

# Интеграция ELMA365 со службой каталога ALD Pro



06/04/2025

## Содержание

1	Документация .....	3
2	Описание стенда .....	4
3	Настройка доступа.....	5
3.1	Создание сервисной учетной записи.....	5
3.2	Настройка прав доступа .....	5
3.3	Проверка доступа .....	5
4	Конфигурация ELMA365.....	7
4.1	Активация модуля LDAP.....	7
4.2	Настройка подключения .....	7
4.3	Проверка подключения .....	9
5	Импорт данных.....	10
5.1	Импорт пользователей.....	10
5.2	Импорт групп.....	10

ELMA365 представляет собой облачное решение для управления бизнес-процессами, построенное на принципах Low-code-разработки, что позволяет максимально быстро превращать бизнес-идеи в работающие цифровые решения.

Данная инструкция описывает процесс интеграции системы управления бизнес-процессами ELMA365 с каталогом LDAP на базе решения ALD Pro.

# 1 Документация

- Настройка подключения LDAP в ELMA365
- Документация по ALD Pro

## 2 Описание стенда

- Контроллер домена ALD Pro, установленный в соответствии с руководством администратора
- Сервер системы ELMA365, установленный в соответствии с документацией по установке и активированный через менеджера ELMA365

## 3 Настройка доступа

### 3.1 Создание сервисной учетной записи

1. Создать файл конфигурации **svc-elma365.update**:

```
dn: uid=svc-elma365,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan
add:objectclass: account
add:objectclass: simplesecurityobject
add:uid: svc-elma365
add:userPassword: <пароль>
add:passwordExpirationTime: 20380119031407Z
add:nsIdleTimeout: 0
```

2. Применить конфигурацию:

```
kinit admin && ipa-ldap-updater svc-elma365.update
```

### 3.2 Настройка прав доступа

Назначить права на чтение атрибута entryUUID:

```
admin@dc01:~$ ldapmodify -x -D "cn=Directory Manager" -w <пароль>
dn: dc=ald,dc=company,dc=lan
changetype: modify
add: aci
aci: (targetattr="entryUUID")(version 3.0; acl "Allow svc-elma365 to read entryUUID";
allow(read,search,compare) userdn="ldap:///uid=svc-
elma365,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan";)
```

### 3.3 Проверка доступа

1. Протестировать подключение к LDAP:

- проверка доступности сервера LDAP:

```
# Проверка TCP-порта
nc -zv <ip-адрес-сервера> 389

# Проверка защищенного порта, если используется
nc -zv <ip-адрес-сервера> 636
```

- базовый поиск в каталоге:

```
# Анонимный поиск базового DN
ldapsearch -x -H ldap://<ip-адрес-сервера> -b "dc=ald,dc=company,dc=lan" -s base

# Поиск с учетными данными сервисной записи
ldapsearch -x -H ldap://<ip-адрес-сервера> \
-D "uid=svc-elma365,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan" \
-w "<пароль>" \
-b "dc=ald,dc=company,dc=lan" \
-s base
```

## 2. Проверить права на чтение атрибутов:

- проверка чтения базовых атрибутов пользователей:

```
# Поиск пользователей и их атрибутов
ldapsearch -x -H ldap://<ip-адрес-сервера> \
-D "uid=svc-elma365,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan" \
-w "<пароль>" \
-b "cn=users,cn=accounts,dc=ald,dc=company,dc=lan" \
-s sub "(objectClass=posixAccount)" \
uid cn mail displayName entryUUID
```

- проверка чтения атрибутов групп:

```
# Поиск групп и их атрибутов
ldapsearch -x -H ldap://<ip-адрес-сервера> \
-D "uid=svc-elma365,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan" \
-w "<пароль>" \
-b "cn=groups,cn=accounts,dc=ald,dc=company,dc=lan" \
-s sub "(objectClass=group)" \
cn member description
```

## 3. Убедиться в корректности работы сервисной учетной записи:

- команды выполняются без ошибок аутентификации;
- в выводе команд присутствуют ожидаемые атрибуты;
- отсутствуют сообщения о недостатке прав;
- возвращаемые данные соответствуют ожидаемым.

