AD/LDAP/ALD Pro

Интеграции с различными службами каталогов

?????????? KUMA ? Active Directory (AD)

> При интеграции с AD/ADFS важно иметь единое время на системах, настоятельно рекомендуется настроить NTP

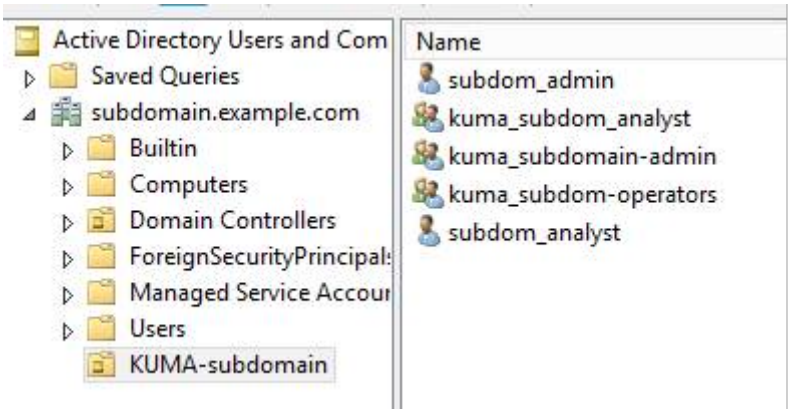
https://www.youtube.com/embed/1Rw6qOWF7jc?si=vOId0Aj4wFH-Vr47

Аутентификация работает только для одного домена. Поэтому все группы должны быть созданы в корневом домене.
Пример инфраструктуры AD:

- корневой домен леса - example.com
- контроллер домена - dc-01.example.com
- дочерний домен - subdomain.example.com

В дочернем домене созданы:

- OU «KUMA subdomain»
- Universal группы безопасности: «kuma_subdomain_analyst», «kuma_subdomain_admin», «kuma_subdomain_operators»
- Пользователи: subdom_admin, subdom_analyst



Пользователи являются членами соответствующих групп:

```
PS C:\Users\Administrator> get-aduser -identity subdom_analyst -properties CN,memberOf,UserPrincipalName

CN                : subdom_analyst
DistinguishedName : CN=subdom_analyst,OU=KUMA-subdomain,DC=subdomain,DC=example,DC=com
Enabled           : True
GivenName         : subdom_analyst
MemberOf          : {CN=kuma_subdom_analyst,OU=KUMA-subdomain,DC=subdomain,DC=example,DC=com}
Name              : subdom_analyst
ObjectClass       : user
ObjectGUID        : 8eaf5558-0966-4de0-a957-5e0cefcb461d
SamAccountName    : subdom_analyst
SID               : S-1-5-21-1445412355-99643495-187345912-1112
Surname           :
UserPrincipalName : subdom_analyst@subdomain.example.com
```

