Роли и разрешения

# Мультитенантное окружение

## Основные сведения

Тенант - это аналог логической базы данных в составе одной физической. Каждая такая база изолирована от других.

В мультитенантном окружении пользователи и роли хранятся в базе дананых каталога а основные данные – в базах сегментов. Каждый сегмент хранит данные одного или нескольких тенантов. Каждый пользователь может входить в один и только один тенант и не имеет доступа к данным других тенантов.

## Настройки

Для переключения системы в режим мультитенантного окружения в файле web.config нужно его включить (ключ multiTenant). Кроме того, обычно в таком окружении разрешена регистрация пользователей (ключ registration).

<appSettings>  
 <add key="multiTenant" value="true" />  
 <add key="registration" value="true" />  
 <add key="customUserMenu" value="a2ui.[TenantMenu.User.Load]"/>  
</appSettings>

Дополнительно, поскольку права для пользователей удобно хранить в базе сегментов, переключим загрузку основного меню системы на базу сегментов и будем выполнять это с помощью пользовательской процедуры (ключ customUserMenu).

## Базы данных

Для начальной работы потребуется две базы данных. Catalog и Segment. Создадим их обе и включим в web.config две строки подключения.

<connectionStrings>  
 <add name="Catalog" connectionString="Data Source=localhost;  
 Initial Catalog=MtCatalog;Integrated Security=True"  
 providerName="System.Data.SqlClient" />  
 <add name="Default" connectionString="Data Source=localhost;  
 Initial Catalog=MtSegment;Integrated Security=True"  
 providerName="System.Data.SqlClient" />  
</connectionStrings>

Обратите внимание, что вторая строка называется Default, а не Segment. Это сегмент по умолчанию, возможно единственный. Если в настройках конкретного пользователя сегмент не указан, берется строка подключения Default. Чаще всего при добавлении сегментов строки подключения Segment1 и Default будут одинаковыми.

После создания баз данных выполните следующие скрипты:

На базе данных каталога:

* a2v10platform.sql

На базе данных сегмента:

* a2v10platform.sql
* a2v10multitenant.sql

## Пользователи

Обычно в мультитенантном окружении пользователи сами регистируются в системе.

Один из пользователей (тот, кто создал тенант) является администратором (владельцем) тенанта. Именно он (и только он) может добавлять других пользователей в тенант и назначать им права доступа (хотя это можно изменить, поскольку эта проверка выполняется на уровне хранимых процедур.

Идентификатор пользователя – администратора тенанта записано в поле [Admin] таблицы a2security.[Tenants]. Обратите внимание, что реальный тенант (в базе сегментов) создается только после подтверждения е-mail пользователя.

### Регистрация пользователя

Регистрация нового пользователя (администратора тенанта) происходит следующим образом:

1. Пользователь заполняет форму регистрации.
2. База Catalog. Система создает запись тенанта в таблице a2security.Tenants и пользователя в таблице a2security.Users. Это делается хранимой процедурой a2security.CreateUser. Обратите внимание, что никаких действий в базе сегмета пока не выполняется.
3. Система отправляет пользователю е-mail с кодом подтверждения.
4. Пользователь вводит код подтверждения в соответствующее поле.
5. Система устанавливает признак подтверждения e-mail в поле EmailConfirmed таблицы a2security.Users и вызывает процедуру

## Главное меню

Для