Интеграция Почты VK WorkSpace с LDAP-каталогами

Инструкция для администраторов

Портал с документацией: https://biz.mail.ru/docs/on-premises/

Оглавление

Назначение документа

В документе описано как настроить интеграцию с LDAP-каталогами, какие данные могут быть перенесены, какие есть ограничения.

Дополнительные материалы

Документ разработан на основе одного из обучающих курсов по Почте.

Обучение по продуктам VK Tech

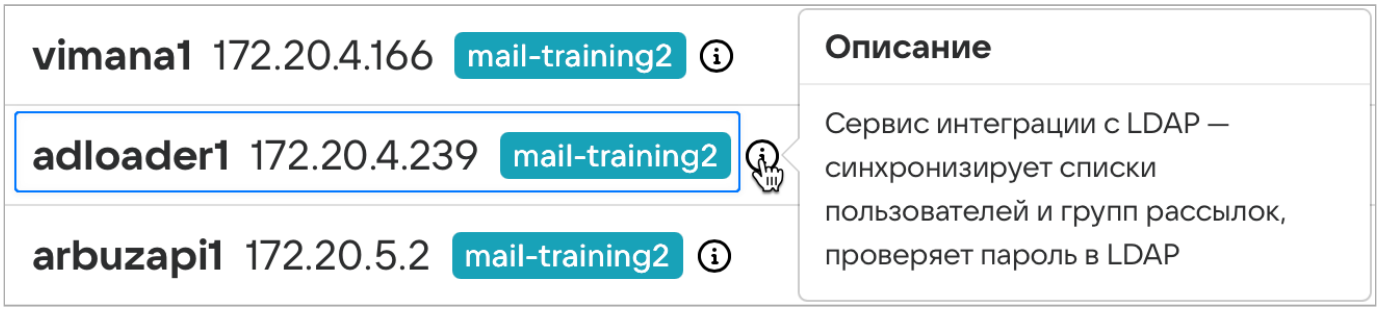
Зарегистрироваться на платформе

Требования к администраторам

- Работа со службами каталогов и с инструментами диагностики LDAP запросов.
- Чтение и анализ системных журналов.
- Знание bash/awk/sed/vim.
- Опыт работы с одной из технологий оркестрации и контейнеризации (docker compose/podman/kubernetes).

Сервис синхронизации и интерфейсы для настройки

За синхронизацию со службами каталогов отвечает сервис **AD Loader**. Несмотря на название, он работает с любыми LDAP-каталогами, не только с Microsoft Active Directory.



Ключевые функции:

- Синхронизация аккаунтов, алиасов (синонимов), контактов, статических групп рассылок и общих ящиков.
- Провайдер авторизации.
- Коннектор к LDAP для других сервисов почтовой системы.

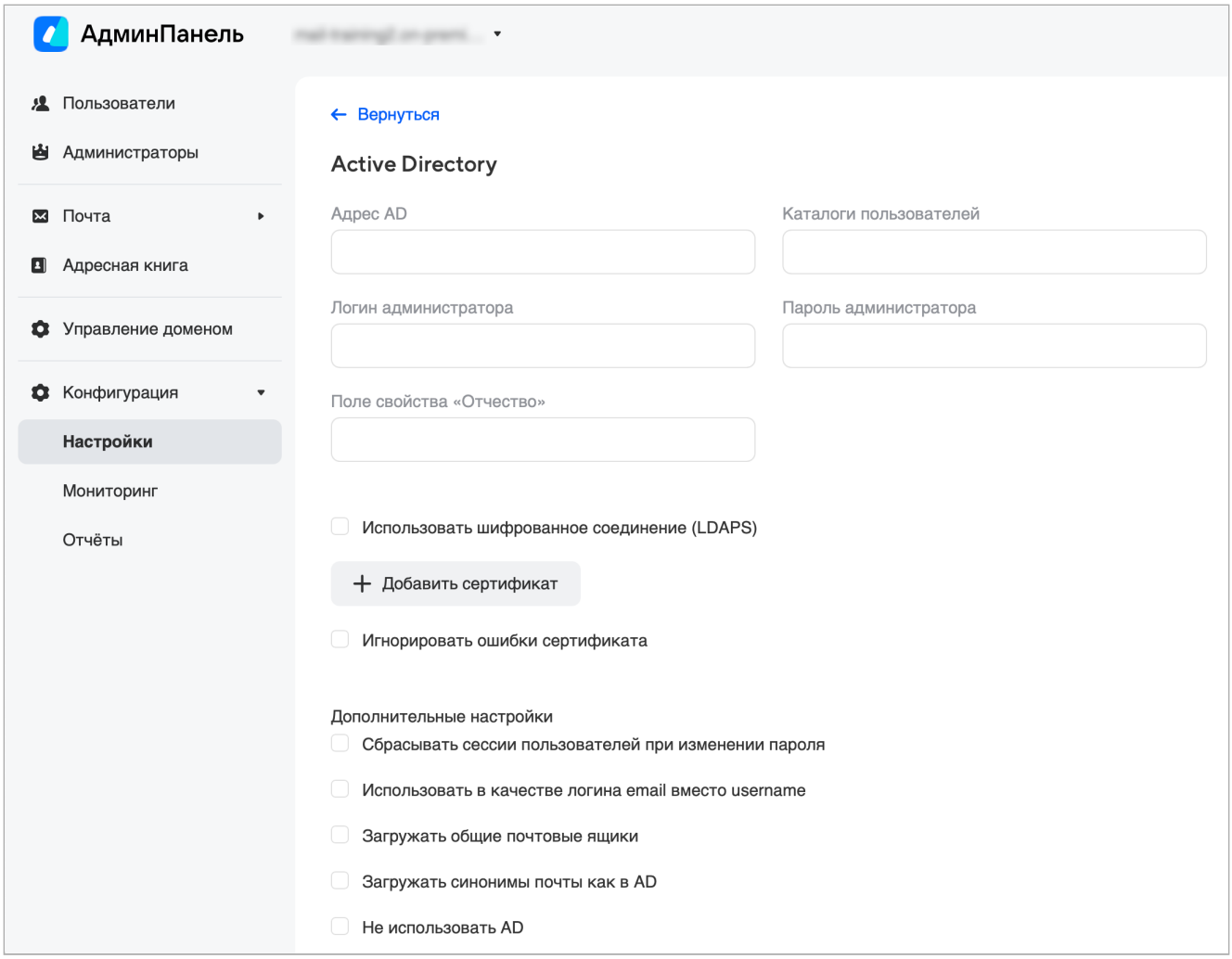
Если при распределении контейнеров вы следовали документации, то контейнеры **adloader*** находятся на машинах с типом Фронт. На главной странице веб-интерфейса установщика вы можете найти контейнеры **adloader*** и узнать на каких машинах они находятся. Чтобы посмотреть логи сервиса используйте команду:

```
sudo journalctl -fu onpremise-container-adloaderN
```

где N – номер AD Loader'a.

Первичная настройка сервиса в панели администратора

1. Авторизуйтесь в панели администратора `https://biz.<ваш домен>`.
2. Перейдите в раздел **Конфигурация → Настройки**. По умолчанию синхронизация отключена.
3. Чтобы включить синхронизацию, нажмите на **Active Directory**. Вы попадете на страницу настройки подключения.
4. Снимите галку с пункта **Не использовать AD**, чтобы поля в форме стали доступными для редактирования.



5. Заполните основные поля:

Поле	Значение	Формат	Комментарии
Адрес AD	IP-адрес каталога	IPv4	
Каталоги пользователей	Значение поля distinguishedNameиз списка атрибутов каталога	OU=<>,DC=<>,DC=<>	
Логин администратора	Distinguished Name (DN) пользователя Active Directory с правами на чтение каталога	CN=<>,OU=<>,DC=<>	Пользователю необходимы права на чтение каталога, пользователь не обязан быть администратором
Пароль администратора	Пароль пользователя, от имени которого		Пароль пользователя, указанного в поле

Поле	Значение	Формат	Комментарии
	происходит подключение к каталогу		Логин администратора
Поле свойства «Отчество»	Отметьте, если хотите синхронизировать отчество. Опционально.		Если используется отчество, указать из какого атрибута в каталоге забирать значение

Совет

Если вы хотите, чтобы по результатам первичной настройки синхронизация не начиналась до момента, пока вы не настроите остальные параметры, оставьте пустым поле **Каталоги пользователей**. В дальнейшем для старта синхронизации вы сможете указать путь к данным в каталоге в режиме расширенной настройки сервиса AD Loader.

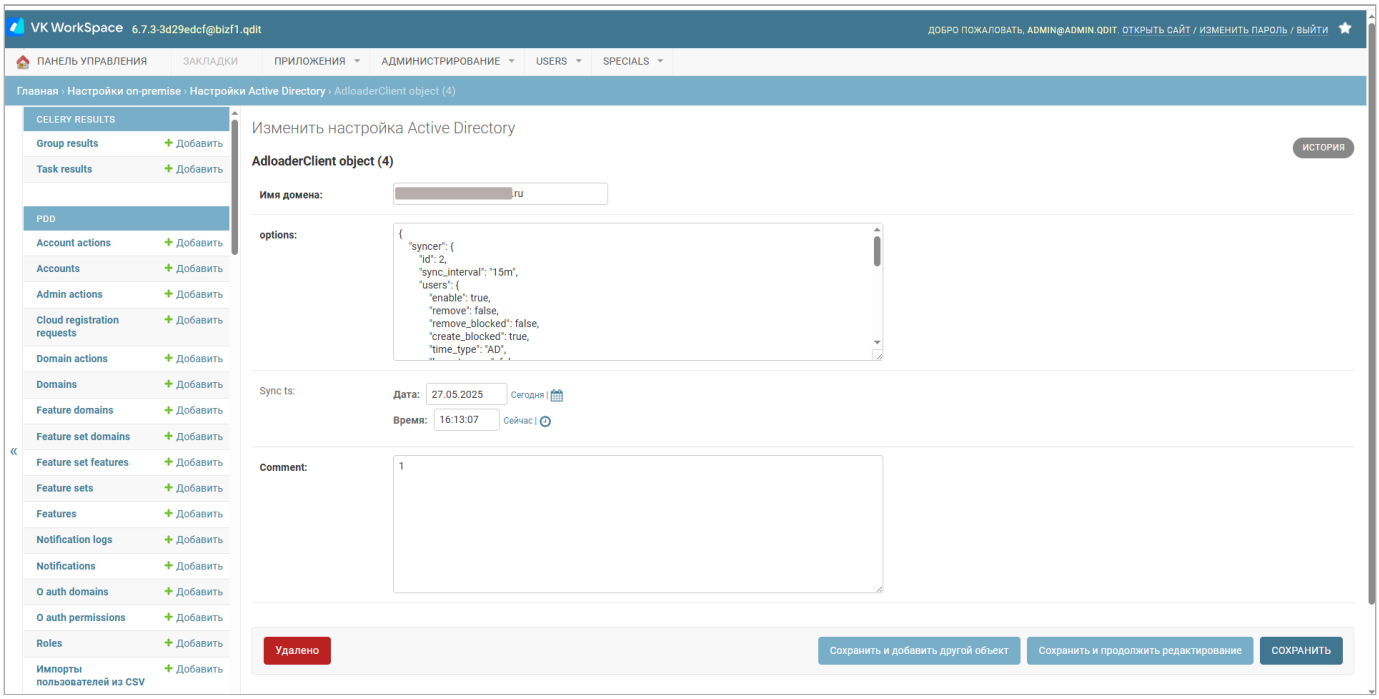
6. Если вы хотите использовать LDAP over SSL (LDAPS), вам необходимо будет настроить LDAPS на контроллере домена и отметить чекбокс **Использовать шифрованное соединение (LDAPS)**. При необходимости вы можете добавить LDAPS сертификат, нажав на соответствующую кнопку. Если CA не корневой, а собственный (не публичный), дополнительно отметьте чекбокс **Игнорировать ошибки сертификата**.
7. Заполните чекбоксы для дополнительных настроек:

