

Интеграция Atlassian Jira со службой каталога ALD Pro



03/10/2026

Содержание

1	Настройка сервисной учетной записи в ALD Pro	3
2	Настройка LDAP/LDAPS в Jira	5
2.1	Настройки сервера (Server settings)	5
2.2	Дополнительные настройки (синхронизация и параметры подключения) ...	7
2.3	Параметры схемы пользователя	8
2.4	Настройки групповой схемы	9
2.5	Сохранение и проверка	10
3	Примечание по LDAPS и "Безопасный SSL"	12

Jira — система управления задачами и проектами, поддерживающая централизованную аутентификацию и синхронизацию пользователей из внешних каталогов.

В настоящей инструкции описана процедура интеграции Jira со службой каталога ALD Pro. Данная интеграция обеспечит аутентификацию через единую точку входа по протоколу LDAP/LDAPS, автоматическую загрузку профиля (имя, фамилия, e-mail), а также даст возможность управлять доступом через группы (в Jira локально или через LDAP — в зависимости от выбранного режима).

1 Настройка сервисной учётной записи в ALD Pro

Аутентификация и авторизация выполняются методом LDAP Bind, для чего необходимо создать в ALD Pro сервисную учётную запись, которая не является POSIX-пользователем, не имеет прав на вход в домен и не отображается в портале управления, а используется только для чтения LDAP.

Порядок создания сервисной учётной записи

1. Перед выполнением команды задайте следующие параметры:

```
PASS='Pa$$w0rd'  
LDAP_USER='system'  
LDAP_BASE_DN='dc=ald,dc=company,dc=lan'
```

Разъяснения:

- `PASS` — пароль сервисной учётной записи,
- `LDAP_USER` — имя создаваемой сервисной LDAP-учётной записи,
- `LDAP_BASE_DN` — базовый DN вашего домена LDAP.

Примеры базового DN:

```
ald.company.lan → dc=ald,dc=company,dc=lan
```

2. Подключитесь по SSH к контроллеру домена и выполните следующую команду:

```
PASS='Pa$$w0rd'  
LDAP_USER='system'  
LDAP_BASE_DN='dc=ald,dc=company,dc=lan'  
  
sudo bash -c '  
PW_B64=$(printf "%s" "$PASS" | base64 -w0)  
LDAP_USER="$LDAP_USER"  
LDAP_BASE_DN="$LDAP_BASE_DN"  
EXPIRATION=$(date -u -d "+5 years" +"%Y%m%d%H%M%SZ")  
  
cat > /tmp/${LDAP_USER}.update <<EOF  
dn: uid=${LDAP_USER},cn=sysaccounts,cn=etc,${LDAP_BASE_DN}  
add:objectclass: account  
add:objectclass: simplesecurityobject  
add:uid: ${LDAP_USER}  
add:userPassword: ${PW_B64}  
add:passwordExpirationTime: ${EXPIRATION}  
add:nsIdleTimeout: 0  
EOF  
  
kinit admin && ipa-ldap-updater /tmp/${LDAP_USER}.update  
'
```

Команда выполняет следующие действия:

- кодирует указанный пароль в Base64 и сохраняет его в переменную `PW_B64`;

- создаёт файл `/tmp/${LDAP_USER}.update` , содержащий LDIF-описание сервисной учётной записи;
- получает Kerberos-билет администратора (`kinit admin`);
- применяет изменения из созданного LDIF-файла к LDAP-каталогу с помощью `ipa-ldap-updater` .

2 Настройка LDAP/LDAPS в Jira

Настройка выполняется в интерфейсе Jira по следующему пути (рис. 1): **Администрирование** → **Управление пользователями** → **Каталоги пользователей** → **Добавить каталог**.