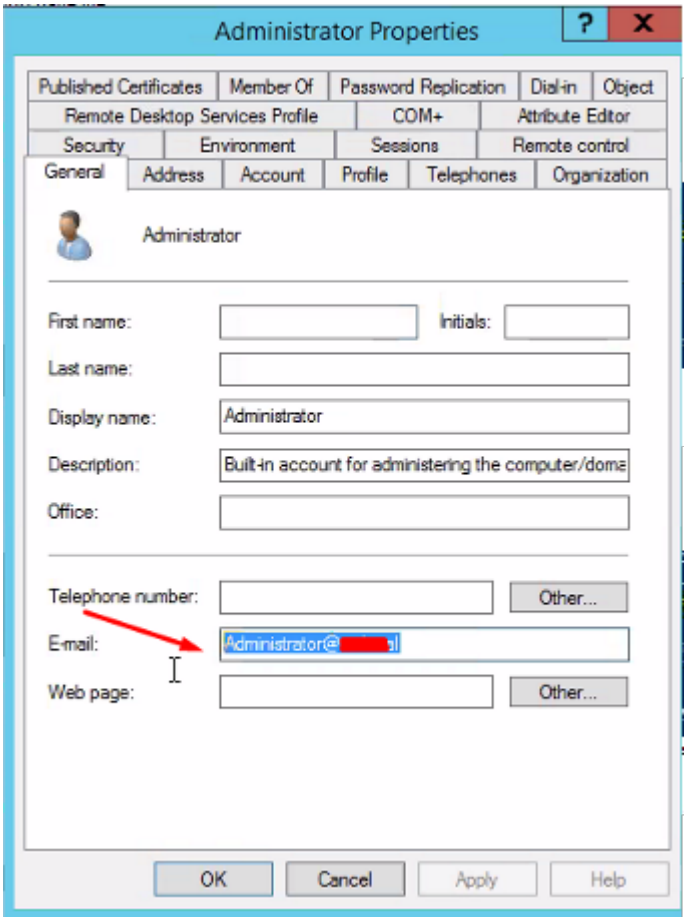
????????? KUMA

Base DN – корневой домен (**не обязательно весь корневой домен**, зависит от вашего AD)

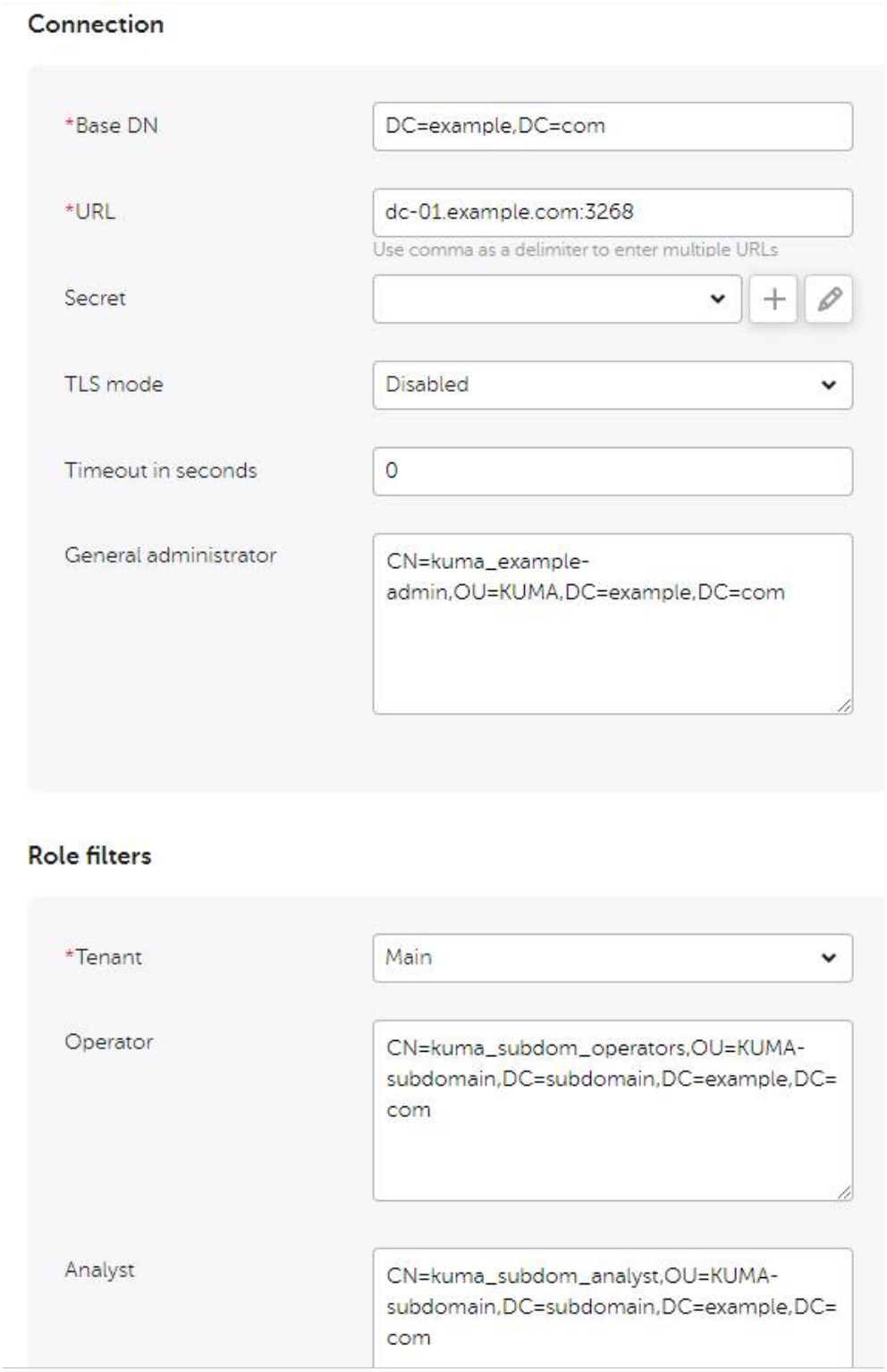
URL – контроллеры корневого домена, порт глобального каталога (**обязательно**)

