ПРОТЕЙ ТЕХНОЛОГИИ

197342, г. Санкт-Петербург,
ул. Белоостровская, д. 6,
литер А, помещ. 30-Н, офис 615

Тел.: +7 (812) 401-63-25
E-mail: sales@protei.ru
Сайт: tl.protei.ru

Версия документа
от 04.04.2025

PromUC 3.0 Настройка LDAP-аутентификации

В данной статье перечислены основные нюансы, связанные с настройкой LDAP-аутентификации для версии 1.20.4.

Для удобства отладки аутентификации предлагается выставить уровень логирования в файле */etc/gitea/app.ini* в блоке *[log]*:

```
LEVEL = Trace
```

Конфигурацию "LDAP (via BindDN)" стоит использовать, если пользователи системы находятся в разных юнитах сложной структуры дерева AD. В таком случае должна быть выделена отдельная сервисная УЗ, с помощью которой будет выполняться поиск пользователей.

Ниже описана конфигурация "LDAP (simple auth)", которую стоит использовать, если **ВСЕ** пользователи находятся в одном юните дерева AD, например в *OU=Service Accounts, OU=GOROD1, OU= ZAVOD, DC=ooo, DC=kompaniya*.

• База для поиска пользователя

Здесь удобнее всего указывать контроллеры домена AD, например:

```
DC=ooo,DC=kompaniya
```

• DN пользователя

"Путь" до записи соответствующего пользователя, с подстановкой логина из формы аутентификации в Gitea:

197342, г. Санкт-Петербург,
ул. Белоостровская, д. 6,
литер А, помещ. 30-Н, офис 615

Тел.: +7 (812) 401-63-25
E-mail: sales@protei.ru
Сайт: tl.protei.ru


```
CN=%s,OU=Service Accounts,OU=ZAVOD,OU=GOROD,DC=ooo,DC= kompaniya
```

(Соответствующий параметр %s будет заменен именем пользователя, указанным в форме входа)

- **Фильтр пользователя**

LDAP – фильтр, однозначно указывающий на запись пользователя в AD. Здесь также используется подстановка, но немного иной формы:

```
(&(sAMAccountName=%[1]s)(objectclass=person)(objectclass=user))
```

(Соответствующий параметр [1]s будет заменен именем пользователя, указанным в форме входа)

Лучше использовать атрибут *sAMAccountName*, указывающий на имя пользователя.

- **Фильтр администратора**

С помощью данного фильтра можно указывать, какие пользователи получат административные права в Gitea. Например, если есть отдельная группа администраторов, в качестве фильтра целесообразно использовать атрибут *memberof*:

```
(memberOf=CN=system_admin,OU=System,OU=Groups,DC=ooo,DC= kompaniya)
```

- **Ограниченный фильтр**

С помощью данного фильтра можно ограничить выбранных пользователей:

```
(|(memberOf=CN=system_operator,...,DC=kompaniya)(memberOf=CN=system_master,...,DC=
```

197342, г. Санкт-Петербург,
ул. Белоостровская, д. 6,
литер А, помещ. 30-Н, офис 615

Тел.: +7 (812) 401-63-25
E-mail: sales@protei.ru
Сайт: tl.protei.ru

kompaniya))

• Атрибут группы, содержащий список пользователей

Здесь уместнее всего использовать атрибут *member.*

• Атрибут пользователя в группе

Здесь уместнее всего использовать атрибут *dn.*

• Сопоставление групп LDAP с командами в Gitea

Обязательно используйте upper case для обозначения объектов AD, таких как CN, OU, DC. В данном поле можно указать несколько групп, и для каждой группы можно указать несколько команд и организаций. Например:

```
{
"CN=system_operator,OU=System,OU=Groups,DC=ooo,DC= kompaniya ":{" System
":["Operators"]},
"CN= system_master,OU= System,OU=Groups,DC= ooo,DC= kompaniya ":{" System
":["Owners"]},
"CN= system_admin,OU= System,OU=Groups,DC= ooo,DC= kompaniya
":{"System":["Owners"],"promuc":["Owners"]}
}
```

