

Интеграция PRO32 Connect со службой каталога ALD Pro



06/04/2025

Pro32connect – это программное обеспечение для удаленного доступа к рабочему столу из браузера. Предназначено для профессионального использования: системного администрирования и технической поддержки.

Интеграция позволяет обеспечить аутентификацию и авторизацию пользователя в системе, а также позволяет разграничивать права пользователей при помощи членства в группах каталога.

Инструкция по интеграции разработана вендором PRO32 Connect, который также оказывает поддержку по проведению пилотного тестирования и внедрению своего программного продукта.

PRO32 Connect

**PRO32 Connect – настройка
интеграции входа учётных
записей операторов через
AD\LDA**

PRO32 Connect – настройка интеграции входа учётных записей операторов через AD\LDAP

1) При использовании версии Self-Hosted, сервер должен быть обновлён до последней версии следующими командами:

```
cd /opt/pro32connect && docker-compose pull && docker-compose up -d
```

2) После обновления сервера, необходимо удалить сохранённые данные веб-панели администрирования в браузере (данные содержимого, кеш, куки) во избежание ошибок отображения элементов меню.

Переходим к настройке интеграции:

1. Создаем токен для аутентификации компонента Gateway, который будет отвечать за синхронизацию пользователей в домене:

The screenshot shows the PRO32 Connect web interface. On the left is a sidebar with navigation items: 'Постоянный доступ', 'Быстрая поддержка', 'Команда', 'История подключений', 'Настройки' (highlighted with a red box), and 'Учетная запись'. The main content area is titled 'Токены' (Tokens) and contains a search bar and a table of tokens. The table has columns: 'Название' (Name), 'Ключ' (Key), 'Роль' (Role), and 'Дата создания' (Creation date). One token is listed: 'LDAP' with a long key and the role 'LDAP', created on '11.12.2023 10:22:43'. A green 'Добавить токен' (Add token) button is highlighted with a red box and an arrow pointing to it from the 'Настройки' menu item.

The 'Добавить токен' (Add token) dialog box is shown. It contains the following fields and options:

- Field: 'Название:' (Name) with the value 'LDAP'.
- Field: 'Роль:' (Role) with three options:
 - Lightweight directory access protocol (LDAP)
 - Wake-on-LAN (скоро)
 - Прoxy (скоро)
- Buttons: 'Добавить' (Add) and 'Отмена' (Cancel).

2. Сформированный ключ доступа будет необходим в следующих шагах:

Название	Ключ	Роль	Дата создания
LDAP	Gjo8Ln3vVReurO7vf6JYSm77q7nbqdWUA1T8BMe3hwkZvYfb1c...	LDAP	11.12.2023 10:22:43

1 ... 1 из 1

3. Загружаем дистрибутив компонента Gateway необходимой платформы
Для установки через Docker пропускаем данный пункт.

The screenshot shows the 'Токены' (Tokens) section of the PRO32 Connect interface. A red box highlights the download links for Windows and Linux, with a red arrow pointing to them. The interface includes a sidebar with navigation options like 'Постоянный доступ', 'Быстрая поддержка', 'Команда', 'История подключений', 'Настройки', and 'Учетная запись'. The main content area shows a search bar and a table of tokens.

Название	Ключ	Роль	Дата создания
LDAP	Gjo8Ln3vVReurO7vf6JYSm77q7nbqdWUA1T8BMe3hwkZvYfb1c...	LDAP	11.12.2023 10:22:43

При необходимости, можно загрузить по прямым ссылкам на сайте:

<https://download.pro32connect.ru/gateway/gateway-windows.zip>

<https://download.pro32connect.ru/gateway/gateway-linux.zip>

4. Настраиваем параметры подключения к домен контроллеру в веб-консоли, параметры будут сохранены в зашифрованном виде в СУБД (возможно указание параметров подключения LDAP в файле конфигурации – рассматривается ниже в инструкции)

Внимание: при указании параметров LDAP одновременно в локальном конфигурационном файле и веб-консоли централизованного управления, коннектор в приоритете использует настройки из веб-консоли. Рекомендуем использовать функционал веб-консоли для внесения настроек подключения LDAP.

The screenshot displays the PRO32 Connect web console interface. On the left sidebar, the 'Настройки' (Settings) menu item is highlighted with a red box. A red arrow points from this menu item to the 'Интеграция с Active Directory (LDAP)' section in the main content area, which is also highlighted with a red box. Within this section, the 'Учетные данные и настройки сервера' (Server credentials and settings) option is selected, opening a modal dialog. The dialog is titled 'Учетные данные и настройки сервера...' and contains the following fields and options:

- Credentials:**
 - URL:
 - Пользователь:
 - Пароль:
 - Проверка сертификата сервера AD
- Request params:**
 - Base DN:
 - Атрибут логина:
 - Пользовательский фильтр:
 - Групповой фильтр:

At the bottom of the dialog are two buttons: 'Сохранить' (Save) and 'Отмена' (Cancel).

5.1 Установка компонента Gateway на Linux платформе:

Для установки через Docker пропускаем данный пункт.

Скачиваем и распаковываем архив с приложением:

cd /opt/getscreens либо cd /opt/pro32connect (в зависимости от даты установки, рабочая директория приложений может отличаться)

```
mkdir gateway
```

```
cd gateway
```

```
wget https://download.getscreen.ru/gateway/gateway-linux.zip
```

```
либо wget https://download.pro32connect.ru/gateway/gateway-linux.zip
```

(в случае недоступности первой ссылки)

```
unzip gateway-linux.zip
```

5.2. Переходим в файл настроек:

```
nano config.json
```

```
GNU nano 3.2
{
  "server": {
    "host": "pro32connect.ru",
    "token": "your-token",
    "secure": false
  },
  "ldap": {
    "url": "ldaps://ip-adress",
    "user": "your-ldap-user",
    "password": "your-ldap-password",
    "filter": "",
    "login-attribute": "userPrincipalName",
    "secure": false
  }
}
```

Вносим следующие изменения в шаблоне:

"host": "pro32connect.ru" => для версии Self-hosted указываем доменное имя сервера, для облачной версии оставляем без изменений

"token": "your-token", => вписываем ключ (токен), полученный на шаге 2 инструкции

на выбор администратора сервера:

"secure": true => Проверка сертификата сервера PRO32 Connect включена

"secure": false => Проверка сертификата сервера PRO32 Connect выключена

Внимание: проверка сертификата сервера включается только при условии, что используется публичный DNS сервера PRO32 Connect с публичными сертификатами или используемый непубличный сертификат добавлен в доверенном корневом ЦС на устройстве.

