

Интеграция Atlassian Confluence со службой каталога ALD Pro



03/10/2026

Содержание

1	Настройка сервисной учетной записи в ALD Pro	3
2	Настройка LDAP/LDAPS в Confluence	5
2.1	Настройки сервера (Server settings)	6
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	Настройка доступа в Confluence	12
4	Примечание по LDAPS и "Безопасный SSL"	14

Confluence – система управления задачами и проектами, поддерживающая централизованную аутентификацию и синхронизацию пользователей из внешних каталогов.

В настоящей инструкции описана процедура интеграции Confluence 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 Confluence 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 Confluence

Настройка выполняется в интерфейсе Confluence по следующему пути (рис. 1 и рис. 2):

Администрирование → **Управление пользователями** → **Каталоги пользователей** → **Добавить каталог**.

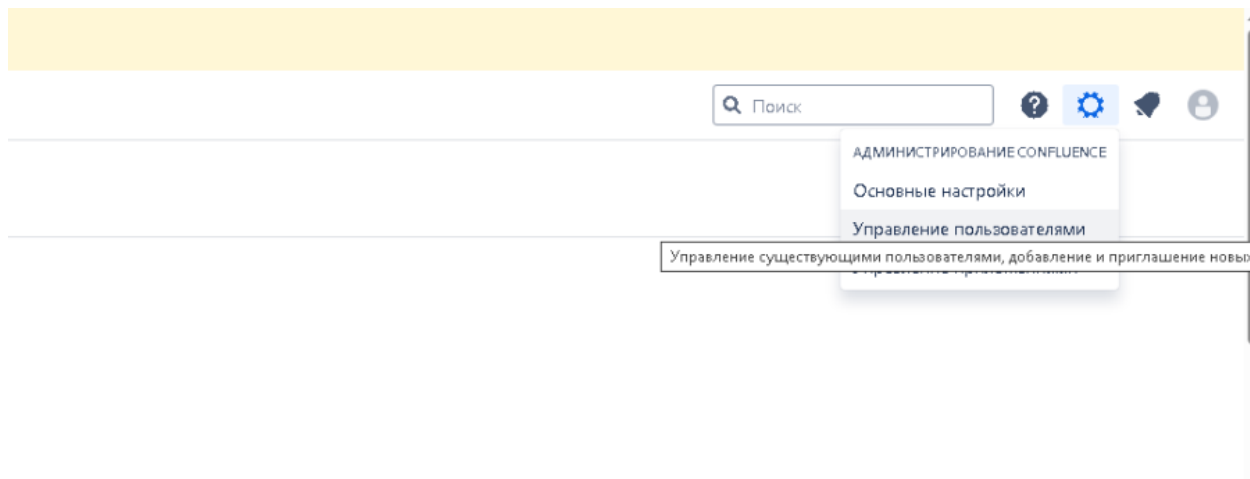


Рисунок 1 — переход в управление пользователями

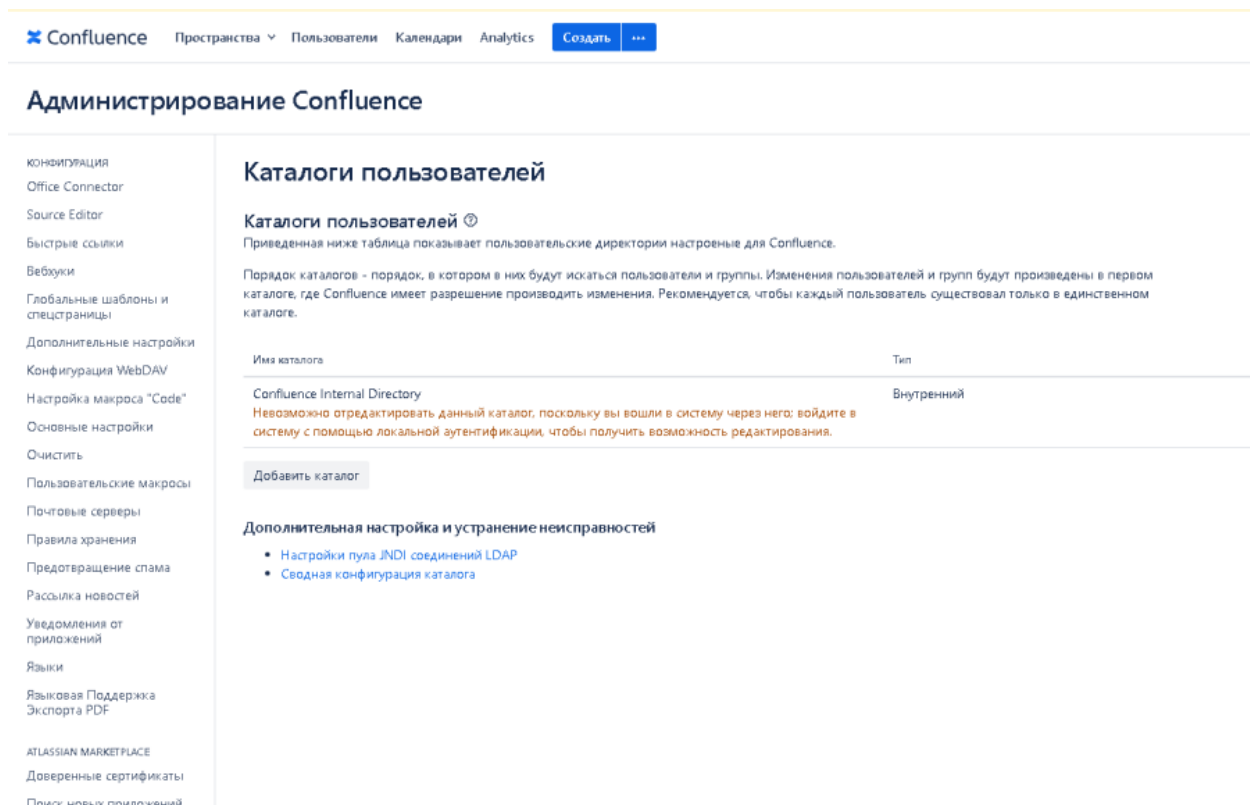


Рисунок 2 — Добавление LDAP-сервера

При добавлении выберите «**Настройки LDAP**» (рис. 3).

Администрирование Confluence

- конфигурация
- Office Connector
- Source Editor
- Быстрые ссылки
- Вебхуки
- Глобальные шаблоны и спецстраницы
- Дополнительные настройки
- Конфигурация WebDAV
- Настройка макроса "Code"
- Основные настройки
- Очистить
- Пользовательские макросы
- Почтовые серверы
- Правила хранения
- Предотвращение спама
- Рассылка новостей
- Уведомления от приложений
- Языки
- Языковая Поддержка
- Экспорт PDF
- ATLASSIAN MARKETPLACE

Каталоги пользователей

Каталоги пользователей ⓘ

Приведенная ниже таблица показывает пользовательские директории настроенные для Confluence.

Порядок каталогов - порядок, в котором в них будут искааться пользователи и группы. Изменения пользователей и групп будут произведены в первом каталоге, где Confluence имеет разрешение производить изменения. Рекомендуется, чтобы каждый пользователь существовал только в единственном каталоге.

Имя каталога	Тип
Confluence Internal Directory	Внутренний

Невозможно отредактировать данный каталог, поскольку вы вошли в систему через него; войдите в систему с помощью [ссылка] для отключения.

Добавить каталог

Тип каталога: Настройки LDAP

Далее

Дополнительная информация

- Настройки пула JNDI соединений LDAP
- Сводная конфигурация каталога

Рисунок 3 – Выбор типа сервера при добавлении

2.1 Настройки сервера (Server settings)

