

[К-4291] Загрузка пользователей из LDAP

При настроенном подключении к LDAP любой доменный пользователь может войти в приложение. Для отключения этой возможности, необходимо перейти в настройки приложения (Администрирование - Настройки - Приложение) и снять галочку "Создавать учетную запись для доменного пользователя".

Для импорта учетных записей пользователей, которые могут авторизовываться в системе по доменной учетке, необходимо перейти в модуль Администрирование - Пользователи - Импорт из LDAP.

Модуль представляет собой мастер, состоящий из нескольких шагов, и доступен в разделе "Администрирование", в меню "Настройки":

- На первом шаге необходимо указать параметры подключения к LDAP-серверу, тип LDAP-каталога и указать домен верхнего уровня, начиная с которого будет выполняться поиск объектов.
- На втором шаге необходимо уточнить метаданные, используемые для получения информации из каталога, название атрибута, отвечающего за имя учетной записи пользователя в домене, и название атрибута, в котором хранится адрес электронной почты. Также необходимо указать запрос поиска объектов в каталоге. По умолчанию подставляются значения, соответствующие выбранному типу LDAP-каталога.
- На третьем шаге отображается иерархия объектов, загруженных из каталога. Организационные единицы и группы отмечены иконками с изображением папки. Учетные записи отображаются без иконок. Вам необходимо отметить галочками те узлы, которые необходимо импортировать, при этом, учетные записи будут импортированы как пользователи, а организационные единицы - как группы пользователей.
- На четвертом шаге отображается содержимое лога, сформированного в результате импорта данных из каталога. В логе отображается информация о том какие пользователи были созданы, какие обновлены, какие группы созданы и в какие группы были включены пользователи. Вы также можете отметить галочкой создание задачи по периодическому обновлению импортированных ранее учетных записей. При выполнении этой задачи будут обновляться адрес электронной почты, описание пользователя.

Использование SSL/TLS

При использовании протокола ldaps или поддержке команды START TLS необходимо учесть особенности работы с самоподписными сертификатами. Это можно сделать в настройках PHP, в файле /etc/php7.4/apache2/conf.d/devprom.ini необходимо добавить два параметра:

```
openssl.cafile=/var/www/devprom/devprom_ru.pem  
openssl.capath=/var/www/devprom
```

Тонкая настройка

Различные службы каталогов могут по-разному определять атрибуты, классы объектов и т.п. Подобные специфические параметры определены в файлах настроек, соответствующих типу LDAP-каталога:

- Active Directory - htdocs/conf/plugins/ee/settings_ldap_ad.php

- OpenLDAP - htdocs/conf/plugins/ee/settings_ldap_ldap.php
- Apache DS - htdocs/conf/plugins/ee/settings_ldap_apacheds.php

```
// имя LDAP-сервера
define(LDAP_SERVER, localhost:10389);

// учетная запись, под которой выполняется подключение к LDAP-серверу
define(LDAP_USERNAME, имя пользователя);

// пароль учетной записи, для подключения к LDAP-серверу
define(LDAP_PASSWORD, secret);

// путь к домену верхнего уровня, с которого начинается построение дерева каталогов
// компании company.ru
define(LDAP_DOMAIN, OU=Users,DC=company,DC=ru);

// запрос поиска объектов в каталоге, используемый для отображения состава каталога
define(LDAP_ROOTQUERY, (!(objectClass=organizationalUnit)
(objectClass=groupOfUniqueNames)(objectClass=person)(objectClass=group)));

// запрос дочерних узлов по идентификатору родительского узла (%1)
define(LDAP_TREEQUERY, (memberOf=%1));

// атрибут определяющий название группы (организационной единицы)
define(LDAP_GROUP_ATTR, cn);

// атрибут определяющий название учетной записи пользователя (имя пользователя)
define(LDAP_TITLE_ATTR, cn);

// атрибут определяющий логин пользователя в Windows
define(LDAP_LOGIN_ATTR, userprincipalname);

// атрибут определяющий адрес электронной почты учетной записи
define(LDAP_EMAIL_ATTR, mail);

// атрибут определяющий описание учетной записи пользователя
define(LDAP_DESCRIPTION_ATTR, title);

// название атрибута OU
define(LDAP_ATTR_OU, ou);

// название атрибута DN
define(LDAP_ATTR_DN, dn);

// название атрибута CN
define(LDAP_ATTR_CN, cn);

// название атрибута, определяющей вхождение объекта в другой объект
define(LDAP_ATTR_MEMBEROF, memberOf);

// список классов, соответствующих учетной записи пользователя
define(LDAP_CLASS_OP, organizationalPerson, person);

// список классов, соответствующих организационной единице (группе)
define(LDAP_CLASS_OU, organizationalUnit, groupOfUniqueNames, group);
```

Журнал подключений к LDAP

По умолчанию, лог-файл с информацией о подключении к LDAP-серверу расположен по пути
 /var/www/devprom/logs/ldap.log

В файле `htdocs/conf/logger.xml` прописан путь к логу подключений к LDAP-серверу. При необходимости вы можете его использовать для выявления проблем при импорте объектов из службы каталогов.