Важно:

- Все группы доступа должны быть UNIVERSAL
- У пользователей в AD должно быть заполнен атрибут **email**



Далее – для каждого тенанта указываете DistinguishedName групп, соответствующих правам доступа.



Информация по ролям и их возможностям: https://support.kaspersky.com/help/KUMA/2.1/ru-RU/218031.htm

Важный момент:

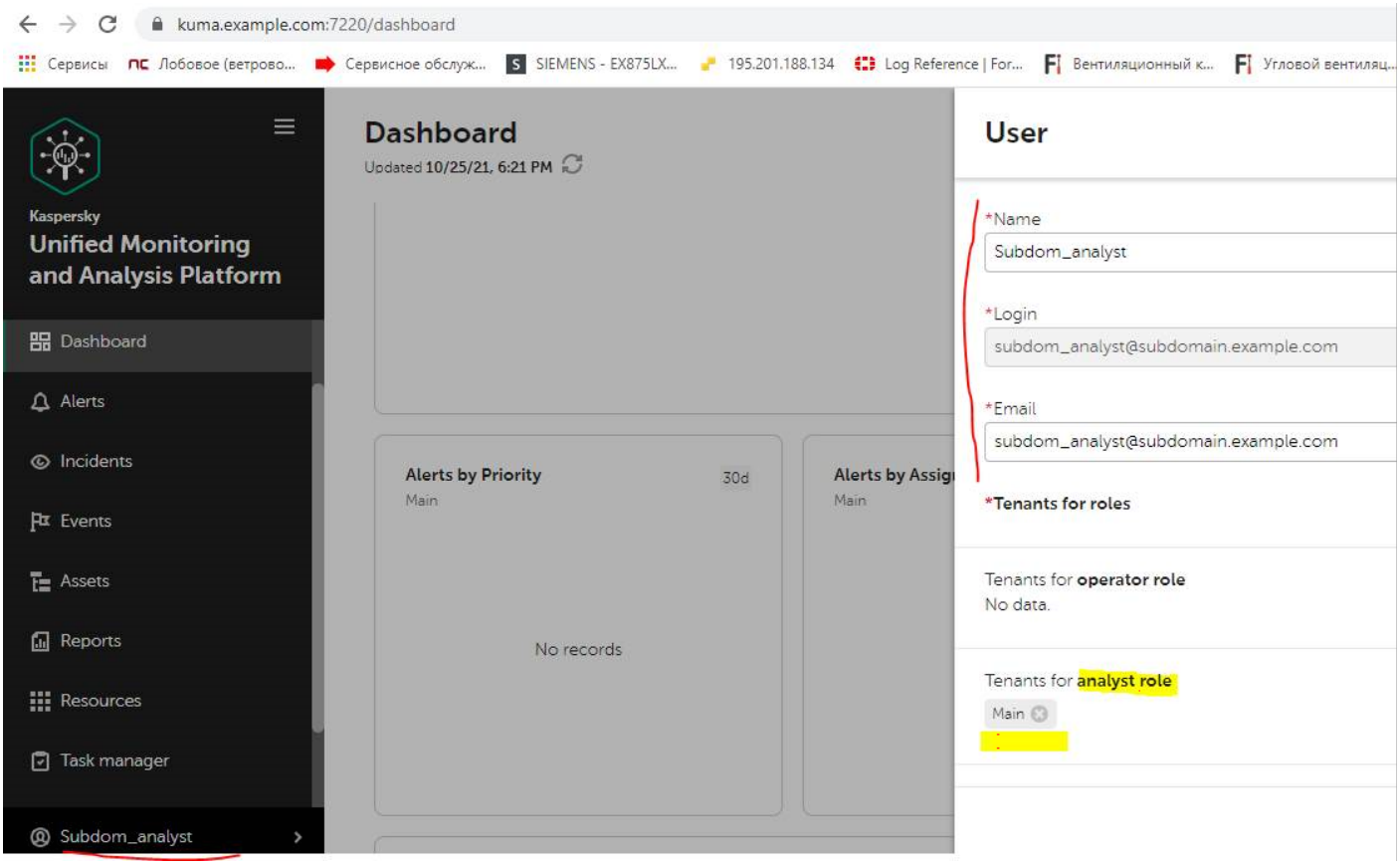
- Предоставление доступа происходит по принципу «**наименьших прав**». Если учетка пользователя одновременно состоит нескольких в группах одного тенанта.
- Например: kuma-analysts и kuma-admins, то пользователь получит права аналитика. Поэтому, при переводе работников из операторов в аналитики или аналитиков в админы, необходимо не только добавить пользователя в соответствующую новую группы, но еще и удалить из старой группы.

