Интеграция MikoPBX со службой каталога ALD Pro

07/09/2025

Содержание

MikoPBX - это бесплатный сервер телефонии с операционной системой и веб-интерфейсом.

Инструкция предназначена для интеграции сервера MikoPBX со службой каталога ALD Pro. Данная интеграция обеспечит возможность сопоставления доменных учетных записей с пользователями MikoPBX по протоколу LDAP.

1 Подготовка учетной записи

В MikoPBX реализована опция, которая позволяет записывать в каталог те изменения, которые были сделаны в веб-интерфейсе. Для этого создадим отдельного пользователя и создадим роль с выделением таких привилегий.

В разделе «Пользователи» создаем нового пользователя, который будет использоваться для привязки к LDAP (рис. 1).

Рисунок 1 – Создание нового пользователя

Далее создаем новую роль, даем ей произвольное имя. После создания роли переходим в ее редактирование. Изначально она может быть неактивна и ее требуется активировать, затем добавляем уже созданного пользователя в группу (рис. 2).

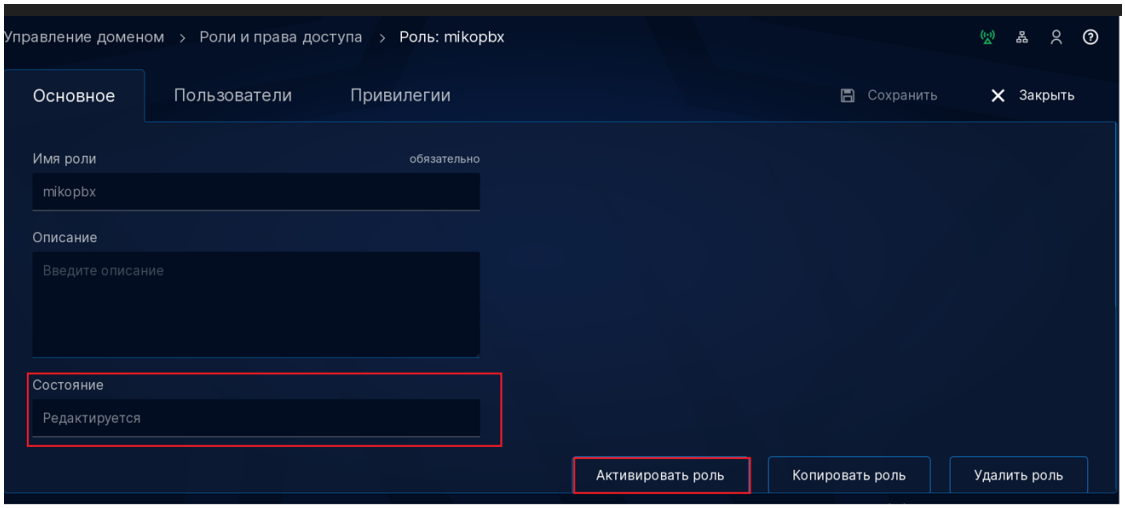

Рисунок 2 – Активация новой роли

Для дальнейшей настройки заходим в раздел «Привилегии» и добавляем привилегии (рис. 3), указанные на изображении ниже.

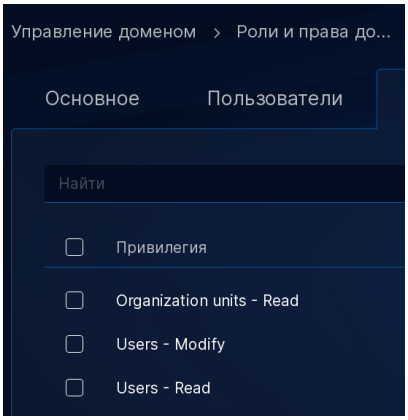

Рисунок 3 – Добавление привилегий

Учетная запись готова, и теперь можно перейти к настройке LDAP.

