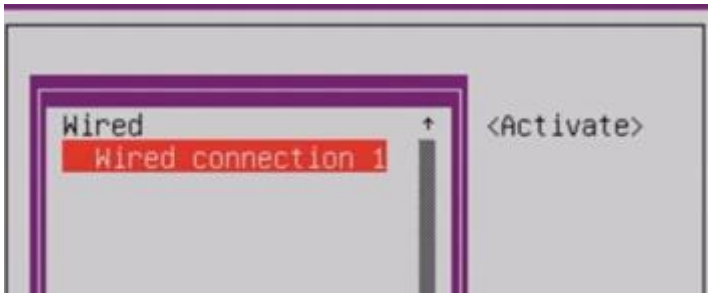


Сохраняем настройки.

Переходим в основные настройки, активируем соединение.



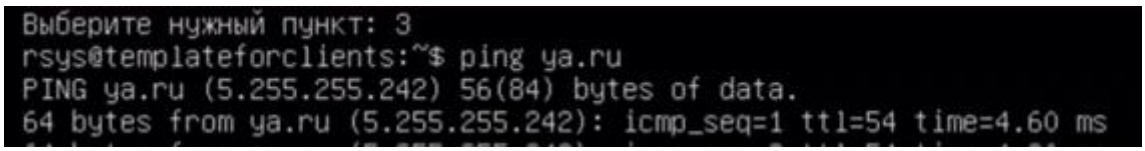
Необходимо деактивировать и активировать соединение.



Настройка сети завершена.

Выходим, в основном меню пункт 3.

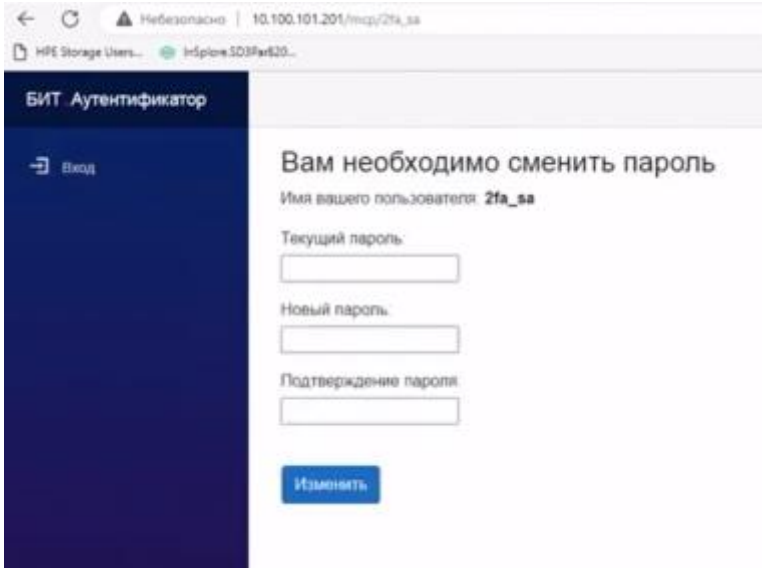
Проверяем доступность внешних ресурсов, например, ping ya.ru.



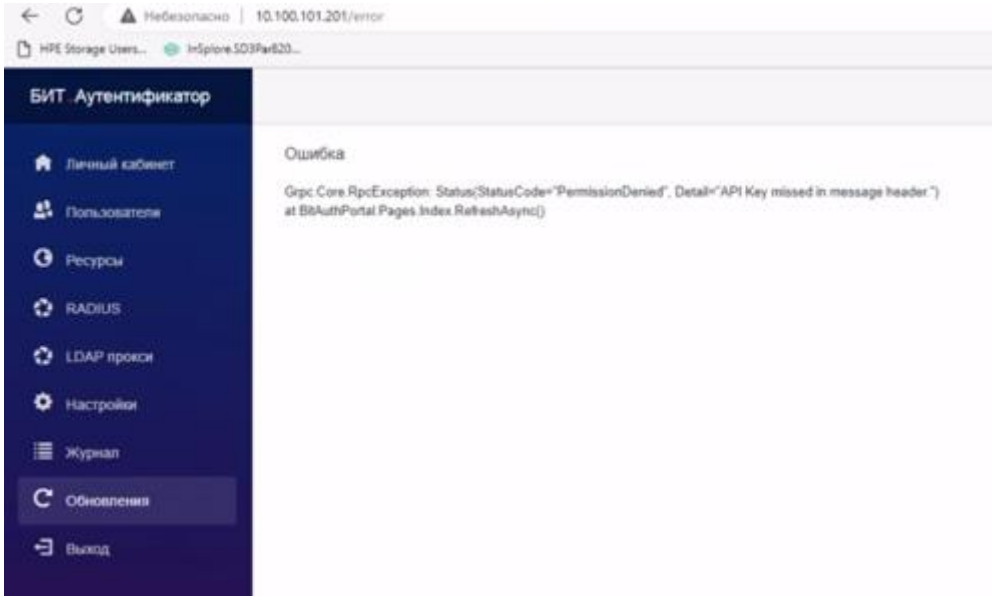
Настройка портала.

В браузере заходим по IP адресу, который указали при настройке.

