

Доступ, пользователи, группы

Общее описание

В модели безопасности **QP7.Framework** есть объекты безопасности, на которые могут быть назначены права доступа и субъекты безопасности (пользователи и группы пользователей, причем группы могут быть вложенными), которым назначаются эти права. В QP7 существуют 3 основные группы прав доступа:

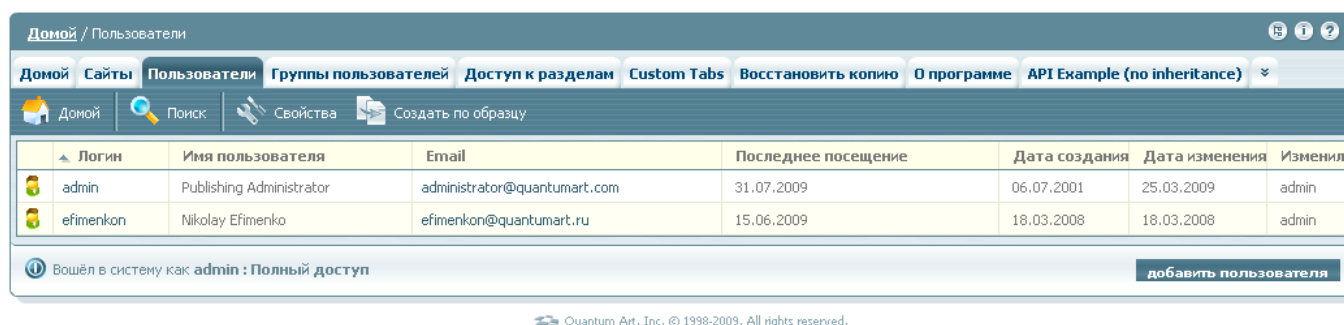
- Права на использование функциональности
 - Права доступа на страницы бэкенда
- Основные права на модификацию данных
 - Права доступа на сайты
 - Права доступа на контенты
 - Права доступа на статьи
- Дополнительные права на модификацию данных
 - Права доступа на Workflow
 - Права доступа на папки библиотеки сайта

Права на использование функциональности определяют, какие вкладки и кнопки показывать пользователю, а права на модификацию данных определяют, какие объекты QP7 разрешено модифицировать (удалять) пользователю. Эффективные права доступа на некоторое действие в бэкенде образуются пересечением прав на использование функциональности и прав на модификацию данных. Например, чтобы иметь возможность редактировать свойства сайта, нужно иметь доступ не ниже **Изменить** на этот сайт (данные) и на вкладку **Свойства сайта** (функциональность).

Пользователь, входящий в группу администраторов автоматически получает полный доступ на всю функциональность бэкенда и все данные.

Пользователи

Управление пользователями осуществляется из корневого каталога через окно **Пользователи** (**Домой/Пользователи**).



Домой / Пользователи						
Домой	Сайты	Пользователи	Группы пользователей	Доступ к разделам	Custom Tabs	Восстановить копию
Домой	Поиск	Свойства	Создать по образцу			
Логин	Имя пользователя	Email	Последнее посещение	Дата создания	Дата изменения	Изменил
admin	Publishing Administrator	administrator@quantumart.com	31.07.2009	06.07.2001	25.03.2009	admin
efimenkon	Nikolay Efimenko	efimenkon@quantumart.ru	15.06.2009	18.03.2008	18.03.2008	admin

Вошёл в систему как **admin** : Полный доступ

добавить пользователя

Quantum Art, Inc. © 1998-2009. All rights reserved.

Настройка пользователя начинается с создания учетной записи пользователя. Учетная запись помогает идентифицировать каждого пользователя в системе и является средством контроля

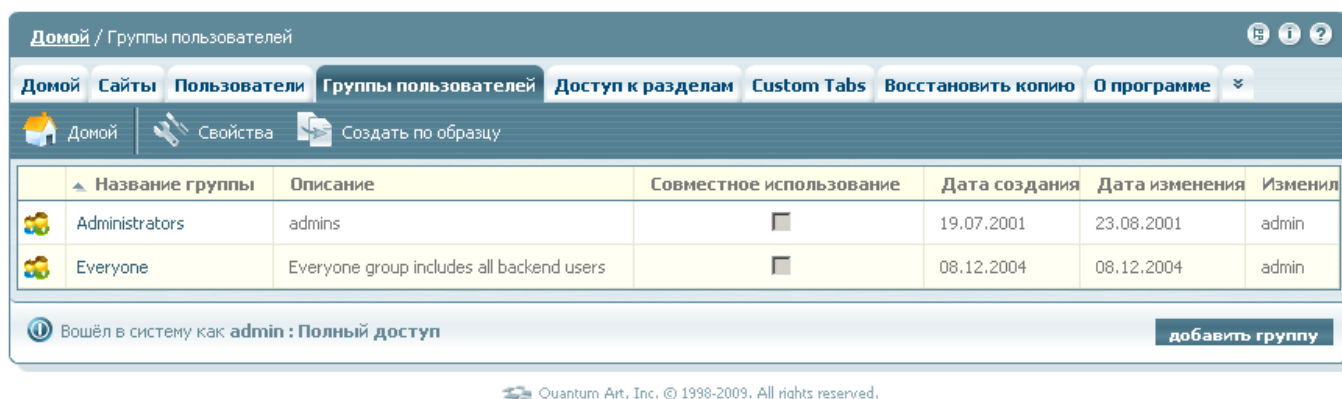
над доступом.

