Механизм единой авторизации

Общие сведения

Смысл механизма в том, что если backend QP7 закрыт NT-авторизацией, то можно настроить его работу так, чтобы пользователю не приходилось еще проходить QP7-авторизацию.

Принцип работы

Механизм работает следующим образом:

1. Пользователь проходит NT-авторизацию
2. Из переменных окружения считывается информацию, какой пользователь прошел NT-авторизацию.
3. В базе данных ищется пользователь по полю NT Login. Если такой пользователь найден, то QP7 -авторизацию уже проходить не надо. Поле NT Login может быть или явно задано в профайле пользователя или получено в процессе импорта из Active Directory, который будет описан в следующем разделе.
4. Пользователю остается ввести только Customer Code, но только один раз, так как введенное значение сохраняется в Cookie.

Импорт из Active Directory

Общие сведения

Этот функционал предназначен для импорта новых и обновления существующих пользователей из Active Directory в Q-Publishing. Синхронизация осуществляется на уровне групп и на уровне пользователей по кнопке Synchronize.

Настройка

Перед началом процесса импорта нужно настроить параметры LDAP-соединения. Для этого в конфигурационном файле QP7 в секции app_vars задаются параметры

```
<app_var app_var_name="ADsConnectionString">Provider=ADsDSOObject;User ID=user;Password=pass;</app_var>
<app_var app_var_name="ADsPath">LDAP://my_server.my_domain.ru/DC=my_domain,DC=ru</app_var>
```

Пользователь должен обладать достаточными правами для выполнения LDAP-запросов.

Синхронизация групп

Перед синхронизацией пользователь должен задать NT_LOGIN группы.

По NT_LOGIN составляется LDAP-запрос для получения пользователей группы и выполняется. Все пользователи, найденные в группе Active Directory, синхронизируются с пользователями, существующими в Q-Publishing группе по следующему алгоритму:

- сопоставление пользователей осуществляется по NT-login.
- новые пользователи (которые есть в AD, но их нет в QP) добавляются, у них прописываются параметры: логин (NT-login от последнего слэша), NT-логин, e-mail, имя, фамилия. Галочка NT-Login выставляется. Генерируется случайный пароль. Если какие-либо необходимые для QP параметры в AD не заданы, то в это поле в QP вставляется значение *Undefined*. Если пользователь есть в AD и он disabled, то он не копируется.
- Для существующих пользователей (есть в AD, есть в QP) обновляются параметры: пароль, e-mail, имя, фамилия. Если какие-либо необходимые для QP параметры в AD не заданы, то в это поле в QP вставляется значение *Undefined*. Если пользователь есть в AD и он является disabled, то параметры переносятся в QP, но пользователь QP также становится disabled.
- Пользователи, удаленные из AD группы (нет в AD, есть в QP) становятся disabled. При этом выполняется проверка, в какие еще группы QP входит пользователь. По группам, которые имеют NT-Login, проверяются группы AD. Но если при этой проверке обнаруживается, что пользователь является disabled в AD, то он становится disabled в QP. И только если пользователь входит еще куда-либо и не disabled в AD, то он не становится disabled.

Синхронизация пользователей

Действия, которые выполняются в цикле для членов группы в функционале Synchronize Group, здесь выполняются только для одного пользовтеля.