Ниже описывается блок настроек LDAP для файла конфигурации, при настройке параметров LDAP подключения внутри веб-консоли – в файле конфигурации не заполняется.

"url": "ldaps://ip-address", => указываем доменное имя сервера контроллера домена, либо его IP адрес в сети.

При использовании LDAP протокола:

"url": "ldap://192.168.0.1" (будет использован порт по умолчанию 389 для TCP соединений с AD\LDAP сервером)

При использовании Secure LDAP протокола:

"url": "ldaps://192.168.0.1" (будет использован порт по умолчанию 636 для TCP соединений с AD\LDAP сервером)

При использовании других портов для соединения с AD\LDAP сервером, указываем данный порт по примеру:

"url": "ldap://192.168.0.1:3268" (3268 в случае Global Catalog)

"url": "ldaps://192.168.0.1:3269" (3269 в случае Global Catalog over SSL)

Далее, указываем доменную учётную запись пользователя и пароль, которые будут использованы для чтения структуры из AD\LDAP, рекомендуем создать сервисную учётную запись с правами только чтения из домена, срок действия пароля не должен быть ограничен, во избежание сбоев синхронизации.

"user": "your-ldap-user",

Необходимо соблюдение форматирования JSON при указании символа “\” в данном поле, таким образом, для учётной записи domain.local\username следует добавить дополнительный символ “\”, пример:

"user": " domain.local\\username ",

Внимание: синхронизация пользователей по LDAP в PRO32 Connect работает на основе групп, рекомендуем создать в домене одну или несколько групп безопасности, добавить в группы необходимых сотрудников, далее указать эти группы в фильтре. Также это необходимо сделать для ограничения выборки количества объектов для синхронизации в том случае, если в журналах компонента gateway будут присутствовать ошибки вида “LDAP size limit was exceeded”.

"filter": "", => необязательное поле, возможно указание LDAP фильтра заданной группы или нескольких групп в домене, члены которых должны синхронизироваться

Примеры настройки:

"filter": "(cn=PRO32ConnectAdmins*)",

- фильтр создает выборку всех групп, имена которых содержат PRO32ConnectAdmins в названии, например PRO32ConnectAdmins-1, PRO32ConnectAdmins-2 и так далее.

"filter": "(cn=PRO32ConnectAdmins)",

- фильтр создает выборку из одной группы, имя которой совпадает с поисковым запросом.

Вместо "filter": "", (для AD/LDAP) можно использовать следующий блок параметров (фильтры по группам и пользователям, актуально, если интеграция не с MS AD/LDAP

```
"ldap": {
  "group-filter": "(|(objectClass=group)(objectClass=organizationalUnit))",
  "user-filter": "(&(|(objectClass=group)(objectClass=user))(!(objectClass=computer)))"
}
```

- Атрибуты из примера заменяются на атрибуты в используемой системе.

- `"login-attribute": "userPrincipalName"`, => обязательное поле, необходимо указать LDAP атрибут (из доступных на сервере LDAP и с заполненными данными для входа), который будет использован при входе в веб-консоли PRO32 Connect. Отображаемый в результатах синхронизации список учетных записей также будет использовать заданное в данной конфигурации значение.

на выбор администратора сервера:

`"secure": false` = проверка сертификата AD\LDAP сервера отключена

`"secure": true` = проверка сертификата AD\LDAP сервера включена (применимо только в случае использования соединений Secure LDAP с сервером AD\LDAP)

Внимание: проверка сертификата AD\LDAP сервера включается только при условии, что используемый сертификат добавлен в доверенном корневом ЦС на устройстве.

Минимальная рабочая конфигурация при использовании LDAP:

```
{
  "server": {
    "host": "pro32connect.ru",
    "token": "your-token",
    "secure": false
  },
  "ldap": {
    "url": "ldap://192.168.0.1",
    "user": "domain.local\\username",
    "password": "your-ldap-password",
    "secure": false
  }
}
```

При сложной доменной структуре, можно дополнительно указать поиск по BaseDN:

```
{
  "server": {
  },
  "ldap": {
    "base": "dc=demostand,dc=local"
  }
}
```

В качестве фильтров групп и пользователей для ALD Pro можно использовать следующие:

```
{
  "server": {
    "host": "pro32connect-server.local",
    "token": "pro32connect-token",
    "secure": false
  },
  "ldap": {
    "url": "ldap://192.168.0.1",
    "user": "uid=admin,cn=users,cn=accounts,dc=aldpro,dc=local",
    "password": "LDAP-password",
    "login-attribute": "mail",
    "base": "dc=aldpro,dc=local",
    "group-filter": "(objectClass=ipausergroup)",
    "user-filter": "(&(objectClass=posixaccount)(objectClass=person))",
    "secure": false
  }
}
```

Для сохранения нажимаем Ctrl + X, далее подтверждаем сохранение Y и Enter.

5.3. Выполняем установку шлюза и его запуск в системе:

Для установки через Docker пропускаем данный пункт.

Назначаем права на запуск приложения:

```
chmod +x ./gateway
```

и выполняем установку службы:

```
./gateway -install
```

Выполняем запуск службы:

```
./gateway -start
```

Все команды для управления шлюзом:

```
./gateway -install - Установка службы
```

```
./gateway -uninstall - Удаление службы
```

```
./gateway -start - Запуск службы
```

```
./gateway -stop - Остановка службы
```

Внимание: при изменении настроек в файле конфигурации, достаточно перезапустить шлюз, переустановка службы не требуется.

6. Установка через Docker:

Редактируем шаблон конфигурации контейнеров:

```
nano /opt/pro32connect/docker-compose.yml
```

В самом конце файла необходимо раскомментировать строки:

```
169 #####
170 # Gateway (optional)
171 # Uncomment to enable
172 #####
173
174 # gateway:
175 #   image: updater.pro32connect.ru/gateway:latest
176 #   container_name: pro32connect-gateway
177 #   restart: always
178 #   volumes:
179 #     - ./gateway/log:/opt/gateway/log:rw
180 #     - ./gateway/config.json:/opt/gateway/config.json:rw
181
```

создаем на хосте рабочие директории для компонента:

```
mkdir /opt/pro32connect/gateway
```

```
mkdir /opt/pro32connect/gateway/log
```

Вносим изменения в шаблоне config.json аналогично п.5.2 инструкции, сохраняем по пути, указанному docker-compose.yml: /opt/pro32connect/gateway/config.json