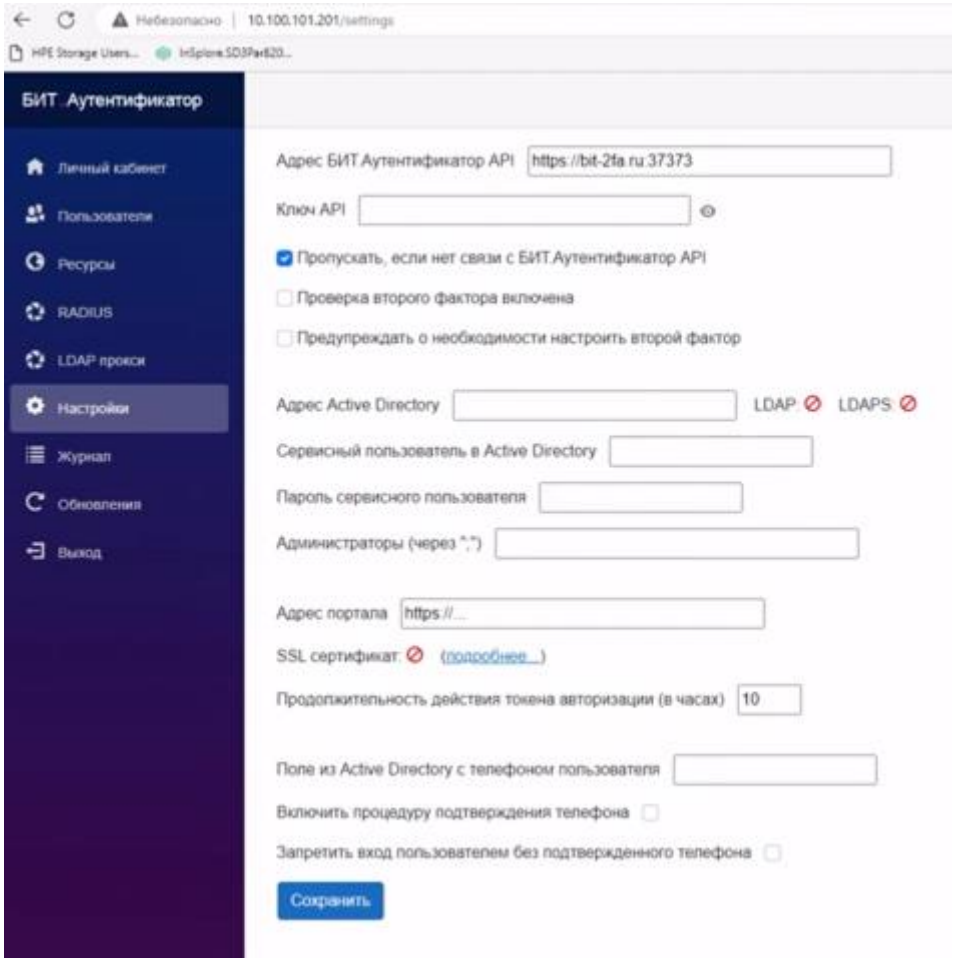
Вводим логин пароль, который предоставили, меняем пароль пользователя:



Выходим и входим на портал под новым паролем.



Ошибка указывает на отсутствие API ключа, переходим к настройке:



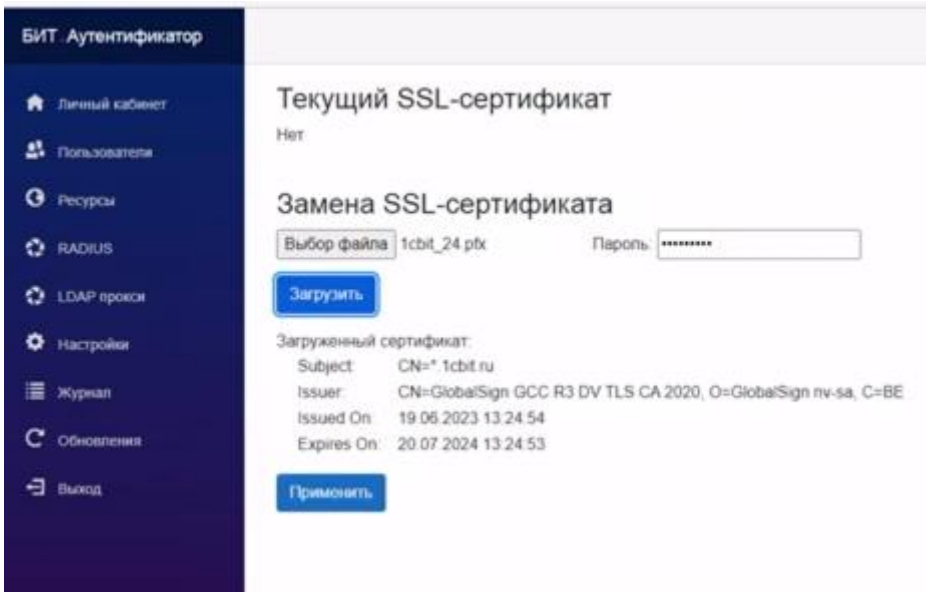
Вводим API ключ, который предоставили вместе с ВМ. Адрес AD, добавляем сервисного пользователя, указываем адрес портала. Нажимаем сохранить. Сервисному пользователю достаточно обычных пользовательских прав в домене, для просмотра и проверки наличия пользователей и групп, которые в дальнейшем будут использоваться.

Сохраняем изменения.

Установка ssl сертификата.

Если Вы используете сертификат в формате .pfx:

Все работы выполняются на портале.Добавляем сертификат, выбираем нужный, вводим пароль, нажимаем загрузить. Проверяем информацию о сертификате, если все корректно, нажимаем применить, соглашаемся с перезапуском необходимых служб.



Проверяем доступность портала по протоколу https.

Если Вы используете свой (самоподписанный) сертификат:

Корневой сертификат в PEM-формате необходимо добавить в хранилище сертификатов ВМ.

Если ваш файл сертификата в формате DER, вы можете конвертировать его в PEM формат с помощью утилиты openssl:

$ openssl x509 -inform der -in сертификат.der -out сертификат.crt

Производим установку:

$ sudo apt-get install -y ca-certificates – установка пакета для Ubuntu.