Чекбокс	Описание
Сбрасывать сессии пользователей	Если чекбокс отмечен, при изменении пароля пользователя в Active Directory будет сбрасываться сессия в Почте.
Использовать в качестве логина email вместо username	В текущей версии поле не используется
Загружать общие почтовые ящики	Отметьте этот чекбокс, чтобы синхронизировать общие ящики с AD
Загружать синонимы почты как в AD	Отметьте этот чекбокс, чтобы синхронизировать почтовые адреса для аккаунта (синонимы) с AD. Перед интеграцией с AD Exchange нужно предварительно завести все домены из

Чекбокс	Описание
	Exchange в Почте VK WorkSpace. Иначе часть синонимов не будет создана.

Расширенная настройка сервиса AD Loader

Расширенная настройка производится в панели администратора по адресу `biz.<mail_domain>/admin/misc/configurations/adloaderclient/`. Чтобы выполнить расширенную настройку нужно предварительно авторизуйтесь в панели администратора `https://biz.<ваш домен>` под пользователем admin@admin.qdit.



Поле	Описание	Комментарии
Имя домена	Имя почтового домена вашей инсталляции	Если у вас в инсталляции несколько почтовых доменов, то для каждого домена AD Loader нужно настраивать отдельно. Для каждого домена должен быть свой конфигурационный файл (JSON)
options	Поле для конфигурационного файла с настройками синхронизации (JSON)	Файл уже будет содержать те первичные настройки, которые вы задали в панели администратора в разделе Конфигурация → Настройки → Active Directory. Помимо стартовых настроек, в этом файле можно указать большое количество тонкостей. Структуру JSON разберем отдельно.
Sync ts:		

Поле	Описание	Комментарии
	Время следующей синхронизации с LDAP-каталогом	Если нужно принудительно запустить синхронизацию, можно установить **Сегодня** и **Сейчас** → сохранить → перезапустить сервис AD Loader'a. Синхронизация начнется.Подобную процедуру на продуктивных инсталляциях рекомендуется выполнять в окно обслуживания, так как в момент перезапуска AD Loader'a перестанет работать авторизация.

Ниже вы найдете описание структуры файла конфигурации, которое задается в поле **options**.

Структура файла конфигурации

> **Внимание**
>
> Описание ниже соответствует версии Почты 1.24. В релизе 25.2 структура значительно изменилась.

Конфигурация задается в JSON (JavaScript Object Notation). В основе конфигурационного файла — два крупных логических блока **syncer** и **ad_client**. В блоке **syncer** задаются параметры синхронизации данных, в блоке **ad_client** — параметры подключения к каталогу.

```
{
    "syncer" : {
        "id" : 1,
        "sync_interval" : "1h",
        "common" : {},
        "users" : {},
        "mailing" : {},
        "contacts" : {},
        "shared" : {}
    },
    "ad_client" : {
        "username" : "",
        "password" : "",
        "base_dn" : [],
        "address" : "",
        "page_size" : 100,
        "use_tls" : false,
        "tls_cert" : "",
        "skip_insecure" : false,
        "auth_timeout": "",
        "fetch_timeout": "",
        "connect_timeout": "",
        "max_conn_per_server": "",
        "max_rps": "",
        "initial_backoff_interval": "",
        "max_backoff_interval": "",
        "authRestrictions":{}
```

```
    }
}
```

Поле	Тип	Описание
username	string	Логин пользователя, под которым происходит подключение к службе каталогов
password	string	Пароль пользователя, под которым происходит подключение к службе каталогов
base_dn	array	Список каталогов, которые необходимо синхронизировать. Это — массив, поэтому можно перечислить несколько каталогов, а не только один, как в веб-интерфейсе первичной настройки.
address	string	Адрес сервера службы каталогов
page_size	number	Количество объектов на один запрос к службе каталогов
use_tls	boolean	Использовать TLS при подключении к серверу службы каталогов
tls_cert	string	Сертификат, удостоверяющий сертификат сервера службы каталогов (или сертификат сервера, или корневой)
skip_insecure	boolean	Не проверять сертификат службы каталогов.
auth_timeout	string	Таймаут на авторизацию AD
fetch_timeout	string	Таймаут на получение данных AD
connect_timeout	string	Таймаут на подключение к AD
max_conn_per_server	string	Максимальное количество подключений к AD
max_rps	string	Максимальное количество запросов к AD в секунду
initial_backoff_interval	string	Начальный интервал для пропуска итерации синхронизации с AD
max_backoff_interval	string	

Поле	Тип	Описание
		Максимальный интервал для пропуска итерации синхронизации с AD
authRestricitons	object	Ограничение SSO-авторизации

Примечание

В поле **tls_cert** можно прописать ваш CA. Если такой необходимости нет, выставите **skip_insecure** в `true`. В этом случае, каким бы CA не был подписан ваш сертификат, AD Loader подключится.

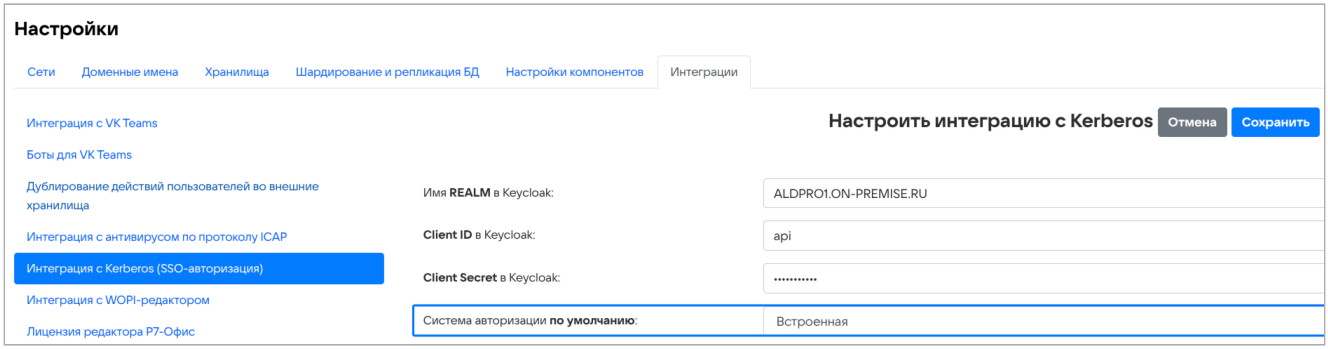
Внимание

AD Loader не умеет работать с редиректами, то есть если у вас распределенный лес, вы столкнетесь с проблемой.AD Loader умеет подключаться к конкретной Active Directory, и конкретная Active Directory должна отвечать. Базовых каталогов при этом может быть несколько. Возможное обходное решение — использовать read-only контроллер домена как некий AD Proxy.

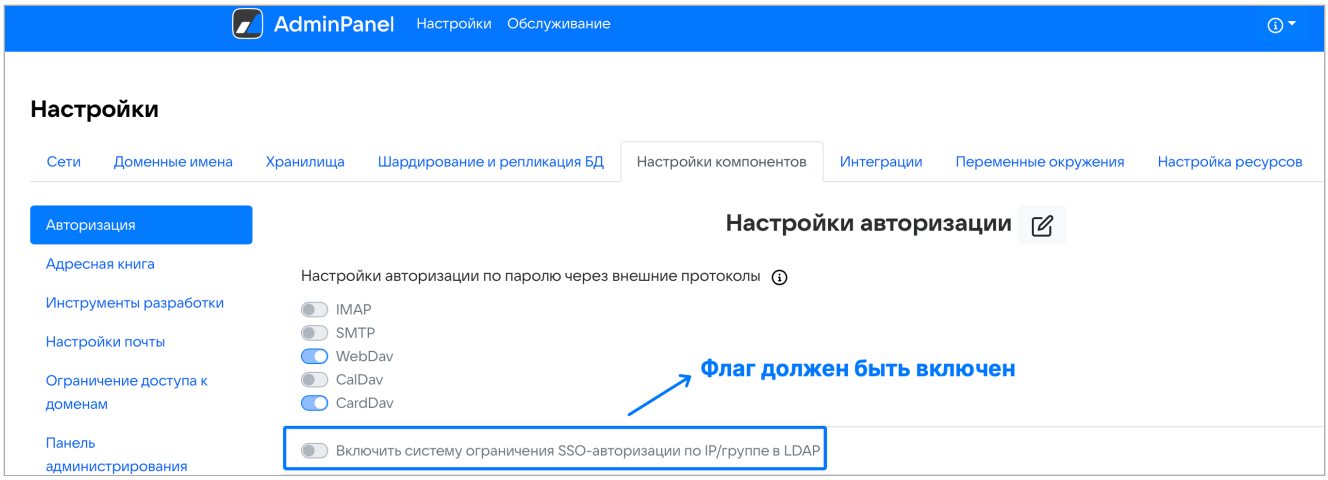
authRestricitons

Блок ad_client может включать блок **authRestricitons**, отвечающий за ограничение SSO-авторизации. Ограничения действуют, только если выполнены два условия:

1. В веб-интерфейсе установщика на вкладке Настройки → Интеграции → Интеграция с Kerberos (SSO-авторизация) в качестве **Системы авторизации** по умолчанию выбрана **Встроенная**.



2. В веб-интерфейсе установщика на вкладке Настройки → Настройки компонентов → Авторизация активирован флаг **Включить систему ограничения SSO-авторизации по IP/группе в LDAP**.



