Инструкция по настройке сервисов для подключения двухфакторной аутентификации от БИТ.Аутентификатор.

1. **Настройка для ADFS.**

Загрузите и распакуйте архив на сервер с ADFS.

Отредактируйте файл конфигурации BitAuthADFS.dll.config:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <appSettings>
    <add key="BitAuth:Resource" value="имя_ресурса" />
    <add key="BitAuth:SecurityCenter" value="https://адрес_портала" />
    <add key="BitAuth:BypassWhenUnreachable" value="true" />
  </appSettings>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.8"/>
  </startup>
</configuration>
```

value="имя_ресурса" – имя ресурса на портале.

value=https://адрес_портала – адрес Вашего портала.

Запустите install с правами администратора.

В консоли управления ADFS, включите для приложения (или группы приложений) дополнительный метод проверки "БИТ.Аутентификатор"

Настройки на портале

Добавьте новый ресурс.

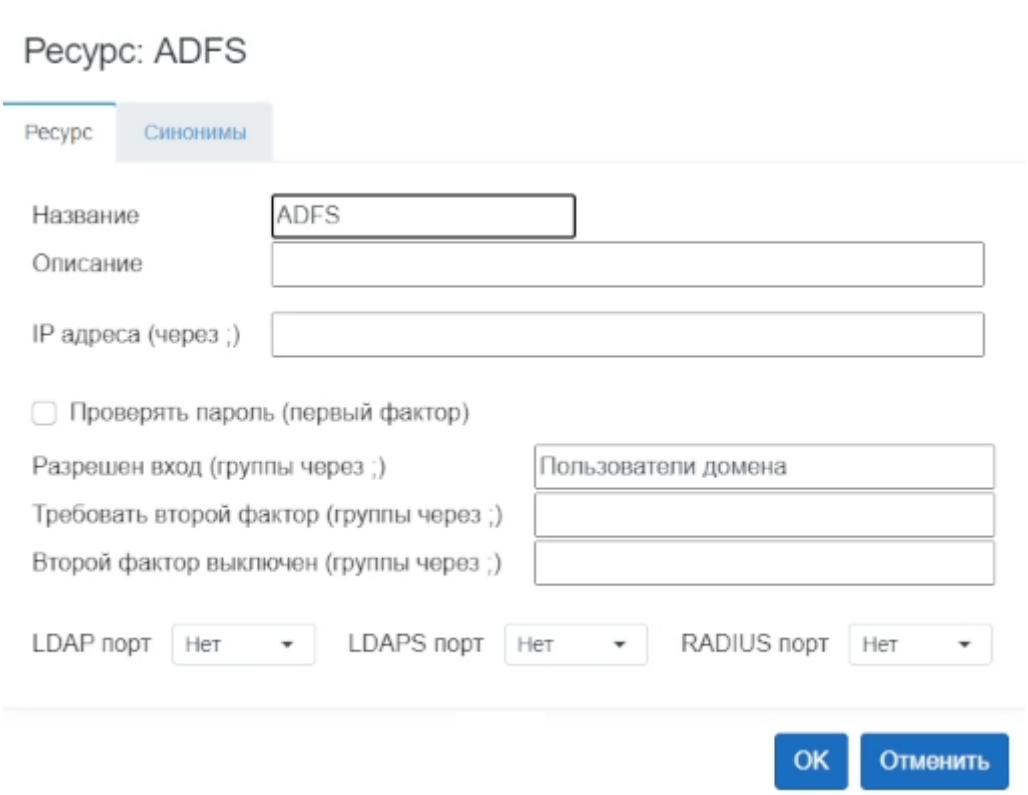
Название ресурса (должно совпадать с названием ресурса, которое указывалось при редактировании BitAuthADFS.dll.config), описание по желанию, IP адрес указывать не нужно.

Группы пользователей из Active Directory для которых:

Разрешен вход (группы через ;) – Будет разрешен вход на данный ресурс.

Требовать второй фактор (группы через ;) – Проверка второго фактора обязательна.

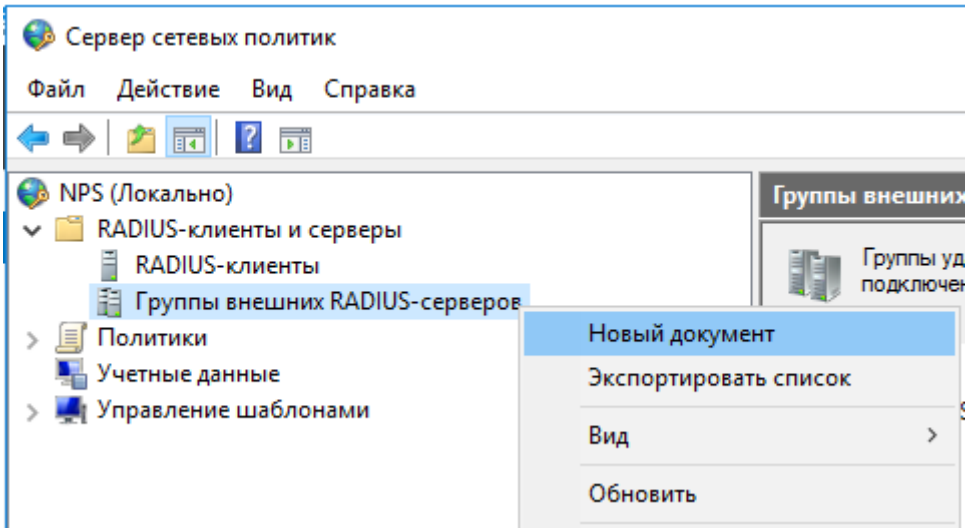
Второй фактор отключен (группы через ;) – Проверка второго фактора будет отключена.



2. **Настройка для Gateway RADIUS.**

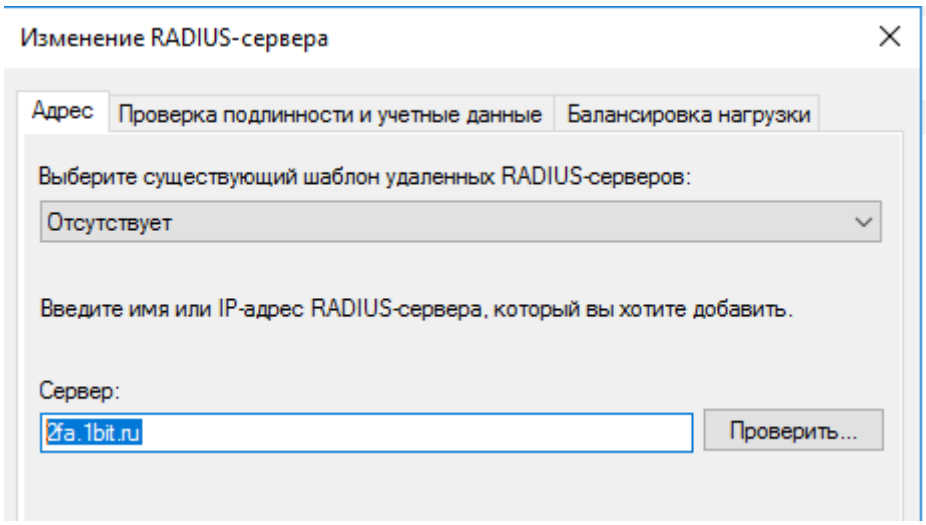
После того, как развернули ВМ с порталом и провели настройки, зайдите на ВМ с Gateway.

Откройте сервер сетевых подключений (nps). Создайте новый документ в группах внешних RADIUS-серверов:

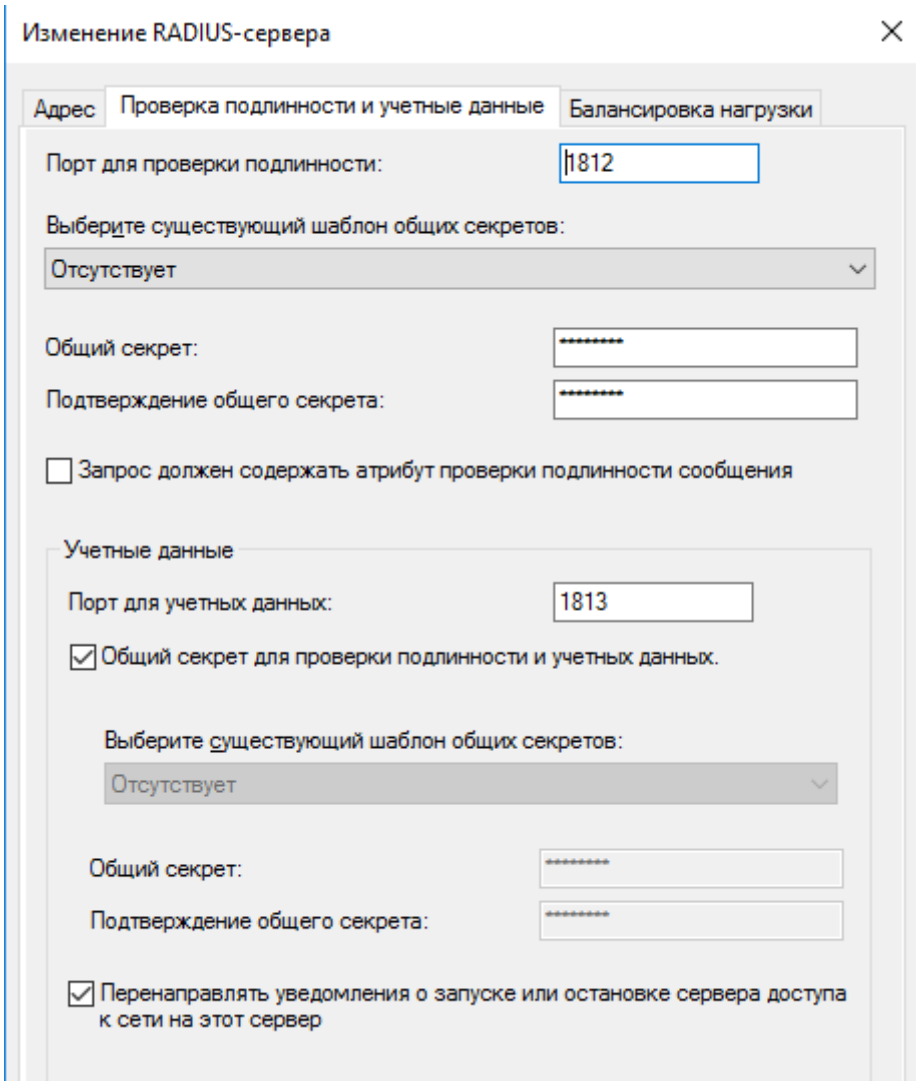


Введите имя группы, нажмите добавить.

Введите dns имя или IP адрес портала, который развернули ранее:

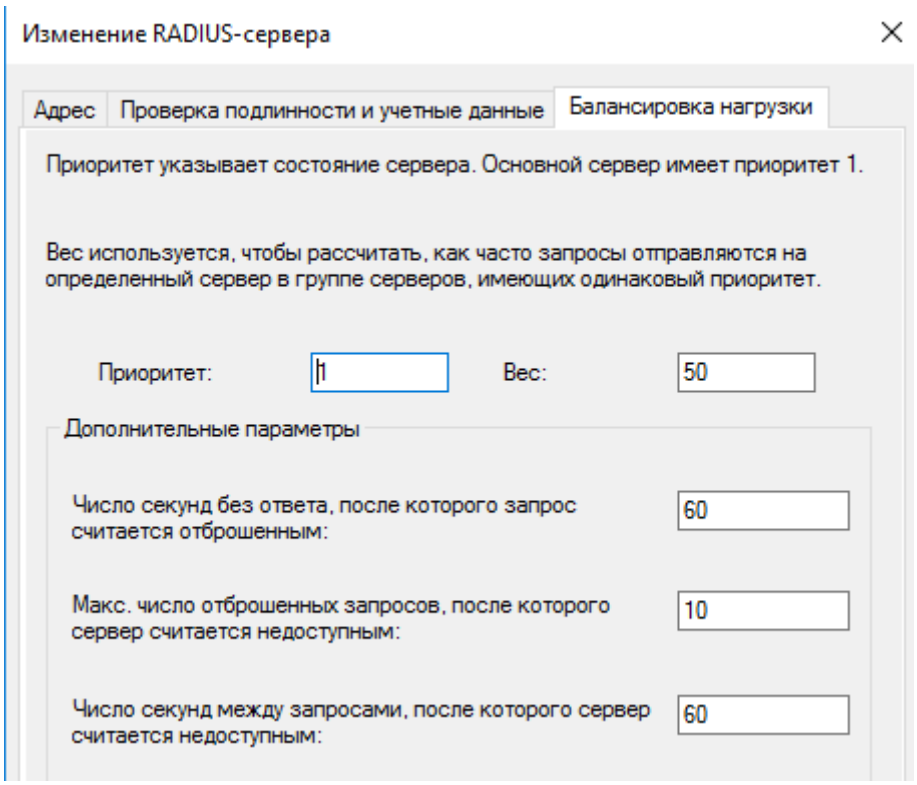


Настройте проверку подлинности:



Укажите порты RADIUS, общий секрет, который можно посмотреть в настройках портала.

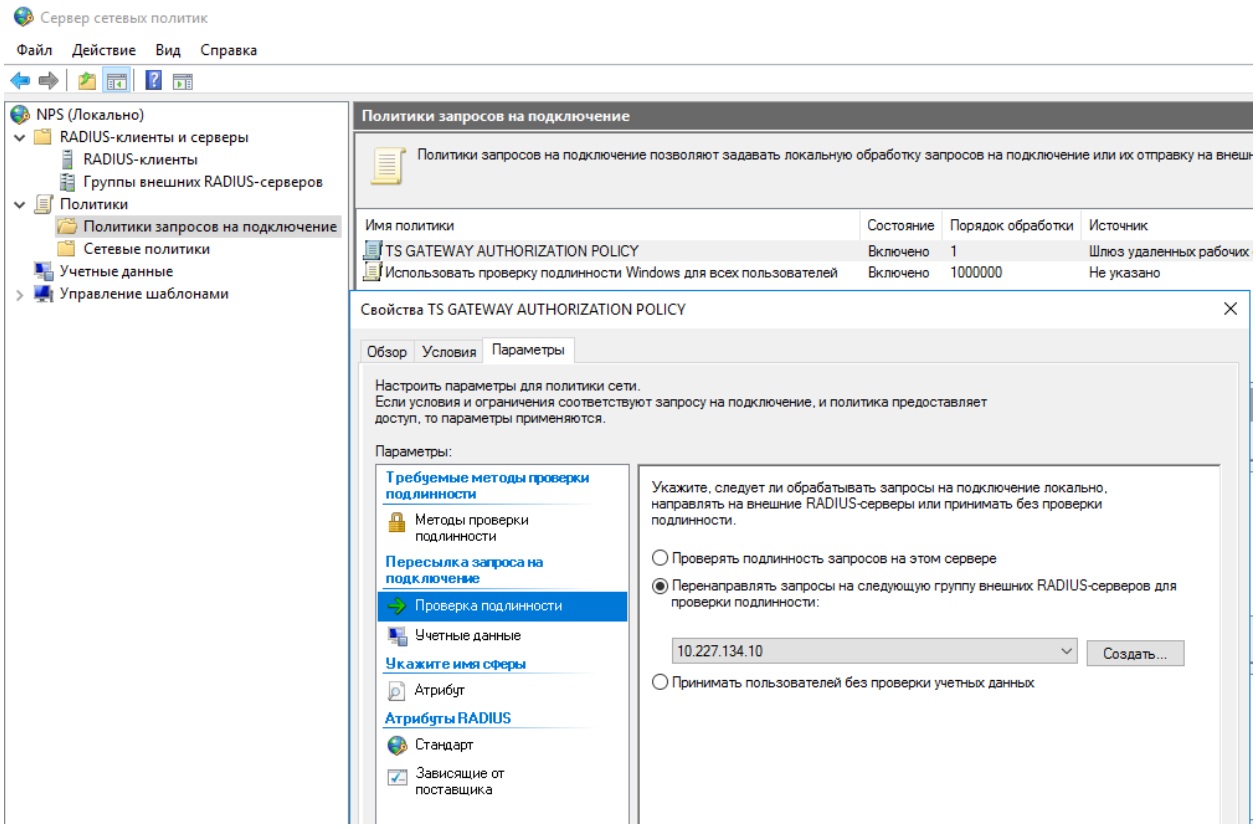
В балансировке нагрузки установите нужные таймауты:



Количество секунд менее 30 лучше не указывать, т.к. отправка запроса, его доставка и ответ может происходить с небольшой задержкой.