В открывшемся окне настроек заполните следующие поля (рис. 4):

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

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 Confluence ведутся локально (в Confluence);
- пользователей из LDAP можно добавлять к группам, ведение которых осуществляется во внутреннем каталоге Confluence;
- пользователи при входе в Confluence добавляются в локальную группу confluence-users.

Членство группы по умолчанию: confluence-users

При выборе «Разрешения LDAP: Только для чтения» пользователей требуется либо добавить к локальным группам доступа вручную, либо добавить разрешения на группы ALD в настройках доступа.

Настройки сервера

Имя:

Тип каталога:

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 Confluence.

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

Чтение/Запись
При модификации пользователей, групп и участия в Confluence 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.

Рисунок 4 – Основные настройки сервера LDAP

2.2 Дополнительные настройки (синхронизация и параметры подключения)

В разделе **Дополнительные настройки** укажите следующее (рис. 5):

- **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 5. Дополнительные настройки

2.3 Параметры схемы пользователя

В разделе **Параметры настройки схемы пользователя** заполните поля следующим образом (рис. 6):

- **Класс объекта пользователя:** inetorgperson
- **Фильтр пользовательских объектов:** (objectClass= inetorgperson)
- **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":** entryUUID

пользователю LDAP необходимы полномочия на изменение в рамках сервера LDAP.

> **Дополнительные настройки**
 v **Параметры настройки схемы пользователя**

Класс объекта*
пользователя: Тип класса объекта пользователя LDAP, используемый при загрузке пользователей.

Фильтр*
пользовательских объектов: Фильтр, используемый при поиске объектов пользователей.

Атрибут «Полное*
имя пользователя»: Поле атрибута, используемое в объекте пользователя. Примеры: cn, sAMAccountName.

Атрибут «RDN*
имени пользователя»: Значение RDN, используемое при загрузке имени пользователя. Пример: cn.

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

Атрибут «Фамилия*
пользователя»: Поле атрибута, используемое при загрузке фамилии пользователя.

Атрибут «Просмотр*
имени пользователя»: Поле атрибута, используемое при загрузке полного имени пользователя.

Атрибут*
«Электронная почта пользователя»: Поле атрибута, используемое при загрузке адреса электронной почты пользователя.