2 Настройка LDAP

Сначала потребуется скопировать сертификат для установки безопасного соединения. Для того, чтобы это сделать, нужно настроить SSH, если это не было сделано ранее (рис. 4).

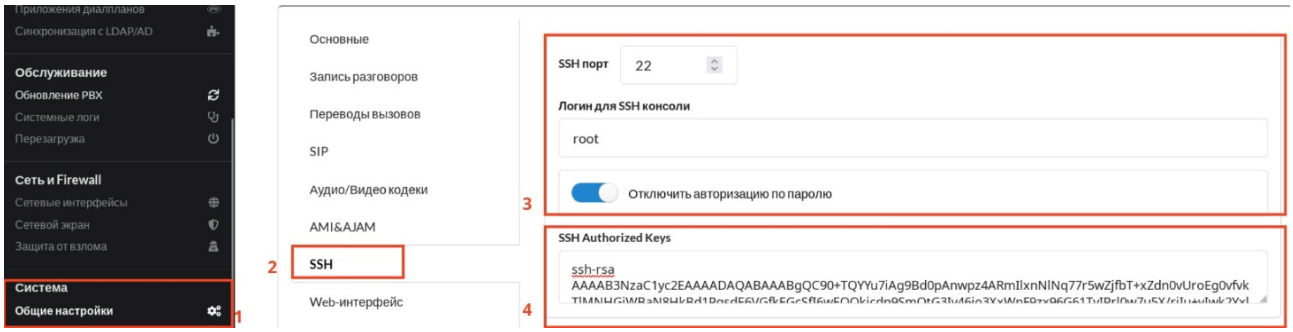

Рисунок 4 – Настройка SSH

1. В веб-интерфейсе заходим в «Общие настройки».
2. Далее переходим в раздел «SSH».
3. По умолчанию в MikoPBX есть только пользователи root и www, и в поставляемых образах отсутствуют утилиты управления пользователями, поэтому указываем root и отключаем авторизацию по паролю.
4. Генерируем SSH-ключ и в поле SSH Authorized-Keys указываем публичный ключ.

```
ssh-keygen
cat ~/.ssh/id_rsa.pub
```

Теперь можно скопировать сертификат в директорию /storage/usbdisk1/mikopbx. Если выбрать другую директорию, то при перезапуске системы скопированные сертификаты будут удалены.

```
scp -i ~/.ssh/id_rsa.pub /etc/ssl/freeipa/ca.crt /storage/usbdisk1/mikopbx/
```

Далее требуется отредактировать файл, отвечающий за подключение по LDAP, /storage/usbdisk1/mikopbx/custom_modules/ModuleLdapSync/Lib/LdapSyncConnector.php. В данном файле, требуется заменить опцию **LDAP_OPT_X_TLS_ALLOW** на **LDAP_OPT_X_TLS_DEMAND**. Это делается для того, чтобы сервер не разрешал подключение по недоверенным сертификатам.
Также добавить опцию **LDAP_OPT_X_TLS_CACERTFILE => '/storage/usbdisk1/mikopbx/ca.crt'**.
Опции разделяются между собой запятыми, в тексте программы это должно выглядеть следующим образом (рис. 5):

```
// Create a new LDAP connection
$this->connection = new \LdapRecord\Connection([
    'hosts' => [$this->serverName],
    'port' => $this->serverPort,
    'base_dn' => $this->baseDN,
    'username' => $this->administrativeLogin,
    'password' => $this->administrativePassword,
    'timeout'  => 15,
    'use_tls'  => $this->useTLS,
    'options' => [
        // See: http://php.net/ldap_set_option
        LDAP_OPT_X_TLS_REQUIRE_CERT => LDAP_OPT_X_TLS_DEMAND,
        LDAP_OPT_X_TLS_CACERTFILE => '/storage/usbdisk1/mikopbx/ca.crt'
    ]
]);
```

Рисунок 5 – Редактирование файла подключения по LDAP

На заметку

Важно помнить, что при обновлении модуля правки, сделанные в коде, изменятся на тот, который идет с обновлением. Если будет установлен параметр LDAP_OPT_X_TLS_ALLOW, то сервер будет доверять любому сертификату, что может привести к MITM-атакам и компрометации учетных данных.