?????????

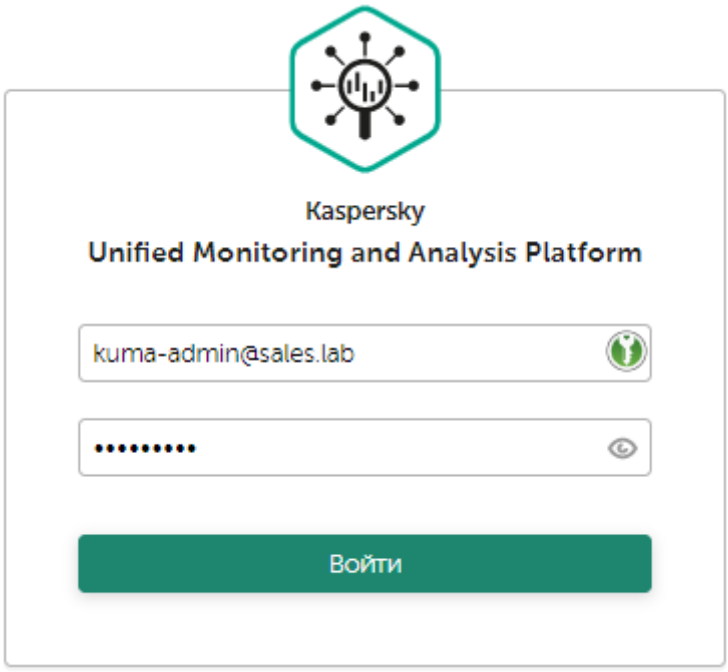
Для доменной аутентификации, как таковой учетки в KUMA не требуется. Когда все настроено, вводится доменный логин и пароль и в этот момент KUMA биндится к LDAP.

При аутентификации, пользователь вводит в консоль свою доменную учетку в формате UPN (user@example.com) и, на основании членства этой учетки в той или иной группе, пользователю предоставляется доступ к разным тенантам с указанными правами.

- Залогинившись под доменной учеткой subdom_analyst@subdomain.example.com
- Получаем права роли analyst в тенанте Main



Пример входа в KUMA с доменной учетной записью (kuma-admin@sales.lab):



Права API можно выдавать только для внутренних пользователей, не из AD

????? AD

- Порт **3268**. Этот порт используется для запросов, специально предназначенных для глобального каталога. Запросы LDAP, отправленные на порт 3268, можно использовать для поиска объектов во всем лесу. Однако могут быть возвращены только атрибуты, помеченные для репликации в глобальный каталог. Например, отдел пользователя не может быть возвращен через порт 3268, так как этот атрибут не реплицируется в глобальный каталог.
- Порт **389**. Этот порт используется для запроса информации с локального контроллера домена. Запросы LDAP, отправленные на порт 389, можно использовать для поиска объектов только в домашнем домене глобального каталога. Однако запрашивающее приложение может получить все атрибуты этих объектов. Например, запрос на порт 389 может быть использован для получения отдела пользователя.
- При интеграции с SSL необходимо использовать сертификат Active Directory. В KUMA поддерживаются открытые ключи сертификата X.509 в Base64. Стандартный порт LDAPS - **636**.