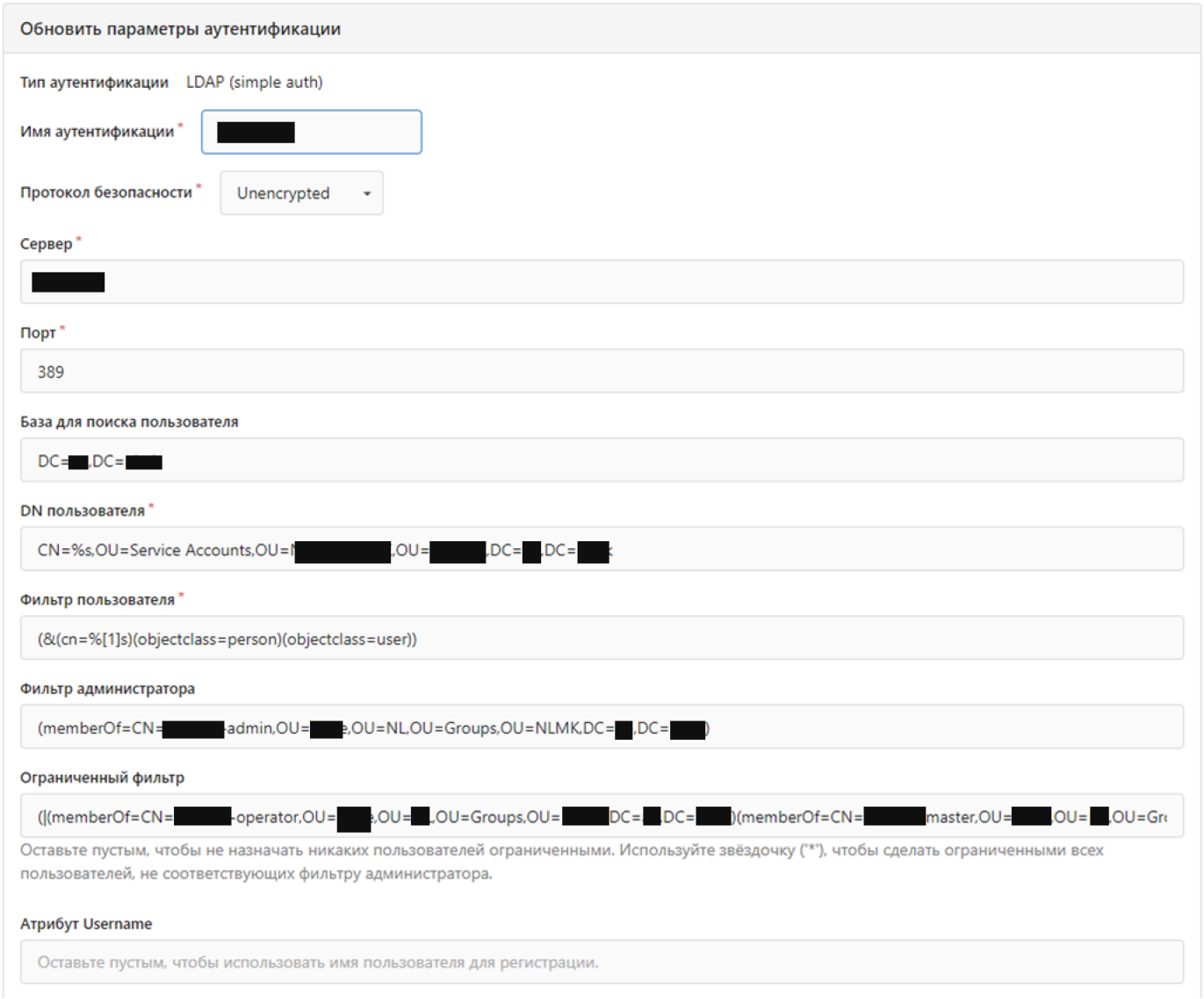
Ниже скриншоты конфигурации "LDAP (simple auth)" для проекта:

ПРОТЕЙ ТЕХНОЛОГИИ

197342, г. Санкт-Петербург,
ул. Белоостровская, д. 6,
литер А, помещ. 30-Н, офис 615

Тел.: +7 (812) 401-63-25
E-mail: sales@protei.ru
Сайт: tl.protei.ru

Версия документа
от 04.04.2025



ПРОТЕЙ ТЕХНОЛОГИИ

197342, г. Санкт-Петербург,
ул. Белоостровская, д. 6,
литер А, помещ. 30-Н, офис 615

Тел.: +7 (812) 401-63-25
E-mail: sales@protei.ru
Сайт: tl.protei.ru

Версия документа
от 04.04.2025

Атрибут Открытый ключ SSH

e.g. SshPublicKey

Характеристики аватара

e.g. jpegPhoto

☑ Включить группы LDAP

Поисковая база групп DN

OU=[redacted],OU=[redacted]OU=Groups,OU=[redacted],DC=[redacted],DC=[redacted]

Атрибут группы, содержащий список пользователей

member

Атрибут пользователя в группе

dn

Проверить принадлежность к группе в LDAP (оставьте фильтр пустым, чтобы пропустить)

e.g. (|(cn=gitea_users)(cn=admins))

Сопоставьте группы LDAP командам организации (оставьте поле пустым, чтобы пропустить)

```
{
"CN=[redacted]-operator,OU=[redacted],OU=[redacted],OU=Groups,OU=[redacted]DC=[redacted],DC=[redacted]":{"[redacted]":["Operators"]},
"CN=[redacted]-master,OU=[redacted],OU=[redacted],OU=Groups,OU=[redacted],DC=[redacted],DC=[redacted]:[redacted]":["Owners"]},
"CN=[redacted]-admin,OU=[redacted],OU=[redacted],OU=Groups,OU=[redacted],DC=[redacted],DC=[redacted]{[redacted]":["Owners"],"promuc":["Owners"]}
}
```

☑ Удалить пользователей из синхронизированных команд, если пользователь не принадлежит к соответствующей группе LDAP

☑ Пропустить локальную двухфакторную аутентификацию

Если значение не задано, локальным пользователям с установленной двухфакторной аутентификацией все равно придется пройти двухфакторную аутентификацию для входа в систему

☐ Разрешить пустой результат поиска для отключения всех пользователей

☑ Источник аутентификации активирован

Обновить источник аутентификации | Удалить этот источник аутентификации

197342, г. Санкт-Петербург,
ул. Белоостровская, д. 6,
литер А, помещ. 30-Н, офис 615

Тел.: +7 (812) 401-63-25
E-mail: sales@protei.ru
Сайт: tl.protei.ru

Версия документа
от 04.04.2025

О компании ПРОТЕЙ Технологии

Компания ПРОТЕЙ Технологии входит в российский IT-холдинг ПРОТЕЙ и занимается реализацией программно-аппаратных продуктов для корпоративного сегмента рынка. ПРОТЕЙ ТЛ предлагает решения для создания и модернизации корпоративной связи на предпри- ятиях из сферы объединённых коммуникаций, телефонии, ВКС-систем и системы управления и мониторинга инфраструктуры предприятий. Решения ПРОТЕЙ разработаны в полном соответствии с международными стандартами и отвеча- ют всем современным требованиям, предъявляемым к объединённым корпоративным коммуни- кациям.