$ sudo cp сертификат.crt /usr/local/share/ca-certificates - копируем файл сертификата в хранилище сертификатов.

$ sudo update-ca-certificates - обновляем хранилище сертификатов.

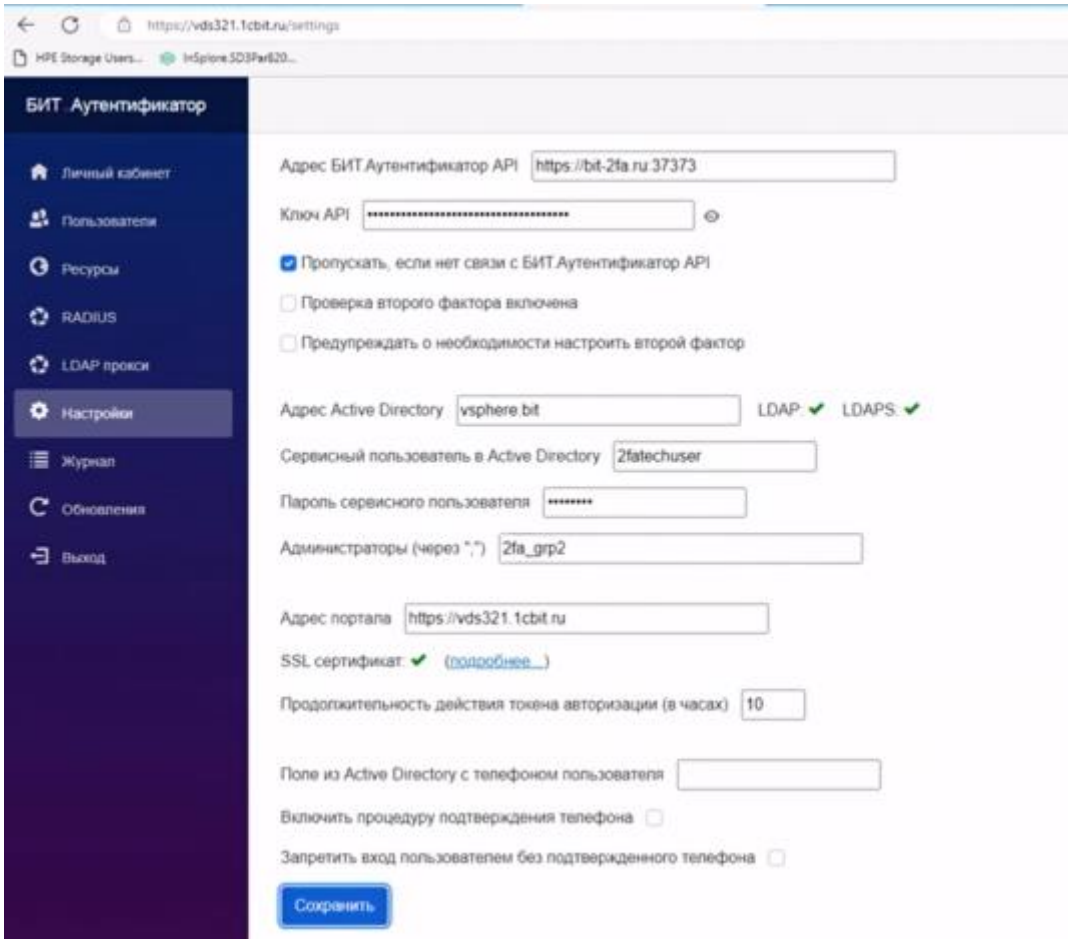
Проверяем, что сертификат добавился после выполнения обновления:

Updating certificates in /etc/ssl/certs…
1 added, 0 removed; done.

Возвращаемся на портал, меню настройки, добавляем сертификат.

Выбираем нужный, вводим пароль, нажимаем загрузить. Проверяем информацию о сертификате, если все корректно, нажимаем применить, соглашаемся с перезапуском необходимых служб.

Проверяем доступность портала по протоколу https.