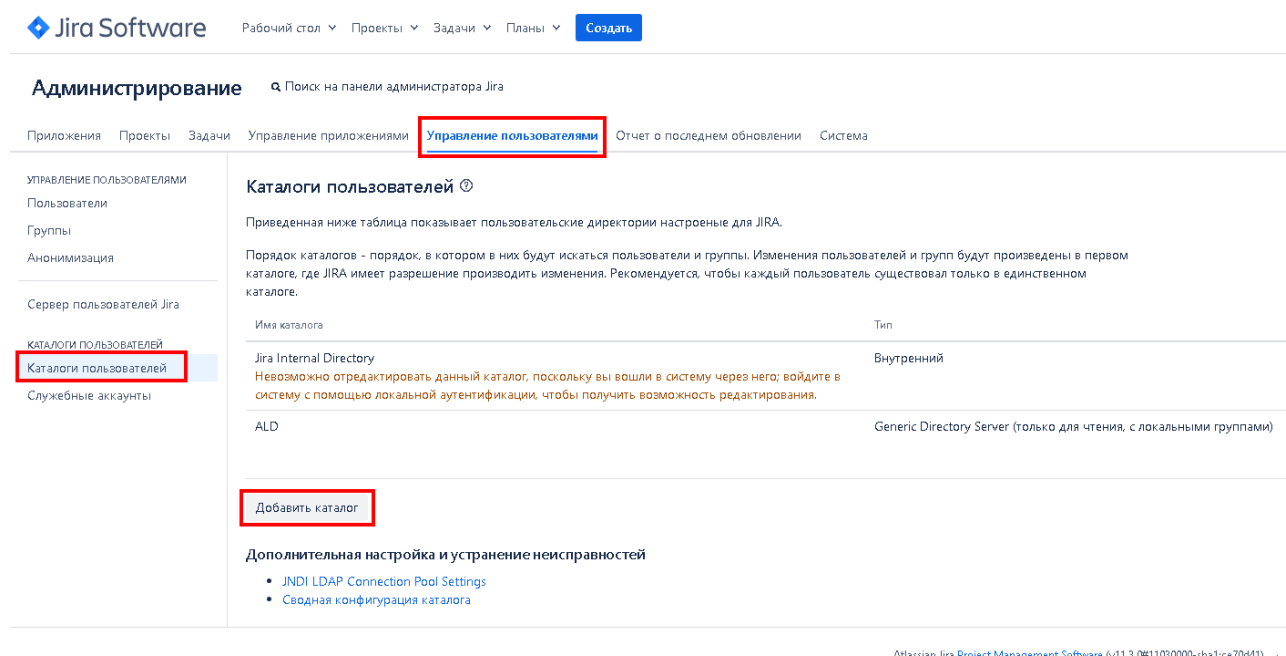


Рисунок 1 – Добавление LDAP-сервера

При добавлении выберите «Настройки LDAP» (рис. 2).

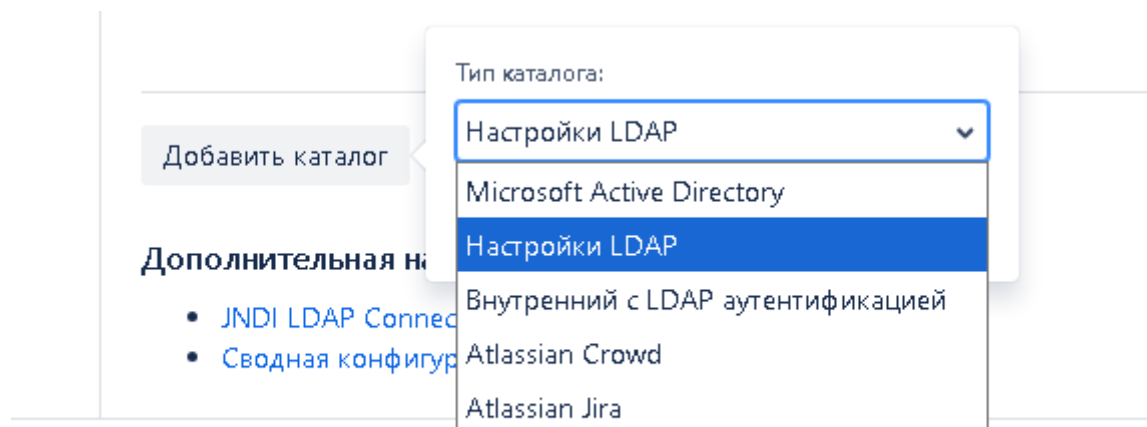


Рисунок 2 – Выбор типа сервера при добавлении

2.1 Настройки сервера (Server settings)