Чтобы упростить администрирование пользователей, **QP7.Framework** также позволяет администраторам объединять пользователей в группы и распределять права между этими группами, вместо того, чтобы распределять их между отдельными пользователями. Пользователь может быть включен во множество групп. В таком случае, пользователь всегда наследует самый высокий уровень прав на конкретное действие среди всех групп.

Чтобы создать нового пользователя, нажмите на кнопку **Добавить пользователя** в правом нижнем углу окна **Пользователи**. **QP7.Framework** открывает окно **Новый пользователь**. После заполнения необходимой информации и нажатия кнопки **Сохранить**, профиль пользователя создается в системе и отображается окно [Профиль пользователя](#). Оно используется для изменения профиля существующего пользователя и включает те же поля, что и окно **Новый пользователь**.

Группы пользователей

Группы пользователей используются для удобства управления правами доступа, когда нескольким пользователям необходимо назначить одни и те же права и упростить задачу добавления нового пользователя, которому нужно дать такие же права, как и существующему.



Название группы	Описание	Совместное использование	Дата создания	Дата изменения	Изменил
Administrators	admins	<input type="checkbox"/>	19.07.2001	23.08.2001	admin
Everyone	Everyone group includes all backend users	<input type="checkbox"/>	08.12.2004	08.12.2004	admin

Вошёл в систему как admin : Полный доступ

добавить группу

Quantum Art, Inc. © 1998-2009. All rights reserved.

Чтобы создать новую группу пользователей, следует нажать кнопку **Добавить группу** в правом нижнем углу окна **Группы пользователей**. Открывается окно **Новая группа**. Оно совпадает по содержимому с окном [Свойства группы](#), которое используется для существующих групп пользователей.

Связывание пользователя и группы

Чтобы связать пользователя и группу, можно использовать страницу **Состав (Membership)** на уровне группы и **Членство (Member Of)** на уровне пользователя. Эти страницы взаимодополняют друг друга. Одна отражает список всех пользователей данной группы, другая – список всех групп, которым принадлежит данный пользователь. С помощью выпадающего списка можно добавить пользователя (группу), который после нажатия на кнопку **Сохранить** также окажется в списке. Теперь пользователь включен в группу.

Чтобы удалить пользователя из группы, выберите в списке флажок **Удалить** рядом с пользователем (группой) и нажмите кнопку **Сохранить**.

О типах доступа

Существует пять уровней прав доступа:

1. **Полный доступ** – разрешены все действия: просмотр, изменение и удаление
2. **Изменение** – удаление запрещено; просмотр и изменение разрешены
3. **Чтение** – изменение и удаление запрещены, но разрешен просмотр
4. **Список** – разрешен только просмотр объектов в списках (страница **Статьи**, список в поле типа **Связь**), просмотр в интерфейсе **Данные статьи** запрещен.
5. **Запретить** – любой доступ запрещен, пользователь не видит соответствующий объект QP7 на этом уровне доступа.

Доной / Sandbox Net / User Questions / Статьи / Доступ к статье

Данные статьи | Расписание | История изменений | Предварительный просмотр статьи | **Доступ к статье** | Workflow статьи

Домой Вверх

Пользователь	Удалить пользователя	Полный доступ	Изменение	Чтение	Список	Запретить
добавить пользователя	Не выбрано					

Название группы	Удалить группу	Полный доступ	Изменение	Чтение	Список	Запретить
добавить группу	Не выбрано					

Если вы хотите изменить разрешения для контента, перейдите по этой [ссылке](#).

Вошёл в систему как **admin** : Полный доступ

Обновить | Удалить выбранные | Отменить

Quantum Art, Inc. © 1998-2009. All rights reserved.

Доступ к разделам

Права доступа и полномочия управляются в секции **Доступ к разделам**. Секция **Доступ к разделам** это корневая вкладка **QP7.Framework**.

Так как навигация в бэкенде **QP7.Framework** осуществляется преимущественно путем вкладок, управление правами доступа пользователей основано на структуре вкладок бэкенда. Необходимо добавить, что окно **Доступ к разделам** содержит полное иерархическое представление структуры вкладок Бэкенда.