Структура блока authRestrictions:

```
"authRestrictions": {
            "web": { // Приложение для ограничения: web (почта в браузере), imap (подключение
по протоколу IMAP), smtp (подключение по протоколу SMTP). Отсутствие блока, означает
отсутствие ограничений на web авторизацию
                "allowByDefault": false, // Поведение по умолчанию разрешено. Т.е. при
значении true всем пользователям, подходящим под перечисленные ниже политики, авторизация
запрещена, остальным разрешена. При false соответственно всем пользователям авторизация
запрещена, а подходящим под критерии разрешена. Далее при описании политик будем считать, что
здесь значение по-умолчанию, т.е. false
                "policies": [
                    { // Разрешить авторизацию пользователям из перечисленных групп с
указанных ip
                        "nets": ["192.168.1.1","172.168.1.0/24","172.20.70.190/31"],
                        "groups": ["CN=adgrouptest,OU=exch,DC=ad,DC=on-
premise,DC=ru","CN=adgrouptest2,OU=exch,DC=ad,DC=on-
premise,DC=ru","CN=adgrouptest3,OU=exch,DC=ad,DC=on-premise,DC=ru"]
                    },
                    { // Разрешить авторизацию всем пользователям (любых групп) при
подключении с IP 192.168.2
                        "nets": ["192.168.2"]
                    },
                    { // Разрешить авторизацию с любых IP пользователям из группы
"CN=adgrouptest4,OU=exch,DC=ad,DC=on-premise,DC=ru"
                        "groups": ["CN=adgrouptest4,OU=exch,DC=ad,DC=on-premise,DC=ru"]
                    }
                ]
            },
            "imap": {...}, // Блок, аналогичный web, но для IMAP клиентов. Отсутствие блока
означает отсутствие ограничений на imap авторизацию
            "smtp": {...} // Блок, аналогичный web, но для SMTP клиентов. Отсутствие блока
означает отсутствие ограничений на smtp авторизацию
        }
```

Блок syncer

Поле	Тип	Описание
id	number	

Поле	Тип	Описание
		id домена, выставляется автоматически при создании подключения из основного интерфейса панели администратора
sync_interval	string	Интервал синхронизации. Значение по умолчанию — 1h, то есть один час.
common	object	Общие настройки для всех задач синхронизации
users	object	Настройки синхронизации пользователей
mailing	object	Настройки синхронизации групп рассылок
contacts	object	Настройки синхронизации контактов
shared	object	Настройки синхронизации общих ящиков

sync_interval — очень важный параметр. На сегодняшний день AD Loader'ы не умеют договариваться между собой о том, какой из них будет синхронизировать, кроме как в момент запуска. Если у вас будет достаточно маленький sync_interval, то несколько AD Loader'ов запустятся одновременно и создадут нагрузку, которая может привести к деградации панели администратора. Поэтому интервал лучше сразу задать побольше. Затем после первой и самой долгой синхронизации вы уже будете знать, сколько времени системе необходимо на синхронизацию, и сможете уменьшить этот интервал.

common — общие настройки для всех задач синхронизации

Логический блок common появился в версии 1.24. В этом блоке собраны все настройки для всех задач синхронизации, в том числе общие настройки маппинга полей.

Маппинг — это сопоставление данных между Почтой и LDAP-каталогом. Разберём на примере привычного, «человеческого» имени пользователя. В Почте предусмотрено поле **first_name**. В LDAP это имя может находиться в разных полях в зависимости от конфигурации. Чтобы данные передавались правильно, мы настраиваем маппинг: указываем, что поле first_name в нашей системе должно заполняться значением из определённого поля в LDAP. По умолчанию всё настроено на Microsoft Active Directory, и в поле **first_name** в нашей системе будет взято значение из поля **givenName**.

> **Примечание**
>
> Если вы используете не Microsoft Active Directory, а ALD Pro, FreeIPA или какой-то другой LDAP-каталог, маппинг полей потребуется отредактировать, чтобы AD Loader знал, откуда брать каждый из параметров.

Маппинг полей задается в логическом блоке **attr_map**. Структура attr_map следующая: слева поле из Почты VK WorkSpace, справа поле из LDAP-каталога. Набор полей Почты VK WorkSpace зафиксирован, нельзя добавить новое поле в левую часть. Некоторые поля, например, middle_name (отчество), можно не синхронизировать.

Пример заполнения для Microsoft Active Directory

```
"common": {
    "attr_map": {
             "account_state":          "userAccountControl",
             "address":                "streetAddress",
             "avatar":                 "thumbnailPhoto",
             "boss":                   "manager",
             "comment":                "description",
             "company":                "company",
             "department":             "department",
             "display_name":           "displayName",
             "dn":                     "distinguishedName",
             "fax_number":             "facsimileTelephoneNumber",
             "first_name":             "givenName",
             "fullAccMembers":         "msExchMailboxSecurityDescriptor",
             "gssapi_mail":            undefined,
             "gssapi_proxy_addresses": undefined,
             "gssapi_unique_name":     undefined,
             "home_number":            "homePhone",
             "initials":               "initials",
             "last_name":              "sn",
             "mail":                   "mail",
             "member":                 "member",
             "member_of":              "memberOf",
             "middle_name":            "",
             "mobile_number":          "mobile",
             "office":                 "physicalDeliveryOfficeName",
             "position":               "title",
             "proxy_addresses":        "proxyAddresses",
             "pwd_last_set":           "pwdLastSet",
             "sendAsMembers":          "nTSecurityDescriptor",
             "sid":                    "objectSid",
             "unique_name":            "userPrincipalName",
             "work_number":            "telephoneNumber"
            }
        },
```

Для удобства разобьем поля на условные группы.

«Простые» поля

Поле	Атрибут из Microsoft Active Directory	Описание
address	streetAddress	Адрес контакта (физический, не MAC)
avatar	thumbnailPhoto	Фото пользователя в кодировке base64

Поле	Атрибут из Microsoft Active Directory	Описание
comment	description	Комментарий к контакту
company	company	Название организации
department	department	Название подразделения в организации, где работает контакт
display_name	displayName	Отображаемое имя объекта — работает для всех блоков, кроме users (пользователи) и contacts (контакты). Для них отображаемое имя пользователя соберётся из других атрибутов
fax_number	facsimileTelephoneNumber	Номер факса
first_name	givenName	«Человеческое» имя пользователя
home_number	homePhone	Домашний телефонный номер
initials	initials	Инициалы пользователя
last_name	sn	Фамилия пользователя
middle_name		Отчество пользователя, по умолчанию не синхронизируем
mobile_number	mobile	Мобильный телефонный номер
office	physicalDeliveryOfficeName	Название офиса организации, где работает контакт
position	title	Должность

Поля mail и proxy_addresses

> **Внимание**
>
> Для Почты VK WorkSpace email пользователя является его основным идентификатором.

Поле	Атрибут из Microsoft Active Directory	Описание
mail	mail	email пользователя. Формат в Active Directory: "user@domain.ru". Строковое поле, т.е. не может содержать несколько значений
proxy_addresses	proxyAddresses	Список альтернативных почтовых адресов (алиасов). Общий формат: `["smtp:alisa@domain.ru"]`, где [] означает, что записей может быть несколько. Префикс заглавными буквами `"SMTP:main@domain.ru"` означает, что этот адрес будет считаться главным, если не указан другой в поле mail.

Поля mail и proxy_addresses унифицированы. В поле mail ожидаем просто email, а в поле proxy_addresses — набор вида `["smtp:alisa@domain.ru", "smtp:alisa1@domain.ru"]`. Строка в поле proxy_addresses тоже допустима, если у нее есть префикс smtp.

В качестве основного email в приоритете пробуем забрать значение из поля mail. Если в поле mail ничего не нашли, или по каким-то причинам найденное значение не подходит, то в качестве основного email заберем email с префиксом SMTP (именно заглавными буквами) из поля proxy_addresses.

Так сделано, потому что каждый домен для синхронизации использует свой файл конфигурации. При кроссдоменных алиасах может возникнуть ситуация, когда в двух доменах будет создан один и тот же пользователь. Чтобы этого не происходило, мы создаем только того пользователя, у которого указан префикс SMTP большими буквами (стандарт Microsoft Exchange).

Авторизация, безопасность, синхронизация групп рассылок и общих ящиков

Поле	Атрибут из Microsoft Active Directory	Описание
account_state	userAccountControl	По этому полю определяем статус пользователя, не заблокирован ли он. Применяется только для блока users. Поддерживается только формат Active Directory (https://learn.microsoft.com/en-us/troubleshoot/windows-server/active-directory/useraccountcontrol-manipulate-account-properties#useraccountcontrol-values. В планах поддержка других LDAP-каталогов
boss	manager	DN руководителя
dn	distinguishedName	Уникальный ключ записи. Не видим в панели администратора. Необходим для установки связей между объектами, например между группой и её участниками/
fullAccMembers	msExchMailboxSecurityDescriptor	Поле ограничения доступа к общему ящику в Microsoft Active Directory. Из этого поля берётся список пользователей общего ящика с ролью “владелец”.
member	member	Список участников группы
member_of	memberOf	Список групп, в которых состоит объект
sendAsMembers	nTSecurityDescriptor	Поле ограничения доступа к общему ящику в MS AD. Из этого поля берётся список пользователей общего ящика с ролью «участник».

Поле	Атрибут из Microsoft Active Directory	Описание
pwd_last_set	pwdLastSet	Дата последней смены пароля пользователя. Все сессии старше этой даты сбрасываем. Попытка сброса будет сделана, даже если сессии старше указанной даты не нашлось. Это отключаемая функция, сессии можно и не сбрасывать. Включается чек-боксом "Сбрасывать сессии пользователей" в настройках подключения к AD в панели администратора
sid	objectSid	Уникальный идентификатор объекта в LDAP. Необходим для установки связи между общим ящиком и объектом, которому назначены права.
unique_name	userPrincipalName	Логин пользователя в AD (нужен для авторизации)

unique_name – поле, в котором лежит логин. К значению из этого поля добавляем пароль, который передает пользователь, и проверяем валидность. Если AD Loader получит пустой **unique_name**, пользователь не будет синхронизирован. Это сделано специально, чтобы избежать ситуации: «пользователь создался, но не может авторизоваться». Если используется не Microsoft Active Directory, а другой LDAP-каталог, настройки маппинга для этого поля нужно будет поменять.

dn, **member** и **member_of** нужны, чтобы найти взаимосвязи между объектами в LDAP. Например, бывают пользователи, которые включены в общие ящики, которые в свою очередь включены в группу рассылки. Важно не потерять эти связи при синхронизации.

Как устроена работа с группами рассылок?

До релиза 1.24 использовался следующий подход: сначала найти пользователя, затем определить группы рассылки, в которые он входит по полю **member_of**.

Начиная с релиза 1.24, появилась возможность действовать наоборот: сначала найти группу рассылки, затем по полю **member** объекта группы рассылки получить список всех пользователей.

По умолчанию этот способ отключен, использовать его рекомендуется аккуратно. Регулируется через **syncByMember: true** в логическом блоке **malings**, отвечающем за синхронизацию групп рассылок.