После изменения данного файла можно приступать к настройке в веб-интерфейсе.

В веб-интерфейсе MikoPBX переходим в раздел Модули (рис. 6) и выполняем действия:

1. Для работы с LDAP в MikoPBX предусмотрен специальный модуль, загрузить который можно в разделе «Маркетплейс модулей».
2. После процедуры добавления модуля его нужно включить.

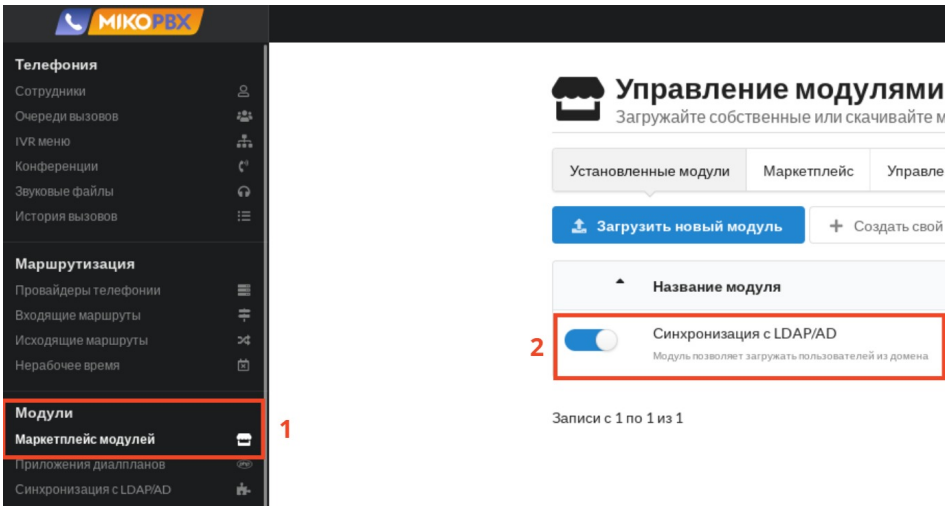

Рисунок 6 – Настройка подключения в веб-интерфейсе MikoPBX

Включите модуль (рис. 7):

1. Далее требуется перейти в раздел Синхронизация с LDAP/AD.
2. Модуль должен быть включен.

3. При добавлении первого сервера LDAP нажимаем «Добавить сервер», данные для заполнения указаны на рис. 8.
4. Когда сервер добавлен, для последующих настроек используется кнопка «Изменить».

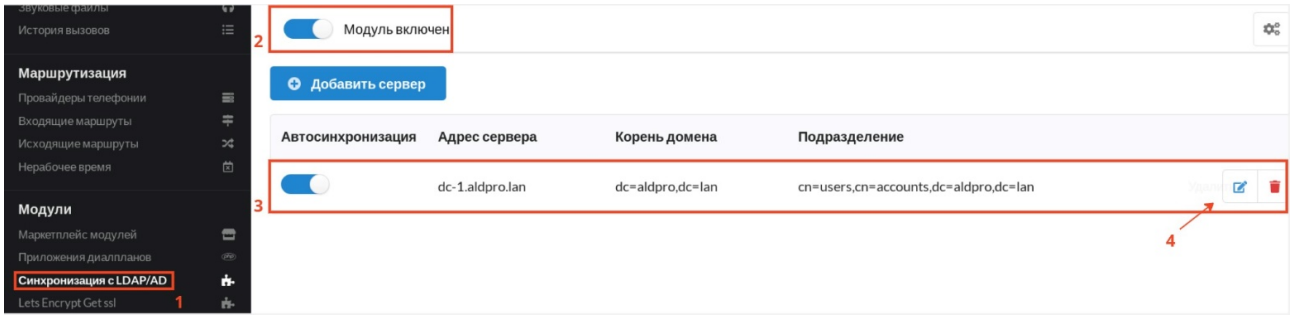

Рисунок 7 – Включение модуля синхронизации с LDAP

Параметры подключения к контроллеру домена (рис. 8):

1. В «Тип сервера» выбираем значение OpenLDAP.