Перейдите в Политики/Политика запросов на подключение.

Выберите TS GATEWAY AUTHORIZATION POLICY, перейдите во вкладку параметры – проверка подлинности. Установите настройку перенаправления запросов на внешний RADIUS-сервер и выберите из списка группу, которую создали ранее.



Настройки на портале

Перейдите на портал, добавьте новый ресурс.

Укажите название ресурса, описание по желанию, ip адрес gw-сервера.

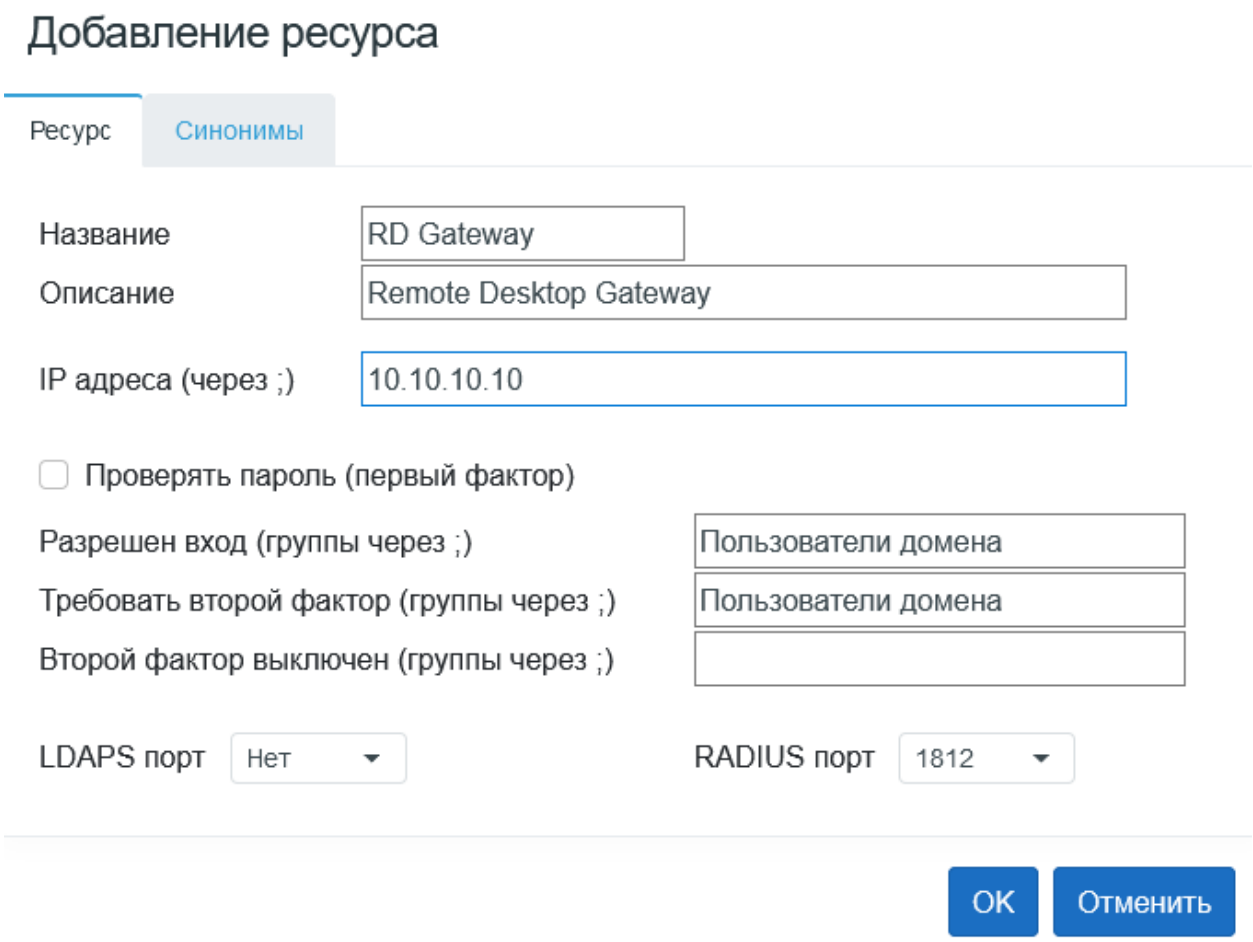
Укажите группы пользователей из Active Directory для которых:

Разрешен вход (группы через ;) – Будет разрешен вход на данный ресурс.

Требовать второй фактор (группы через ;) – Проверка второго фактора обязательна.

Второй фактор отключен (группы через ;) – Проверка 2FA будет отключена.

Укажите порт RADIUS, по умолчанию 1812.



3. Настройка IIS (Internet Information Services) для 1С.

Для корректной работы должен быть установлен .net framework 4.8.

Загрузите и распакуйте архив на сервер iis.

Скопируйте все файлы из папки в каталог публикации базы \bin. Каталог по умолчанию

C:\inetpub\wwwroot\имя_БД\bin\.

Если какой-то из файлов требует перезаписи, то может возникнуть конфликт с другими установленными плагинами.

Сделайте резервную копию файла конфигурации C:\inetpub\wwwroot\имя_БД\web.config для возможности восстановления первоначального состояния.

Откройте web.config для редактирования и добавьте в него следующие строчки:

Внутрь раздела <modules>

<modules>

…

<add name="BitAuthIISModule" type="BitAuthIIS.BitAuthIISModule" />

…

</modules>

Если раздел отсутствует, то добавьте:

<system.webServer></system.webServer>, после обработчиков (handlers)

Внутрь раздела <appSettings>

<appSettings>

…

<add key="BitAuth:Resource" value="1C" />

<add key="BitAuth:ResourceUrl" value="https://ссылка на публикацию ИБ" />

<add key="BitAuth:SecurityCenter" value="https://адрес портала" />

<add key="BitAuth:BypassWhenUnreachable" value="true" />

…

</appSettings>

Где,
Параметр BitAuth:Resource соответствует названию ресурса на портале, который будете создавать далее.

value="https:// https://ссылка на публикацию ИБ" – адрес веб публикации информационной базы 1С.

value="https://адрес портала" – адрес Вашего портала.

Сохраните web.config и перезапустите IIS.

Пример содержимого web.config с уже добавленными настройками:

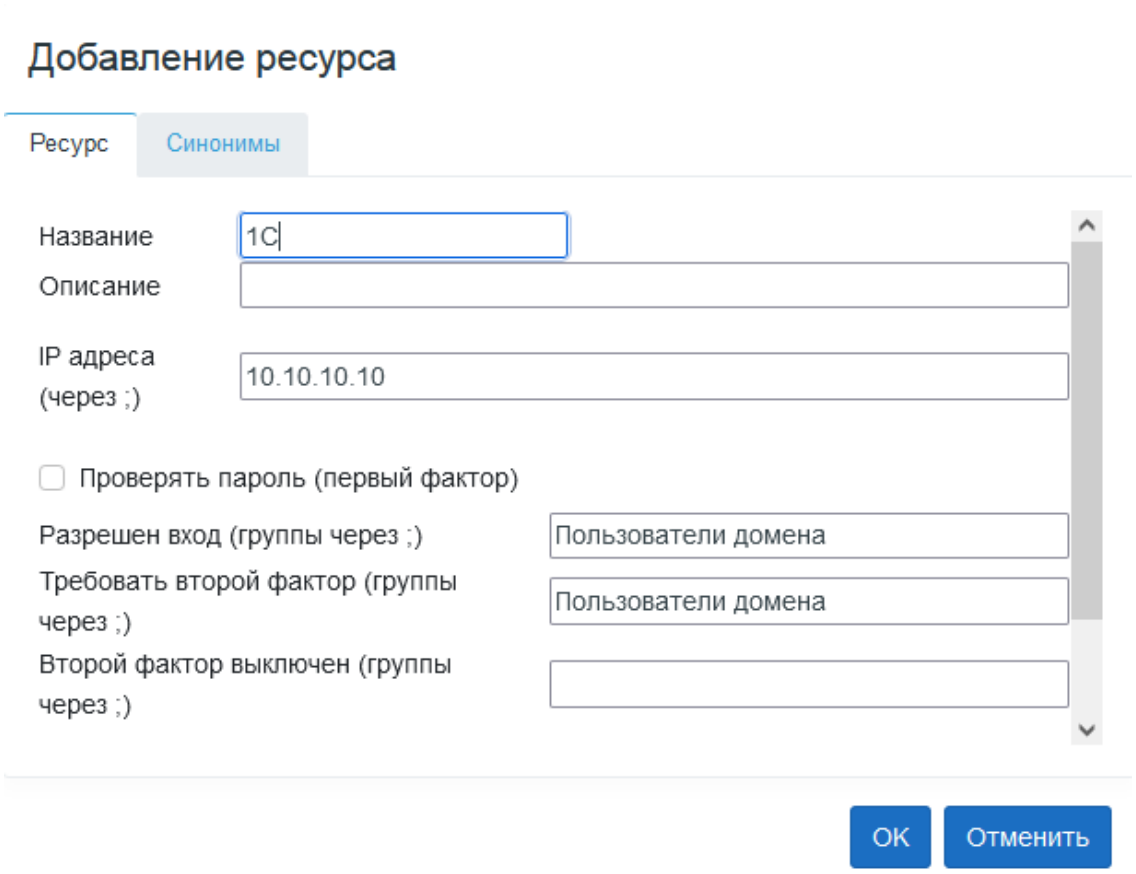
```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <system.web>
        <customErrors mode="Off"/>
    </system.web>
    <system.webServer>
        <handlers>
            <add name="1C Web-service Extension" path="*" verb="*" modules="IsapiModule"
        </handlers>
        <modules>
           <add name="BitAuthIISModule" type="BitAuthIIS.BitAuthIISModule" />
        </modules>
    </system.webServer>

  <appSettings>
    <add key="BitAuth:Resource" value="1C" />
    <add key="BitAuth:SecurityCenter" value="https://vds321.1cbit.ru:37374" />
    <add key="BitAuth:BypassWhenUnreachable" value="true" />
    <add key="BitAuth:ResourceUrl" value="https://2fa1c.1cbit.ru/buh/" />
  </appSettings>

</configuration>
```

Настройки на портале

Добавьте новый ресурс на портале.



Укажите имя ресурса, которое указали в параметре BitAuth:Resource при редактировании web.config, описание по желанию и IP адрес сервера iis.

Укажите группы пользователей из Active Directory для которых:

Разрешен вход (группы через ;) – Будет разрешен вход на данный ресурс.

Требовать второй фактор (группы через ;) – Проверка второго фактора обязательна.

Второй фактор отключен (группы через ;) – Проверка 2FA будет отключена.

4. **Настройка IIS (Internet Information Services) для Exchange OWA ECP (Outlook Web Application).**

Для корректной работы должен быть установлен .net framework 4.8.

Загрузите и распакуйте архив на сервер.

Скопируйте все файлы из папки в каталог в C:\Program Files\Microsoft\Exchange Server\V15\ClientAccess\ecp\Bin\. Если какой-то из файлов требует перезаписи, то может возникнуть конфликт с другими установленными плагинами.

Сделайте резервную копию файла конфигурации C:\Program Files\Microsoft\Exchange Server\V15\ClientAccess\ecp\web.config для возможности восстановления первоначального состояния.

Откройте web.config для редактирования и добавьте в него следующие строчки:

Внутрь раздела <modules>

```
<modules>
    …
    <add name="BitAuthIISModule" type="BitAuthIIS.BitAuthIISModule" />
    …
</modules>
```

Внутрь раздела <appSettings>

```
<appSettings>
    …
    <add key="BitAuth:Resource" value="ecp" />
    <add key="BitAuth:ResourceUrl" value="https://адрес почты/ecp" />
    <add key="BitAuth:SecurityCenter" value="адрес портала" />
    <add key="BitAuth:BypassWhenUnreachable" value="true" />
    …
  </appSettings>
```

Где,

Параметр BitAuth:Resource соответствует названию ресурса на портале, который будете создавать далее.

value="https://адрес почты/ecp" – адрес почты.