???????? ???????

```
PS C:\Users\osepov> Get-ADUser -Identity kuma-admin


DistinguishedName : CN=kuma-admin,OU=admins,OU=Users,OU=MSK,DC=sales,DC=lab
Enabled           : True
GivenName         : kuma-admin
Name              : kuma-admin
ObjectClass       : user
ObjectGUID        : 0d81928e-e8db-48bb-84b9-d00ad552bdd9
SamAccountName    : kuma-admin
SID               : S-1-5-21-781213047-594974509-2262175553-1700
Surname           :
UserPrincipalName : kuma-admin@sales.lab
```

?????????? KUMA ? ALD Pro ? FreeIPA

> Интеграция является не официальной

> Документация по службе каталогов для Linux Astra ALD Pro: https://astra.ru/software-services/application-software-astra-group/ald-pro/#docs

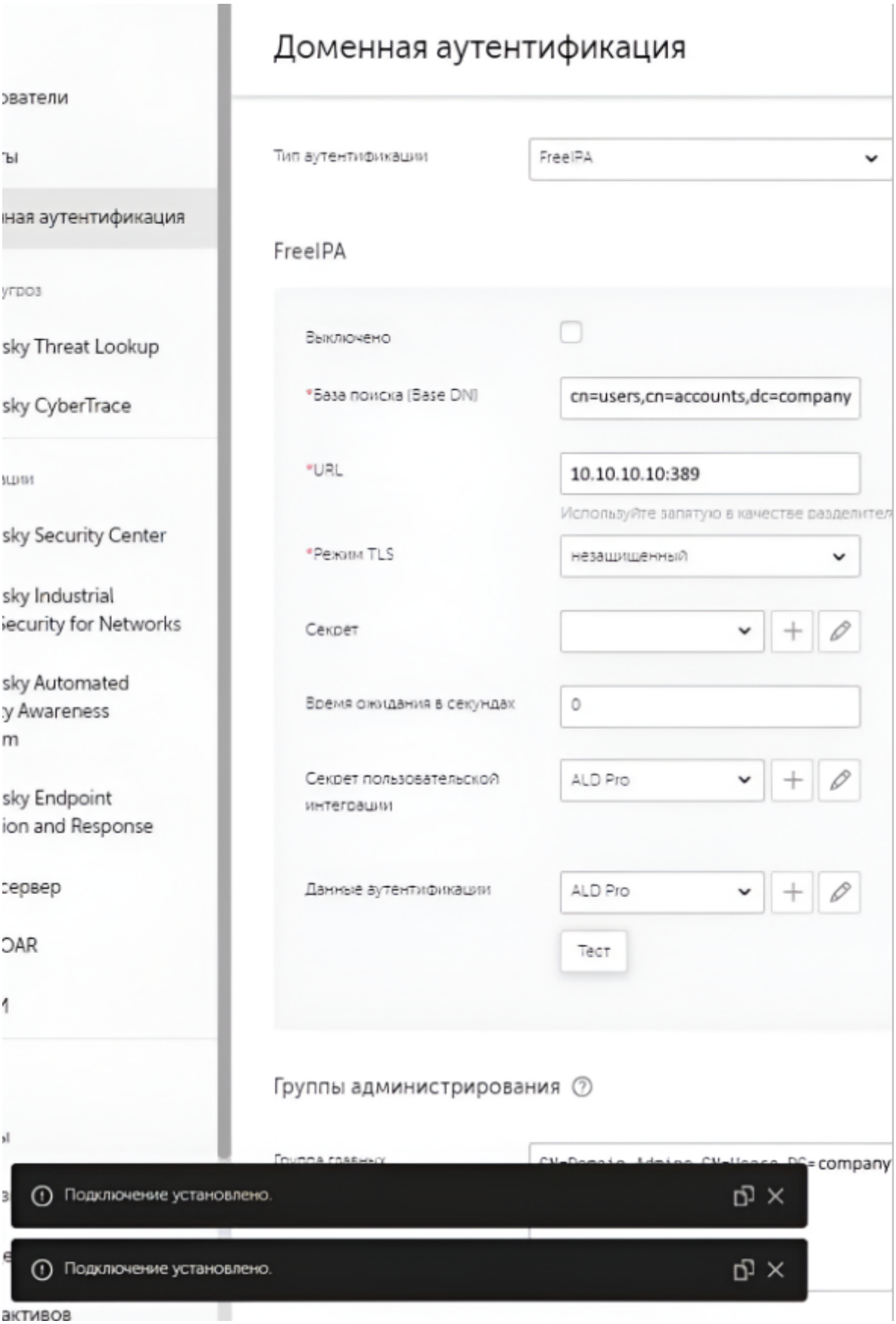
> Настройки выполняются по налогии со статьей: https://kb.kuma-community.ru/books/integracii/page/integraciia-kuma-s-active-directory-ad