Примечание

Синхронизируются только статические группы рассылок. Динамические группы рассылок, представляющие собой некий запрос к каталогу, не синхронизируются.

Как устроена работа с общими ящиками?

Для общих ящиков не предусмотрена синхронизация по списку пользователей: AD Loader не может просмотреть, к каким общим ящикам есть доступ у каждого пользователя, и автоматически перенести этот доступ.

Работает следующий механизм: найти общий ящик и идентифицировать всех его пользователей. У общего ящика есть атрибуты, в которых прописано, кто из пользователей и с какими правами имеет доступ к ящику.

В Microsoft Active Directory, это атрибуты **msExchMailboxSecurityDescriptor** и **nTSecurityDescriptor**. Соответственно, маппинг выглядит так:

```
"fullAccMembers": "msExchMailboxSecurityDescriptor", //список пользователей общего ящика с ролью “владелец”
"sendAsMembers": "nTSecurityDescriptor", // список пользователей общего ящика с ролью “участник”
```

Примечание

В Почте VK WorkSpace нет возможности заблокировать общий ящик. Если общий ящик найден по фильтру, то он будет перенесен, несмотря на статус.

Kerberos авторизация

Отдельно рассмотрим группу полей с префиксом **gssapi**. Эти поля используются в случае Kerberos-авторизации.

Поле	Описание	Комментарий
gssapi_mail	Аналог mail для gssapi запросов. По умолчанию значение не не задано и равно mail.	Используется только в том случае, если по каким-то причинам email при синхронизации (и парольной авторизации) и kerberos (gssapi) авторизации отличаются
gssapi_proxy_addresses	Аналог proxy_addresses для gssapi запросов. По умолчанию не задано и равно proxy_addresses.	Используется только в том случае, если по каким-то причинам списки дополнительных почтовых адресов при синхронизации (и парольной авторизации) и kerberos (gssapi)

Поле	Описание	Комментарий
		авторизации отличаются. Например, когда при синхронизации дополнительные почтовые адреса учитывать не нужно (proxy_addresses= gssapi_proxy_addresses= proxyAddresses)
gssapi_unique_name	Аналог unique_name для gssapi запросов. По умолчанию не задано и равно unique_name.	Используется только в том случае, если по каким-то причинам логины (идентификаторы пользователей) при парольной и kerberos (gssapi) авторизации отличаются

Блок синхронизации пользователей (users)

> **Внимание**
>
> В каждом из блоков — users, contacts, mailing и shared — есть свой собственный attr_map, обладающий более высоким приоритетом по сравнению с attr_map блока common. Например, если для контактов имя должно извлекаться из одного поля, а для пользователей — из другого, эти настройки следует указать в attr_map блоков contacts и users, соответственно.

Пример заполнения для Microsoft Active Directory

```
        "users": {
            "enable":            true,
            "remove":            true,
            "filter":            "&(objectclass=user)(objectCategory=person)",
            "logout_users":      false,
            "block_removed":     true,
            "remove_blocked":    false,
            "create_blocked":    true,
            "aliasSync":         false,
            "aliasRemove":       false,
            "aliasAsUserRemove": false,
            "time_type":         "AD",
            "loginFilter":       "",
            "gssapiFilter":      "",
            "attr_map": {
                "account_state":          "userAccountControl",
                "avatar":                 "thumbnailPhoto",
                "boss":                   "manager",
                "comment":                "description",
                "company":                "company",
                "department":             "department",
                "dn":                     "distinguishedName",
                "fax_number":             "facsimileTelephoneNumber",
```

```
            "first_name":             "givenName",
            "gssapi_mail":            undefined,
            "gssapi_proxy_addresses": undefined,
            "gssapi_unique_name":     undefined,
            "home_number":            "homePhone",
            "initials":               "initials",
            "last_name":              "sn",
            "mail":                   "mail",
            "member_of":              "memberOf",
            "middle_name":            "",
            "mobile_number":          "mobile",
            "office":                 "physicalDeliveryOfficeName",
            "position":               "title",
            "proxy_addresses":        "proxyAddresses",
            "pwd_last_set":           "pwdLastSet",
            "sid":                    "objectSid",
            "unique_name":            "userPrincipalName",
            "work_number":            "telephoneNumber"
        }
    },
```

Поле	Тип	Описание	Комментарий
enable	boolean	Включить синхронизацию пользователей	
remove	boolean	Удалять пользователей, отсутствующих в AD	
filter	string	AD фильтр для поиска пользователей	По умолчанию используется **"&(objectclass=user)(objectCategory=person)"**
logout_users	boolean	Сбрасывать сессию пользователям при изменении пароля в AD	
block_removed	boolean	Блокировать не найденных в AD пользователей вместо удаления	Для блокировки и значение в поле remove должен быть выставлено в true
remove_blocked	boolean	Удалять заблокированных пользователей	

Поле	Тип	Описание	Комментарий
create_blocked	boolean	Создавать в панели администратора пользователей, заблокированных в AD, и сразу блокировать их в панели администратора	
aliasSync	boolean	Включить синхронизацию алиасов	
aliasRemove	boolean	Удалять алиасы пользователей, отсутствующих в AD	
aliasAsUserRemove	boolean	Удалять алиасы пользователей, созданные как отдельные пользователи	Более подробное описание под таблицей
time_type	string	Формат времени в LDAP клиента	- "AD" — формат времени, используемый в ActiveDirectory. - "FreeIPA" — формат времени, используемый во freeIPA. Любое другое значение не будет распознано и сессии пользователей не будут сброшены.
loginFilter	string	AD фильтр для поиска пользователей при парольной авторизации. По умолчанию пуст и равен filter.	Нужен только в том случае, если по каким-то причинам фильтр авторизации по паролю отличается от фильтра синхронизации пользователей. Например, когда нужно синхронизировать всех пользователей, а разрешить авторизовываться только тем, кто не в отпуске.

Поле	Тип	Описание	Комментарий
			Фильтр не поддерживает подстановки ("%[1]s")
gssapiFilter	string	AD фильтр для поиска пользователей при kerberos (gssapi) авторизации.По умолчанию пуст и равен filter.	Нужен только в том случае, если по каким-то причинам фильтр авторизации по kerberos отличается от фильтра синхронизации пользователей. Например, когда почтовых доменов много, а kerberos (AD) домен общий. **Фильтр не поддерживает постановки ("%[1]s")**
attr_map	object	Поле для кастомизации отображения AD пользователей в пользователи панели администратора.	Набор пар вида "поле в панели администратора" : "поле в AD"

Механизм синхронизации алиасов изменился, начиная с версии 1.24. Независимо от того, синхронизируете вы алиасы или нет, они больше не создаются как обычные пользователи.

Алиасы, которые ранее были созданы как пользователи, регулируются полем **aliasAsUserRemove**:

- `"aliasAsUserRemove": true` — такие пользователи будут удалены.
- `"aliasAsUserRemove": false` — пользователи обновляться не будут, а в логе AD Loader'a появится ошибка вида `we are not syncing aliases`.

attr_map по составу аналогичен attr_map блока common. Напоминаем, что индивидуальный маппинг в конкретном блоке приоритетнее общего в **common**.

Поле	Атрибут из Microsoft Active Directory	Описание
account_state	userAccountControl	По этому полю определяем статус пользователя, не заблокирован ли он. Поддерживается только формат Active Directory (https://learn.microsoft.com/en-us/troubleshoot/windows-server/active-directory/

Поле	Атрибут из Microsoft Active Directory	Описание
		useraccountcontrol-manipulate-account-properties#useraccountcontrol-values.
address	streetAddress	Адрес контакта (физический, не MAC)
avatar	thumbnailPhoto	Фото пользователя в кодировке base64
boss	manager	DN руководителя
comment	description	Комментарий к контакту
company	company	Название организации, где работает пользователь. Синхронизируем только если выполняются оба условия: - Выключена синхронизация контактов — в блоке contacts enable выставлено в false - В фичах включена общая адресная книга По умолчанию фича включена, если что-то пойдет нет так — см. раздел Траблшутинг
department	department	Название организации, где работает пользователь. Синхронизируем только если выполняются оба условия: - Выключена синхронизация контактов — в блоке contacts enable выставлено в false - В фичах включена общая адресная книга По умолчанию фича включена, если что-то пойдет нет так — см. раздел Траблшутинг
dn	distinguishedName	Уникальный ключ записи. Не видим в панели администратора.

Поле	Атрибут из Microsoft Active Directory	Описание
		Необходим для установки связей между группой и пользователем.
fax_number	facsimileTelephoneNumber	Номер факса. Синхронизируем только если выполняются оба условия: - Выключена синхронизация контактов — в блоке contacts enable выставлено в false - В фичах включена общая адресная книга По умолчанию фича включена, если что-то пойдет нет так — см. раздел Траблшутинг
first_name	givenName	Имя пользователя
gssapi_mail	undefined	Аналог mail для gssapi запросов. По умолчанию не задано и равно mail. Используется только в том случае, если по каким-то причинам email при синхронизации (и парольной авторизации) и kerberos (gssapi) авторизации отличаются.
gssapi_proxy_addresses	undefined	Аналог proxy_addresses для gssapi запросов. По умолчанию не задано и равно proxy_addresses. Используется только в том случае, если по каким-то причинам списки дополнительных почтовых адресов при синхронизации (и парольной авторизации) и kerberos (gssapi) авторизации отличаются.
gssapi_unique_name	undefined	Аналог unique_name для gssapi запросов. По умолчанию не задано и равно uniq_name. Используется только в том случае, если по каким-то причинам логины

Поле	Атрибут из Microsoft Active Directory	Описание
		(идентификаторы пользователей) при парольной и kerberos (gssapi) авторизации отличаются
home_number	homePhone	Домашний телефонный номер. Синхронизируем только если выполняются оба условия: - Выключена синхронизация контактов — в блоке contacts enable выставлено в false - В фичах включена общая адресная книга По умолчанию фича включена, если что-то пойдет нет так — см. раздел Траблшутинг
initials	initials	Инициалы пользователя
last_name	sn	Фамилия пользователя
mail	mail	email пользователя. Формат в AD: "user@domain.ru". Строковое поле, т.е. не может содержать несколько значений
member_of	memberOf	Список групп, в которых состоит пользователь
middle_name	""	Отчество пользователя
mobile_number	mobile	Мобильный телефонный номер. Синхронизируем только если выполняются оба условия: - Выключена синхронизация контактов — в блоке contacts enable выставлено в false - В фичах включена общая адресная книга По умолчанию фича включена, если что-то пойдет нет так — см. раздел Траблшутинг

Поле	Атрибут из Microsoft Active Directory	Описание
office	physicalDeliveryOfficeName	Название офиса организации, где работает контакт
position	title	Должность. Синхронизируем только если выполняются оба условия: - Выключена синхронизация контактов — в блоке contacts enable выставлено в false - В фичах включена общая адресная книга По умолчанию фича включена, если что-то пойдет нет так — см. раздел Траблшутинг
proxy_addresses	proxyAddresses	Список альтернативных почтовых адресов (алиасов). Формат в AD: ["smtp:alisa@domain.ru"], где [] означает, что записей может быть несколько
pwd_last_set	pwdLastSet	Дата последней смены пароля пользователя
sid	objectSid	Уникальный идентификатор объекта в LDAP. Необходим для установки связи между общим ящиком и объектом, которому назначены права.
unique_name	userPrincipalName	Логин пользователя в AD (нужен для авторизации).
work_number	telephoneNumber	Рабочий телефонный номер. Синхронизируем только если выполняются оба условия: - Выключена синхронизация контактов — в блоке contacts enable выставлено в false - В фичах включена общая адресная книга

Поле	Атрибут из Microsoft Active Directory	Описание
		По умолчанию фича включена, если что-то пойдет нет так — см. раздел Траблшутинг

Блок синхронизации контактов (contacts)

> **Внимание**
>
> В каждом из блоков — users, contacts, mailing и shared — есть свой собственный attr_map, обладающий более высоким приоритетом по сравнению с attr_map блока common. Например, если для контактов имя должно извлекаться из одного поля, а для пользователей — из другого, эти настройки следует указать в attr_map блоков contacts и users, соответственно.