2. В адресе контроллера домена устанавливаем ldaps:// и для установки соединения будет использовать StartTLS . Если установить не ldaps, то передаваемые данные будут передаваться в открытом виде, включая логины и пароли. Указываем адрес, порт и RDN доменного имени.

3. Указываем запись ранее созданного пользователя и пароль.

4. Указываем запись подразделения, где по умолчанию хранятся пользователи.

5. Добавляем фильтр для того, чтобы при синхронизации не добавлялись заблокированные пользователи:

```
(&(uid=*)(objectClass=PosixAccount)(nsAccountLock=False))
```

Если вы не хотите, чтобы учетная запись, при помощи которой происходит синхронизация, попадала в список, то в фильтр можно добавить ее исключение:

```
(&(uid=*)(!(uid=mikoPBX))(objectClass=PosixAccount)(nsAccountLock=False))
```

6. Если требуется, чтобы данные, которые были изменены в веб-интерфейсе MikoPBX записывались в LDAP-каталог, то активируем данный параметр, у данной функции есть ограничения, которые описаны в соответствующем пункте.

7. Если требуется, то включаем синхронизацию по расписанию.

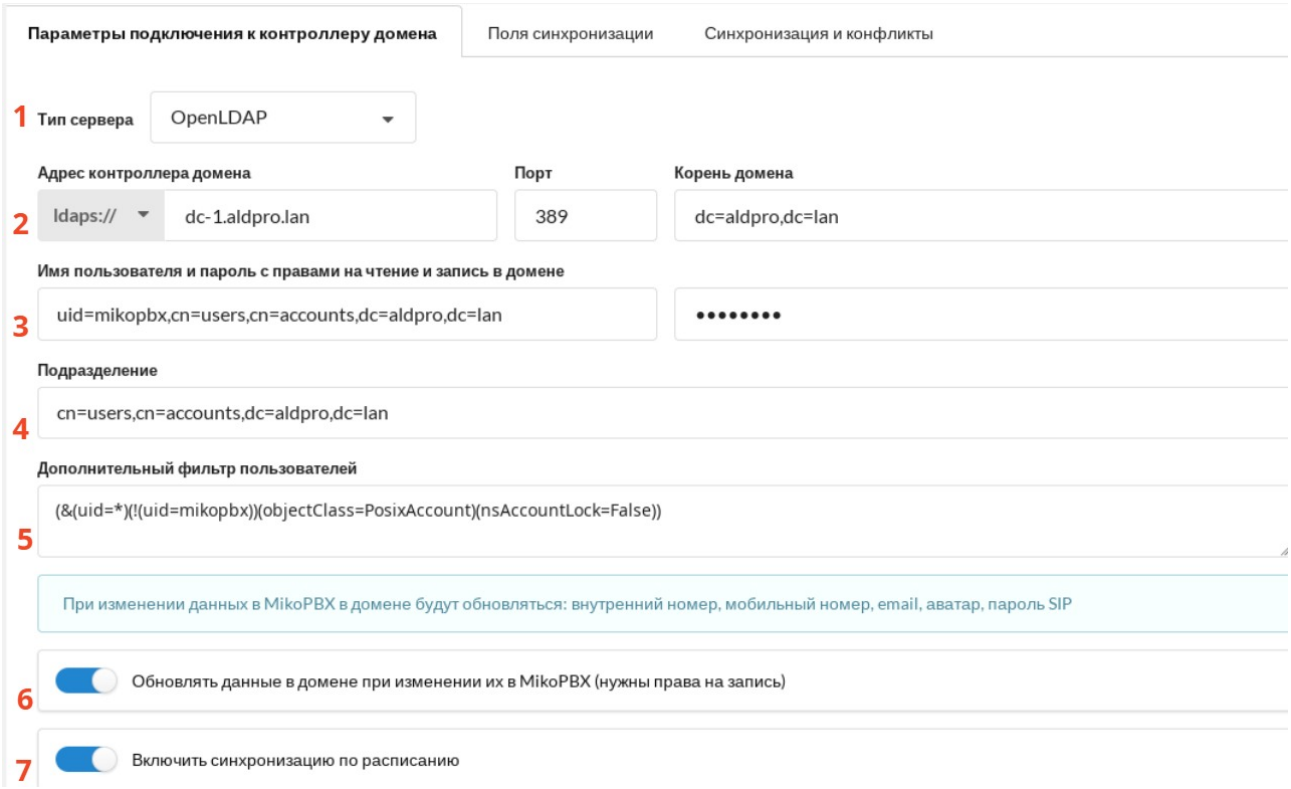

Рисунок 8 – Параметры подключения к контроллеру домена

3 Поля синхронизации

Для корректной работы требуется указать следующие атрибуты (рис. 9):

1. displayName
2. telephoneNumber
3. mobile
4. mail
5. «–» (Данный параметр используется для хранения статуса блокировки. В Active Directory это userAccountControl, который хранит в себе не только статус блокировки, но и другие свойства учетной записи. В ALD Pro статус блокировки хранит атрибут nsAccountLock, который может принимать значение True или False, и при его использовании синхронизация отрабатывает некорректно, но если указать несуществующий атрибут, например, символ «-», то синхронизация будет работать. Заблокированные учетные записи не будут синхронизироваться, так как в параметрах подключения к контроллеру домена был указан фильтр для таких записей.)
6. jpegPhoto
7. Не указываем, MikoPBX может генерировать пароль на своей стороне.
8. Тестовый запрос для проверки работоспособности.