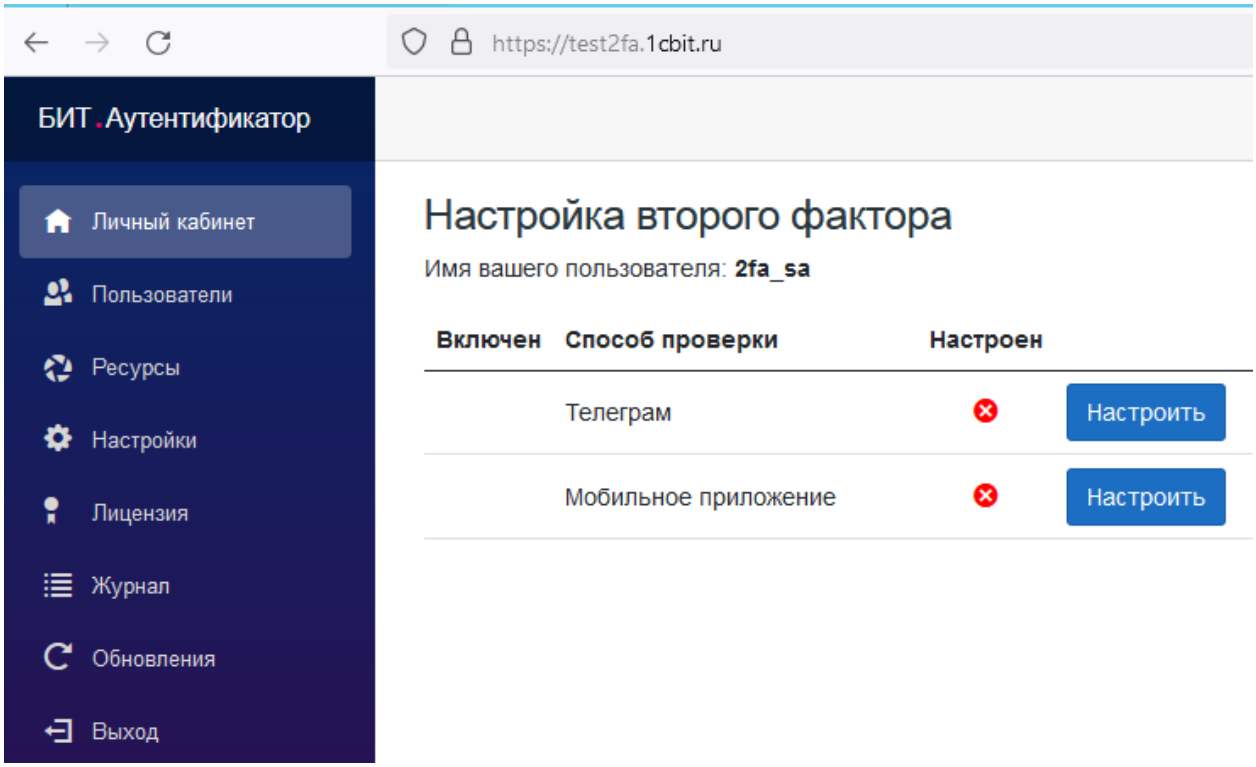
Добавляем группу или группы администраторов из AD. Все пользователи из указанных групп будут иметь доступ к администрированию портала БИТ.Аутентификатор.

Начальная настройка портала завершена.

Настройка клиентского портала

После разворачивания виртуальной машины и настройки сети авторизуемся на портале.

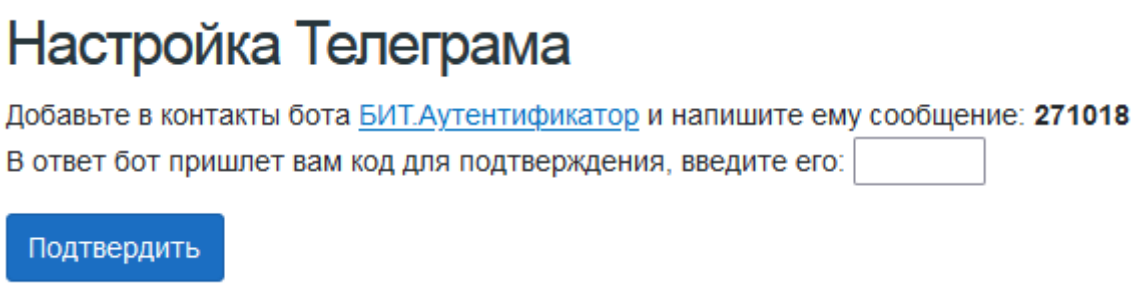
При первом входе основное меню выглядит так:



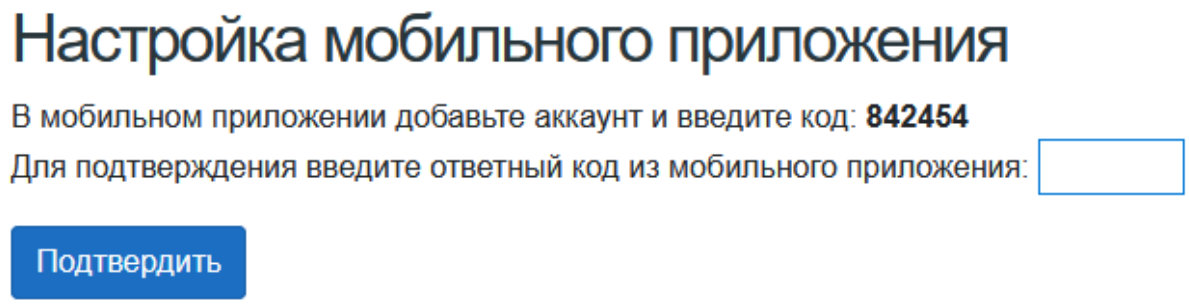
Личный кабинет.

На вкладке личный кабинет настраиваем второй фактор. Нажимаем кнопку настроить, для телеграма или мобильного приложения, которое доступно в App Store или Google Play.

Вводим указанный код в чат-боте телеграма (доступен по кликабельной ссылке):



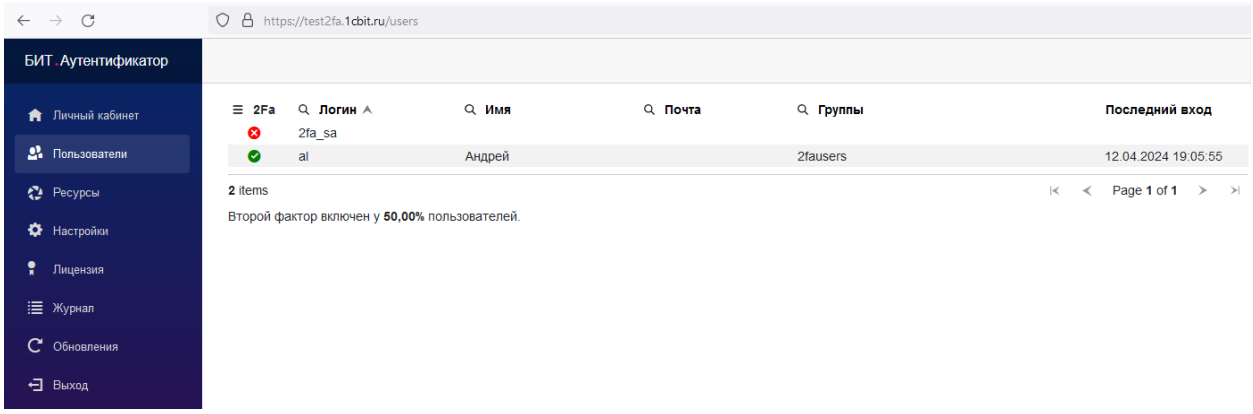
Или добавляем аккаунт в мобильном приложении и вводим код:



При необходимости можно сбросить настройки.