Пример заполнения для Microsoft Active Directory

```
"contacts": {
            "enable": true,
            "remove": false,
            "filter": "(&(|(mail=*)(proxyAddresses=*))(|(objectclass=contact)
(&(objectclass=user)(objectCategory=person))(&(objectCategory=group)(!groupType:
1.2.840.113556.1.4.803:=2147483648))))",
            "base_dn": [
                "dn1",
                "dn2",
                "dn3"
            ],
            "white_list_domains": [
                "mail.ru",
                "ya.ru",
                "my-domain.ru"
            ],
            "black_list_domains": [
                "outlook.com",
                "dev.local",
                "ad.on-premise.ru"
            ],
            "attr_map": {
                "address":         "streetAddress",
                "boss":            "manager",
                "comment":         "description",
                "company":         "company",
                "department":      "department",
                "display_name":    "name",
                "dn":              "distinguishedName",
                "fax_number":      "facsimileTelephoneNumber",
                "first_name":      "givenName",
                "home_number":     "homePhone",
                "initials":        "initials",
                "last_name":       "sn",
                "mail":            "mail",
```

```
                "middle_name":      "",
                "mobile_number":    "mobile",
                "office":           "physicalDeliveryOfficeName",
                "position":         "title",
                "proxy_addresses":  "proxyAddresses",
                "work_number":      "telephoneNumber",
            }
        },
```

Поле	Тип	Описание	Комментарий
enable	boolean	Включить синхронизацию контактов	
remove	boolean	Удалять контакты, отсутствующие в AD	
filter	string	AD фильтр для поиска контактов	По умолчанию используется "(&(|(mail=)(proxyAddresses=))(|(objectclass=contact)(&(objectclass=user)(objectCategory=person))(&(objectCategory=group)(!groupType:1.2.840.113556.1.4.803:=2147483648))))"
base_dn	array	Кастомный набор директорий в AD для поиска контактов	По-умолчанию пуст — в таком случае используется общий список директорий, откуда синхронизируются пользователи и рассылки.
white_list_domains	array	Белый список почтовых доменов	Если не пуст, то AD Loader будет забирать только те контакты, у которых есть email хотя бы из одного из перечисленных доменов.
black_list_domains	array	Черный список почтовых доменов	Если не пуст, то AD Loader будет забирать только контакты, у которых есть email хотя бы из одного из доменов, не входящих в этот список. То есть если у контакта несколько email, в карточку контакта попадут

Поле	Тип	Описание	Комментарий
			только те, которые не в черном списке.
attr_map	object	Поле для кастомизации отображения AD контактов в контакты панели администратора	Набор пар вида "поле в панели администратора" : "поле в AD".

Контакты и пользователи связаны, то есть если для блока `contacts enable=false`, контакты будут синхронизироваться вместе с пользователями. Это значит, что контакты синхронизируются вместе с пользователями и в контакты попадают только пользователи из вашего домена, контакты из внешних доменов не попадут.

Если в вашем случае список контактов отличается от списка пользователей:

1. Включите блок синхронизации контактов.
2. Задайте фильтр.
3. При необходимости переопределите базовый набор каталогов.
4. Задайте `blacklist` и `whitelist`, чтобы домены вида `dev.local` не попадали в список email'ов.

Описание блока `attr_map`:

Поле	Атрибут из Microsoft Active Directory	Описание
address	streetAddress	Адрес контакта (физический, не email, не MAC)
boss	manager	Руководитель контакта
comment	description	Комментарий к контакту
company	company	Название организации, где работает контакт
department	department	Названия подразделения в организации, где работает контакт
display_name	name	Альтернативное имя контакта. Используется, когда фамилия и имя

Поле	Атрибут из Microsoft Active Directory	Описание
		контакта пусты, например когда контакт — это группа, а не пользователь.
dn	distinguishedName	Уникальный ключ записи. Не видим в панели администратора. Необходим для установки связей между контактами
fax_number	facsimileTelephoneNumber	Номер факса
first_name	givenName	Имя
home_number	homePhone	Домашний телефонный номер
initials	initials	Инициалы — будут использованы в случае отсутствия имени
last_name	sn	Фамилия
mail	mail	Основной email. Формат в AD: "user@domain.ru" — строковое поле, т.е. не может содержать несколько значений.
middle_name	""	Отчество
mobile_number	mobile	Мобильный телефонный номер
office	physicalDeliveryOfficeName	Название офиса организации, где работает контакт
position	title	Должность
proxy_addresses	proxyAddresses	Алиасы (альтернативные почтовые адреса)
work_number	telephoneNumber	Рабочий телефонный номер

Блок синхронизации групп рассылок (mailing)

> **Внимание**
>
> В каждом из блоков — users, contacts, mailing и shared — есть свой собственный attr_map, обладающий более высоким приоритетом по сравнению с attr_map блока common. Например, если для контактов имя должно извлекаться из одного поля, а для пользователей — из другого, эти настройки следует указать в attr_map блоков contacts и users, соответственно.

Пример для Microsoft Active Directory

```
"mailing": {
            "enable":        true,
            "remove":        false,
            "filter":        "(&(objectCategory=group)(!(groupType:
1.2.840.113556.1.4.803:=2147483648)))",
            "syncByMember":  false,
            "membersFilter": "|(&(objectCategory=group)(groupType:
1.2.840.113556.1.4.803:=2147483648))(&(objectclass=user)(objectCategory=person)(!
(msExchRecipientDisplayType=0)))",
            "name_is_email": false,
            "remove_users":  false,
            "attr_map": {
                "display_name":    "name",
                "dn":              "distinguishedName",
                "mail":            "mail",
                "member":          "member",
                "proxy_addresses": "proxyAddresses"
            }
        },
```

Поле	Тип	Описание	Комментарий
enable	boolean	Включить синхронизацию групп рассылки	Значение по умолчанию true
remove	boolean	Удалять группы рассылки, отсутствующие в AD	Значение по умолчанию: false
filter	string	AD фильтр для поиска групп рассылки	По умолчанию используется "(&(objectCategory=group)((groupType: 1.2.840.113556.1.4.803:=2147483648)))"
syncByMember	boolean		

Поле	Тип	Описание	Комментарий
		Значение по умолчанию: false. BETA! Синхронизировать группы рассылки по полю "member" объекта рассылки, вместо поля "member_of" объектов-получателей.	Такой тип синхронизации увеличивает количество запросов к LDAP, так как в поле member лежат DN'ы, а не email'ы. Также в этом режиме AD Loader рекурсивно обойдёт вложенные группы.
membersFilter	string	Поле используется для фильтрации записей в поле "member" при "syncByMember" : true	Значение по умолчанию: "|(&(objectCategory=group)(groupType:1.2.840.113556.1.4.803:=2147483648))(&(objectclass=user)(objectCategory=person)(!(msExchRecipientDisplayType=0)))"
name_is_email	boolean	Если у группы рассылки отсутствует почтовый адрес, попытаться использовать в качестве такового её название.	Значение по умолчанию: false
remove_users	boolean	Управляет удалением пользователей из групп, которые синхронизированы с AD. Работает только при "remove": false. При "remove": true, параметр игнорируется и считается выставленным в true	Значение по умолчанию: true.
attr_map	object	Поле для кастомизации	

Поле	Тип	Описание	Комментарий
		отображения AD групп рассылки в группы рассылки панели администратора	Набор пар "поле в панели администратора" : "поле в AD".

Описание блока `attr_map` :

Поле	Атрибут из Microsoft Active Directory	Описание
display_name	name	Человекочитаемое имя группы
dn	distinguishedName	Адрес рассылки в каталоге AD. Если рассылка есть в списке member_of пользователя в AD, то пользователь будет добавлен в рассылку в панели администратора.
mail	mail	Почтовый адрес рассылки либо её часть до @. Также используется для получения почтового адреса участников рассылки при разборе объекта участника
member	member	Список участников группы
proxy_addresses	proxyAddresses	Список альтернативных почтовых адресов (алиасов). Общий формат: ["smtp:alisa@domain.ru"], где [] означает, что записей может быть несколько. Префикс заглавными буквами "SMTP:main@domain.ru" означает, что этот адрес будет считаться главным, если не указан другой в поле mail и именно он будет использоваться в качестве email, если совпадёт по почтовому домену и в поле mail не будет валидной записи. Работает как для самой рассылки, так и для участников.

Блок синхронизации общих ящиков (shared)

> **Внимание**
>
> В каждом из блоков — users, contacts, mailing и shared — есть свой собственный attr_map, обладающий более высоким приоритетом по сравнению с attr_map блока common. Например, если для контактов имя должно извлекаться из одного поля, а для пользователей — из другого, эти настройки следует указать в attr_map блоков contacts и users, соответственно.