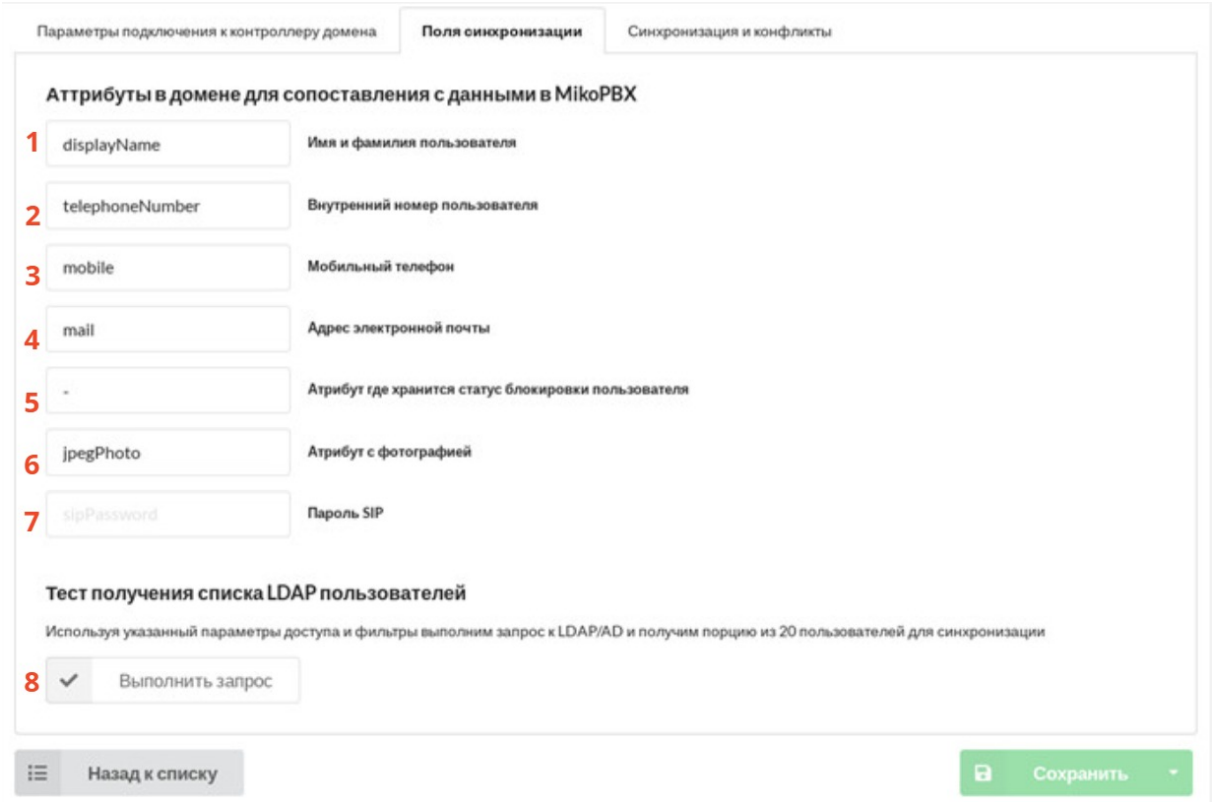

Рисунок 9 – Настройка сопоставления атрибутов для синхронизации

4 Синхронизация и конфликты

После проведенных настроек можно приступить к синхронизации данных (рис. 10).

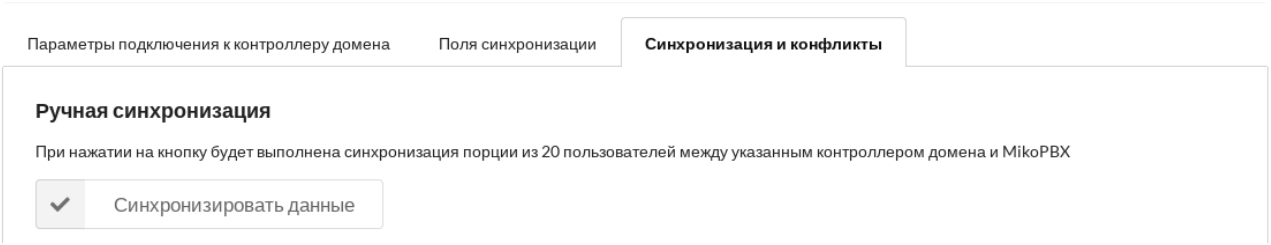

Рисунок 10 – Запуск синхронизации данных

После синхронизации пользователи LDAP попадут в раздел «Сотрудники» в интерфейсе MikoPBX.

На заметку

По умолчанию в MikoPBX для внутреннего номера сотрудника используется 3 цифры из атрибута telephoneNumber. Данную особенность нужно учитывать при синхронизации. Количество цифр можно изменить в основных настройках системы.

4.1 Ограничения

Текущая интеграция не поддерживает атрибут userAccountControl, и по мере блокировки старых пользователей они не будут блокироваться в базе MikoPBX. Блокировку пользователей придется проводить другими способами. При добавлении фильтра, который указан в инструкции, при синхронизации заблокированные пользователи не будут загружаться в MikoPBX.

4.2 Модуль «Управление доступом в систему»

Также в MikoPBX доступен модуль «Управление доступом в систему», при помощи которого можно настроить доступ к веб-интерфейсу MikoPBX и предоставить выборочно права доступа к функциям системы, в том числе управлению другими модулями. При этом есть возможность настройки LDAP-аутентификации (рис. 11).