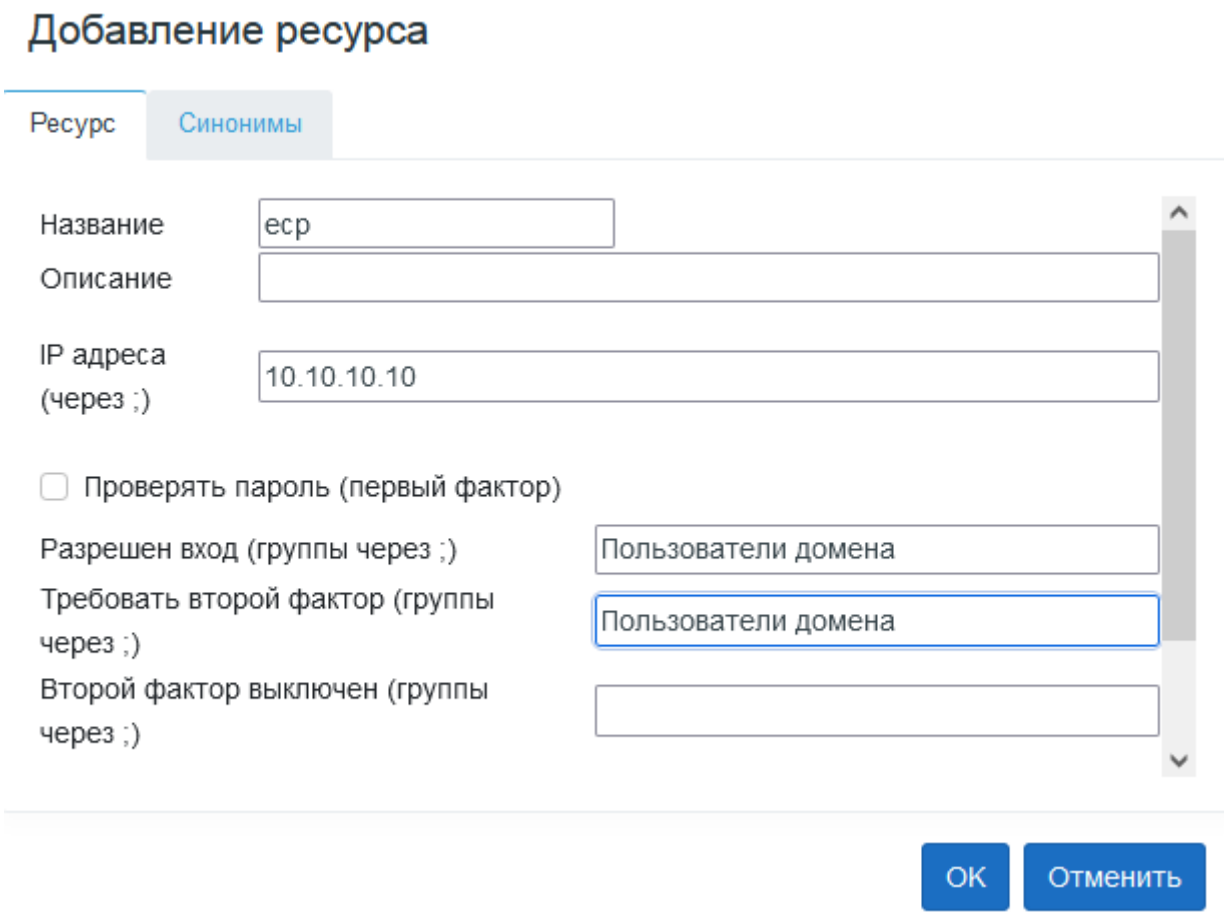
value="адрес портала" – адрес Вашего портала.

Сохраните web.config и перезапустите Exchange.

Настройка на сервере завершена.

Настройки на портале

Добавьте новый ресурс на портале:



Укажите имя ресурса, которое указали в параметре BitAuth:Resource при редактировании web.config. Описание по желанию и IP адрес сервера.

Укажите группы пользователей из Active Directory для которых:

Разрешен вход (группы через ;) – Будет разрешен вход на данный ресурс.

Требовать второй фактор (группы через ;) – Проверка второго фактора обязательна.

Второй фактор отключен (группы через ;) – Проверка 2FA будет отключена.

5. **Настройка IIS (Internet Information Services) для Exchange OWA (Outlook Web Application).**

Для корректной работы должен быть установлен .net framework 4.8.

Загрузите и распакуйте архив на сервер.

Скопируйте все файлы из папки в каталог C:\Program Files\Microsoft\Exchange Server\V15\ClientAccess\Owa\Bin\. Если какой-то из файлов требует перезаписи, то может возникнуть конфликт с другими установленными плагинами.

Сделайте резервную копию файла конфигурации C:\Program Files\Microsoft\Exchange Server\V15\ClientAccess\Owa\web.config для возможности восстановления первоначального состояния.

Откройте web.config для редактирования и добавьте в него следующие строчки:

Внутрь раздела <modules>

```
<modules>
    …
    <add name="BitAuthIISModule" type="BitAuthIIS.BitAuthIISModule" />
    …
</modules>
```

Внутрь раздела <appSettings>

```
<appSettings>
    …
    <add key="BitAuth:Resource" value="OWA" />
    <add key="BitAuth:ResourceUrl" value="https://адрес почты/owa" />
    <add key="BitAuth:SecurityCenter" value="адрес портала" />
    <add key="BitAuth:BypassWhenUnreachable" value="true" />
    …
  </appSettings>
```

Где,

Параметр BitAuth:Resource должен соответствовать названию ресурса на портале, который будете создавать далее.

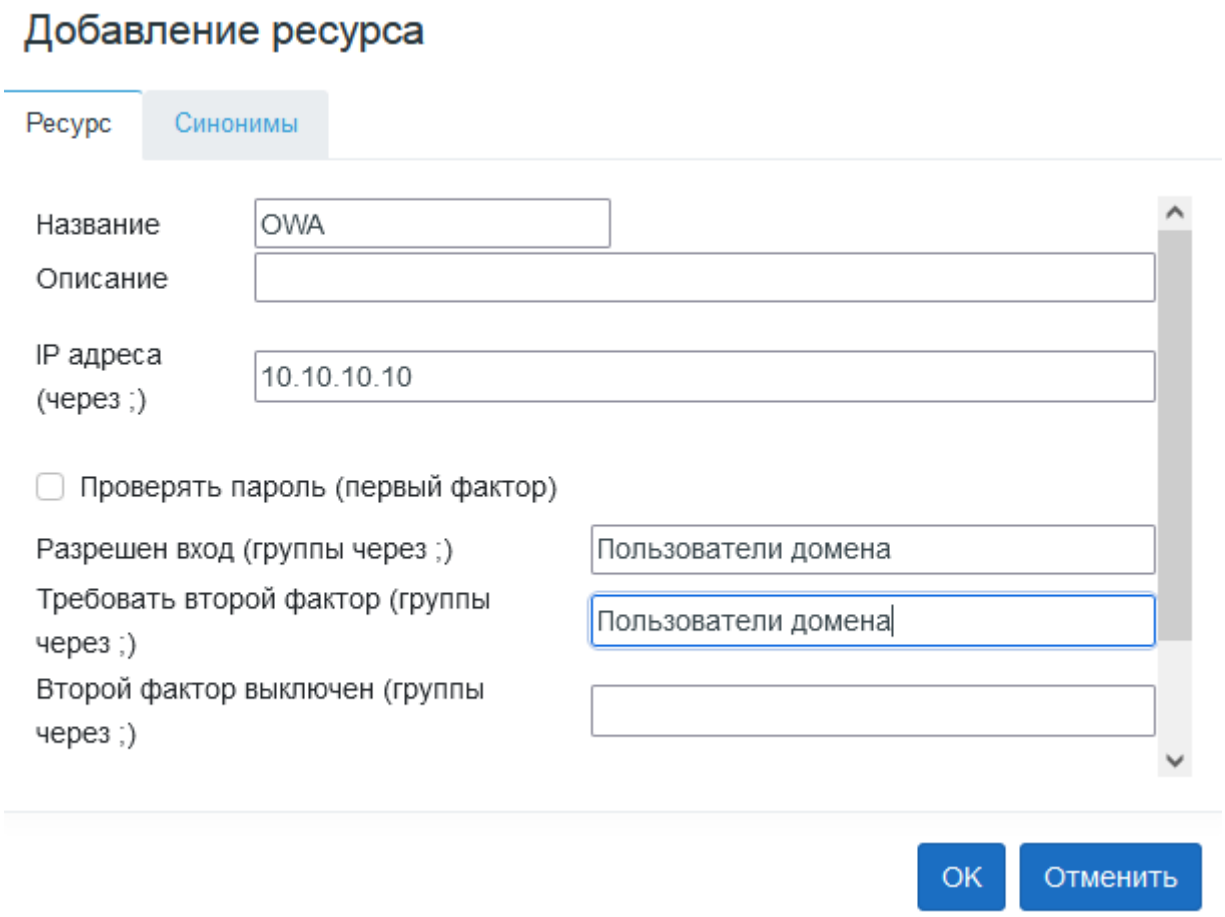
value="https://адрес почты/owa " – адрес почты.

value="https://адрес портала" – адрес Вашего портала.

Сохраните web.config и перезапустите Exchange.

Настойки на портале

Добавьте новый ресурс на портале:



Укажите имя ресурса, которое указали в параметре BitAuth:Resource при редактировании web.config. Описание по желанию и IP адрес сервера iis.

Укажите группы пользователей из Active Directory для которых:

Разрешен вход (группы через ;) – Будет разрешен вход на данный ресурс.

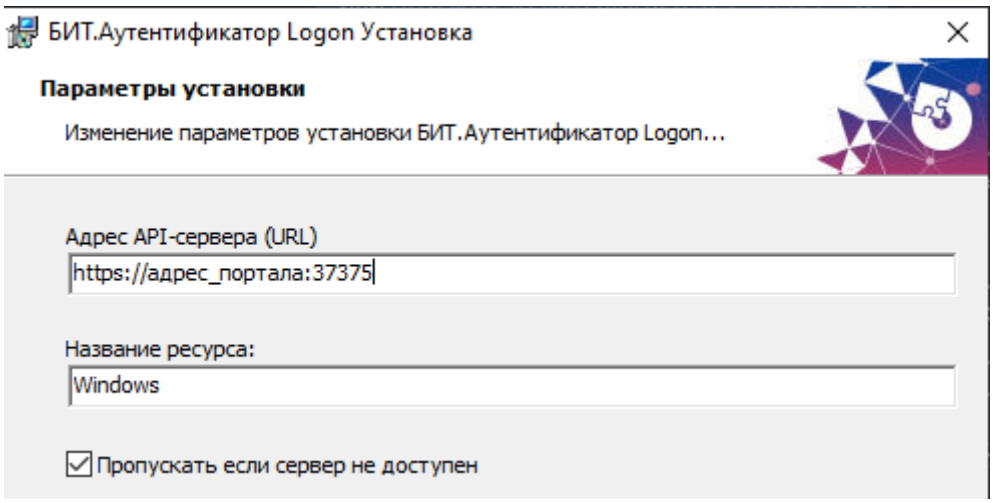
Требовать второй фактор (группы через ;) – Проверка второго фактора обязательна.

Второй фактор отключен (группы через ;) – Проверка 2FA будет отключена.

6. **Настройка для RDP при интеграции с доменом (AD).**

Загрузите и распакуйте архив на сервер.

Запустите установщик BitAuthLogon, укажите место установки, нажмите далее.

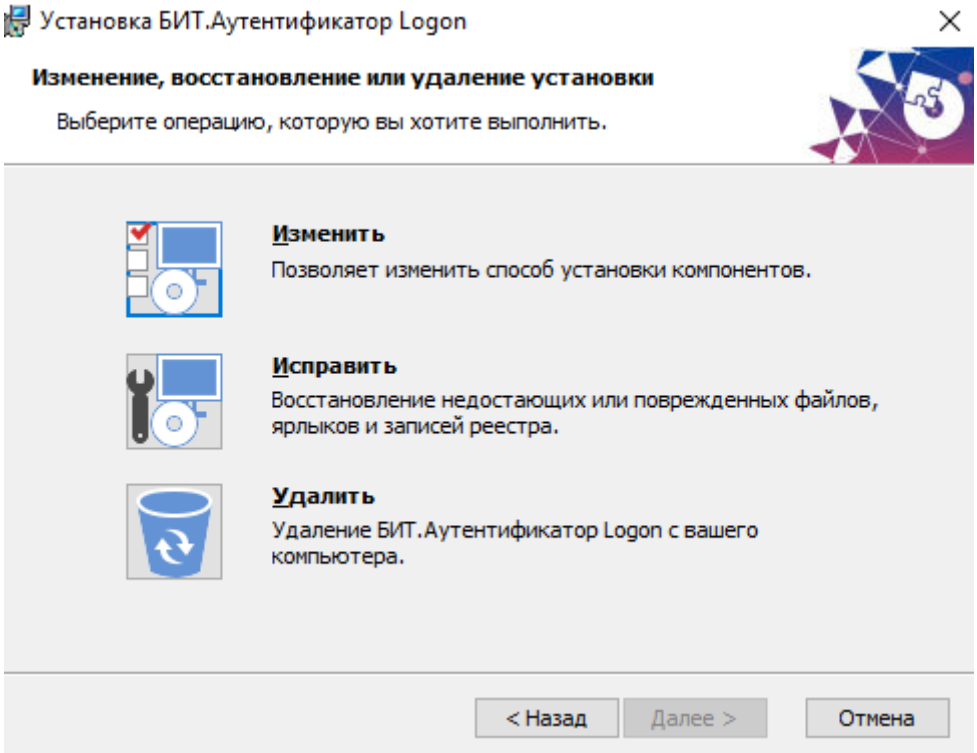


Адрес API сервера (URL) – укажите адрес Вашего портала с портом 37375.

Название ресурса – укажите название ресурса, оно должно совпадать с названием ресурса, который далее будете создавать на портале.

После установки может потребоваться перезагрузка ПК.

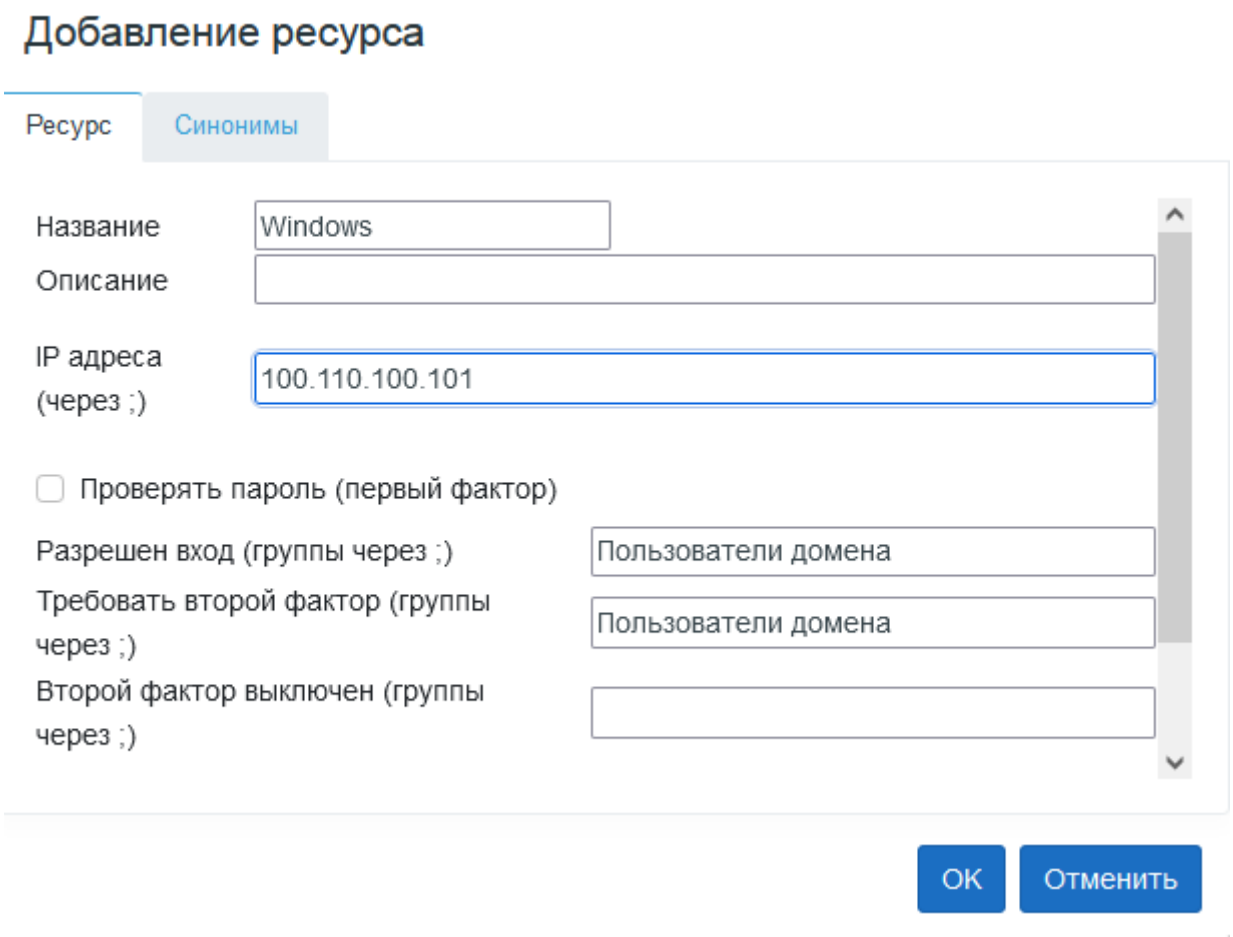
Для удаления или изменения параметров установки, повторно запустите установщик BitAuthLogon и выберите необходимый пункт.