Настройка завершена.

Пользователи.



Параметр в столбце 2fa показывает кто из пользователей настроил второй фактор , а кто нет .

Логин – имя входа пользователя из Active Directory.

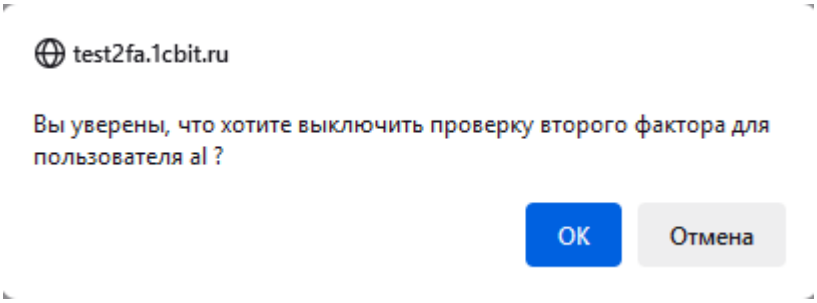
Имя – имя пользователя из Active Directory.

Почта - почта пользователя из Active Directory.

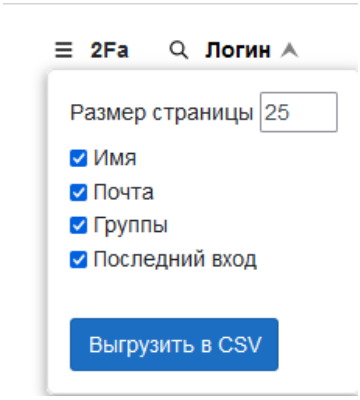
Группы – указаны группы пользователей из Active Directory, которые задействованы на портале или в его настройках.

Последний вход – дата и время последней авторизации на ресурсе/портале, при условии, что второй фактор настроен. Если настройка не выполнена, поле остается пустым.

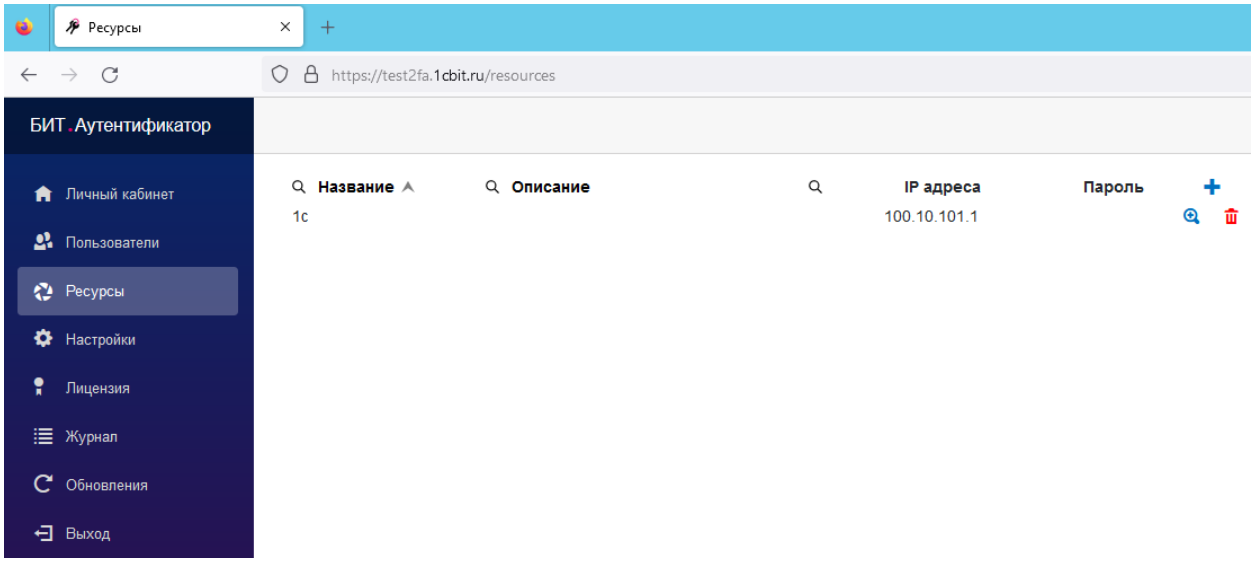
При необходимости из данного раздела администратор портала может выключить проверку второго фактора для пользователей. Нажав напротив пользователя и подтвердить выполнение:



Для удобства работы с пользователями есть возможность настроить размер страницы, отображаемые столбцы или выгрузить список пользователей в CSV, для этого используется ☰:



Ресурсы.



В данном разделе содержится вся информация по созданным ресурсам организации.

Данная закладка содержит вся информация по созданным ресурсам организации и определяет политики использования сервисов, даже если пользователю разрешён доступ на уровне AD, но запрещён на уровне закладки “Ресурсы”, пользователь не сможет авторизоваться.