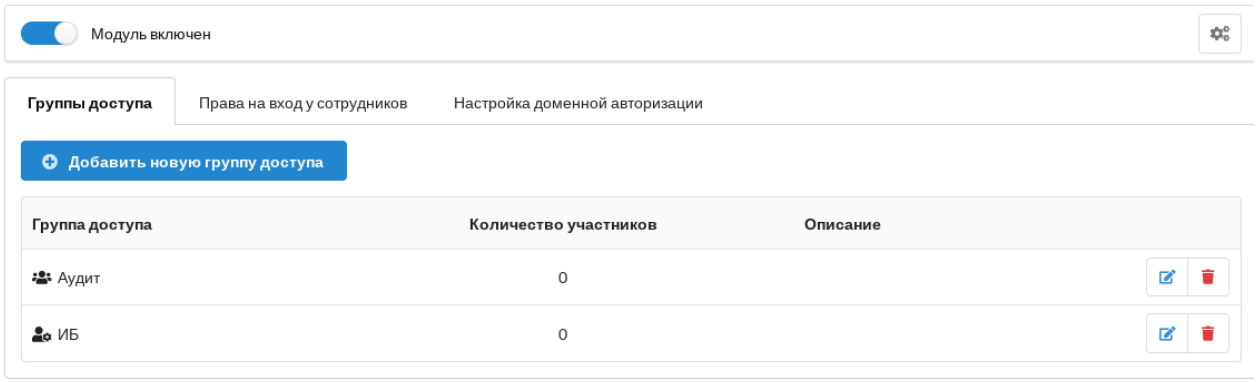

Рисунок 11 – Интерфейс модуля «Управление доступом в систему»

Управление доступом осуществляется на основе групп. Настройка доменной авторизации выполняется аналогично тому, как это делалось в предыдущем модуле. При переходе на страницу группы появляется возможность изменения ее параметров (рис. 12, 13, 14).