Атрибут «Пароль*
пользователя»: Поле атрибута, используемое при управлении паролем пользователя.

Шифрование пароля
пользователя: Выберите алгоритм шифрования паролей в вашем каталоге.

Атрибут
«Уникальный ID пользователя»: Поле атрибута, используемое для отслеживания личности пользователя при смене имени пользователя.

Рисунок 6 – Схема пользователя

2.4 Настройки групповой схемы

В разделе **Настройки групповой схемы** заполните поля следующим образом (рис. 7):

- **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

дания

э

ожки и

осов

нды

ва

ти

▼ **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

> **Настройки пула соединений LDAP**

Рисунок 7 – Настройка групповой схемы

2.5 Сохранение и проверка

- Нажмите **«Быстрый тест»**, если подключение пройдет успешно, то вы увидите сообщение, приведенное на рисунке 8.

регулярно синхронизироваться с ним. 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 8 – 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 9.

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 9 – Проверка настроек

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

3 Настройка доступа в Confluence

Настройка производится на странице «Глобальные разрешения», переход на которую осуществляется через пункт бокового меню «Глобальные права» (рис. 10).

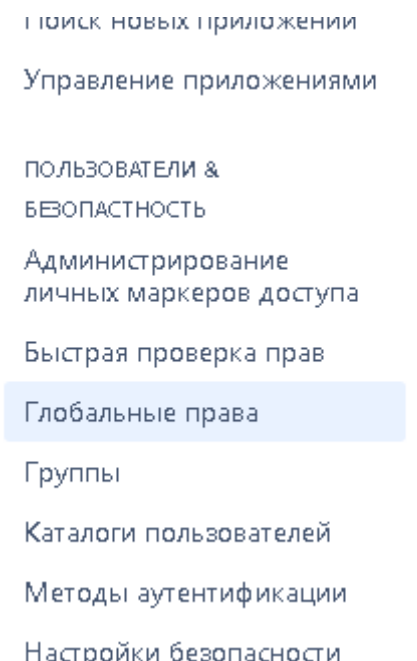


Рис 10. Переход на страницу "Глобальные разрешения"

Если в разделе **Разрешение LDAP** переключатель установлен в положение «Только для чтения» и в поле **Членство группы по умолчанию** указано «confluence-users» (см. рис. 4), то пользователь получит доступ с правами, которые по умолчанию настроены в Confluence для группы «confluence-users» в настройках глобальных разрешений. Вы можете создавать свои группы доступа и добавлять в них пользователей по умолчанию в настройках пункта 2.1.

Также в настройках глобальных разрешений можно добавить доменные группы ALD Pro по вводу имени группы в поле **Grant browse permission to** и нажатию кнопки «Добавить». Например, добавим группу `irausers` (рис. 11). В этом случае можно в настройках пункта 2.1 в разделе **Разрешения LDAP** установить переключатель в положение «Только для чтения» и не добавлять пользователей при входе в локальные группы Confluence.

Администрирование Confluence

- конфигурация
- Office Connector
- Source Editor
- Быстрые ссылки
- Выборки
- Глобальные шаблоны и стилизации
- Дополнительные настройки
- Конфигурация WebDM
- Настройка макроса "Code"
- Основные настройки
- Очистить
- Пользовательские макросы
- Прогнозе серверы
- Права хранения
- Предотвращение спама
- Расширка новостей
- Уведомления от приключений
- Явки
- Явки из Поддержка Экспорт PDF
- Личная разметка
- Доверенные сертификаты

Редактировать Глобальные Разрешения

Глобальные разрешения определяют возможности пользователей сайта. Можно предоставлять разрешения группам и отдельным лицам, а также открывать доступ к сайту анонимным пользователям. В [Обзор глобальных разрешений](#) можно найти более подробную информацию об управлении разрешениями для сайта Confluence.

Лицензированные пользователи

Группы

Предоставьте полномочия на использование всех функций сайта всем участникам группы.

		Личное пространство	Содать пространство(s)	Просмотр учетной записи групп	Администрат
confluence-administrators	<input type="checkbox"/> Разрешено	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
confluence-users	<input checked="" type="checkbox"/> Разрешено	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
visitors	<input checked="" type="checkbox"/> Разрешено	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Grant browse permissions to

Индивидуальные пользователи

Предоставьте разрешения для отдельных пользователей, независимо от того, участниками каких групп они являются.

В настоящий момент пользователи не имеют индивидуальных глобальных разрешений.

Grant browse permissions to

Анонимный доступ

Откройте доступ к своему сайту Confluence. Можно выбрать разделы, доступные для анонимных пользователей. Анонимные пользователи не включаются в количество лицензий.

[Использовать Confluence](#)

[Просмотр профиля Пользователя](#)

Рис 11. Глобальные Разрешения

4 Примечание по LDAPS и "Безопасный SSL"

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

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

После этого обязательно требуется перезапустить сервис Confluence – `systemctl restart confluence`.