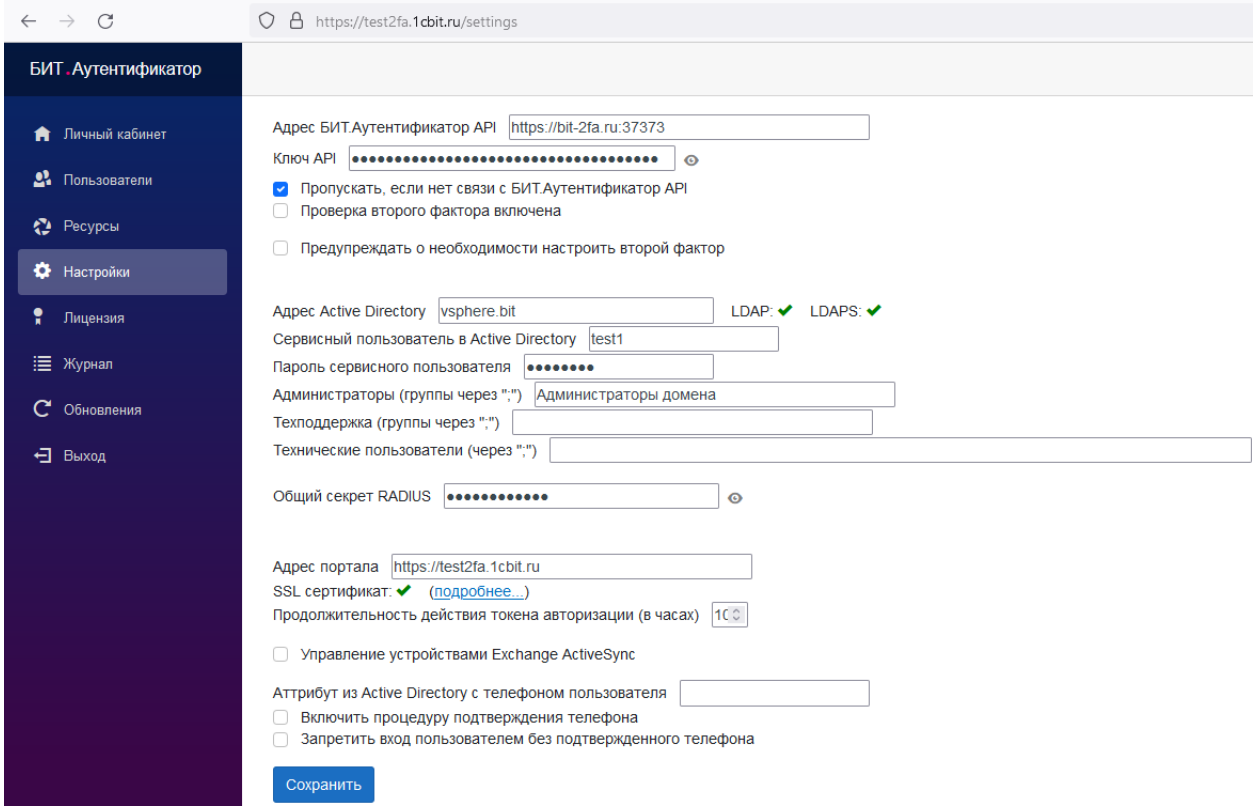
- **Название** – название ресурса, использующееся в настройке всех внутренних сервисов.

К одному ресурсу может быть привязано несколько сервисов, для которых будет схожа политика авторизации. Название ресурса приходит пользователю в запросе предоставления доступа

- **Описание** – понятное для администраторов описание политики, либо сервиса, который будет использовать ресурс. Указывается по Вашему усмотрению.
- **IP адреса** – здесь перечислены адреса устройств, с которых будет производиться проверка второго фактора в соответствии с настройками ресурса.
- **Пароль** – нужно ли порталу проверять первый фактор своими силами, проксируя запрос в AD. Данная настройка используется при настройке не доменных сервисов, интегрированных в домен с помощью функционала LDAP.

-  - добавление нового ресурса.  - удаление ресурса.  - изменение, просмотр настроек ресурса.

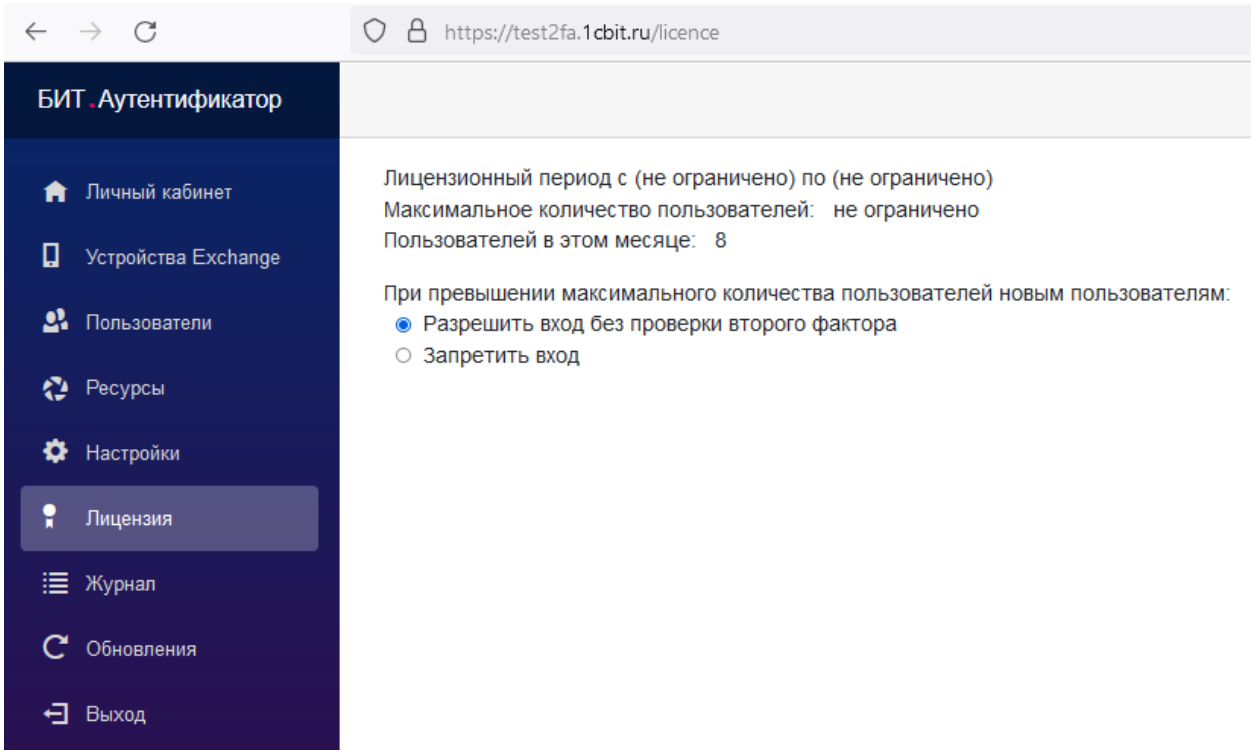
Настройки.



