

[К-5219] Авторизация на сайте тех. поддержки через LDAP

Для настройки авторизации пользователей сайта тех. поддержки через LDAP-каталог (например, Active Directory, ApacheDS и др.) откройте на редактирование файл `app/co/bundles/Devprom/ServiceDeskBundle/Resources/config/settings.yml` и добавьте в конец следующие настройки:

```
fr3d_ldap:
  driver:
    host:          127.0.0.1
    port:          10389
    username:      uid=admin,ou=system
    password:      secret
    #useSsl:       true
    #useStartTls: true
  user:
    baseDn:       ou=system
    filter:        (&(objectClass=*))
    usernameAttribute: uid
    attributes:
      - { ldap_attr: uid,   user_method: setUsername }
      - { ldap_attr: cn,   user_method: setName }
      - { ldap_attr: mail, user_method: setEmail }

security:
  encoders:
    FOS\UserBundle\Model\UserInterface: sha512
  providers:
    chain_provider:
      chain:
        providers: [fos_userbundle, fr3d_ldapbundle]
    fos_userbundle:
      id: fos_user.user_provider.username_email
    fr3d_ldapbundle:
      id: fr3d_ldap.security.user.provider
  firewalls:
    main:
      pattern: ^/
      fr3d_ldap: ~
      provider: chain_provider
      form_login:
        default_target_path: /issues
        always_use_default_target_path: true
      logout: true
      anonymous: true
      http_basic: false
      remember_me:
        secret: secret
        lifetime: 31536000
        path: /
        always_remember_me: true
```

Отредактируйте параметры подключения к LDAP-каталогу:

Название параметра	Назначение параметра
fr3d_ldap.driver.host	Имя или адрес сервера с LDAP-каталогом
fr3d_ldap.driver.port	Номер порта LDAP-каталога, по умолчанию 389
fr3d_ldap.driver.username	DN-имя учетной записи, под которой будет осуществляться подключение к LDAP-каталогу для аутентификации пользователей
fr3d_ldap.driver.password	Пароль учетной записи, используемой для поиска в каталоге
fr3d_ldap.driver.useSsl	<p>Раскомментируйте строку, если необходимо использовать подключение к LDAP-каталогу по протоколу ldaps.</p> <p>При использовании самоподписных сертификатов, может потребоваться явно указать пути расположения корневого сертификата. Это можно сделать в настройках PHP, в файле /etc/php7.4/apache2/conf.d/devprom.ini необходимо добавить два параметра:</p> <pre>openssl.cafile=/var/www/devprom/devprom_ru.pem openssl.capath=/var/www/devprom</pre>
fr3d_ldap.driver.useStartTls	Раскомментируйте строку, если ваш LDAP поддерживается подключение через START TLS
fr3d_ldap.user.baseDn	Общая часть DN-имен (имя каталога) в LDAP
fr3d_ldap.user.filter	Фильтр запроса поиска учетных записей при аутентификации
fr3d_ldap.user.usernameAttribute	Атрибут в каталоге, используемый для уникальной идентификации пользователей (uid или sAMAccountName)

Пример настройки подключения к LDAP для случая использования Active Directory:

```
fr3d_ldap:
  driver:
    host: "ad.loc",
    port: 389,
    username: "CN=DevProm,OU=Service,OU=Domain Users,DC=company,DC=loc",
    password: "*****"
  user:
    baseDn: "DC=company,DC=loc",
    filter: "(objectClass=*)",
    usernameAttribute: samaccountname,
    attributes: [{ ldap_attr: samaccountname, user_method: setUsername },
{ ldap_attr: mail, user_method: setEmail },{ ldap_attr: displayName, user_method: setName }] }
```

Чтобы запретить пользователям самостоятельно регистрироваться на сайте и запрашивать ссылку для сброса пароля, установите параметры **registration_enabled** и **resetting_enabled** в значение **false**. Эти параметры расположены в начале файла

app/co/bundles/Devprom/ServiceDeskBundle/Resources/config/parameters.yml

Для получения дополнительной отладочной информации, для диагностики подключения к LDAP в частности, настройте расширенное логирование - измените level на debug как показано ниже в файле app/co/bundles/Devprom/ServiceDeskBundle/Resources/config/config.yml

```
monoLog:
  handlers:
    appLog:
      type: rotating_file
      path: "%kernel.logs_dir%/servicedesk_system.log"
```

```
level: debug  
max_files: 5 # Set up to keep log files for 5 recent days only
```

Чтобы изменения вступили в силу, необходимо очистить кеш приложения. Для этого перейдите в Администрирование - Настройки - Приложение и нажмите кнопку "Очистить кеш".