Пример для Microsoft Active Directory

```
"shared": {
            "enable": false,
            "remove": false,
            "filter": "&(objectclass=user)(objectCategory=person)
(msExchRecipientDisplayType=0)",
            "membersRemove": false,
            "membersFilter": "|(&(objectCategory=group)(groupType:
1.2.840.113556.1.4.803:=2147483648))(&(objectclass=user)(objectCategory=person)(!
(msExchRecipientDisplayType=0)))",
            "membersEncode": "AD",
            "base_dn": [
                "dn2",
                "dn3"
            ],
            "attr_map": {
                "display_name": "displayName",
                "dn": "distinguishedName",
                "fullAccMembers": "msExchMailboxSecurityDescriptor",
                "mail": "mail",
                "member": "member",
                "proxy_addresses": "proxyAddresses",
                "sendAsMembers": "nTSecurityDescriptor",
                "sid": "objectSid",
        }
```

Поле	Тип	Описание	Комментарий
enable	boolean	Включить синхронизацию общих ящиков	Значение по умолчанию: fa есть синхронизация общи ящиков отключена.
remove	boolean	Удалять общие ящики, отсутствующие в AD	Значение по умолчанию: fa
filter	string	AD фильтр для поиска общих ящиков	По умолчанию использует "&(objectclass=user) (objectCategory=person) (msExchRecipientDisplayTy

Поле	Тип	Описание	Комментарий
membersRemove	boolean	Управляет удалением пользователей из общих ящиков, которые синхронизированы с AD. Работает только если выполнено условие из колонки "Комментарий".	Значение по умолчанию: fa Работает только при "remo false. При "remove": true, параме игнорируется и считается выставленным в true.
membersFilter	string	Фильтр для поиска участников общего ящика. По умолчанию считаем участниками УЗ пользователей и участников групп безопасности (рекурсивно)	Значение по умолчанию: "|(&(objectCategory=group (groupType: 1.2.840.113556.1.4.803:=2147 (&(objectclass=user) (objectCategory=person)(! (msExchRecipientDisplayTy
membersEncode	string	Возможные значения: "dnList" и "AD". Если указано значение "dnList", то AD Loader ожидает в полях "fullAccMembers" и "sendAsMembers" список DN'ов. В противном случае в этих полях ожидаются nTSecurityDescriptor, как в ActiveDirectory, https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/1522b774-6464-41a3-87a5-1e5633c3fbbb).	Значение по умолчанию: "A
base_dn	array	Кастомный набор директорий в LDAP для поиска общих ящиков	По умолчанию пуст. В этом используется общий спис директорий, откуда синхронизируются пользо и рассылки.
attr_map	object	Поле для кастомизации отображения общих ящиков AD в общие ящики в панели администратора.	Набор пар "поле в панели администратора" : "поле в Сюда передаются парамет `syncer.users.attr_map`, то при кастомизации полей д синхронизации пользовате одноименные параметры переданы и сюда

Описание блока `attr_map`:

Поле	Атрибут из Microsoft Active Directory	Описание
display_name	displayName	Человекочитаемое имя общего ящика.
dn	distinguishedName	Уникальный ключ записи. Невидим в панели администратора. Необходим для установки связей между группой [безопасности] и пользователем.
fullAccMembers	msExchMailboxSecurityDescriptor	Поле ограничения доступа к общему ящику в MS AD. Из этого поля берётся список пользователей общего ящика с ролью "владелец".
mail	mail	Основной email
member	member	Список участников группы [безопасности].
proxy_addresses	proxyAddresses	Алиасы пользователей. Общий формат: ["smtp:alisa@domain.ru"], где [] означает, что записей может быть несколько. Префикс заглавными буквами "SMTP:main@domain.ru" означает, что этот адрес будет считаться главным, если не указан другой в поле mail и именно он будет использоваться в качестве email, если совпадёт по почтовому домену, и в поле mail не будет валидной записи.
sendAsMembers	nTSecurityDescriptor	Поле ограничения доступа к общему ящику в MS AD. Из этого поля берётся список пользователей общего ящика с ролью "участник".
sid	objectSid	Уникальный идентификатор объекта в LDAP. Необходим для установки связи между общим ящиком и

Поле	Атрибут из Microsoft Active Directory	Описание
		объектом, которому назначены права

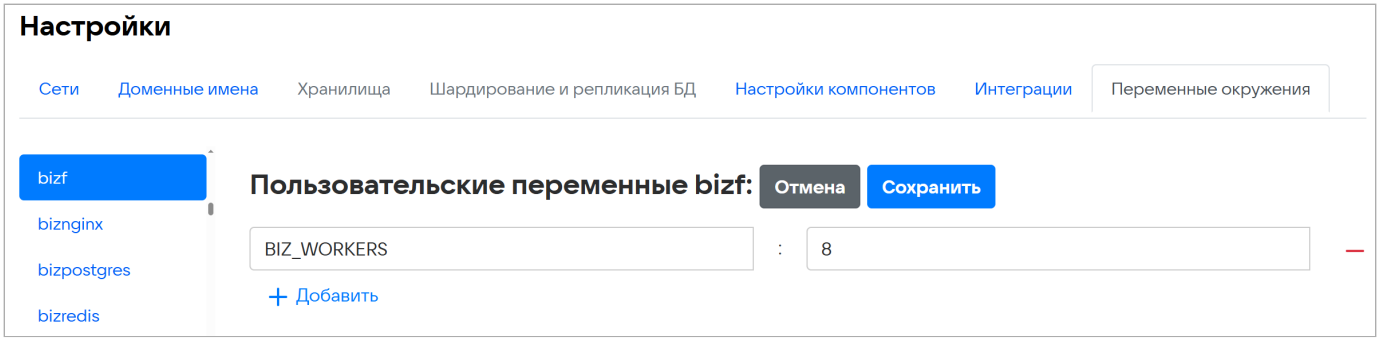
Как ускорить синхронизацию

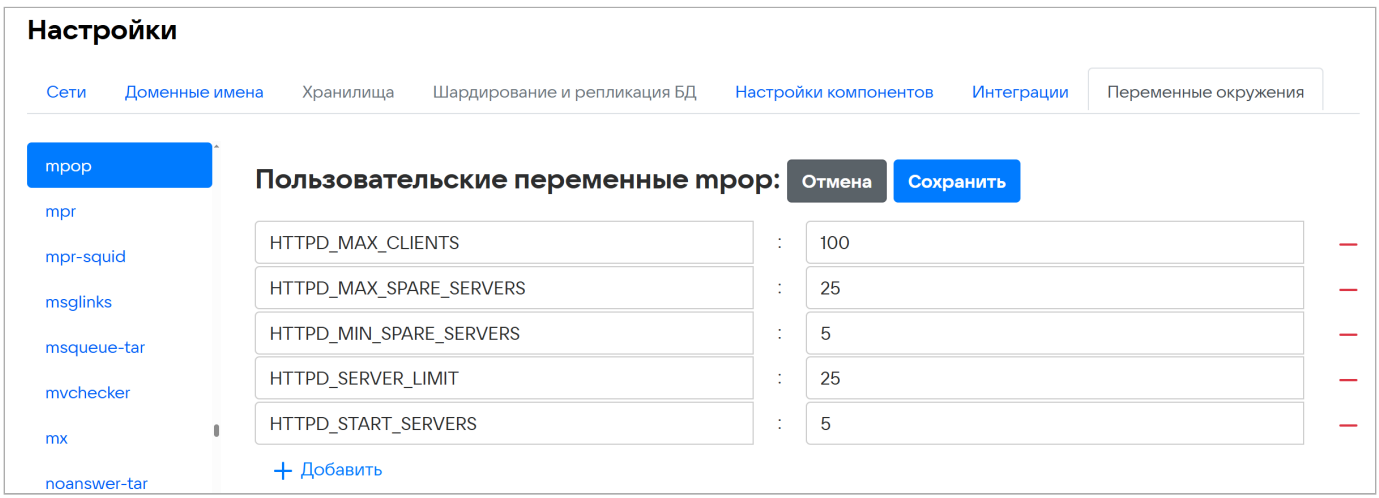
Скорость синхронизации зависит от трех взаимосвязанных настроек, эти параметры работают только вместе. Если вы измените один или два из них, оставив остальные без изменений, то это может привести к деградации тех или иных компонент системы.

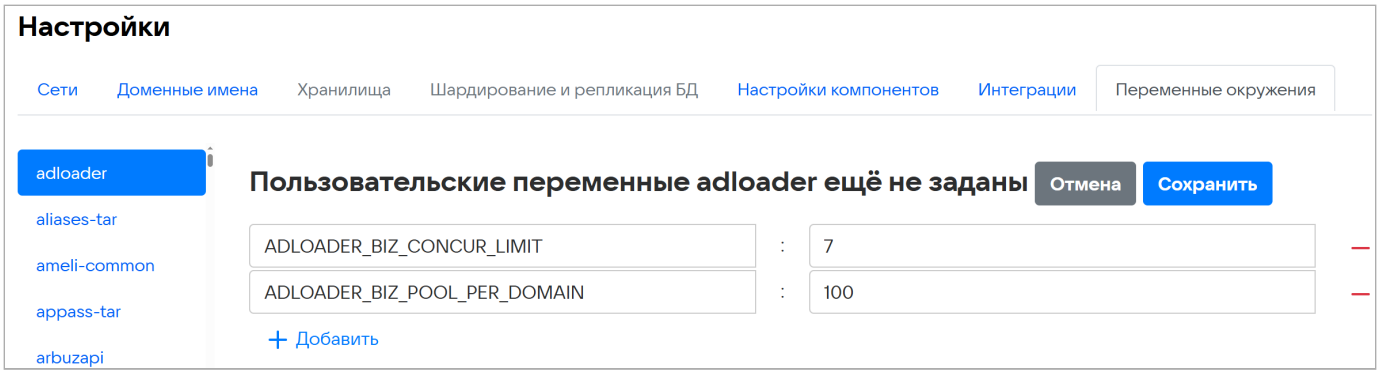
Параметры задаются в переменнных окружения сервисов adloader, mpop и bizf. Чтобы задать переменные окружения:

1. В веб-интерфейсе установщика, перейдите в раздел **Настройки** → **Переменные окружения**.
2. В левом боковом меню найдите необходимый сервис.
3. Нажмите кнопку редактировать .
4. Нажмите на кнопку **+ Добавить**.
5. Заполните поля **Название переменной** и **Значение переменной**.
6. Нажмите **Сохранить**.

Названия переменных и значения, которые нужно установить, приведены на скриншотах ниже.