- **Адрес БИТ.Аутентификатор API** – адрес центрального сервера, проверяющего лицензии
- **Ключ API** – ключ, доступный для генерации администраторами клиента после приобретения лицензии
- **Пропускать, если нет связи с БИТ.Аутентификатор API** – поведение, если нет связи с центральным сервисом, проверка 2fa отключается, ресурсы, работающие с проверкой 2fa будут либо пускать пользователей, либо отклонять все запросы.

- **Проверка второго фактора включена** – включение второго фактора.
- **Предупреждать о необходимости настроить второй фактор** – если у пользователя второй фактор не настроен и при этом нет никаких дополнительных ограничений, при входе на ресурс будет получать предупреждение о необходимости настроить второй фактор. Работает только в тех сервисах, где есть возможность передать сообщение пользователю.
- **Адрес Active Directory** – имя домена, к которому будет подключаться второй фактор
- **Сервисный пользователь в Active Directory** – технический пользователь с правами чтения Active Directory.
- **Пароль сервисного пользователя** – пароль сервисного пользователя.
- **Администраторы (через “;”)** – администраторы портала, перечисленные через точку запятой, могут быть как группы Active Directory, так и отдельные пользователи. Администраторы, как и владелец имеет полные права на портале.
- **Техподдержка (группы через ";")** - сотрудники, которые будут сбрасывать пользователям второй фактор в случае необходимости, а также видеть журнал.
- **Технические пользователи (через ";") -** технические пользователи для ресурсов, использующих LDAP подключение.
- **Общий секрет RADIUS** – произвольный набор символов, указывается при настройке сервисов, использующих RADIUS протокол.
- **Адрес портала** – DNS адрес портала, по которому пользователь сможет попасть на портал, при начальной настройке необходимо использовать split-brain DNS чтобы портал отвечал по одному и тому же имени, как снаружи, так и внутри.
- **SSL сертификат (подробнее) -** возможность обновить SSL сертификат в .pfx или .pem формате.
- **Продолжительность действия токена авторизации (в часах)** – через сколько часов любой веб ресурс повторно запросит авторизацию пользователя.
- **Управление устройствами Exchange ActiveSync** – Включается для управления устройствами Exchange ActiveSync. При включении в основном меню появляется новая вкладка устройствами Exchange.
- **Поле из Active Directory с телефоном пользователя** - атрибут в Active Directory, в соответствии с которым портал проверяет номер телефона сотрудника.
- **Включить процедуру подтверждения телефона** - Включение\отключение функционала проверки телефона. Работает только для Telegram.
- **Запретить вход пользователем без подтвержденного телефона** - Включение\Отключение возможности входа без подтверждённого телефонного номера.

Лицензия.

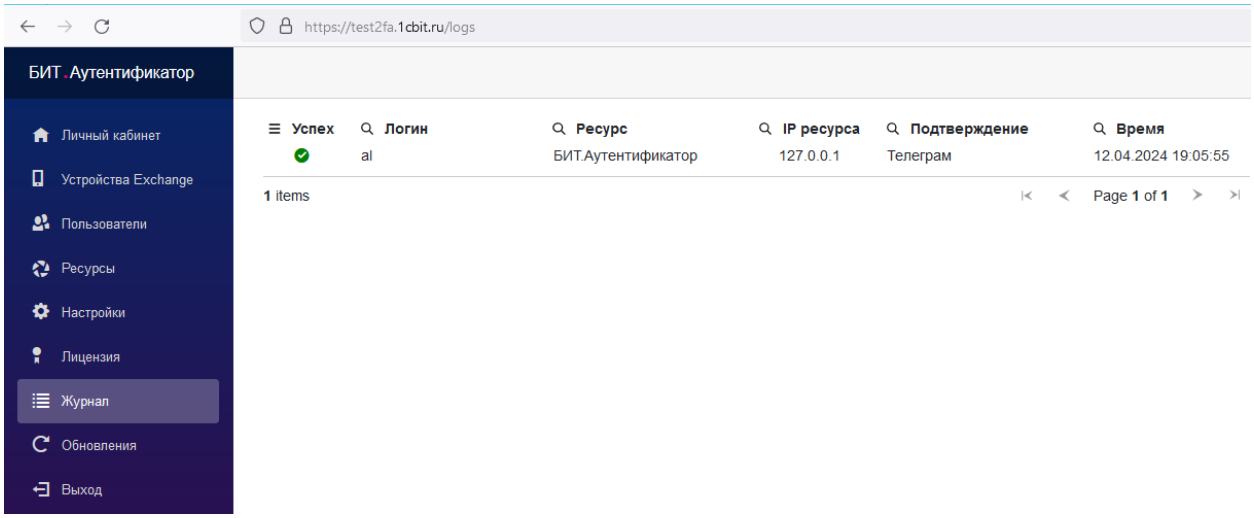


Содержит информацию о сроке лицензионного периода, количестве доступных лицензий и количестве активных пользователей в текущем месяце.