Рисунок 12 – Основные настройки группы

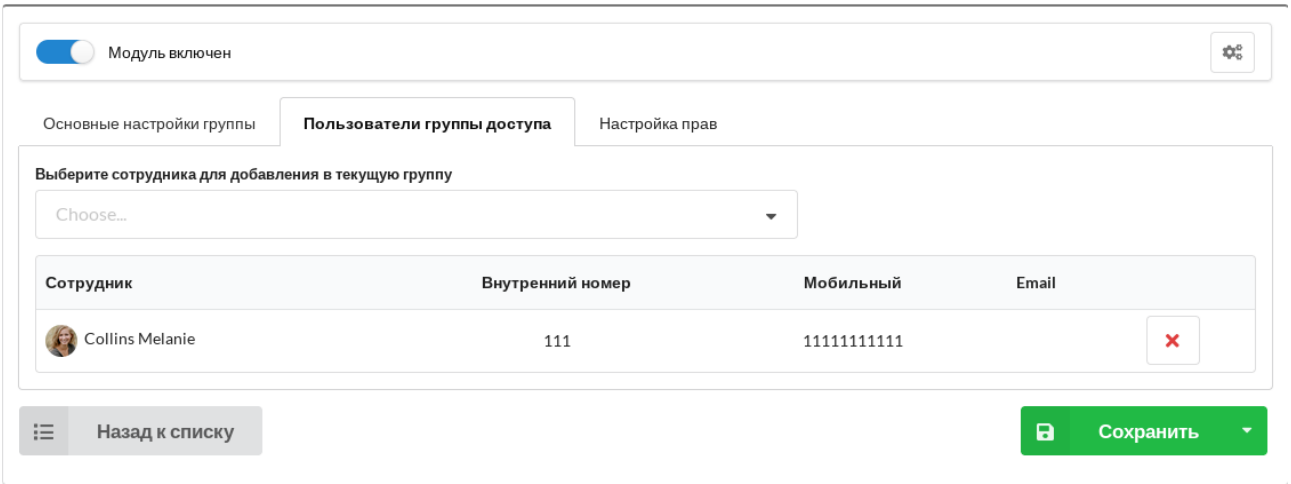

Рисунок 13 – Пользователи группы доступа

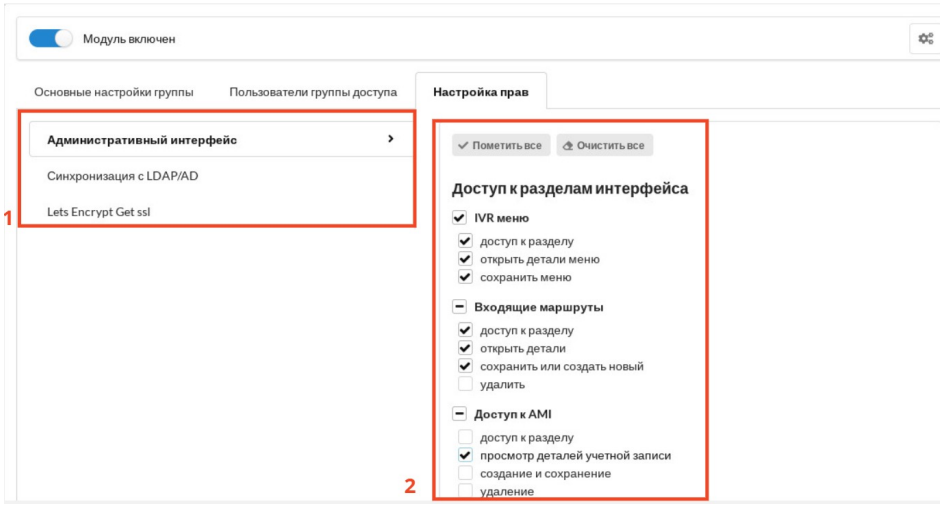

Рисунок 14 – Настройка прав

4.3 Права на вход у сотрудников

После того как группы настроены, в разделе «Права на вход у сотрудников» назначаются параметры входа для каждого сотрудника (рис. 15). Важно отметить, что логин для входа изначально генерируется самостоятельно, и не