В открывшемся окне настроек заполните следующие поля (рис. 3):

- **Имя:** ALD

- **Тип каталога:** Generic Directory Server
- **Имя хоста:** dc01.ald.domain.lan
- **Порт:** 636
- **Использовать SSL:** да
- **Имя пользователя (Bind DN):** uid=bind_jira,cn=users,cn=accounts,dc=ald,dc=domain,dc=lan
- **Пароль:** пароль сервисной учетной записи bind_jira

В блоке **Схема LDAP** укажите следующее:

- **Base DN:** dc=ald,dc=domain,dc=lan
- **Дополнительные DN (ограничение области поиска):**
 - **Дополнительное DN пользователя:** cn=users,cn=accounts
 - **Дополнительные DN группы:** cn=groups,cn=accounts

Это уменьшает объем поиска и ускоряет синхронизацию.

- **Разрешения LDAP:** Только для чтения, с локальными группами

Данное разрешение означает следующее:

- пользователи загружаются из LDAP;
- группы для прав в Jira ведутся локально (в Jira);
- пользователей из LDAP можно добавлять к группам, ведение которых осуществляется во внутреннем каталоге JIRA.

Членство группы по умолчанию: jira-users

Настройки сервера

Имя:

Тип каталога:

При выборе будут автоматически введены значения по умолчанию для некоторых из представленных ниже опций.

Имя хоста:

Имя сервера LDAP. Пример: ldap.example.com

Порт: Использовать SSL

Имя пользователя:

Пользователь, входящий в систему LDAP. Примеры: user@domain.name или cn=user,dc=domain,dc=name.

Пароль:

Схема LDAP

Base DN:

Корневой узел LDAP, с которого начинается поиск пользователей и групп. Пример: cn=users,dc=example,dc=com.

Дополнительное DN пользователя:

Добавляется к базовому DN для ограничения объема при поиске пользователей.

Дополнительные DN группы:

Добавляется к базовому DN для ограничения объема при поиске групп.

Разрешения LDAP

Только для чтения
Информация о пользователях, группах и участиях получается с сервера LDAP и не может изменяться в JIRA.

Только для чтения, с локальными группами
Информация о пользователях, группах и участиях получается с сервера LDAP и не может изменяться в JIRA. Пользователей из LDAP можно добавлять к группам, ведение которых осуществляется во внутреннем каталоге JIRA.

Чтение/Запись
При модификации пользователей, групп и участия в JIRA изменения применяются непосредственно на сервере LDAP. Настроенному пользователю LDAP необходимы полномочия на изменение в рамках сервера LDAP.

Членство группы по умолчанию:

Список групп, разделенных запятыми, к которым добавляются пользователи при первом входе в систему. Выполняется один раз для каждого пользователя. Эти группы будут созданы, если еще не существуют.

> **Дополнительные настройки**

Рисунок 3 – Основные настройки сервера LDAP

2.2 Дополнительные настройки (синхронизация и параметры подключения)

В разделе **Дополнительные настройки** укажите следующее (рис. 4):

- **SSL и опции каталога** : Безопасный SSL
- **Обновлять участие в группах при входе**: При каждом входе пользователя
- **Интервал синхронизации (в минутах)**: 60
- **Время ожидания чтения (в секундах)**: 120
- **Тайм-аут поиска (в секундах)**: 60

▼ Дополнительные настройки

Безопасный SSL
 Убедитесь, что сертификат SSL действителен для данного соединения

Включить вложенные группы
 Если включено, группы могут содержать в себе другие группы. Включение этой опции может привести к снижению производительности.