Настройки на портале

Зайдите на портал под владельцем или администратором организации.

Добавьте новый ресурс:



Укажите имя ресурса, которое указали ранее в названии ресурса при установке BitAuthLogon. Описание по желанию и IP адрес целевого сервера.

Укажите группы пользователей из Active Directory для которых:

Разрешен вход (группы через ;) – Будет разрешен вход на данный ресурс.

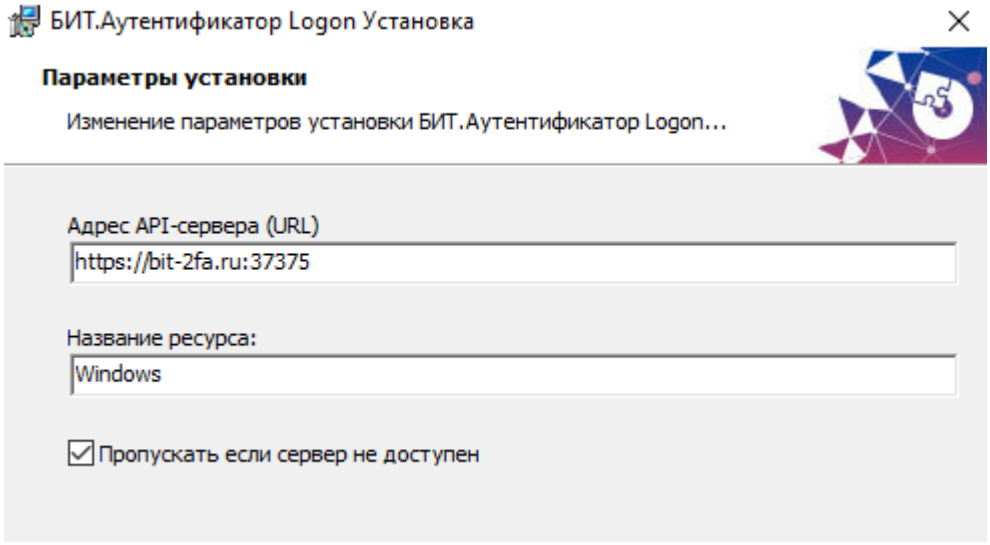
Требовать второй фактор (группы через ;) – Проверка второго фактора обязательна.

Второй фактор отключен (группы через ;) – Проверка 2FA будет отключена.

7. **Настройка для RDP без интеграции с доменом (AD).**

Загрузите и распакуйте архив на сервер.

Запустите установщик BitAuthLogon, укажите место установки и нажмите далее.

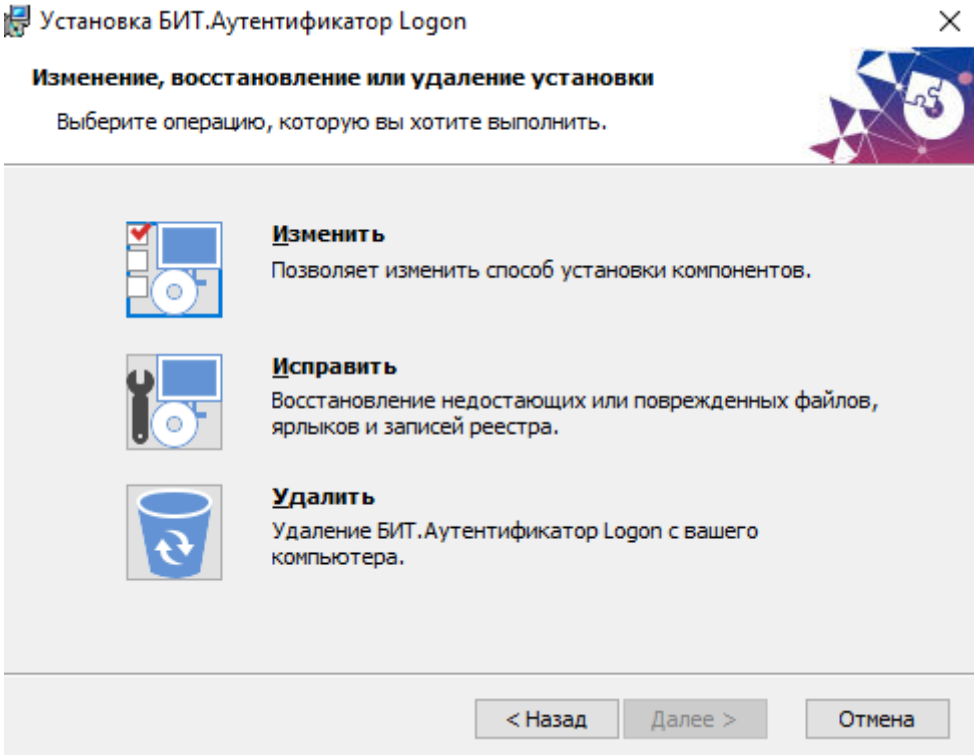


Адрес API сервера (URL) – укажите адрес портала https://bit-2fa.ru:37375.

Название ресурса – укажите название ресурса, оно должно совпадать с названием ресурса, который далее будете создавать на портале.

После установки может потребоваться перезагрузка ПК.

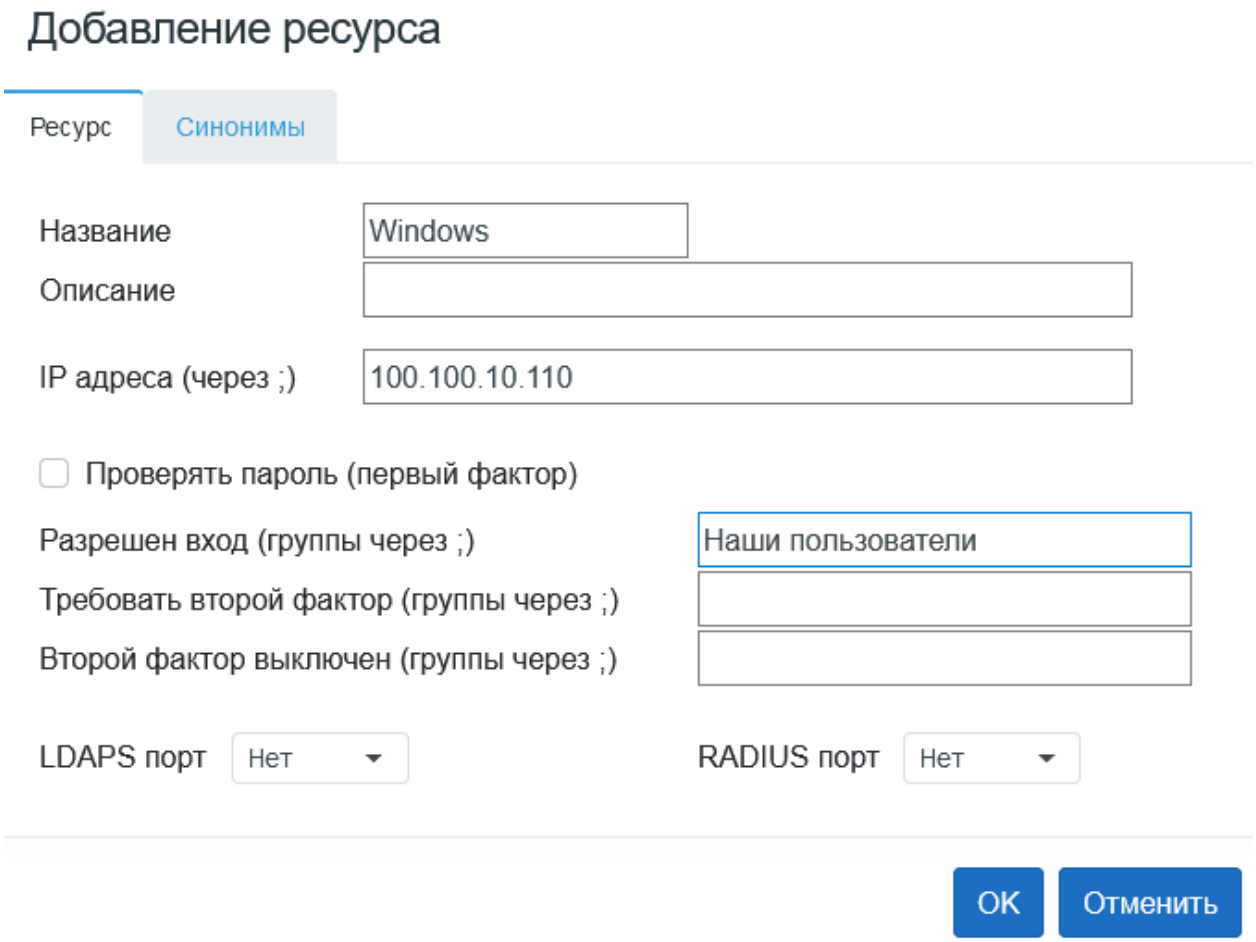
Для удаления или изменения параметров установки, повторно запустите установщик BitAuthLogon и выберите необходимый пункт.



Настройки на портале

Зайдите на портал https://bit-2fa.ru под владельцем или администратором организации.

Добавьте новый ресурс:



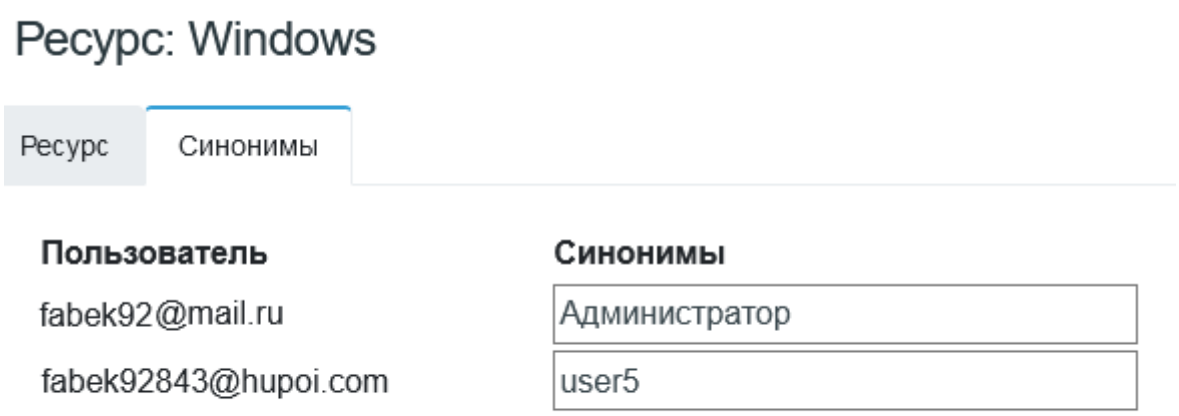
Укажите имя ресурса, которое указали ранее в названии ресурса при установке BitAuthLogon. Описание по желанию и IP адрес целевого сервера.

Разрешен вход (группы через ;) – группы, для которых разрешен вход на ресурс. Можно указать всех пользователей из списка в разделе "Пользователи" - группа Наши пользователи.

Требовать второй фактор (группы через ;) – Указываются группы пользователей, для которых проверка второго фактора обязательна.

Второй фактор отключен (группы через ;) – Указываются группы пользователей, для которых проверка второго фактора будет отключена.

Перейдите на вкладку синонимы:



Тут будет выведен весь список добавленных пользователей организации.

Каждый пользователь удаленного рабочего стола должен быть добавлен в поле синоним соответствующему сотруднику. Пользователь – почта сотрудника при регистрации на портале, синоним – логин подключения к серверу. Это требуется для отправки запроса на устройство соответствующего пользователя.

8. **Настройка для SSH.**

На ВМ установите пакет, добавляющий возможность использовать радиус в Pam, на примере убунту: libpam-radius-auth.

Внесите изменения в файл конфигурации: /etc/pam_radius_auth.conf

Добавьте строку:

host SECRET 40

где:

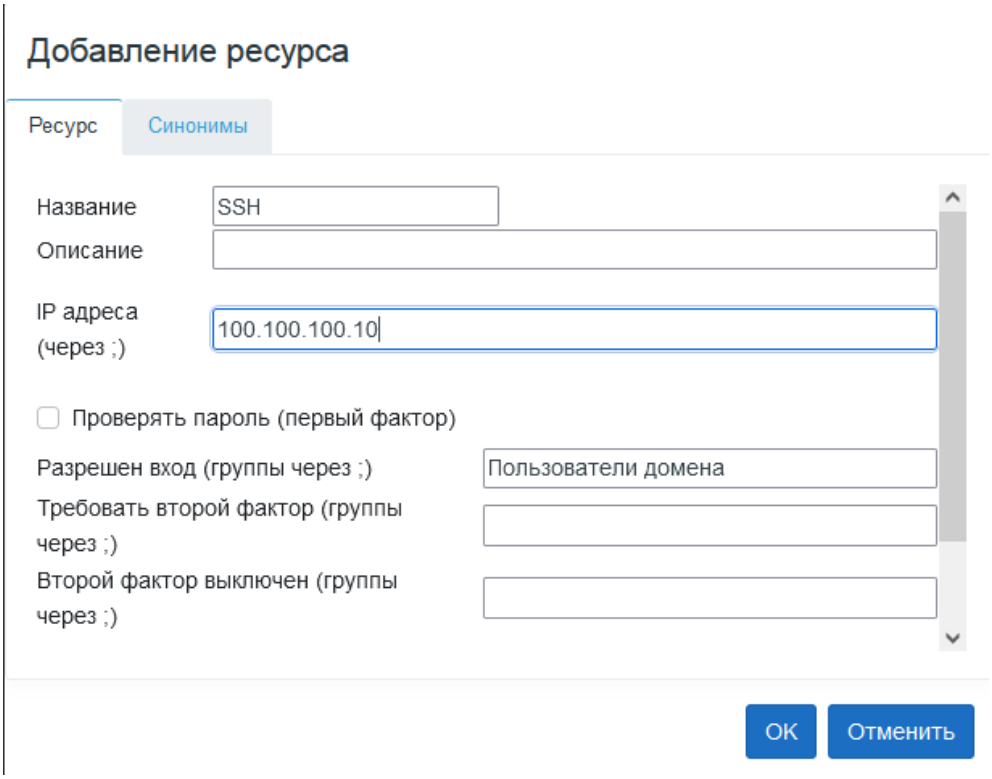
- host: адрес портала;
- SECRET: Общий секрет RADIUS в настройках портала;
- 40: таймаут ожидания запроса с запасом.