## 4 Конфигурация ELMA365

### 4.1 Активация модуля LDAP

1. Перейти в раздел “Модули”.
2. Включить модуль LDAP (рис. 1):

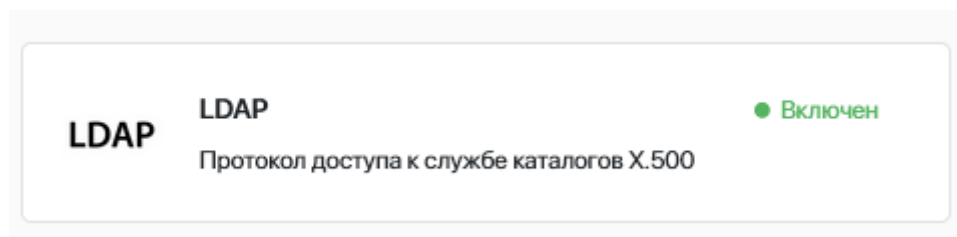


Рисунок 1 – Состояние модуля LDAP

### 4.2 Настройка подключения

- Заполнить параметры подключения (таблица 1):

Таблица 1 – Описание параметров подключения

Параметр	Значение	Описание
Наименование	ALD	Отображаемое имя подключения
Адрес сервера	89.169.164.206	IP-адрес контроллера домена ALD Pro
Использовать TLS	нет	Защищенное подключение
Поддержка контроллеров	нет	Мультимастер режим
Пользователь	uid=svc-elma365,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan	DN сервисной учетной записи, созданной для системы ELMA365
Домен	ald.company.lan	Имя домена ALD Pro
Шаблон авторизации	uid={\$login},cn=users,cn=accounts,dc=ald,dc=company,dc=lan.	Шаблон для поиска пользователей в домене

Поля “Пользователь” и “Шаблон авторизации” специфичны именно для ALD Pro и должны быть указаны в соответствии с примером выше с поправкой на свой домен.

- Настроить параметры сопоставления атрибутов пользователей и групп (рис. 2, 3, 4).

Серверы: редактирование

Основное **Дополнительно**

Наименование\*

Адрес сервера\*

Использовать TLS  Да  Нет  
Использовать защищенное подключение к серверу

Поддержка нескольких контроллеров домена  Да  Нет  
Загружать список контроллеров домена по указанному адресу и подключаться к первому доступному

Пользователь\*

Пароль\*

Домен

Шаблон авторизации\*

Тип аутентификации

Путь к пользователям\*

Фильтр для импорта пользователей\*

Параметр "Логин"

Параметр "Имя"

Параметр "Фамилия"

Параметр "Отчество"

Параметр "Рабочий телефон"

Рисунок 2 - Настройка параметров сервера, часть 1 (подключение и сопоставления атрибутов пользователей)

Серверы: редактирование

Параметр "Мобильный телефон"

Параметр "Дата рождения"

Параметр "Дата приёма"

Параметр "Отображаемая должность"

Параметр "Email"

Параметр "Статус блокировки"   
Атрибут, хранящий статус блокировки пользователя

Параметр "Дополнительные данные"   
Поле для строковых служебных данных

Путь к группам\*

Фильтр для импорта групп\*

Параметр "Имя группы"

Параметр "Описание группы"

Параметр "Члены группы"

Импорт внешних пользователей  Да  Нет

Путь к внешним пользователям

Фильтр внешних пользователей

Рисунок 3 – Настройка параметров сервера, часть 2 (сопоставления атрибутов пользователей и групп)

**Серверы: редактирование** ? X

Автоматическая синхронизация внешних пользователей

Синхронизировать изменения импортированных внешних пользователей

Параметр "DN"

Атрибут, хранящий уникальное имя объекта

Параметр "Дата создания"

Используется для фильтрации объектов при автоимпорте. Если оставить пустым, объекты запрашиваются без данного фильтра.

Параметр "Дата обновления"

Используется для фильтрации объектов при автосинхронизации. Если оставить пустым, объекты запрашиваются без данного фильтра.

Автосинхронизация пользователей

Синхронизировать изменения импортированных пользователей

Автоимпорт пользователей

Автоматически импортировать пользователей из сервера

Автосинхронизация групп

Синхронизировать изменения импортированных групп

Автоимпорт групп

Автоматически импортировать группы из сервера

Частота синхронизации, мин.

Автосоздание сотрудника

Автоматическое создание сотрудника при импорте пользователей с сервера

Обновление сотрудника

Обновление данных сотрудника при синхронизации изменений импортированных пользователей

Рисунок 4 – Настройка параметров сервера, часть 3 (сопоставления атрибутов групп)

## 4.3 Проверка подключения

1. Сохранить конфигурацию.
2. Убедиться в успешном подключении.

## 5 Импорт данных

### 5.1 Импорт пользователей

1. Выполнить импорт пользователей в соответствии с документацией.
2. Проверить корректность импорта.

### 5.2 Импорт групп

1. Выполнить импорт групп в соответствии с документацией.
2. Проверить права доступа.