Запускаем сервер командой и переходим к пункту 8 инструкции

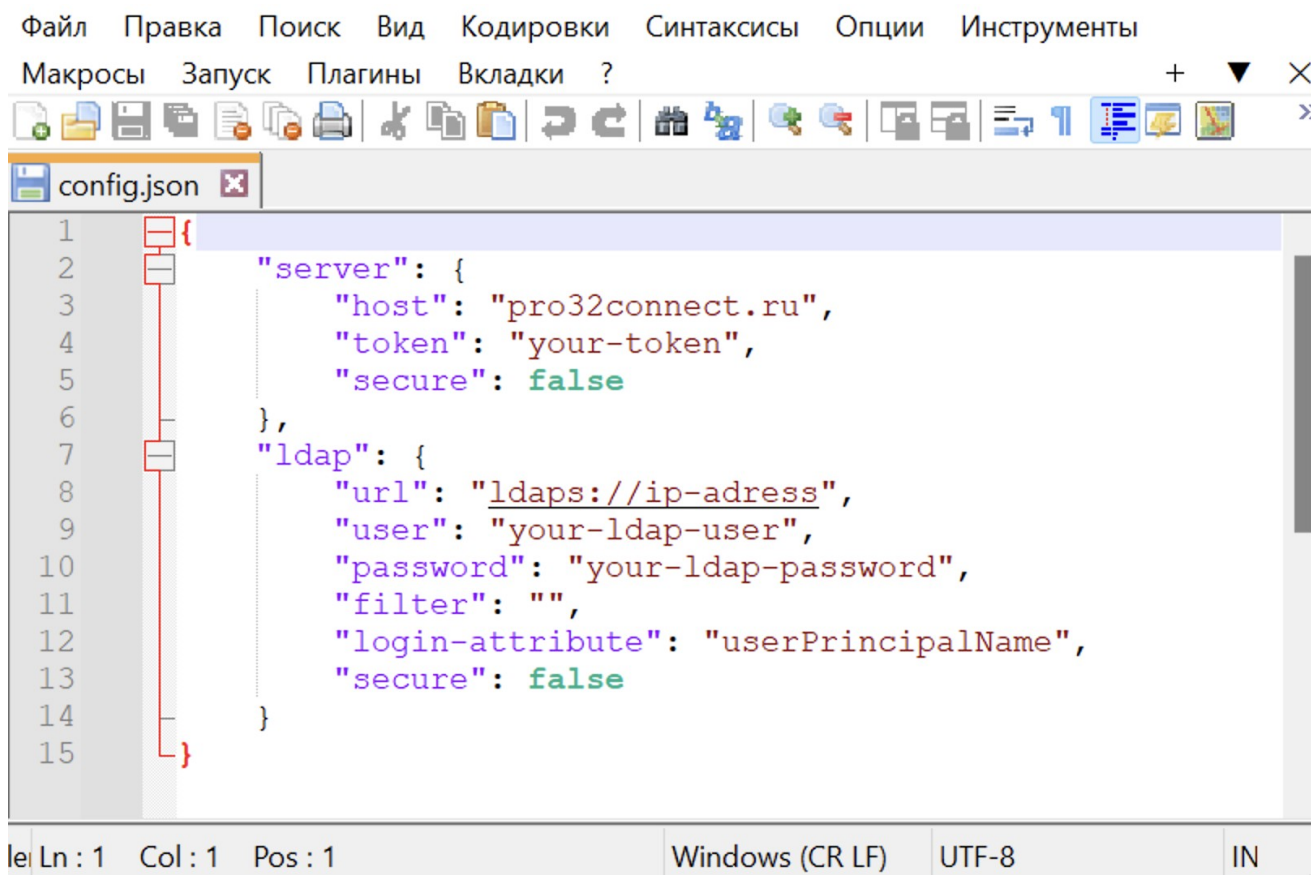
```
cd /opt/pro32connect && docker-compose pull && docker-compose up -d
```

Внимание: при изменении настроек в файле конфигурации, достаточно перезапустить шлюз.

7. Установка компонента Gateway на Windows платформе:

Загружаем дистрибутив (пункт 3 инструкции)

Распаковываем архив, переходим в файл настроек config.json:



The screenshot shows a text editor window titled 'config.json'. The menu bar includes 'Файл', 'Правка', 'Поиск', 'Вид', 'Кодировки', 'Синтаксисы', 'Опции', 'Инструменты', 'Макросы', 'Запуск', 'Плагины', and 'Вкладки'. The toolbar contains various icons for file operations. The main text area displays the following JSON configuration:

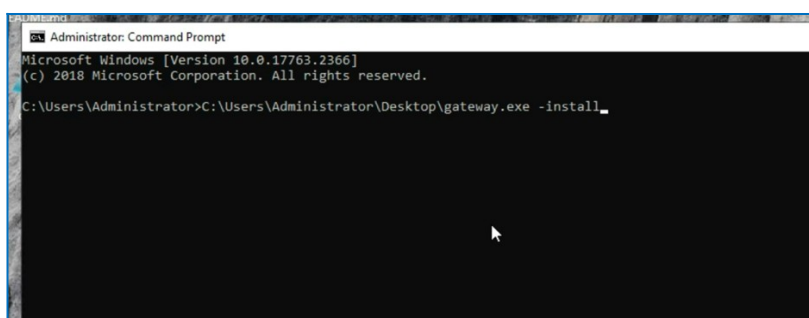
```
1 {
2   "server": {
3     "host": "pro32connect.ru",
4     "token": "your-token",
5     "secure": false
6   },
7   "ldap": {
8     "url": "ldaps://ip-address",
9     "user": "your-ldap-user",
10    "password": "your-ldap-password",
11    "filter": "",
12    "login-attribute": "userPrincipalName",
13    "secure": false
14  }
15 }
```

The status bar at the bottom indicates 'Ln: 1 Col: 1 Pos: 1', 'Windows (CR LF)', 'UTF-8', and 'IN'.

Вносим изменения в шаблоне аналогично п.5.2 инструкции.