Далее внесите изменения в конфигурацию Pam для ssh, файл /etc/pam.d/sshd

Добавьте следующую строку ниже обычной авторизации, чтобы проверка второго фактора выполнялось только после успешного выполнения первого:

auth [success=done default=bad authinfo_unavail=bad ignore=ignore] pam_radius_auth.so localifdown

На портале создайте новый ресурс:



Укажите название, ip адрес целевого ПК и описание по желанию.

Укажите группы пользователей из Active Directory для которых:

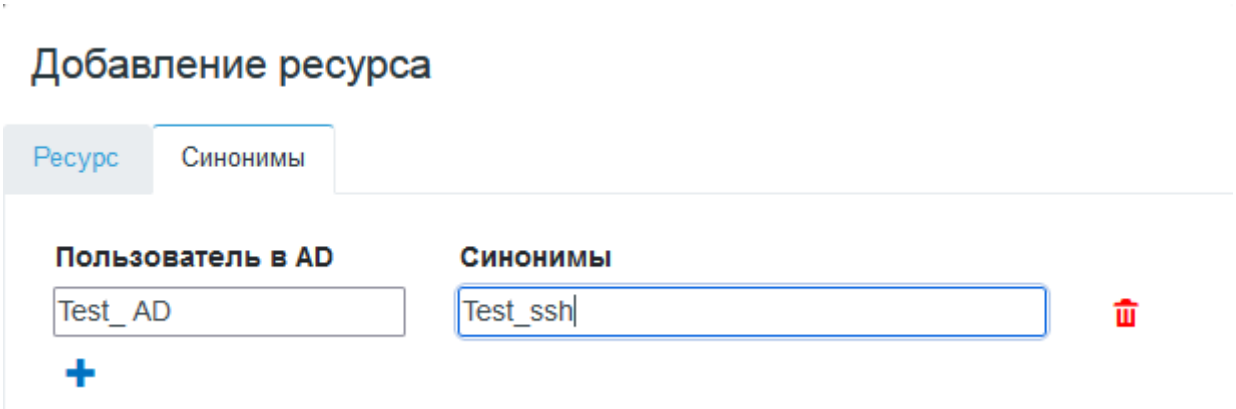
Разрешен вход (группы через ;) – Будет разрешен вход на данный ресурс.

Требовать второй фактор (группы через ;) – Проверка второго фактора обязательна.

Второй фактор отключен (группы через ;) – Проверка 2FA будет отключена.

Укажите порт RADIUS, по умолчанию 1812.

На вкладке синонимы, есть возможность привязать пользователя из AD к пользователю на целевой ВМ:



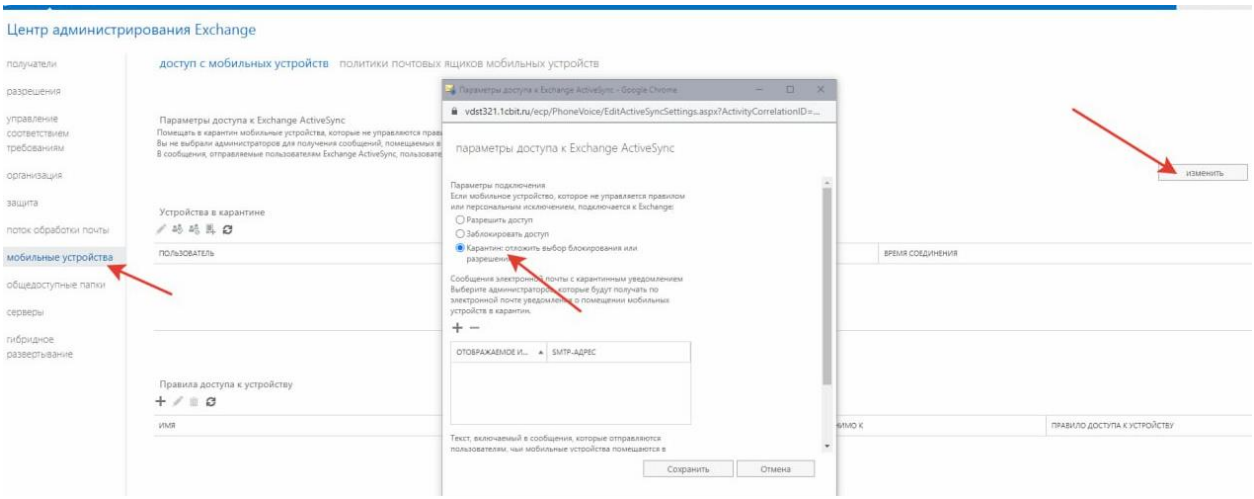
Т.е. при подключении к ВМ под пользователем «Test_ssh» проверка второго фактора будет запрошена у пользователя из AD «Test_ AD».

9. Настройка для Exchange ActiveSync.

Откройте Центр администрирования Exchange.

Перейдите в раздел «Мобильные устройства».

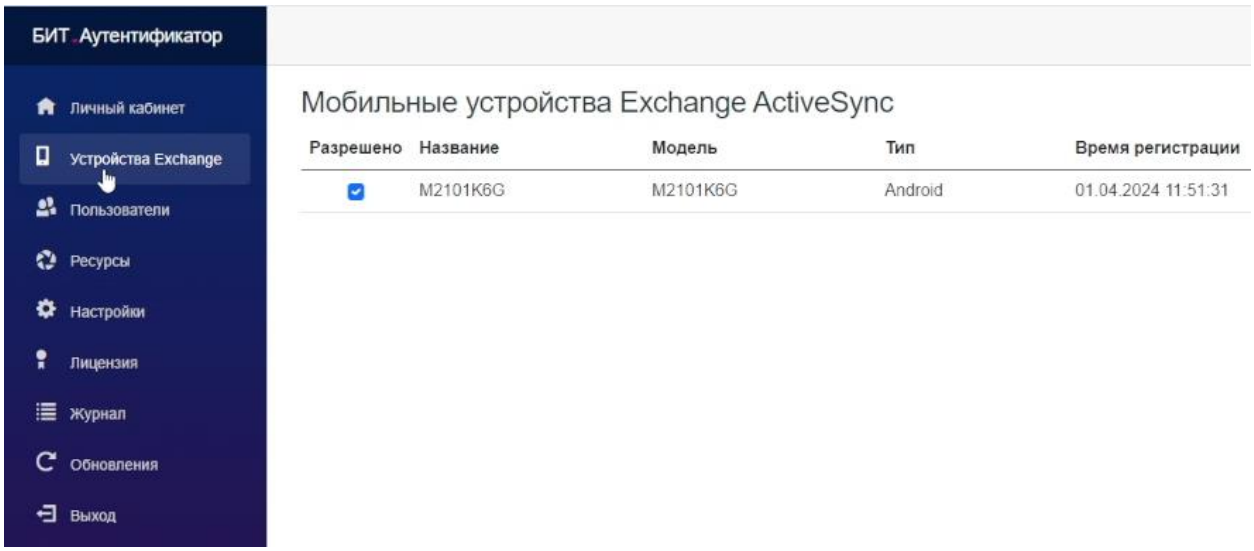
Нажмите «Изменить».



В параметрах подключения выберите «Карантин: отложить выбор блокирования или разрешения».

Использовав +, можно добавить пользователей (администраторов), кому на почту будет отправлены сообщения о помещении в карантин, для последующего разрешения входа на портале.

Настройки на портале



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

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

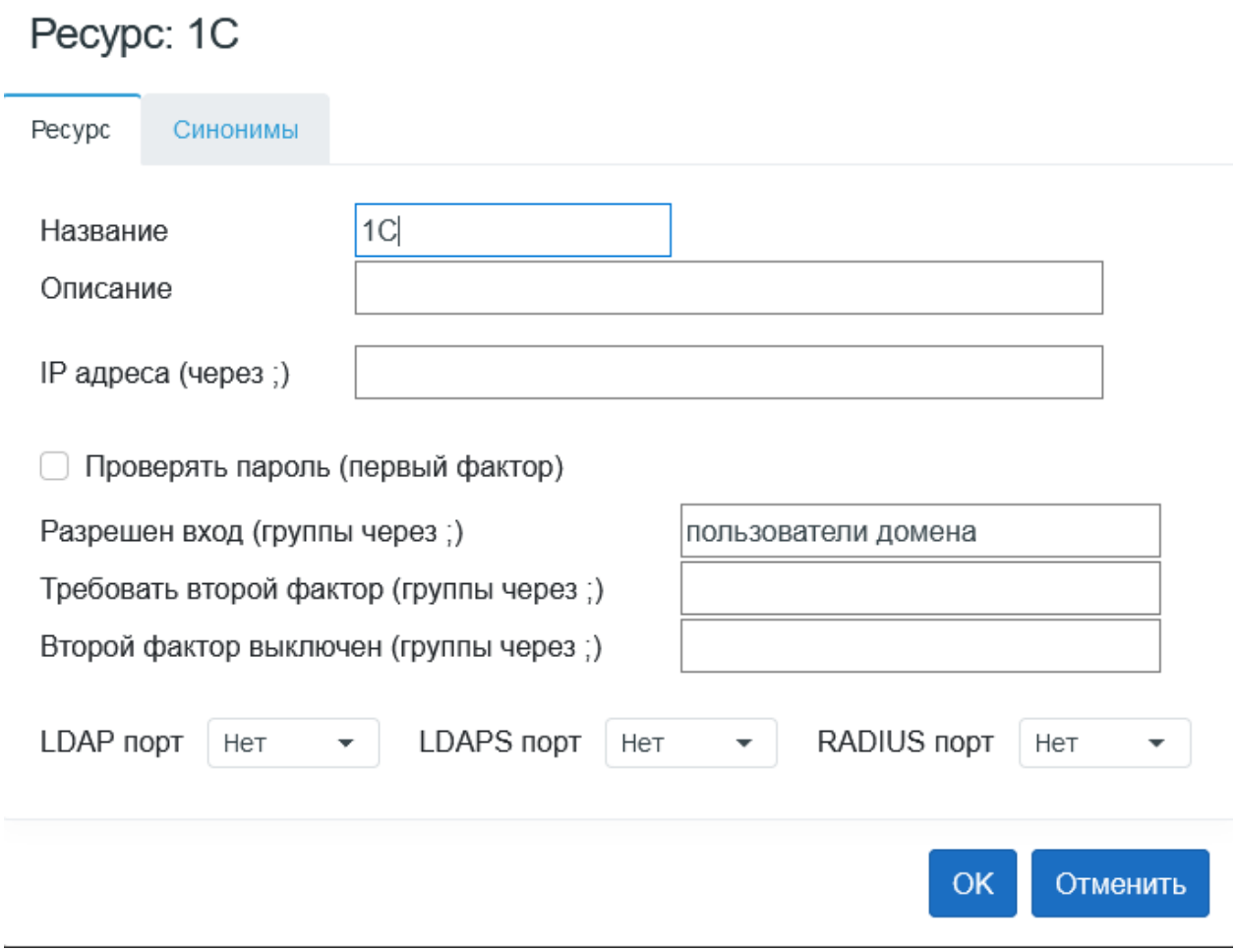
После настройки почты на мобильном устройстве оно появится в данной вкладке.

Для разрешения подключения необходимо администратору или владельцу портала разрешить подключение. После чего почта будет доступна на мобильном устройстве.

На этой вкладке предоставлена информация об устройстве, с которого происходит подключение, его тип и дату регистрации.

10. Настройка для базы 1С при интеграции с доменом (AD).

На портале БИТ.Аутентификатор добавьте ресурс.



Название – имя ресурса, оно будет требоваться в дальнейшем, при настройке расширения в базе 1С.

Описание - по усмотрению.

IP адреса – оставляем поле пустым.

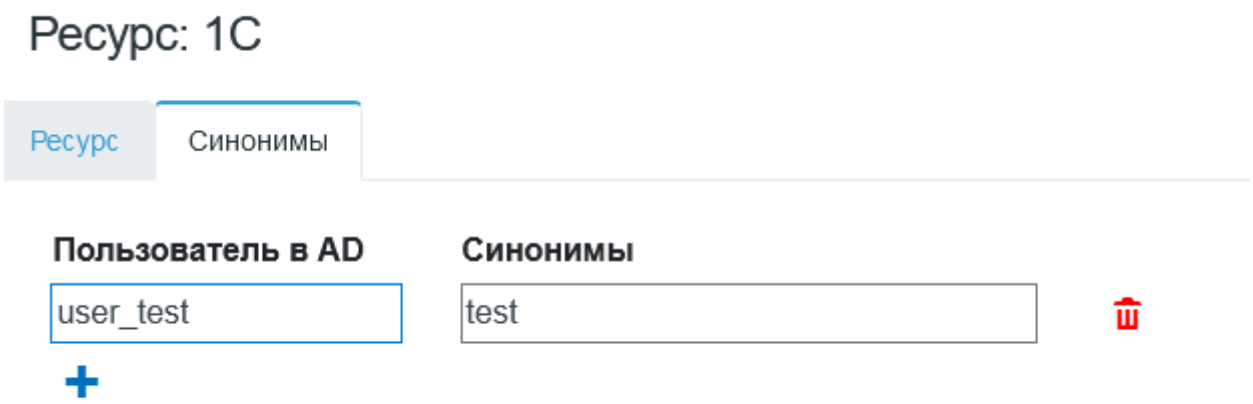
Разрешен вход (группы через ;) – Указываются группы пользователей, для которых будет разрешен вход на данный ресурс.

Требовать второй фактор (группы через ;) – Указываются группы пользователей, для которых проверка второго фактора обязательна.

Второй фактор отключен (группы через ;) – Указываются группы пользователей,

для которых проверка будет отключена.