Использовать результаты, разделенные по страницам результатов на страницу

Отслеживание рефералов
 Разрешить LDAP сервер для перенаправления запросов на другие серверы.

Примитивное сопоставление DN
 Если каталог постоянно возвращает единообразное представление строки DN, можно активировать примитивное сопоставление DN. Использование примитивного сопоставления DN существенно эффективнее, поэтому рекомендуется использовать его везде, где только возможно.

Обновлять участие в группах при входе
 Обновлять или не обновлять участие пользователя в группах при каждом входе. Это обеспечивает актуальность перечня групп, но может замедлить процесс аутентификации.

Интервал* синхронизации (в минутах):
 Время ожидания между обновлениями каталога.

Время ожидания чтения (в секундах):
 Время ожидания отклика. Если за указанный период времени нет ответа, попытка чтения будет прервана. Значение «0» свидетельствует об отсутствии лимита.

Тайм-аут поиска (в секундах):
 Время ожидания ответа от операции поиска. Значение 0 означает неограниченное время.

Тайм-аут соединения(в секундах):
 Time limit within which the connection to new server must be made. Value of 0 means the TCP network timeout will be used, which may be several minutes. When using JNDI connection pooling, this parameter also specifies the time to wait for a connection after the pool has been exhausted. Set to 0 for no limit. [Learn More](#)

Максимальное количество повторных попыток аутентификации
 Максимальное количество повторных попыток аутентификации при возникновении операционной ошибки во время аутентификации пользователя (по умолчанию 0).

Минимальная задержка между повторными попытками (мс)
 Минимальная задержка между повторными попытками аутентификации с экспоненциальной задержкой при возникновении операционной ошибки (по умолчанию 0).

Рисунок 4. Дополнительные настройки

2.3 Параметры схемы пользователя

В разделе **Параметры настройки схемы пользователя** заполните поля следующим образом (рис. 5):

- **Класс объекта пользователя:** person
- **Фильтр пользовательских объектов:** (objectClass=person)
- **Атрибут "Полное имя пользователя":** uid
- **Атрибут "RDN имени пользователя":** cn
- **Атрибут "Имя пользователя":** givenName
- **Атрибут "Фамилия":** sn
- **Атрибут "Просмотр имени":** cn
- **Атрибут "Электронная почта":** mail
- **Атрибут "Пароль пользователя":** userPassword
- **Шифрование пароля пользователя:** SHA

- Атрибут "Уникальный ID пользователя": uid

▼ Параметры настройки схемы пользователя

Класс объекта* пользователя:	<input type="text" value="person"/>	Тип класса объекта пользователя LDAP, используемый при загрузке пользователей.
Фильтр* пользовательских объектов:	<input type="text" value="(objectClass=person)"/>	Фильтр, используемый при поиске объектов пользователей.
Атрибут «Полное* имя пользователя»:	<input type="text" value="uid"/>	Поле атрибута, используемое в объекте пользователя. Примеры: cn, sAMAccountName.
Атрибут «RDN имени пользователя»:	<input type="text" value="cn"/>	Значение RDN, используемое при загрузке имени пользователя. Пример: cn.
Атрибут «Имя* пользователя»:	<input type="text" value="givenName"/>	Поле атрибута, используемое при загрузке имени пользователя.
Атрибут «Фамилия* пользователя»:	<input type="text" value="sn"/>	Поле атрибута, используемое при загрузке фамилии пользователя.
Атрибут «Просмотр* имени пользователя»:	<input type="text" value="cn"/>	Поле атрибута, используемое при загрузке полного имени пользователя.
Атрибут* «Электронная почта пользователя»:	<input type="text" value="mail"/>	Поле атрибута, используемое при загрузке адреса электронной почты пользователя.
Атрибут «Пароль* пользователя»:	<input type="text" value="userPassword"/>	Поле атрибута, используемое при управлении паролем пользователя.
Шифрование пароля пользователя:	<input type="text" value="SHA"/>	Выберите алгоритм шифрования паролей в вашем каталоге.
Атрибут «Уникальный ID пользователя»:	<input type="text" value="uid"/>	Поле атрибута, используемое для отслеживания личности пользователя при смене имени пользователя.