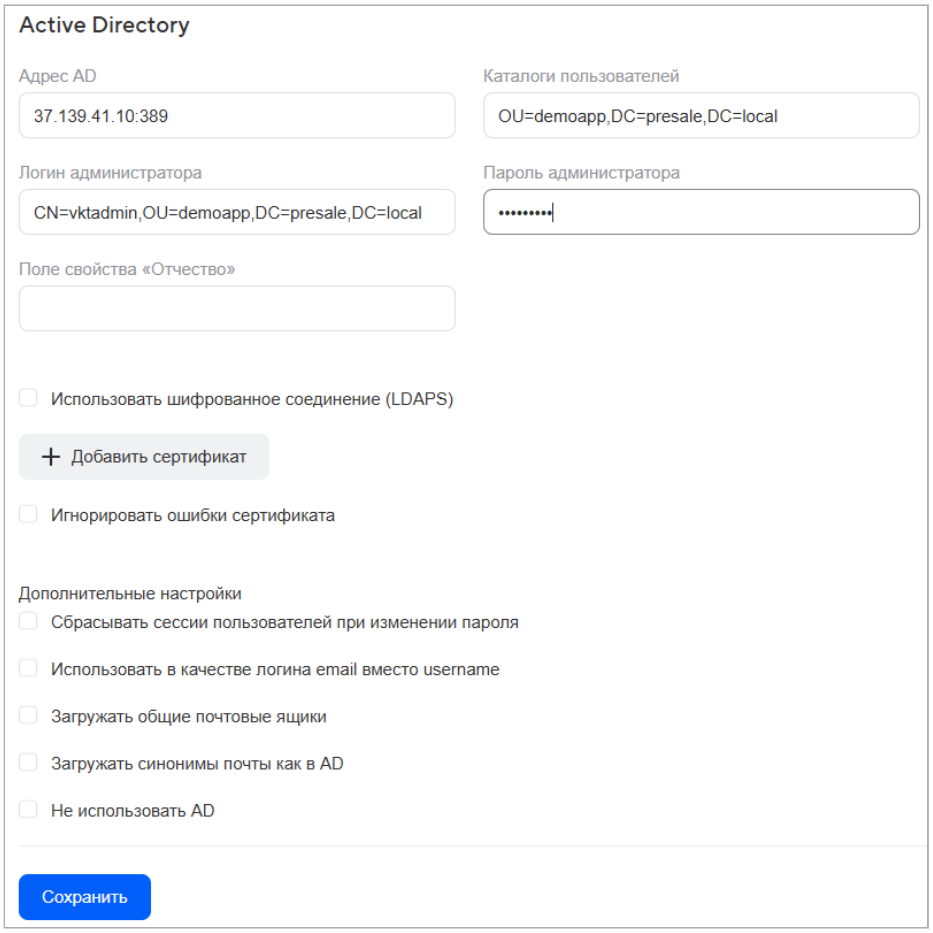






Интеграция с ALDPro

1. Перейдите в административную панель по адресу `biz.<mail_domain>` и далее в раздел **ActiveDirectory**.
2. Заполните все необходимые поля для интеграции с AD:

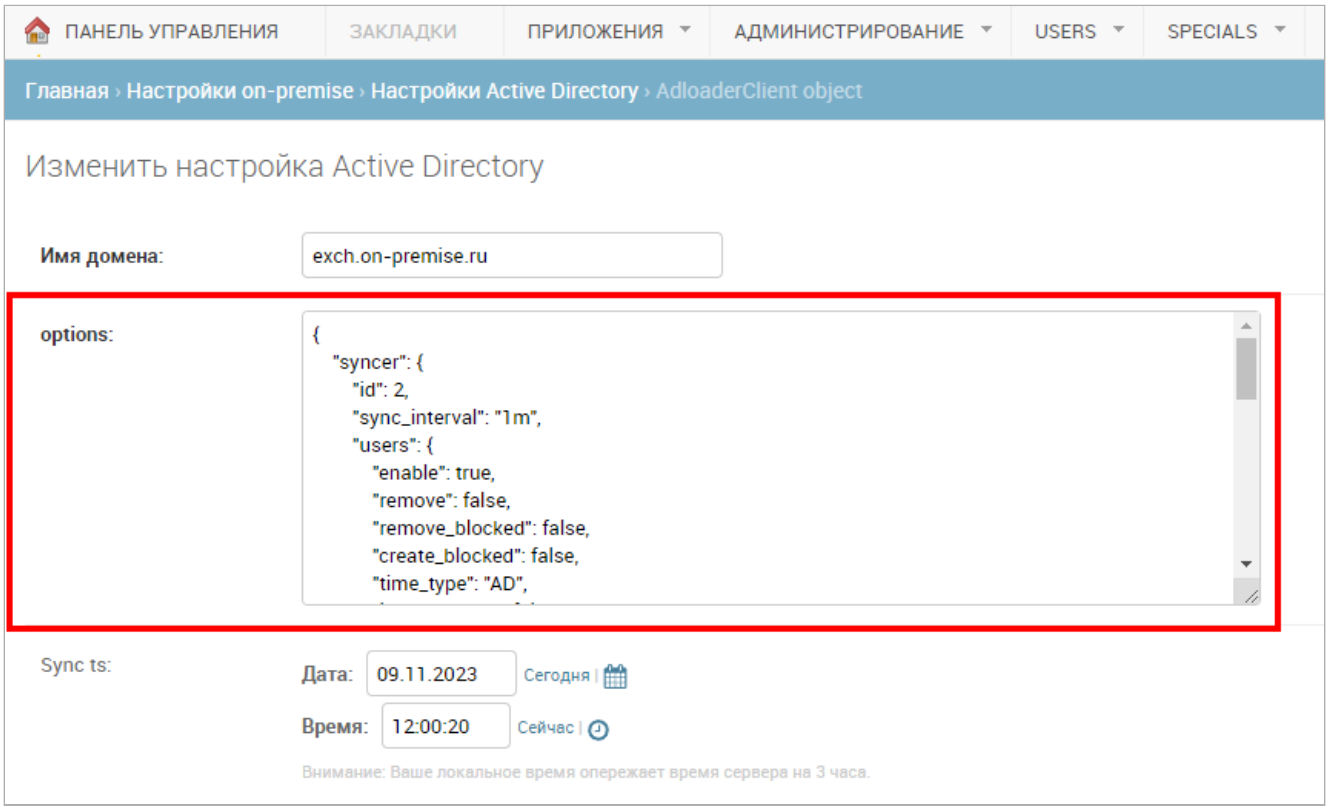


3. Перейдите по адресу `biz.<mail_domain>/admin/misc/configurations/adloaderclient/`.
4. Кликните по домену, для которого необходимо настроить интеграцию.
5. Внести изменения в конфигурацию в поле **options**:
    - В модели объекта `attr_map` в поле `unique_name` указать значение `entryDN`.

- В модели объекта `users` в поле `filter` прописать значение `rbtadp`. rbtadp — это аналог организационных единиц (OU). Если организационных единиц много, то нужно перечислить их с помощью логического «или».

```
"filter":"(&(mail=*@aldpro.company.ru)
(rbtadp=ou=vk2.ou=aldpro.company.ru,cn=orgunits,cn=account,dc=aldpro,dc=company,dc=ru))
"
```

- В модели объекта `mailing` в поле `name_is_email` указать значение `true`, если именем группы рассылки является email. По умолчанию принимает значение `false`.



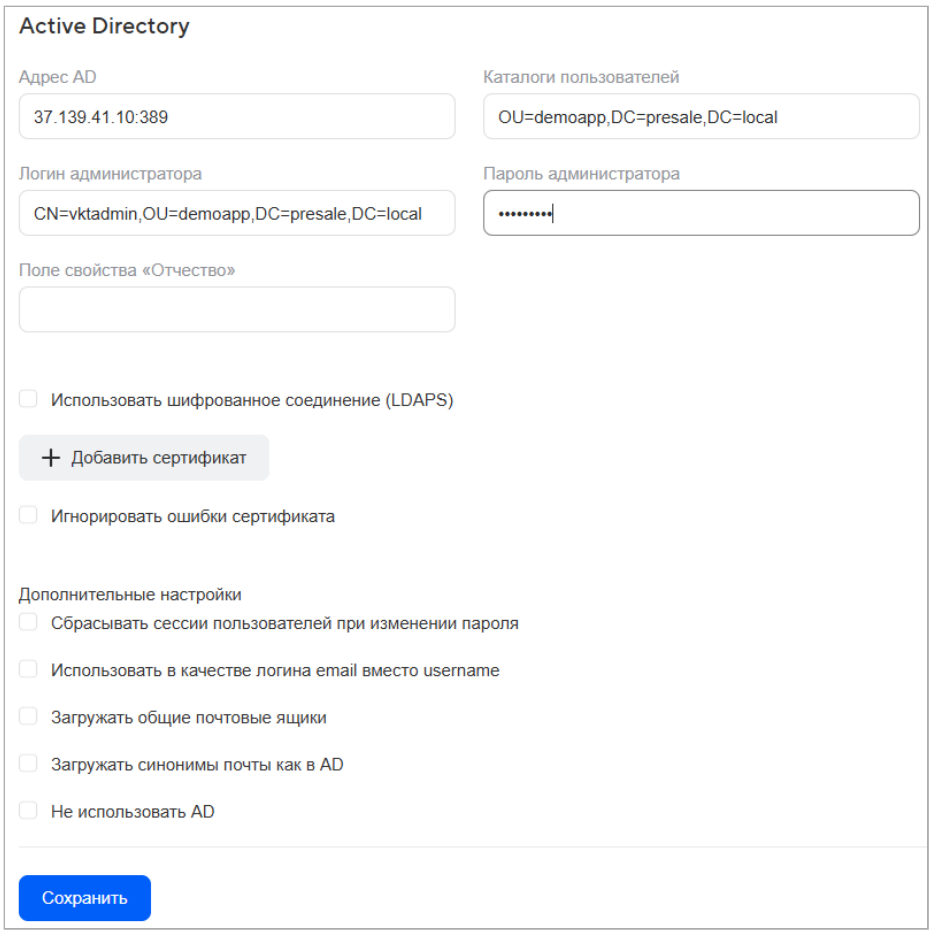
Пример конфигурации:

```
{
    "syncer": {
        "id": 1,
        "sync_interval": "5m",
        "users": {
            "enable": true,
            "remove": false,
            "filter":"(&(mail=*@aldpro.company.ru)
(rbtadp=ou=vk2.ou=aldpro.company.ru,cn=orgunits,cn=account,dc=aldpro,dc=company,dc=ru))",
            "attr_map": {
                "unique_name": "entryDN",
                "department": "rbtadp"
            },
            "remove_blocked": false,
            "create_blocked": false,
            "time_type": "FreeIPA",
            "logout_users": false,
            "pool_size": 50
        },
        "mailing": {
            "enable": true,
```

```
            "remove": false,
            "name_is_email": true
        }
    },
    "ad_client": {
        "username": "uid=vkldap,cn=users,cn=accounts,dc=aldpro,dc=company,dc=ru",
        "password": "",
        "base_dn": [
            "dc=aldpro,dc=company,dc=ru"
        ],
        "address": "10.1.100.100:389",
        "page_size": 100,
        "use_tls": false,
        "tls_cert": "",
        "skip_insecure": false
    }
}
```