Перейдите на вкладку синонимы:



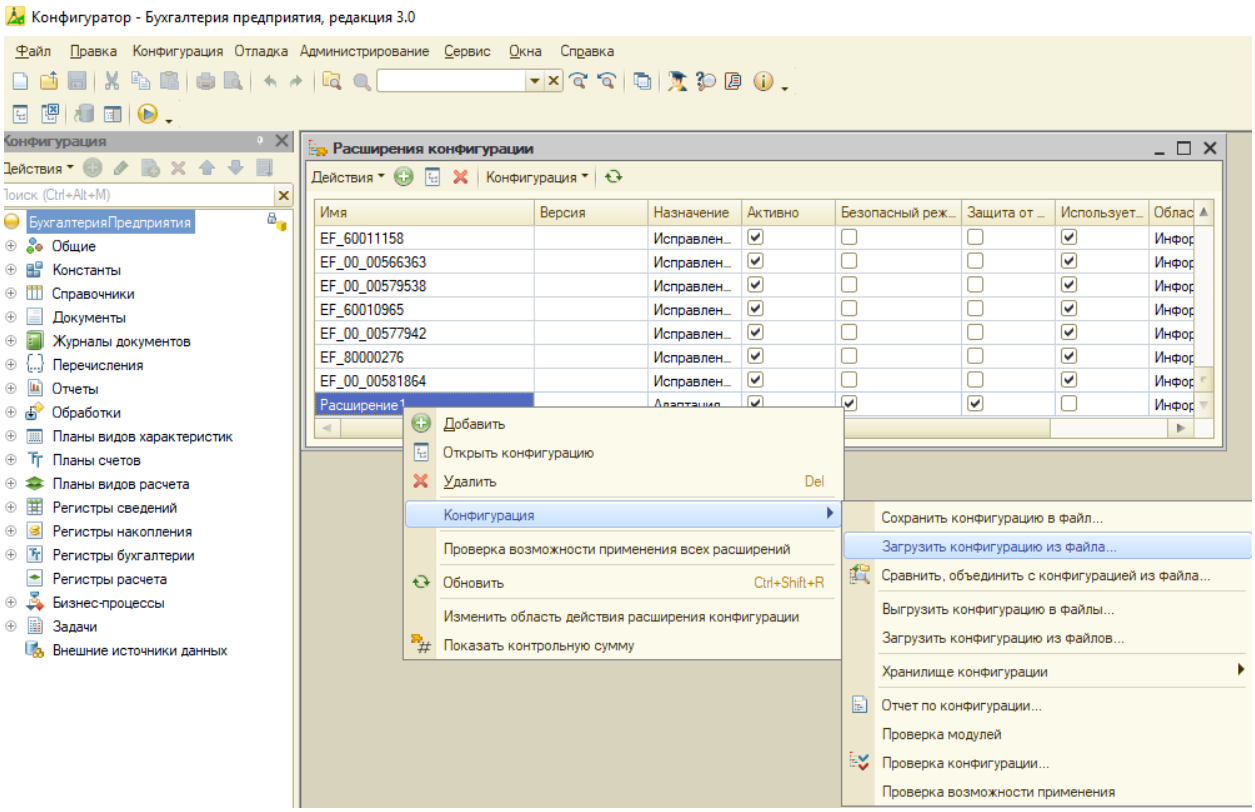
Необходимо добавить и сопоставить пользователей 1С и пользователей домена, в поле «Синоним» внесите пользователя базы 1С, в поле «Пользователь в AD» логин доменного пользователя.

Каждый пользователь базы 1С должен быть добавлен в поле синоним соответствующему пользователю из AD. Это требуется для отправки запроса на устройство соответствующего пользователя.

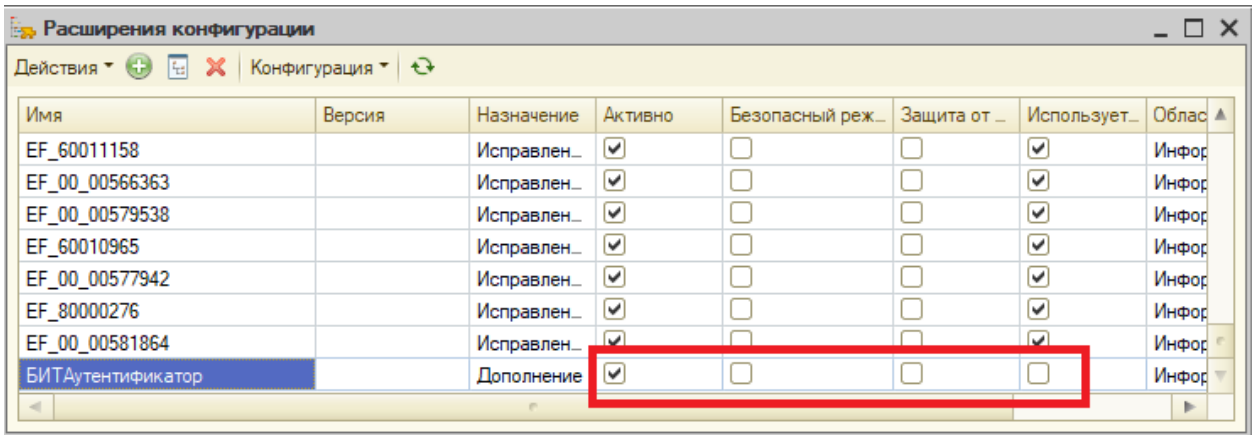
Если баз на сервере несколько, а пользователи в базах различаются, то для каждой из баз необходимо создать новый ресурс, с другим именем, которое в дальнейшем указывается в настройках расширения 1С.

Настройки в базе 1С

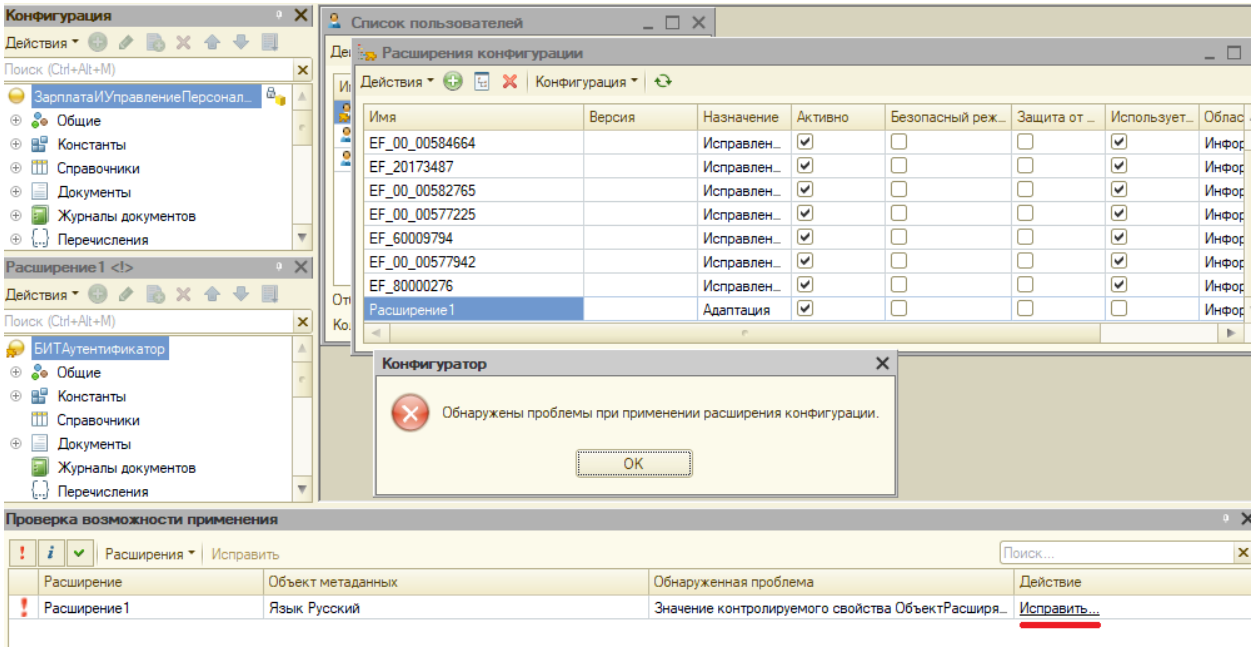
Скачайте расширение для базы 1С. Откройте конфигуратор – расширения конфигурации. Добавьте расширение. Загрузите из файла, выбрав ранее скаченное расширение:



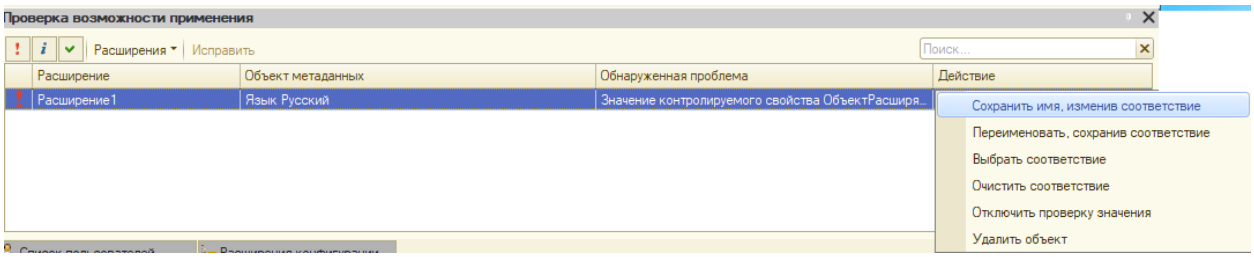
Уберите галки для безопасного режима и защиты от опасных действий:



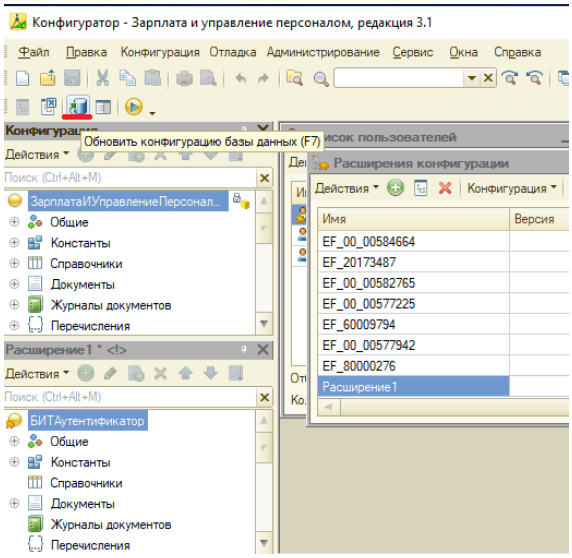
При установке расширения может возникнуть ошибка:



Нажмите исправить – Сохранить имя, изменив соответствие.

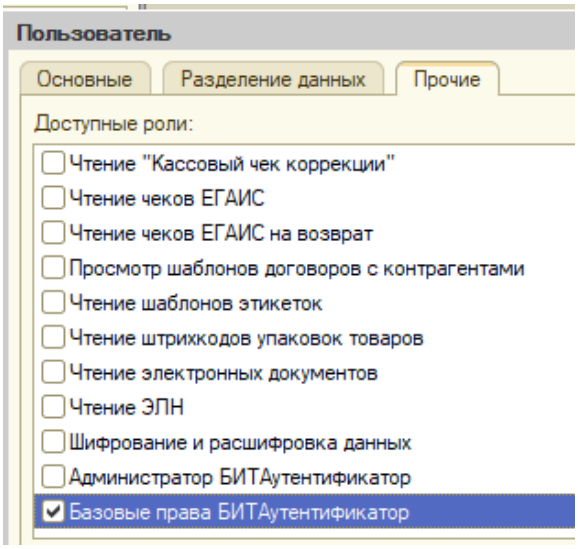


Обновите конфигурацию базы данных (F7 или по значку, указанному ниже).

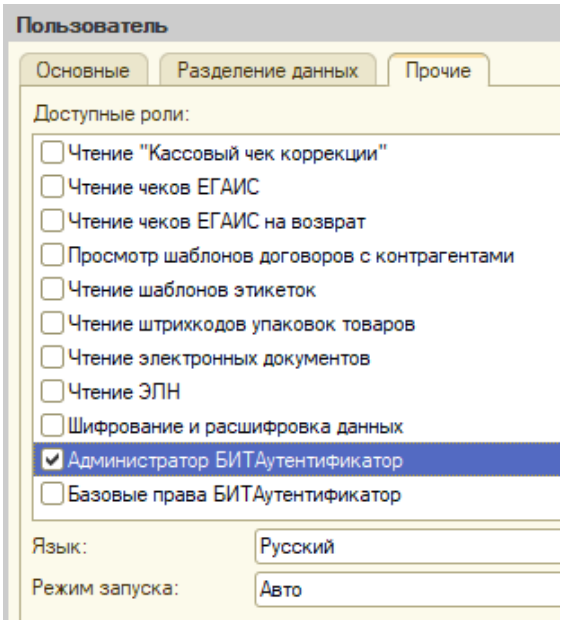


Для некоторых конфигураций может понадобится добавить роли всем пользователям базы.

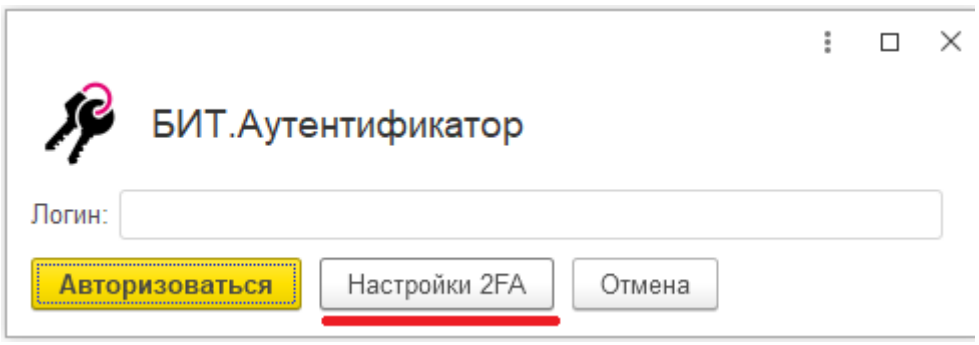
Откройте конфигуратор, пользователи, выберите пользователя, вкладка прочие, установите роль «Базовые права БИТАутентификатор».



Для возможности изменения настроек 2FA или его отключения в базе 1С в режиме предприятия, пользователю необходимо назначить соответствующую роль. Откройте конфигуратор, пользователи, выберите пользователя, кому будут доступны настройки, вкладка прочие, установите роль «Администратор БИТАутентификатор».

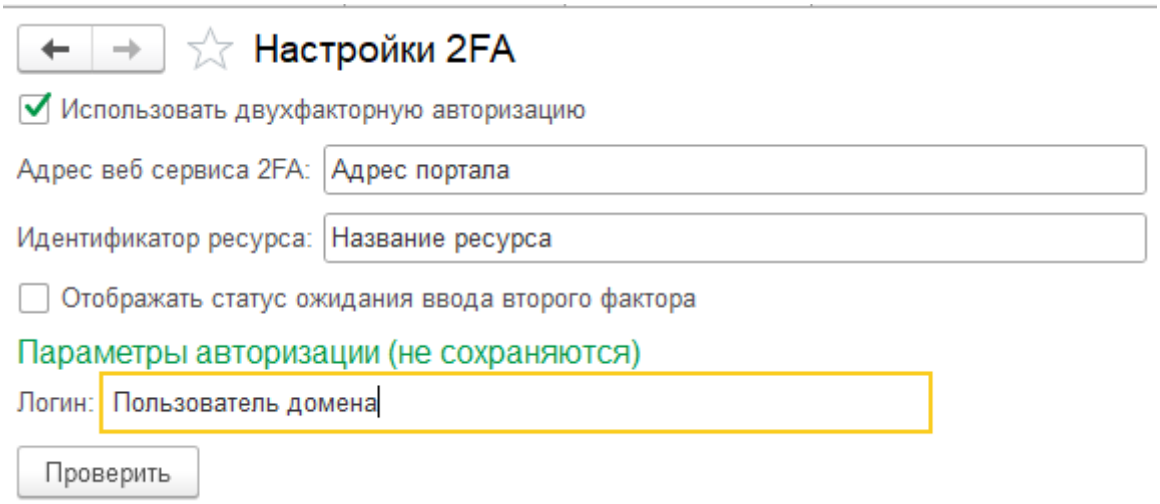


Теперь при входе под этим пользователем появится возможность изменения настроек до подтверждения второго фактора.



Для удаления расширения из базы 1С выберите его из списка установленных расширений, снимите галку напротив активно и нажмите удалить.