> При интеграции с ALD Pro важно иметь единое время на системах, настоятельно рекомендуется настроить NTP

Выберите тип интеграции FreeIPA и группы для учетных записей заводите в таком виде:

```
uid=is.ldap.usr,cn=users,cn=accounts,dc=company,dc=com
```

Пример настроенной интеграции:



В итоге доменная аутентификация работает и пользователи появлялись с заданными правами.

Для успешной аутентификации необходимо соблюдать следующие условия при входе в систему пользователю следует указывать в логине домен заглавными буквами. Пример: user@FREEIPA.COM.

Также проверьте пожалуйста что у пользователя задана почта. Почта является обязательным параметром при создании учетной записи в KUMA.

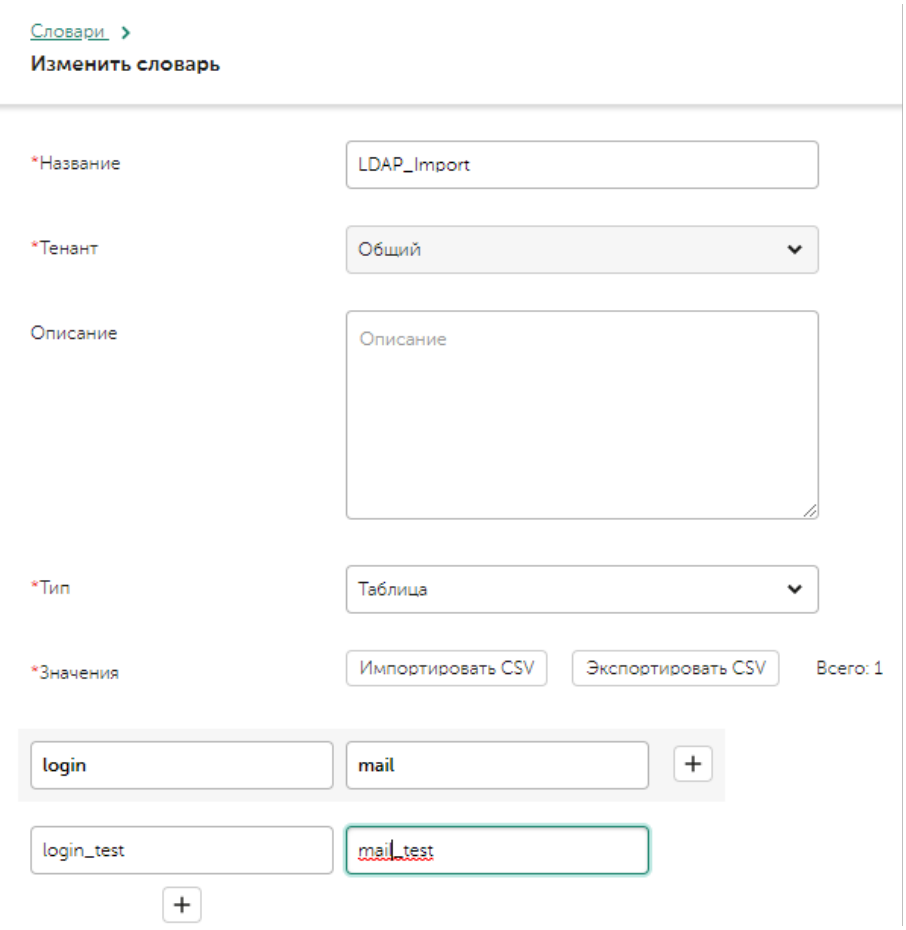
???????? LDAP ????????? ? ??????? KUMA

> Предварительно нужно выполнить настройку обогащение по этой статье https://kb.kuma-community.ru/books/integracii/page/ldap-obogashhenie

????????? ??? KUMA ?? ?????? 4.0

??? 1.