соответствует доменному логину. Его нужно редактировать вручную, назначив логин данного пользователя из LDAP. Если этого не сделать, авторизация работать не будет.

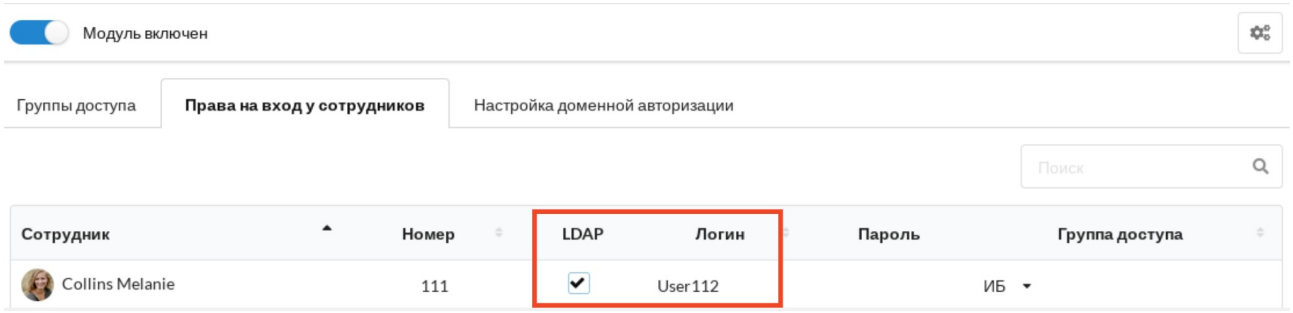

Рисунок 15 – Назначение прав на вход у сотрудников

Все настройки проведены. Теперь администраторам MikoPBX доступен механизм синхронизации сотрудников с каталогом LDAP, а также возможность авторизации на портале используя LDAP-аутентификацию.