Запустите базу в предприятии под пользователем с административными правами, в основном меню появится вкладка БИТ.Аутентификатор. Включите использование двухфакторной авторизации.



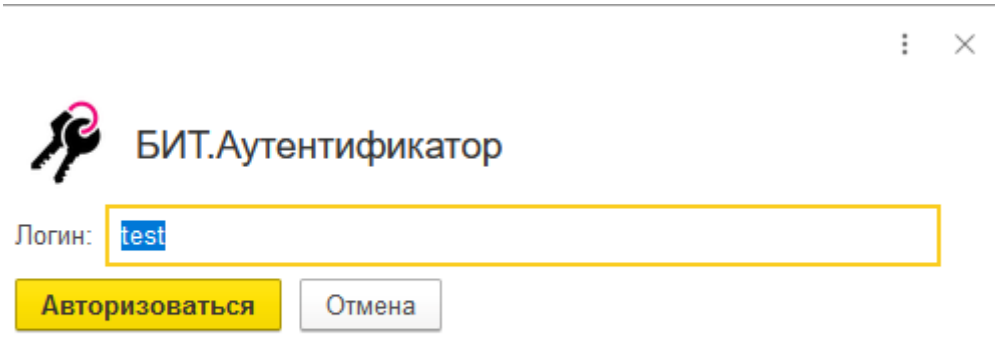
Адрес веб сервисов 2FA – укажите адрес портала.

Идентификатор ресурса – укажите название ресурса, созданного ранее.

Логин для проверки – укажите пользователя AD.

Проверьте настройки. Если все настроено правильно, то соответствующему пользователю придет запрос проверки второго фактора.

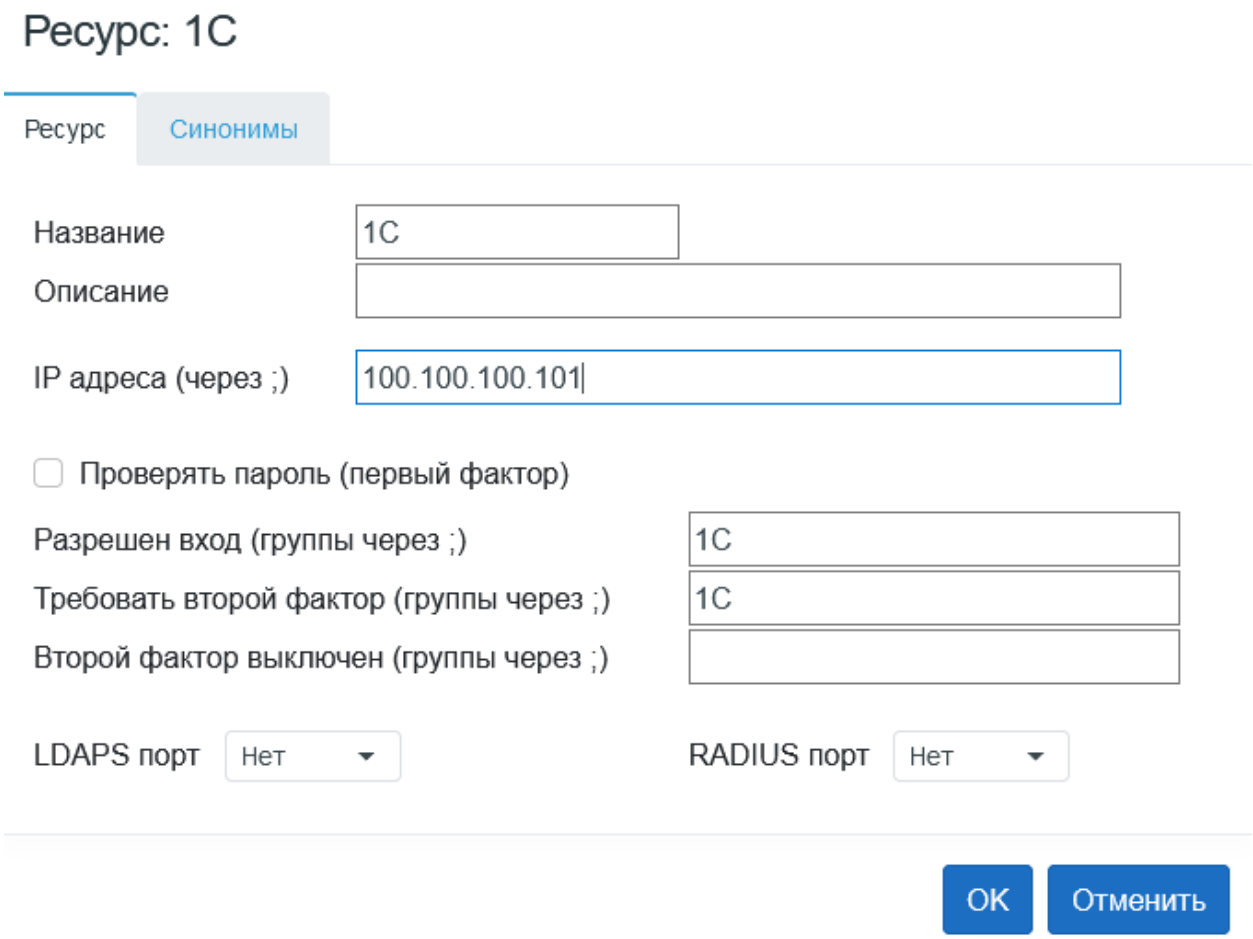
После того как пользователь введет свой пароль от базы 1С будет запрошен второй фактор пользователя из AD, которому был назначен синоним test (пользователь базы 1С).



После подтверждения база запустится.

11. Настройка для базы 1С без интеграции с доменом (AD).

На портале bit-2fa.ru добавьте новый ресурс.



Название – имя ресурса, оно будет требоваться в дальнейшем, при настройке расширения в базе 1С.

Описание - по усмотрению.

IP адреса – указывается ip адрес сервера, где располагается база данных 1С.

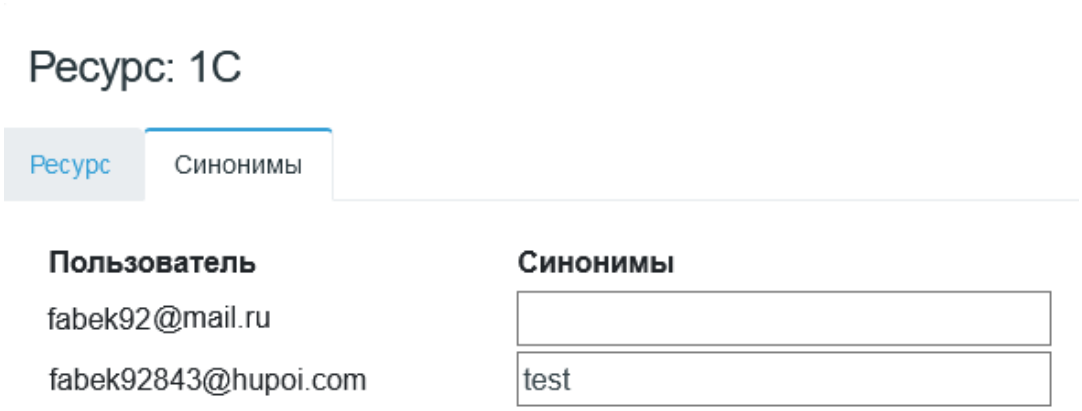
Разрешен вход (группы через ;) – Указываются группы пользователей, для которых будет разрешен вход на данный ресурс.

Требовать второй фактор (группы через ;) – Указываются группы пользователей, для которых проверка второго фактора обязательна.

Второй фактор отключен (группы через ;) – Указываются группы пользователей

для которых проверка будет отключена.

Перейдите на вкладку синонимы:



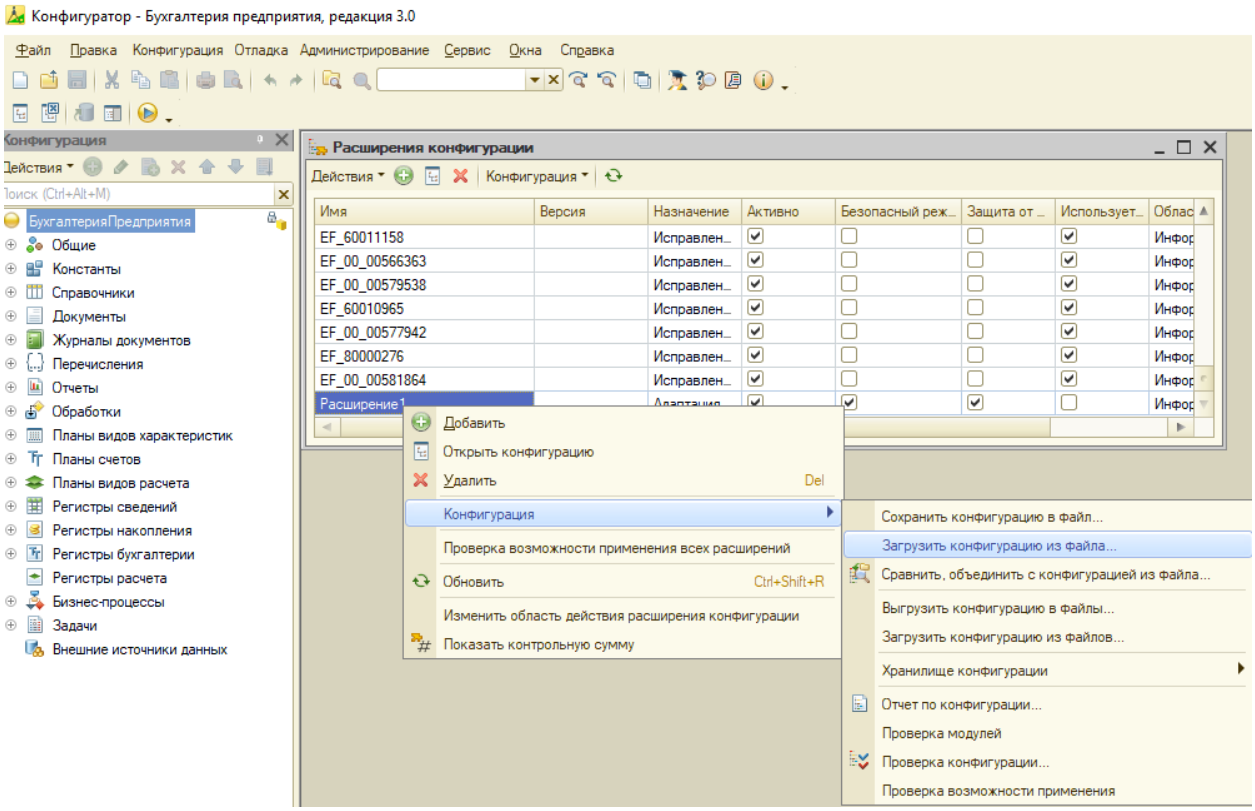
Тут будет выведен весь список добавленных пользователей организации.

Каждый пользователь базы 1С должен быть добавлен в поле синоним соответствующему сотруднику, который должен пройти регистрацию на портале https://bit-2fa.ru/. Это требуется для отправки запроса на устройство соответствующего пользователя.

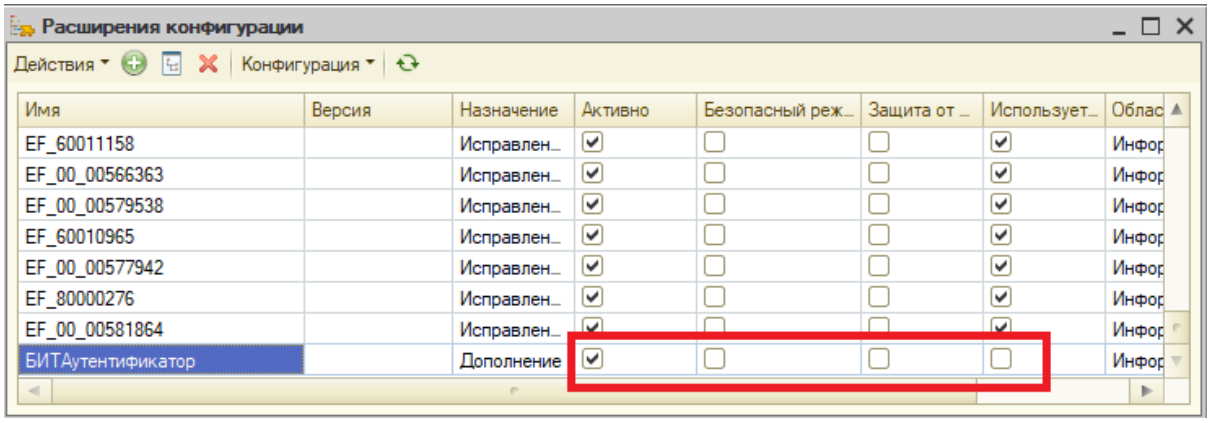
Если баз на сервере несколько, а пользователи в базах различаются, то для каждой из баз создается отдельный ресурс с уникальным названием.