Нам нужно выгрузить сопоставление, например login(sAMAccountName)-mail. Создаете словарь типа таблица (важно), ключ login, колонка mail. Добавляете одну запись любую, чтобы сохранить словарь можно было.



Если нужно выгрузить другое поле, посмотрите его название по примеру вывода одной записи из обогащения:

```
/opt/kaspersky/kuma/mongodb/bin/mongo localhost/kuma --quiet --eval
```

`"db.accounts.findOne({"archived":false})"`

??? 2.

Выбираете пользователя в KUMA, даете ему права на запрос POST /dictionaries/update, генерируете токен и записываете себе куда-нибудь (например в блокнот).

??? 3.

На коре выполняете скрипт (нужно поставить утилиту jq):

```
echo 'login,mail' > /tmp/accounts.csv; /opt/kaspersky/kuma/mongodb/bin/mongo localhost/kuma --eval 'DBQuery.shellBatchSize=<SIZE>; db.accounts.find({"archived":false},{"displayName":1, "sAMAccountName":1, "_id":0})' | grep -E '^{' | jq '.sAMAccountName,.displayName'| sed 'N;s/\n/,/' | sed 's/\"//g' >> /tmp/accounts.csv; curl -k --request POST 'https://<KUMA_IP>:7223/api/v1/dictionaries/update?dictionaryID=<DICTIONARY_ID>' --header 'Content-Type: multipart/form-data' --header 'Authorization: Bearer <TOKEN>' --form 'file=@"/tmp/accounts.csv"'; rm -rf /tmp/accounts.csv
```

- где **<SIZE>** - число записей в выводе, нужно ставить значение кол-во пользователей*1.1
  /opt/kaspersky/kuma/mongodb/bin/mongo localhost/kuma --quiet --eval "db.accounts.find({"archived":false},{"displayName":1, "sAMAccountName":1, "_id":0}).count()" полученное число умножить на 1.1 Или сразу посчитать с помощью: perl -w -e "use POSIX; print ceil($(/opt/kaspersky/kuma/mongodb/bin/mongo localhost/kuma --quiet --eval "db.accounts.find({"archived":false},{"displayName":1, "sAMAccountName":1, "_id":0}).count()")*1.1), qq{\n}"
- **<KUMA_IP>** - ip-адрес ядра KUMA
- **<DICTIONARY_ID>** - id словаря, можно скопировать из строки браузера, если зайти в словарь
- **<TOKEN>** - токен для доступа к API, скопированный на Шаге 2.

После выполнения скрипта, в словарь запишутся логины и их электронная почта, импортированные из AD.

Более продвинутый заполненный запрос с автоподсчетом **<SIZE>**:

```
SIZE=$(perl -w -e "use POSIX; print ceil($(/opt/kaspersky/kuma/mongodb/bin/mongo localhost/kuma --quiet --eval "db.accounts.find({"archived":false},{"sAMAccountName":1, "mail":1, "_id":0}).count()")*1.1), qq{\n}"); echo 'login,mail' > /tmp/accounts.csv;
```

```
/opt/kaspersky/kuma/mongodb/bin/mongo localhost/kuma --eval 'DBQuery.shellBatchSize='$SIZE';
db.accounts.find({"archived":false},{"sAMAccountName":1, "mail":1, "_id":0})' | grep -E '^{' |
jq '.sAMAccountName,.mail'| sed 'N;s/\n/,/' | sed 's/\"//g' >> /tmp/accounts.csv; curl -k --
request POST 'https://10.68.85.125:7223/api/v1/dictionaries/update?dictionaryID=72323930-c4fb-
43c7-9360-5f8d5d929bbb' --header 'Content-Type: multipart/form-data' --header 'Authorization:
Bearer 29ed4e42e25f7877c5ceb435736f860f' --form 'file=@"/tmp/accounts.csv"'; rm -rf
/tmp/accounts.csv
```

?????????? ??? KUMA ?? ?????? 4.0

> Воспользуйтесь скриптом из https://github.com/KUMA-Community/KUMA-sqlite-to-table