Выполняем установку службы:

```
gateway.exe -install
```



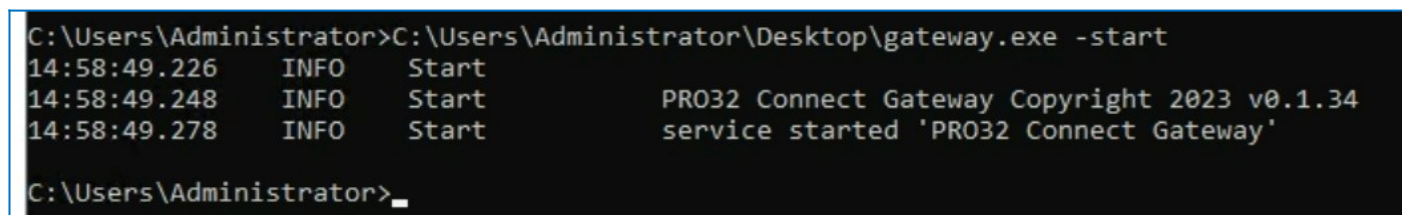
The screenshot shows a Command Prompt window titled 'Administrator: Command Prompt'. The text in the window is:

```
Microsoft Windows [Version 10.0.17763.2366]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>C:\Users\Administrator\Desktop\gateway.exe -install
```

выполняем запуск службы:

```
gateway.exe -start
```

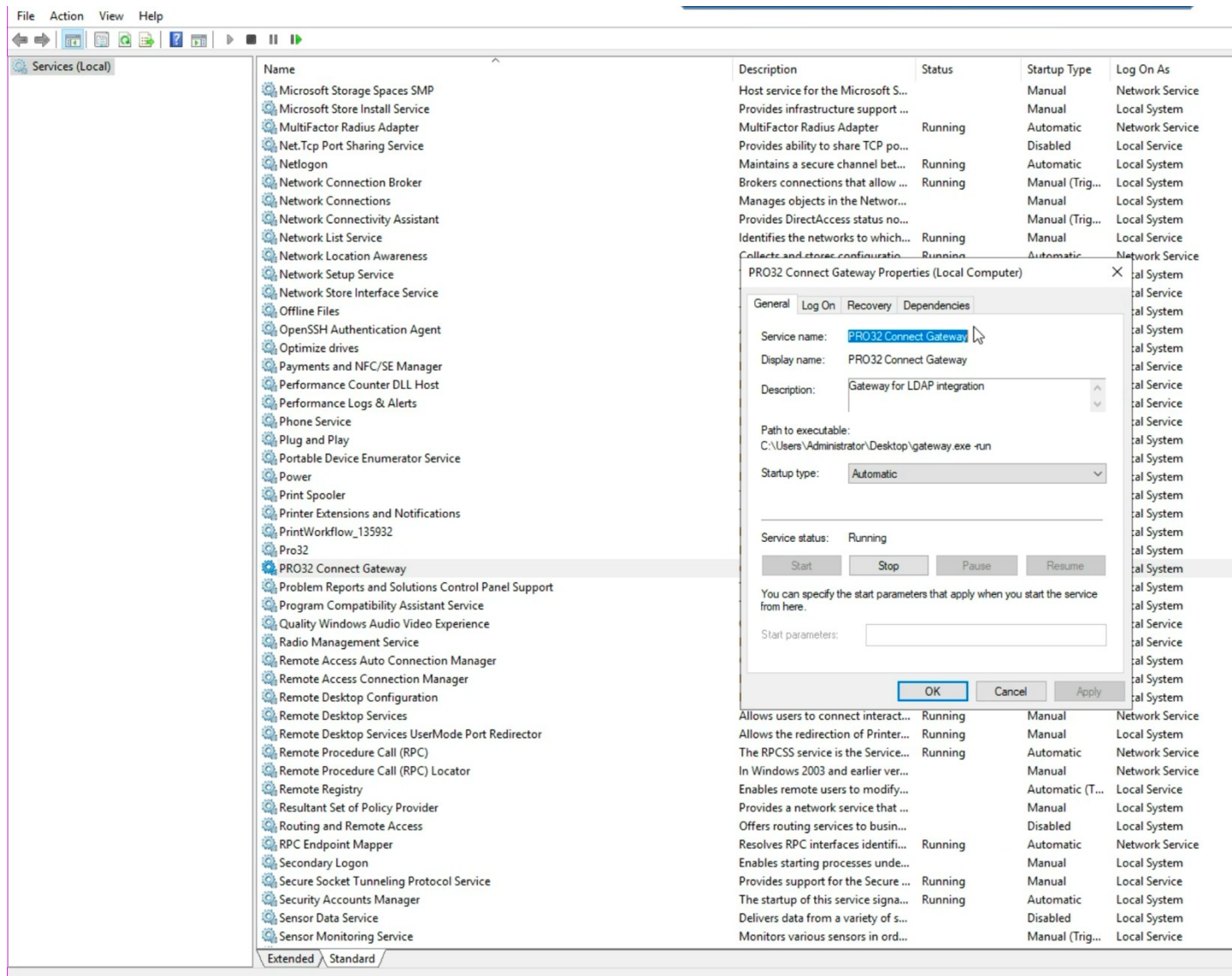


The screenshot shows a Command Prompt window with the following output:

```
C:\Users\Administrator>C:\Users\Administrator\Desktop\gateway.exe -start
14:58:49.226      INFO      Start
14:58:49.248      INFO      Start      PRO32 Connect Gateway Copyright 2023 v0.1.34
14:58:49.278      INFO      Start      service started 'PRO32 Connect Gateway'

C:\Users\Administrator>
```

При отсутствии ошибок, служба будет запущена и начнёт работать в автоматическом режиме (автозапуск при загрузке системы)



Все команды для управления шлюзом

- | Команда | Описание |
|---------------------------------------|------------------|
| <code>`gateway.exe -install`</code> | Установка службы |
| <code>`gateway.exe -uninstall`</code> | Удаление службы |
| <code>`gateway.exe -start`</code> | Запуск службы |
| <code>`gateway.exe -stop`</code> | Остановка службы |

Внимание: при изменении настроек в файле конфигурации, достаточно перезапустить шлюз, переустановка службы не требуется.

8. После старта шлюза, если нет ошибок вывода службы Gateway, проверяем соединение в консоли управления:

PRO32 Getscreen

Токены
Ключи для подключения шлюзов к вашей учетной записи

Добавить токен

Скачать программу шлюза для Windows

Общие Брендирование Журнал Интеграция **Токены**

Поиск по названию и ключу

Имя	Ключ	Роль	Дата создания
LDAP	0j08Ln3vVReur07vf62YSm77g7nbqdmUA1T8BMe3hwkzvYfb1c17Si03npVFkYeU92VzrFQ2fB13e1w69bA5h3a1pe7KIMBv7FW3ke2...	LDAP	11.12.2023 10:22:43