Рисунок 5 – Схема пользователя

2.4 Настройки групповой схемы

В разделе **Настройки групповой схемы** заполните поля следующим образом (рис. 6):

- **Класс группы объектов:** ipausergroup
- **Фильтр объектов группы:** (objectclass=ipausergroup)
- **Атрибут "Имя группы":** cn
- **Атрибут "Описание группы":** description

В разделе **Параметры настройки схемы участия** заполните следующее:

- **Атрибут Членов Группы:** member

- Атрибут «Участие пользователя»: memberof

▼ Настройки групповой схемы

Класс Группы*
Объектов: LDAP добавляет значение 'objectClass' к поиску при загрузке групп.

Фильтр объектов*
группы: Фильтр, используемый при поиске группы объектов.

Атрибут «Имя»*
группы: Поле атрибута, используемое при загрузке имени группы.

Атрибут «Описание»*
группы: Поле атрибута, используемое при загрузке полного описания группы.

▼ Параметры настройки схемы участия

Атрибут Членов*
Группы: Поле атрибута, используемое при загрузке участников группы из группы.

Атрибут «Участие»*
пользователя: Поле атрибута, используемое при загрузке пользовательских групп.

Используйте атрибут «Участие пользователя»: При поиске участия для группы пользователя

Рисунок 6 – Настройка групповой схемы

2.5 Сохранение и проверка

- Нажмите «Быстрый тест». Если подключение пройдет успешно, то вы увидите сообщение, приведенное на рисунке 7.

результаты синхронизироваться с LDAP. Обратитесь к администратору сервера, чтобы узнать требуемые параметры настройки для сервера LDAP.

✓ Подключение прошло успешно.
 Здесь просто выполняется проверка доступности сервера и действительности предоставленных регистрационных данных. После сохранения конфигурации можно провести более глубокую проверку с помощью ссылки «Тест» на странице поиска по каталогам.

Настройки сервера

Имя*

Тип каталога*

Рисунок 7 – Быстрый тест

- При успешном завершении теста нажмите «**Сохранить и протестировать**».

- Убедитесь, что тест показывает успешное подключение и поиск объектов. При тестировании можно проверить аутентификацию пользователя ALD Pro. Пример приведён на рисунке 8.

Проверка подключения к удалённому каталогу [?]

Используйте эту форму, чтобы проверить подключение к Generic Directory Server (только для чтения, с локальными группами) каталог 'ALD'.

В целях расширенного тестирования необходимо ввести регистрационные данные пользователя в удалённом каталоге.

✔ Тест базового соединения : Успешно

✔ Тест получения пользователя : Успешно

✔ Тест запроса данных об участии пользователей : Успешно получено групп: 2

✔ Тест получения группы : Успешно

✔ Тест получения участников группы : Успешно вызвано пользователей: 6

✔ Тестовый пользователь может проходить аутентификацию : Успешно

Имя пользователя

Пароль

[Проверить настройки](#)

[Редактировать настройки](#)

[Вернуться в список директорий](#)

Рисунок 8 – Проверка настроек

- Проверьте вход в Jira пользователем из ALD Pro и создание/обновление его профиля (имя, фамилия, mail).

3 Примечание по LDAPS и "Безопасный SSL"

Если включены **SSL (636)** и "**Безопасный SSL**", система Jira должна доверять сертификату LDAP-сервера (CA). Если у вас установлена java вместе с jira, то, возможно, java находится в каталоге /opt/atlassian/jira/jre.

Импортировать сертификат aldpro в локальное хранилище можно командой /opt/atlassian/jira/jre/bin/keytool -importcert -noprompt -alias aldpro-ca -file /etc/ipa/ca.crt -keystore /opt/atlassian/jira/jre/lib/security/cacerts.