Настройка аутентификации LDAP

Настройка аутентификация LDAP выполняется пользователем с правами администратора. В Панели администратора откройте раздел **Настройки**, перейдите на вкладку **Провайдеры аутентификации**, выберите **LDAP**.

Настройки

- Установите флаг **Включить LDAP аутентификацию**.
  Проверьте, что в файле *admin/config.inc.php* для параметра **$conf['auth_remote']** установлено значение **1**.
  Чтобы отключить аутентификацию LDAP, для параметра **$conf['auth_remote']** установите значение **0**.
- Выполните настройку параметров LDAP:
  - В поле **Хост** укажите имя хоста вашего LDAP сервера.
  - В поле **Порт** укажите порт для LDAP сервера. По умолчанию порт для LDAP через соединение SSL равен 636, для LDAP через соединение TCP, UDP или для TLS – 389.
  - В поле **DN** укажите DN для вашего домена.
  - В поле **DN пользователя** введите DN, который будет использоваться для связи и поиска.
  - В поле **Пароль** введите пароль для DN пользователя, указанного в предыдущем поле.
    Для анонимной связи оставьте поля **DN пользователя** и **Пароль** пустыми.

  Чтобы использовать вложенные группы в Active Directory, установите атрибут членства LDAP в:
  member:1.2.840.113556.1.4.1941:
  Это специальное правило для рекурсивного группового поиска.

  Для получения дополнительной информации смотрите следующие ссылки:
  https://msdn.microsoft.com/en-us/library/aa746475(v=vs.85).aspx
  https://blogs.technet.microsoft.com/...explore-group-membership-with-powershell/

- Настройте параметры **конфигурации**.
  - Укажите, разрешена ли **локальная** (встроенная) **аутентификация**.
  - Введите **IP адреса** для аутентификации в KBPublisher.
  - Поле **Переписать пользователя при входе в систему** предназначено для задания времени в секундах, необходимое для перезаписи пользовательских данных при входе в систему. Введите **0**, чтобы отключить обновления данных пользователя при входе. Введите **1** для перезаписи пользовательских данных в KBPublisher каждый раз, когда приходит запрос на аутентификацию.
  - Укажите **Ссылку сброса пароля**, т.е. ссылку, по которой удаленные пользователи могут сбросить свой пароль.
  - Поле **Информация об учетной записи** пользователя указывает, может ли пользователь обновлять информацию о своей учетной записи. Доступны значения:
    - **0** - Выключено, пользователь не может обновлять информацию о своем аккаунте;
    - **1** - Включено, пользователь может обновлять информацию о своем аккаунте;
    - **2** - Авто, зависит от других настроек.
- Настройте параметры **Соответствия групп**:
  - В поле **Тип LDAP-группы** выберите поведение соответствия групп LDAP. LDAP-группы могут быть статическими или динамическими. Статическая группа содержит список ее пользователей. При динамической группе запись пользователя сама содержит список групп, к которым он принадлежит. Некоторые серверы LDAP могут не поддерживать динамические группы.
  - В поле **LDAP атрибут членства пользователя** в динамической группе по умолчанию равен 'memberOf', для статической – 'member'.
- Настройте **пользовательские поля**:
  - В поле **LDAP для ID удаленного пользователя** введите уникальный идентификатор пользователя для сервера LDAP. По умолчанию для серверов Active Directory установлено значение 'sAMAccountName', для других LDAP-серверов – 'UID'.
  - В поле **LDAP атрибут для имени** введите атрибут для имени пользователя. По умолчанию для большинства серверов LDAP установлено значение 'givenName'. Если запись пользователя не имеет этого атрибута, то можно указать атрибут, который содержит полное имя пользователя (такие как 'displayName', 'fullName', 'cn' и т.д.) и регулярное выражение для получения имени пользователя из этого атрибута. Используйте круглые скобки, чтобы указать нужную часть. При необходимости используйте разделители и модификаторы. Пример: cn|/^([A-Z][a-z]+)/
  - В поле **LDAP атрибут для фамилии** введите атрибут для фамилии пользователя. По умолчанию для большинства серверов LDAP установлено значение 'sn'. Правила ввода такие же, как и для предыдущего атрибута. Пример: ... cn|/S([AZ][AZ]+)$/
  - В поле **LDAP атрибут для email** введите атрибут для адреса электронной почты пользователя. По умолчанию для большинства LDAP серверов установлено значение 'mail'.
  - Чтобы сопоставить атрибуты группы LDAP с привилегиями и ролями пользователя KBPublisher, настройте **Атрибут LDAP для привилегий** и **Атрибут LDAP для ролей** с помощью кнопок [**...**].

    Обратите внимание: Если сопоставить группы LDAP с привилегиями KBPublisher, то всем подходящим пользователям будет назначена указанная привилегия. Если у вас отсутствует Неограниченная лицензия (**Unlimited**), и превышено количество разрешенных пользователей-администраторов, то привилегия не назначится.

    Важно! Если оставить эти поля пустыми, они не будут обновляться при входе пользователя в систему.

- Настройте **опции тестирования/отладки** аутентификации для пользователя LDAP. Параметры необязательны.

Совет: Вы можете отключить аутентификацию LDAP. Для этого в файле */kbp_dir/admin/config.inc.php* для параметра $conf['auth_remote'] установите значение **0**.

ID статьи: 371
Последнее обновление: 25 окт., 2017
Обновлено от: Черевко Ю.
Ревизия: 8
Руководство пользователя v8.0 -> Единый вход -> LDAP аутентификация -> Настройка аутентификации LDAP
https://www.kbpublisher.ru/kb/entry/371/