1 ... 1 из 1

Настройка

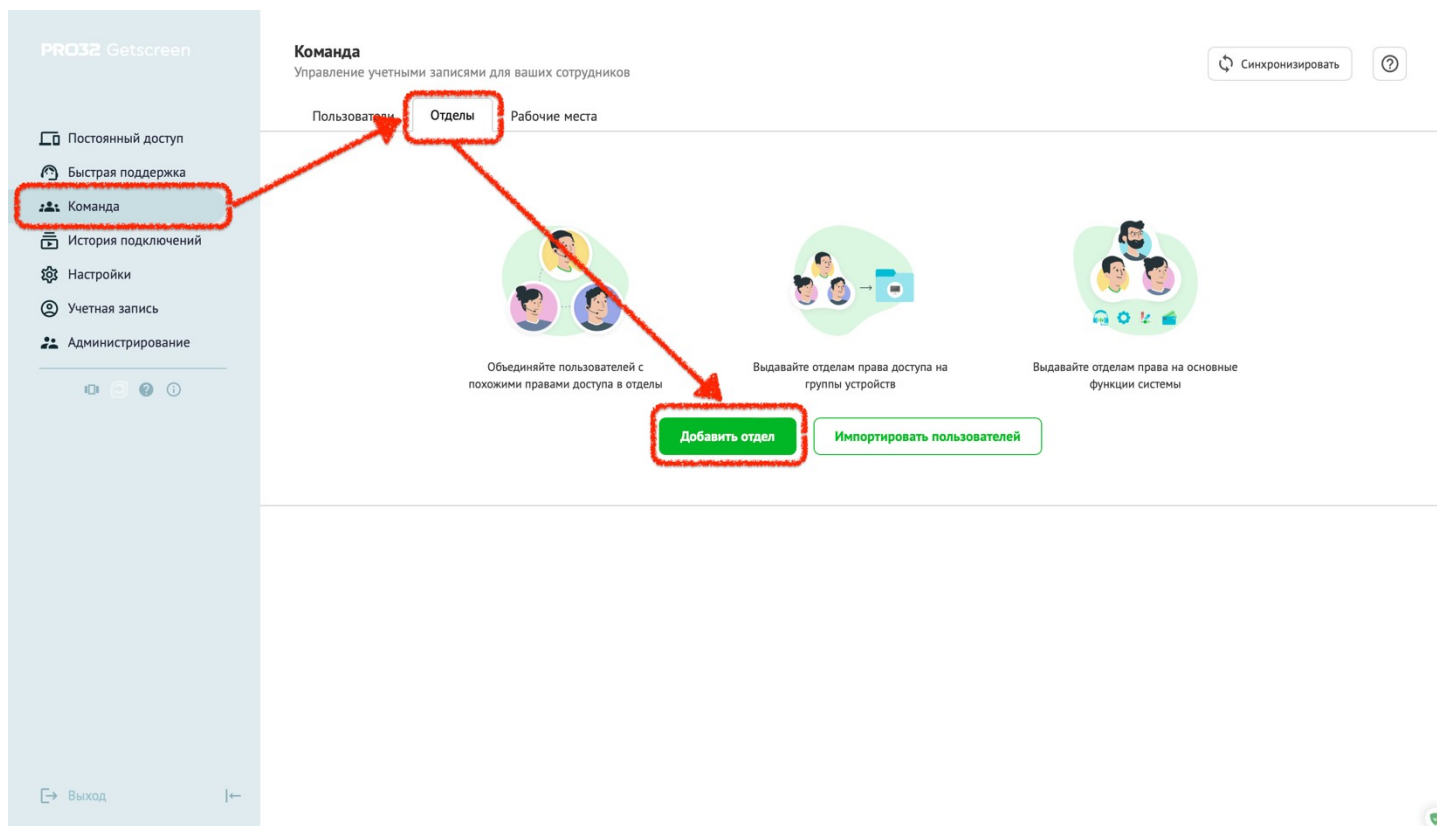
Запущенные шлюзы

Изменить

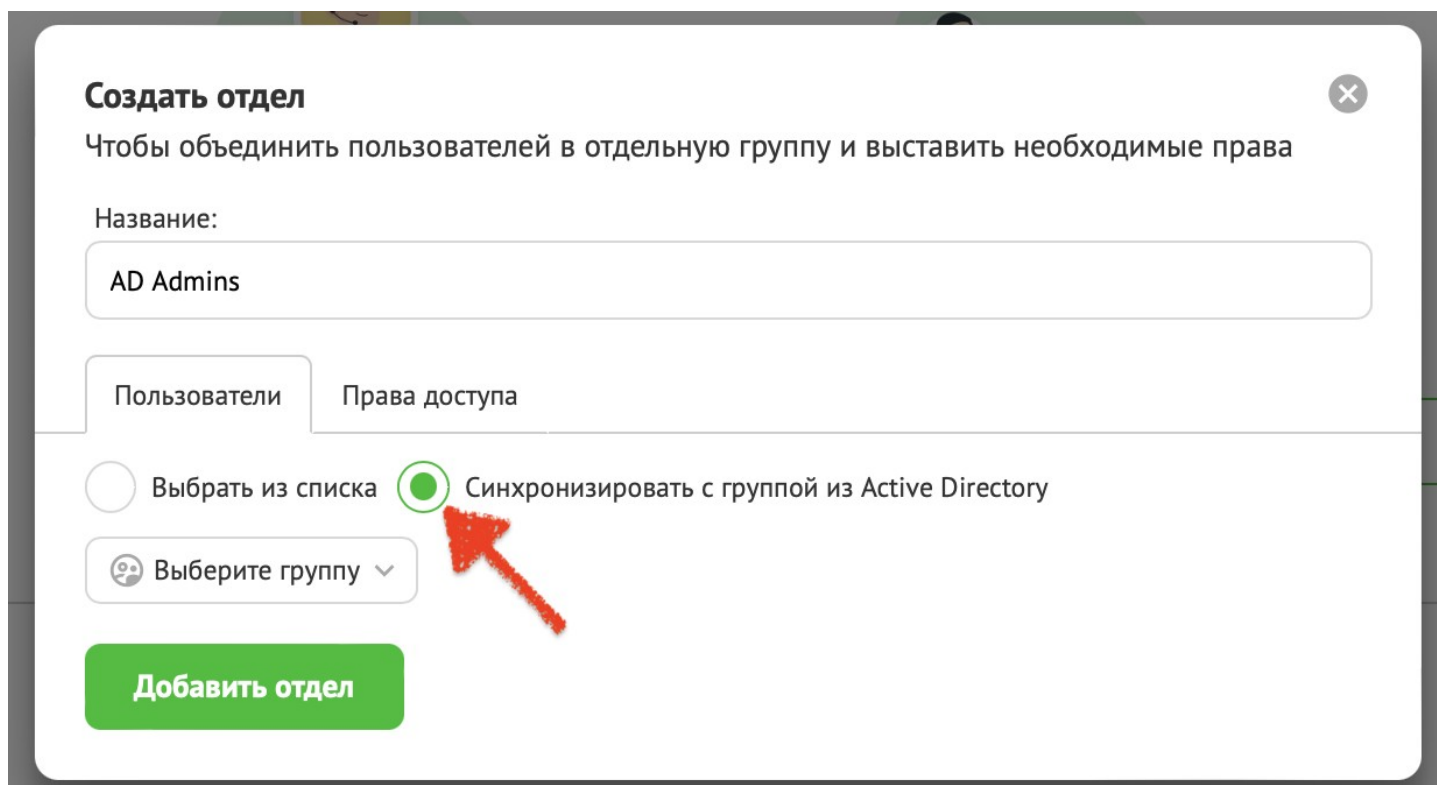
Удалить

Выход

9. Переходим в раздел команды, добавляем новый отдел (ВАЖНО – ранее созданные отделы, без интеграции с AD\LDAP не будут доступны для синхронизации и кнопка «Синхронизировать с группой из Active Directory» будет неактивной)



10. Указываем название отдела: выбираем пункт «Синхронизировать с группой из Active Directory»



11. Выбираем подразделение из Active Directory, в котором присутствуют пользователи (будут отображены в превью).