Позволяет настроить действие, при превышении максимального количества пользователей.

Количество лицензий и срок предоставления лицензий согласовывается с менеджером.

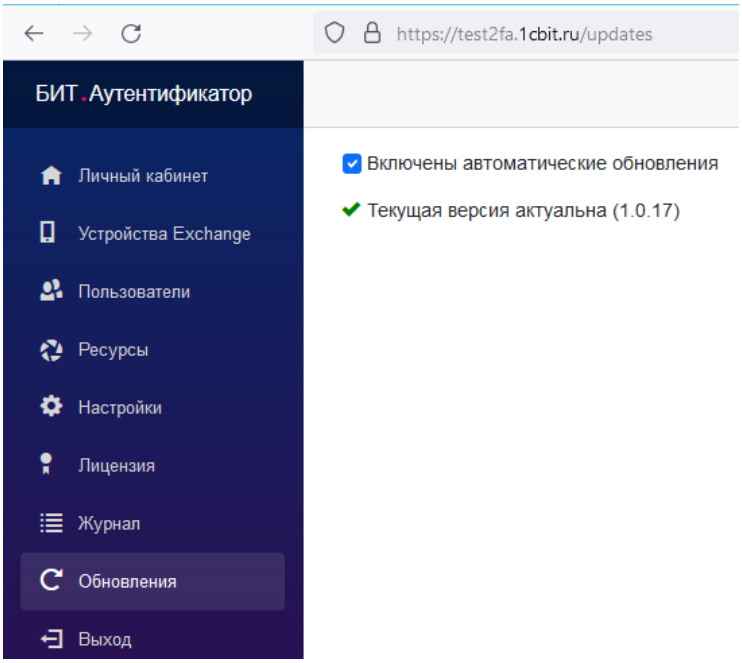
Журнал.



В журнале содержится информация по всем попыткам авторизации на созданных ресурсах, в том числе на портале, если настроен второй фактор.

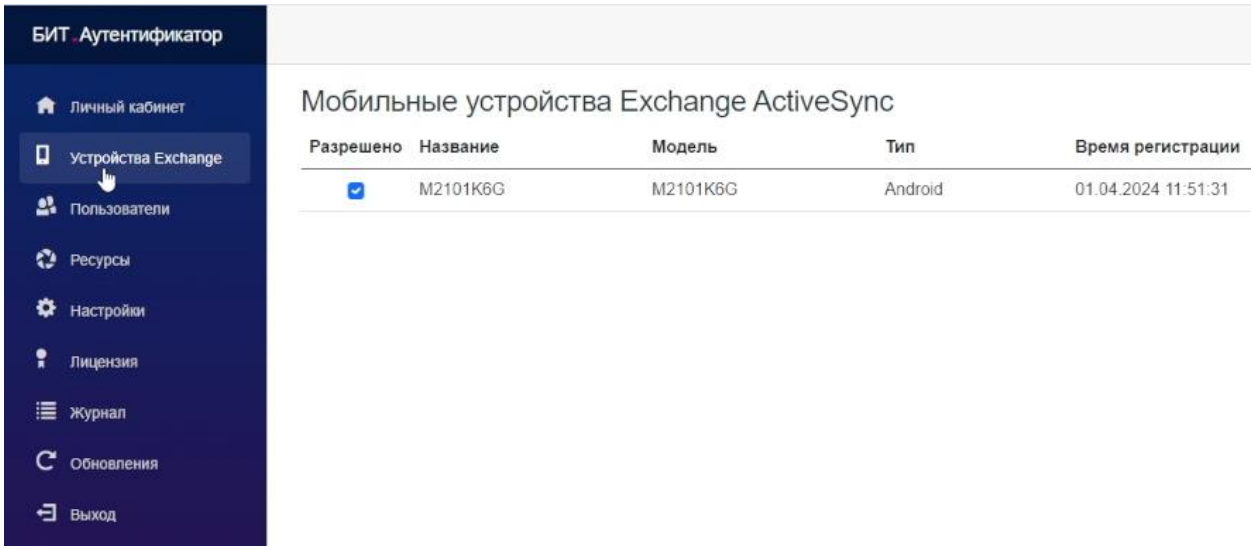
Включает результат авторизации (удачно/нет), логин авторизации, наименование ресурса, IP адрес ресурса, способ подтверждения двухфакторной авторизации и время подключения.

Обновления.



Информация о текущей версии портала и возможность включения/отключения автоматического обновления.

Устройства Exchange.



При включении Управление устройствами Exchange ActiveSync в настройках портала появляется новое вкладка в основном меню.

Для корректной работы, сервисный пользователь, который указан в настройках, должен состоять в группе безопасности Exchange Trusted Subsystem.

После настройки почты на мобильном устройстве появляется само устройство в данной вкладке.

Для разрешения подключения необходимо администратору или владельцу портала разрешить подключение.

Предоставляет информацию об устройстве, с которого происходи подключение, его тип и дату регистрации.

Выход.

Выход в меню авторизации на портале.