Настройки в базе 1С

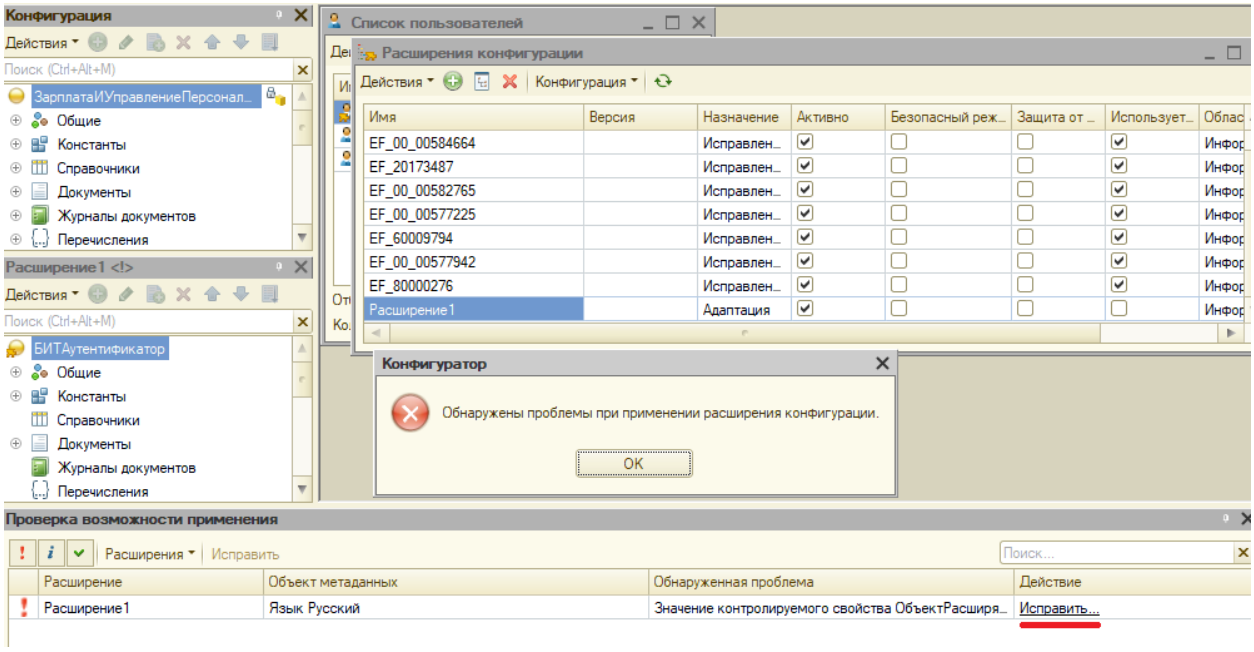
Скачайте расширение для базы 1С. Откройте конфигуратор – расширения конфигурации. Добавьте расширение. Загрузите из файла, выбрав ранее скаченное расширение:



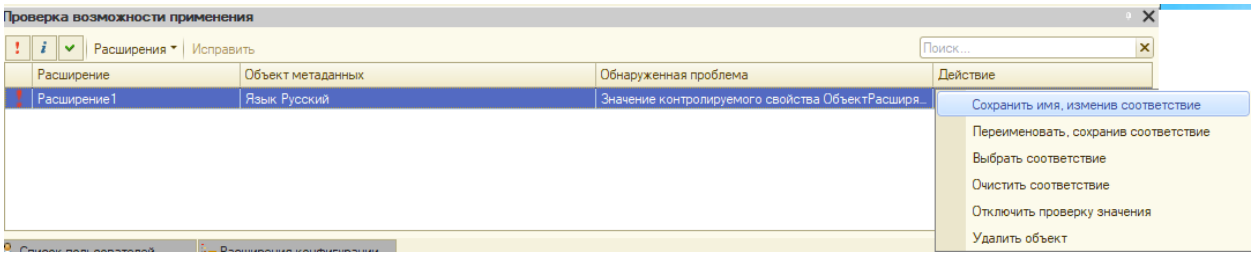
Уберите галки для безопасного режима и защиты от опасных действий:



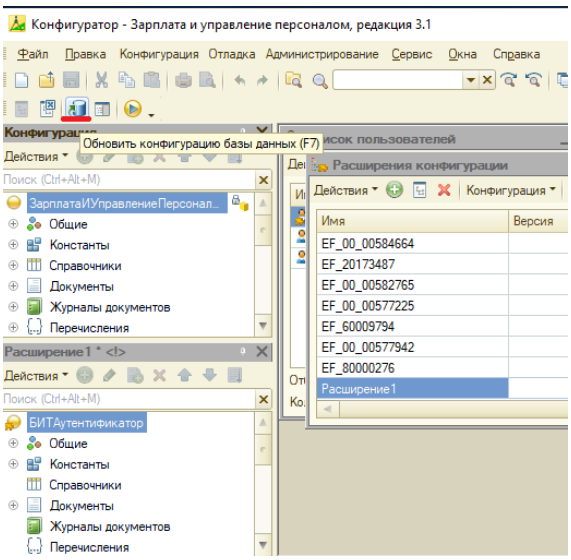
При установке расширения может возникнуть ошибка:



Нажмите исправить – Сохранить имя, изменив соответствие.

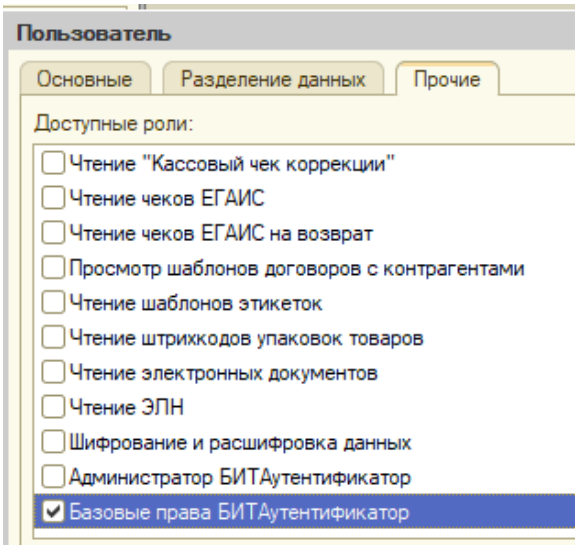


Обновите конфигурацию базы данных (F7 или по значку, указанному ниже).

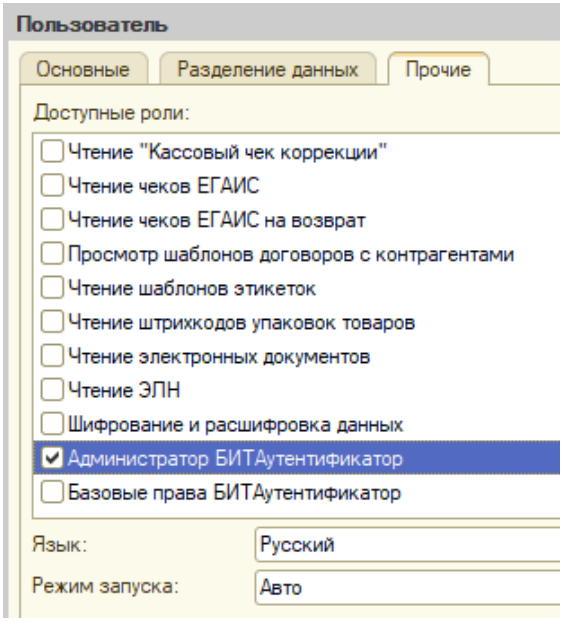


Для некоторых конфигураций может понадобится добавить роли всем пользователям базы.

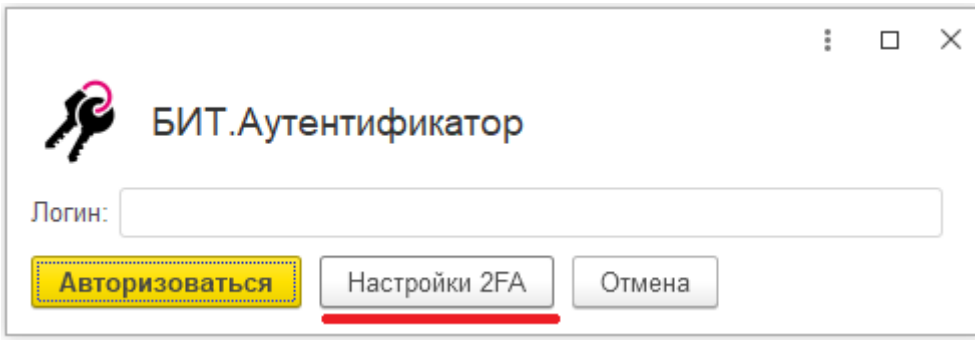
Откройте конфигуратор, пользователи, выберите пользователя, вкладка прочие, установите роль «Базовые права БИТАутентификатор».



Для возможности изменения настроек 2FA или его отключения в базе 1С в режиме предприятия, пользователю необходимо назначить соответствующую роль. Откройте конфигуратор, пользователи, выберите пользователя, кому будут доступны настройки, вкладка прочие, установите роль «Администратор БИТАутентификатор».

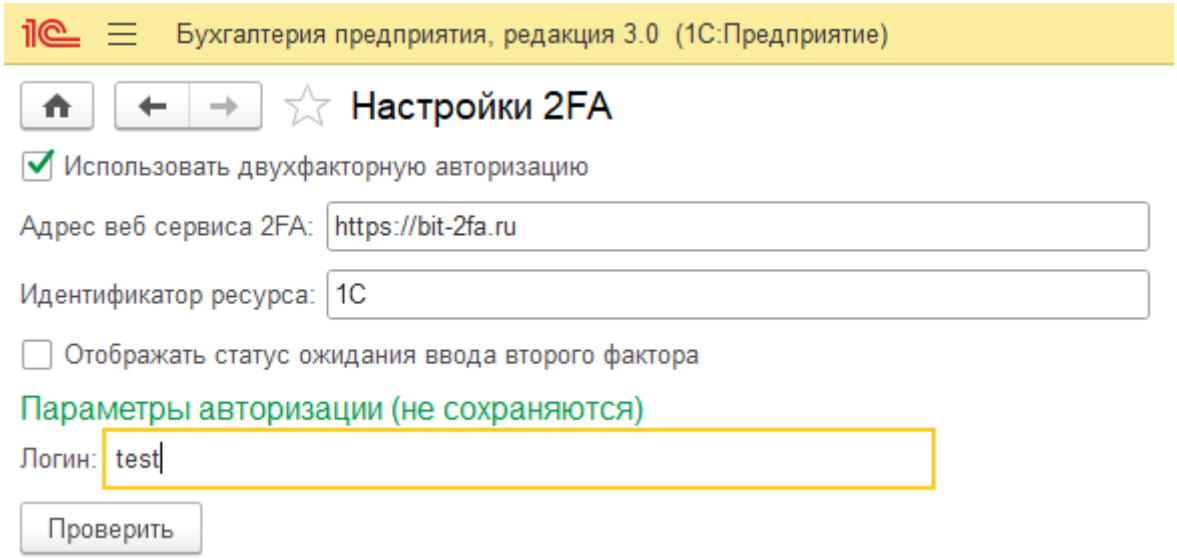


Теперь при входе под этим пользователем появится возможность изменения настроек до подтверждения второго фактора.



Для удаления расширения из базы 1С выберите его из списка установленных расширений, снимите галку напротив активно и нажмите удалить.

Запустите базу в предприятии под пользователем с административными правами, в основном меню появится вкладка БИТ.Аутентификатор. Включите использование двухфакторной авторизации.



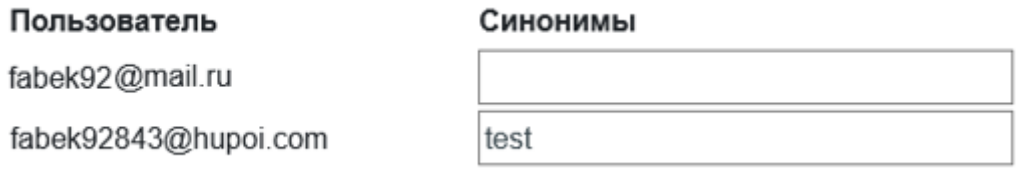
Адрес веб сервисов 2FA – укажите адрес портала - https://bit-2fa.ru

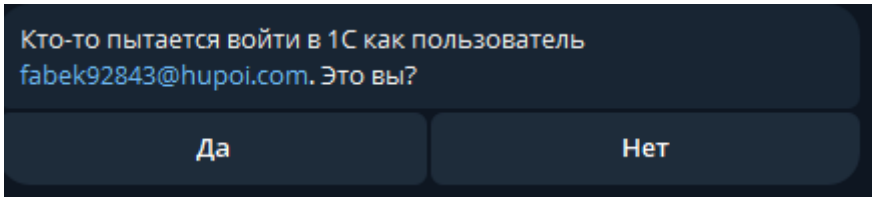
Идентификатор ресурса – укажите название ресурса, созданного ранее.

Логин – укажите синоним пользователя.

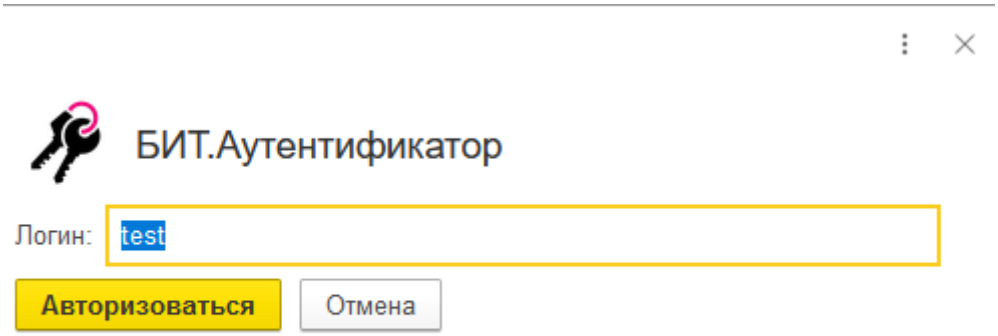
Проверьте настройки. Если все настроено правильно, то соответствующему пользователю придет запрос проверки второго фактора.

В нашем случае это пользователь fabek92843@hupoi.com, которому присвоен синоним пользователя test в базе 1С и выбран способ проверки Telegram.





После того как пользователь введет свой пароль от базы 1С будет запрошено подтверждение входа, для групп пользователей, которые указаны при создании ресурса.



После подтверждения база запустится

12. **Настройка для VPN (Virtual Private Network).**

Обновите систему: **sudo apt-get update && sudo apt-get diss-upgrade**

Перегрузите систему: **sudo reboot**

Удалите ненужные пакеты: **sudo apt autoremove**

Скачайте скрипт быстрой установки vpn: **curl -O https://raw.githubusercontent.com/angristan/openvpn-install/master/openvpn-install.sh**

Сделайте его исполняемым: **chmod +x openvpn-install.sh**

Запустите, установите: **sudo ./openvpn-install.sh**

Установите нужную библиотеку радиус-авторизации: **sudo apt-get install libpam-radius-auth**

Создайте конфиг: **sudo nano /etc/openvpn/server/pam_radius_auth.conf**

Содержимое (менять первый параметр и второй по мере

надобности/цели):***SERVERADDRESS SERVERKEY*** 30

Создайте конфиг: **sudo nano /etc/pam.d/openvpn**

Содержимое:

auth [success=1 default=ignore] pam_radius_auth.so conf=/etc/openvpn/server/

pam_radius_auth.conf

auth requisite pam_deny.so

auth required pam_permit.so

account required pam_permit.so

Откройте конфиг: **sudo nano /etc/openvpn/server.conf**

Приведите примерно к такому виду, имена сертификатов уникальны:

port
1194
proto
udp dev
tun
persist-
key
persist-
tun
keepalive 10
120topology
subnet
server 10.8.0.0 255.255.255.0
dh none
tls-crypt tls-
crypt.key crl-verify
crl.pem
ca ca.crt
cert
server_***o7UFcDRJOctNV1Pk***.crt
key
server_***o7UFcDRJOctNV1Pk***.key
auth SHA256
cipher AES-256-
CBCverb 3
explicit-exit-notify
mute-replay-
warningsduplicate-
cn

log /var/log/openvpn.log

setenv deferred_auth_pam 1
plugin /usr/lib/x86_64-linux-gnu/openvpn/plugins/openvpn-plugin-auth-pam.so «openvpn
login USERNAME password PASSWORD»

Перезагрузите опенвпн: **sudo systemctl restart openvpn@server.service**

В домашней директории возьмите клиентский файл .ovpn и поменяйте в нём следующие параметры:

remote SERVERIPADDRESS 1194
cipher AES-256-CBC

Добавьте 1 новый параметр:

auth-user-pass

Пример готового конфига (после verb 3 идут сертификаты, тут опущены):

client

proto
udp
explicit-exit-notify
remote 193.227.134.6 1194
dev tun
resolv-retry
infinitenobind
persist-
key
persist-
tun
remote-cert-tls server
verify-x509-name server_o7UFcDRJOctNV1Pk
nameauth SHA256
auth-nocache
cipher AES-256-
CBCtls-client
tls-version-min 1.2
tls-cipher TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256

ignore-unknown-option block-outside-dns
setenv opt block-outside-dns # Prevent Windows 10
DNS leakauth-user-pass
verb 3

Скачайте клиентский конфиг на ПК, проверьте, что всё работает корректно.