Создать отдел ✕

Чтобы объединить пользователей в отдельную группу и выставить необходимые права

Название:
AD Admins

Пользователи | Права доступа

Выбрать из списка Синхронизировать с группой из Active Directory

Выберите группу ^

Поиск по названию

- Access Control Assistance Operators
- Account Operators
- Administrators
- Allowed RODC Password Replication G...
- Backup Operators

12. Подразделения, в которых пользователей нет (в превью ни одного пользователя) – не выбираем для интеграции!

Создать отдел ✕

Чтобы объединить пользователей в отдельную группу и выставить необходимые права

Название:
AD Admins

Пользователи | Права доступа

Выбрать из списка Синхронизировать с группой из Active Directory

Administrators ▾

Administrator@demostand.local gs@demostand.local maxk@demostand.local
dimal123@demostand.local dlantsevskikh@esetnod32.ru admin-1@demostand.local
dimal-esa@demostand.local dimal01@demostand.local dimal@demostand.local

Добавить отдел

13. Переходим в права доступа (соседняя вкладка) и настраиваем необходимый шаблон разрешений прав доступа, в самом конце нажимаем «Добавить отдел»

Создать отдел ✕

Чтобы объединить пользователей в отдельную группу и выставить необходимые права

Название:

AD Admins

Пользователи **Права доступа**

Группы устройств: ?

Demostand	Администратор
ДИТ	Техник

Выберите группу ▾

Отдельные устройства: ?

Android SDK built for arm64	Администратор
alse-vanilla-gui	Техник

Выберите устройство ▾

Быстрая поддержка:

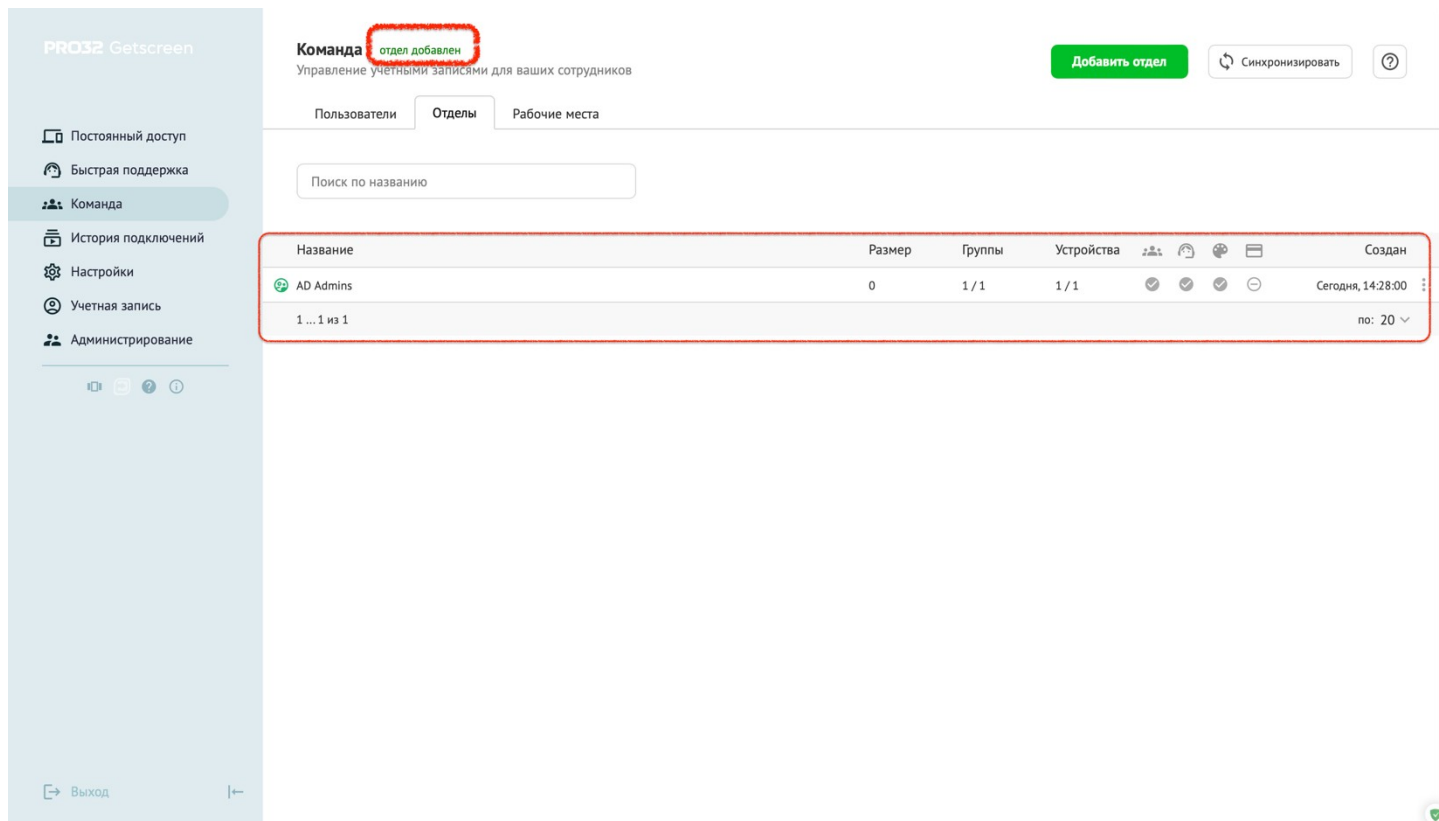
Доступ только к своим приглашениям ▾

Управление другими опциями:

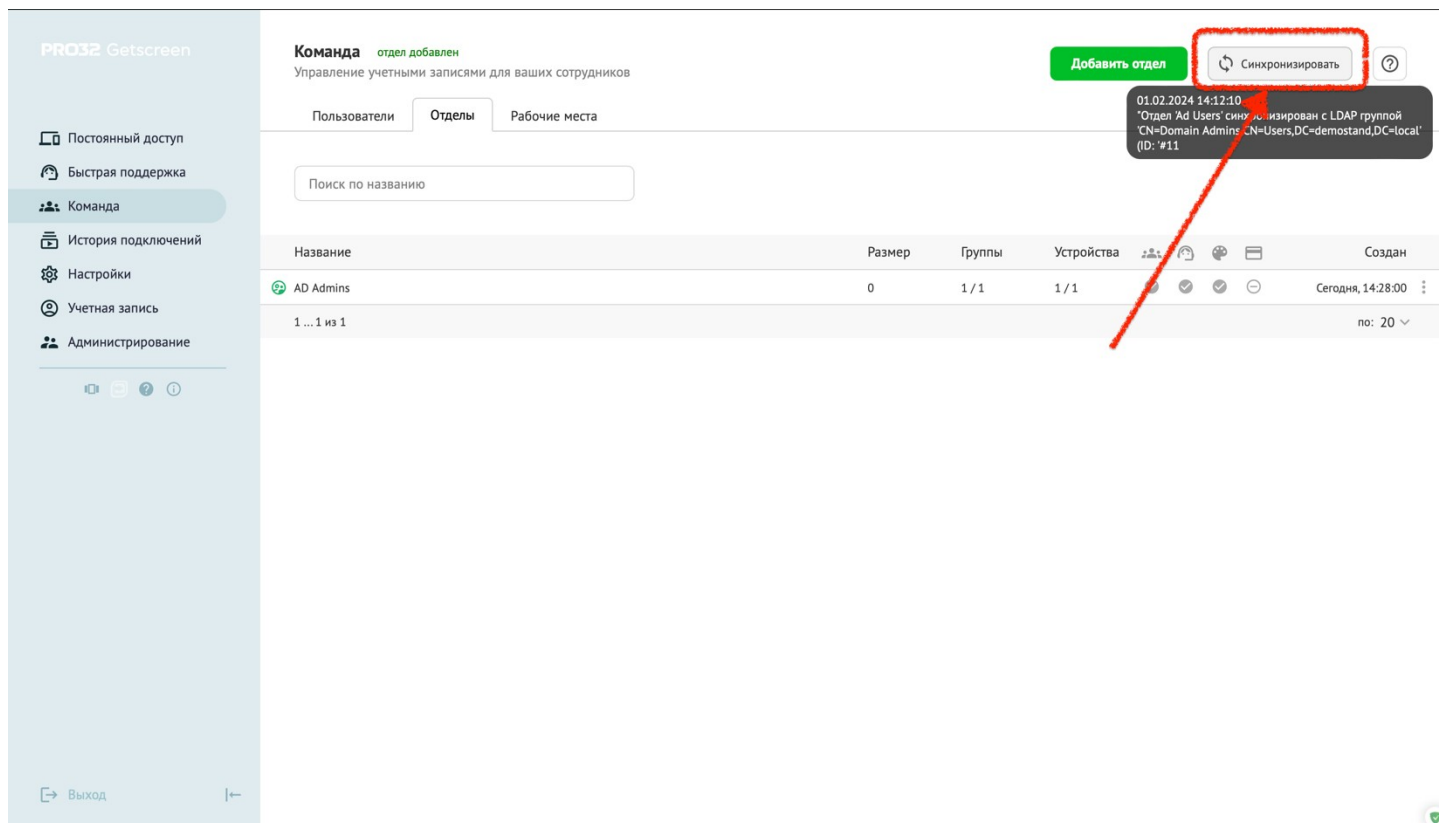
- Брендинг ?
- Настройки и пользователи ?

Добавить отдел

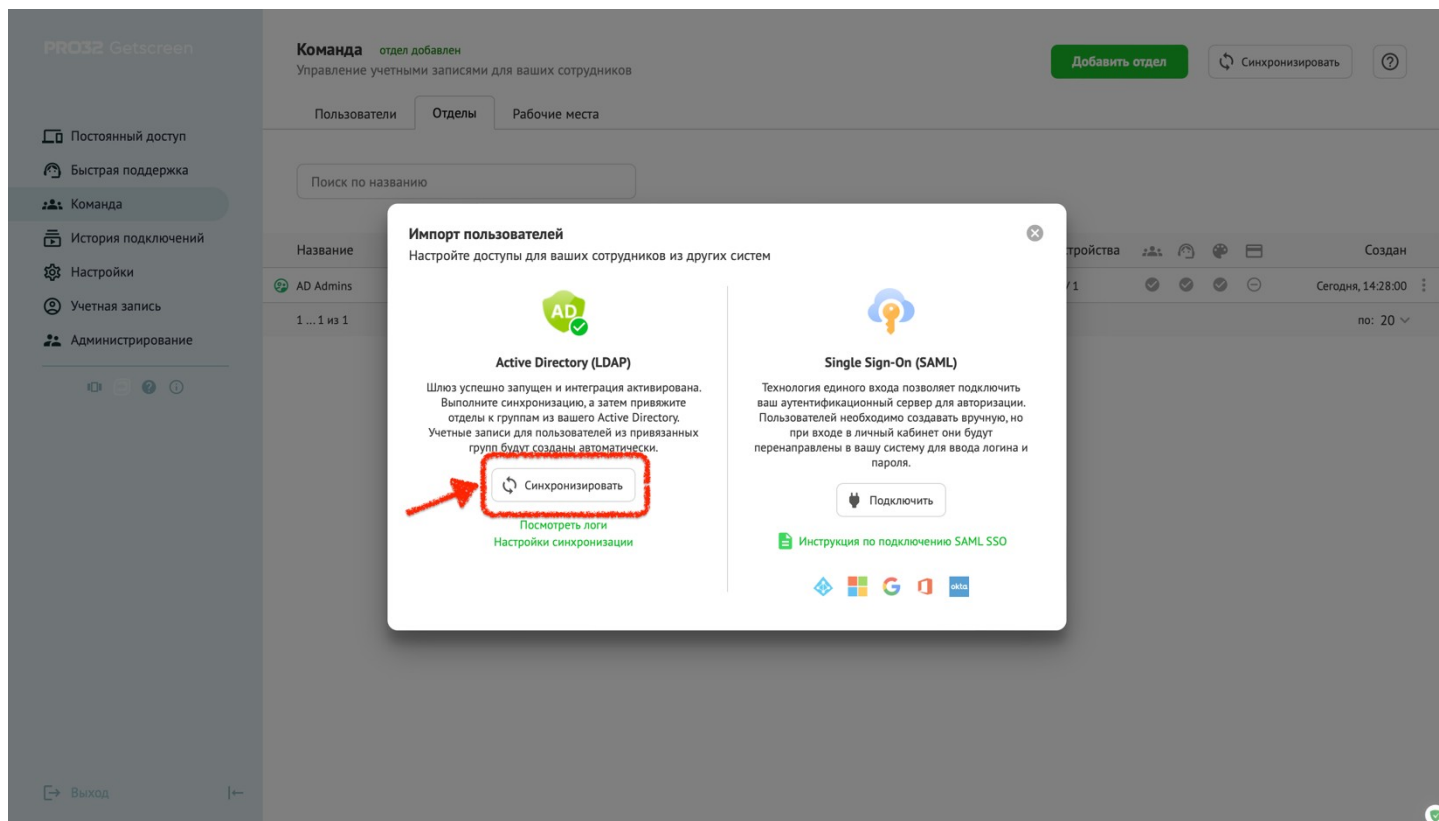
14. Если добавление отдела выполнено успешно, рядом с надписью команда будет следующий статус и ниже в списке появится данный отдел:



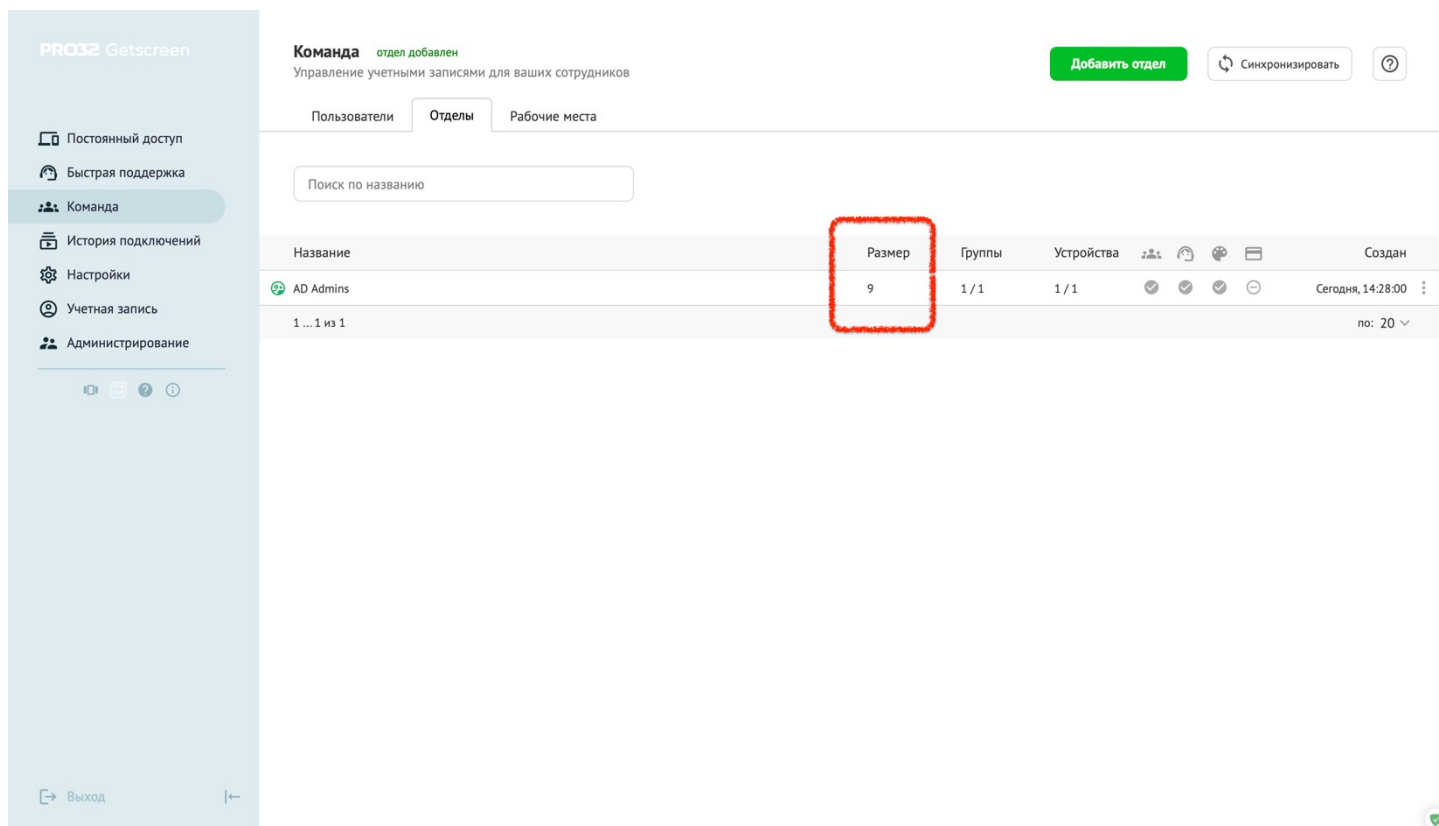
15. Далее необходимо запустить первую синхронизацию вручную:



Нажимаем «Синхронизировать»



После выполнения команды, при успешной синхронизации, размер должен увеличиться на число пользователей выбранного подразделения:



16. Для настройки автоматической синхронизации: переходим в раздел настроек: вносим параметры и сохраняем изменения

The screenshot displays the PRO32 Connect settings page. The left sidebar contains navigation options: 'Постоянный доступ', 'Быстрая поддержка', 'Команда', 'История подключений', 'Настройки', 'Учетная запись', and 'Администрирование'. The 'Настройки' (Settings) option is highlighted with a red box and an arrow pointing to the 'Общие' (General) tab in the top navigation bar. The 'Общие' tab is also highlighted with a red box. Below the navigation bar, the 'Общие' section includes a text input field for 'Публичное название для отдела поддержки:' with the value 'Pro32 Support'. The 'Устройства' (Devices) section has a checked checkbox for 'Снимать скриншоты с рабочего стола для превью-изображений'. The 'Подключения' (Connections) section includes several unchecked checkboxes and input fields for timeouts. The 'Пользователи' (Users) section includes a text input for a whitelist of IP addresses, a checked checkbox for 'Автоматическая синхронизация с Active Directory', and two more checked checkboxes: 'Периодичность:' set to 5 minutes and 'Таймаут для пользователей:' set to 50 minutes. A red box highlights the 'Импорт пользователей' (Import users) button and the 'Автоматическая синхронизация с Active Directory' section. A red arrow points from the 'Общие' tab to the 'Импорт пользователей' button.