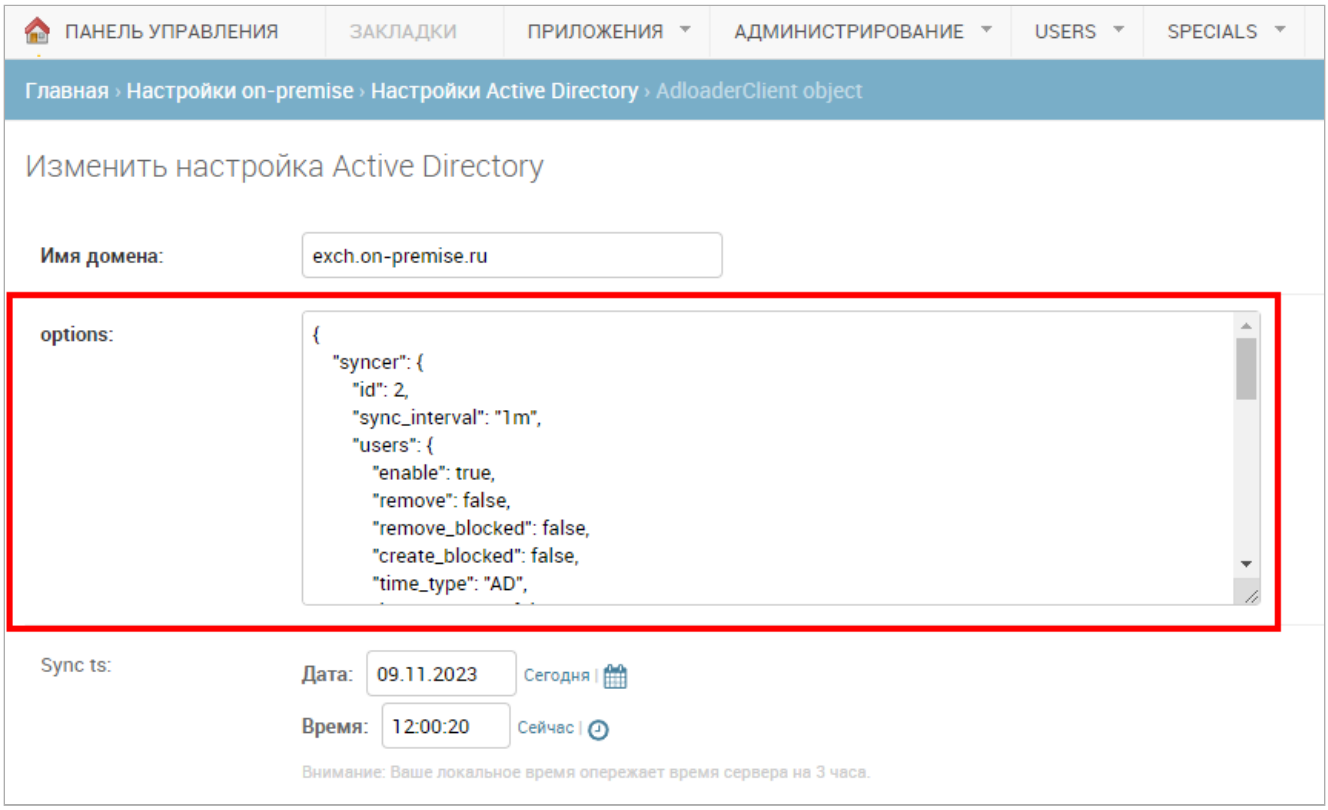
Интеграция с FreeIPA

1. Перейдите в административную панель по адресу `biz.<mail_domain>`.
2. Перейдите в раздел **Конфигурация** → **Настройки** → **ActiveDirectory**.
3. Заполните все необходимые поля для интеграции с AD:



4. Перейдите по адресу `biz.<mail_domain>/admin/misc/configurations/adloaderclient/`.
5. Кликните по домену, для которого необходимо настроить интеграцию.

6. Внести изменения в конфигурацию в поле **options** в соответствии с примером ниже.



Пример конфигурации:

```
{
    "syncer": {
        "id": 1,
        "sync_interval": "5m",
        "users": {
            "enable": true,
            "remove": false,
            "filter": "(&(objectClass=person)(mail=*@%[1]s))",
            "attr_map": {
                "unique_name": "dn",
                "mail": "mail",
                "first_name": "givenName",
                "second_name": "sn"
            },
            "remove_blocked": false,
            "create_blocked": false,
            "time_type": "FreeIPA",
            "logout_users": false,
            "pool_size": 50
        },
        "mailing": {
            "enable": true,
            "remove": false,
            "name_is_email": false
        }
    },
    "ad_client": {
        "username": "uid=service-vkt,cn=users,cn=accounts,dc=abc123,dc=abc",
        "password": "",
        "login_field": "dn",
        "base_dn": [
            "cn=users,cn=accounts,dc=abc123,dc=abc"
```

```
        ],
        "address": "10.1.100.100:389",
        "page_size": 100,
        "use_tls": false,
        "tls_cert": "",
        "skip_insecure": false
    }
}
```

Как блокировать и удалять пользователей при удалении из каталога AD

Чтобы настроить автоматическую блокировку пользователей в Почте при удалении из каталога:

1. Перейдите по адресу `biz.<mail_domain>/admin/misc/configurations/adloaderclient/`.
2. Кликните по домену, для которого необходимо настроить блокировку пользователей.
3. Для полей `remove` и `block_removed` в разделе `users` установите значение `true`:

```
{
    "syncer": {
        "id": 1,
        "sync_interval": "5m",
        "users": {
            …,
            "remove": true,
            "remove_blocked": true,
        },
        …,
    },
    …
}
```

Чтобы удалять пользователей, которые удалены в каталоге, установите следующие параметры:

```
{
    "syncer": {
        "id": 1,
        "sync_interval": "5m",
        "users": {
            …,
            "remove": true,
            "remove_blocked": false,
        },
        …,
    },
    …
}
```

Траблшутинг

Логи сервисов

Чтобы посмотреть логи сервиса AD Loader, выполните команду:

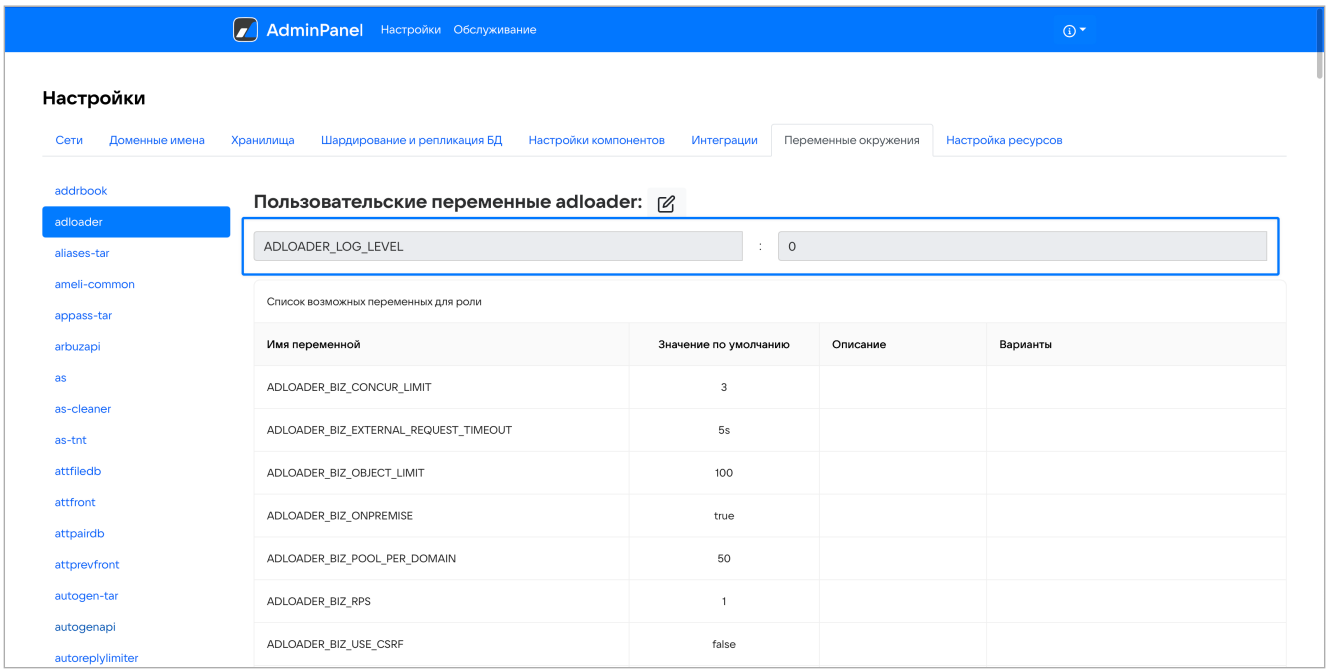
```
sudo journalctl -fu onpremise-container-adloader*.service
```

где * – номер AD Loader'а.

У сервиса AD Loader есть несколько уровней логирования, от выбранного уровня зависит детализация информации в логах. Значение по умолчанию — 2, WarnLevel. Для диагностики и исследования проблем рекомендуется установить 0 — DebugLevel.

ADLOADER_LOG_LEVEL	2	Уровень логирования	0 1 2 3 4 5 6 7 -1

1. В веб-интерфейсе установщика, перейдите в раздел **Настройки → Переменные окружения**.
2. В левом боковом меню найдите **adloader**.
3. Нажмите кнопку редактировать .
4. Нажмите на кнопку **+ Добавить**.
5. В поле **Название переменной** введите `ADLOADER_LOG_LEVEL`, в поле **Значение переменной** введите **0**
6. Нажмите **Сохранить**.



Также рекомендуем собрать логи контейнеров bizf и mpop:

- **mpop** — основное API почты VK WorkSpace:

```
sudo journalctl -fu onpremise-container-mpopN.service
```

- **bizf** — API панели администратора VK WorkSpace:

```
sudo journalctl -fu onpremise-container-bizfN.service
```

Утилита ldapsearch

Если с синхронизацией что-то пошло не так, то воспользуйтесь утилитой ldapsearch (https://docs.ldap.com/ldap-sdk/docs/tool-usages/ldapsearch.html). Попробуйте с помощью утилиты получить список пользователей с тем же фильтром и из того же каталога, из которого переносите их в Почту.

Например:

```
ldapsearch -v -x -D "login" -w 'pass' -b "OU=ou,DC=dev,DC=local" -H "ldap://ip"
'(&(objectclass=user)(objectCategory=person)(mail=*@domain))'
```

Наиболее частые ошибки

1. Нет сетевой связанности.
2. Неверные логин и пароль у учетной записи, которая используется для доступа к каталогу.
3. Неверный фильтр или фильтры — проверяйте поле **filter** логических блоков users, contacts, mailing и shared в файле конфигурации.
4. Неверный маппинг атрибутов. Проверьте attr_map'ы логических блоков common, users, contacts, mailing, shared. Помните, что общий attr_map в блоке common имеет более низкий приоритет по сравнению с частными attr_map'ами.
5. Неверный **base_dn** — вы пытаетесь получить данные не из той директироии в LDAP-каталоге. Помните, что если в интерфейсе первичной настройки в панели администратора вы можете указать только один конкретный OU, то в файле конфигурации в блоках ad_client и shared объект base_dn — это массив, соответственно, можно передать несколько значений, если это необходимо.
6. У учетной записи пользователя в Microsoft Active Directory не заполнено поле email или proxyAddresses.

7 ноября 2025 г.