Права доступа на страницы вычисляются с учетом иерархии страниц. Если для данной страницы и данного пользователя не найдена запись о правах доступа, то алгоритм поиска переходит на уровень выше, и далее, пока не найдет такую запись, либо не дойдет до корня (точнее, до одной из корневых страниц, так как единой корневой страницы в бэкенде нет). Так как для страниц поддерживается иерархия, то для того, чтобы быстро настроить редакторские права доступа, достаточно дать пользователю право **Чтение** на страницу **Сайты** (а значит, на всю иерархию) и **Изменение** на **Данные статьи**. С другой стороны, если нужно закрыть от пользователя нежелательные дочерние страницы, то придется явно прописывать право доступа **Запретить**. Общие правила соответствия функций и необходимого уровня доступа приведены ниже:

- Требуемый уровень доступа - **Полный доступ**

- Удалить
- Собрать
- Восстановить резервную копию
- Импорт
- Синхронизировать
- Требуемый уровень доступа - **Изменение**
 - Добавить новый
 - Сохранить
 - Обновить
 - Создать по образцу
 - Архивировать
 - Восстановить
 - Экспорт
 - Создать резервную копию
- Требуемый уровень доступа - **Чтение**
 - Свойства
 - Предварительный просмотр
 - Отмена
 - OnScreen

Домой / Доступ к разделам

Домой Сайты Пользователи Группы пользователей **Доступ к разделам** Custom Tabs Восстановить копию

Домой

[-] Домой

Пользователи	Уровень доступа
Пользователи не указаны	
Группы	Уровень доступа
Everyone	Полный доступ

[-] Сайты

Пользователи	Уровень доступа
demo demo	Чтение
Группы	Уровень доступа
Editors	Чтение

[+ Новый сайт
 [+ Свойства сайта
 [+ Копировать сайт
 [+ Копия сайта
 [+ OnScreen
 [+ Контенты
 [+ Шаблоны
 [+ Библиотека сайта
 [+ Стили
 [+ Workflow
 [+ Статусы
 [+ Доступ к сайту
 [+ Обновление сайта

Вошёл в систему как **admin** : Полный доступ

Доступ к объектам QP7

Общий принцип

В отличие от прав доступа на страницы, эффективные права доступа на данные не вычисляются иерархически, поэтому на каждый объект безопасности они должны быть заданы явно. Из этого правила есть единственное исключение: если для контента сброшена опция **Использовать права доступа статей (Allow Article Permissions)**, то запрос на вычисление прав доступа к статье данного контента переадресуется на уровень контента.

Права доступа на создаваемые объекты

Действует общее правило: пользователь, создающий объект безопасности, автоматически получает уровень доступа **Полный доступ (Full Access)** на него. Существует модификация данного правила для статей: если создатель статьи входит в группу с установленной опцией **Совместное использование статей (Shared Ownership)**, то все члены данной группы получают **Полный доступ (Full Access)** на данную статью.

Кроме того, для контентов и статей предусмотрен механизм копирования правил доступа с верхнего уровня (сайта и контента, соответственно). Для его реализации предусмотрена специальная опция **Применить к новому потомку (Apply To New Child)**. Она задается для конкретного правила доступа. Если она установлена, то соответствующее правило будет скопировано при создании элемента нижнего уровня. То есть, например, если у пользователя выставить такую опцию на уровне Доступ к сайту (**Site Permissions**), то для всех контентов, которые будут созданы после этого, данное правило доступа будет скопировано. Замечание: при создании виртуальных контентов опция **Применить к новому потомку (Apply To New Child)** автоматически сбрасывается.

При создании новой папки в **Библиотеке сайта (Site Library)** права на нее автоматически копируются с сайта. При создании новой папки в **Библиотеке контента (Content Library)** права на нее автоматически копируются из контента. В дальнейшем в случае изменения прав доступа к контенту права доступа на папки контента синхронизируются с правами на сам контент.

Изменение прав доступа к существующим объектам

Стандартный функционал является общим для всех объектов безопасности. Он достаточно прост и самоочевиден. Стоит только отметить галочку **Применить к новому потомку (Apply To New Child)** для контентов и сайтов (про нее говорилось в предыдущем разделе) и то, что в данном интерфейсе не отображаются встроенный пользователь *Administrator* и встроенная группа *Administrators*, так как они всегда имеют полный доступ на все объекты безопасности.

Домой / Sandbox Net / Доступ к сайту

Свойства сайта OnScreen Контенты Шаблоны Библиотека сайта Стили Workflow Статусы **Доступ к сайту** Обновление сайта Резервная копия сайта

Домой Вверх

Вы хотите:

- ☒ Изменить разрешения для этого сайта
- ☐ Перенести разрешения сайта на контенты и статьи
- ☐ Посмотреть разрешения дочерних контентов

Права доступа

Пользователь	Удалить пользователя	Полный доступ	Изменение	Чтение	Список	Запретить	Применить к новому потоку
demo demo	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
добавить пользователя	Не выбрано						

Название группы	Удалить группу	Полный доступ	Изменение	Чтение	Список	Запретить	Применить к новому потоку
Editors	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
добавить группу	Не выбрано						

Вошёл в систему как admin : Полный доступ

Обновить Отменить

Так как права доступа на данные должны быть заданы явно на каждом уровне иерархии, то в бэкенде предусмотрены функции, облегчающие такую настройку. Это механизмы **Перенести разрешения сайта на контенты и статьи (Propagate site permissions to contents and articles)** и **Перенести разрешения контента на статьи (Propagate content permissions to articles)**. При копировании можно выбрать правило или набор правил, которые будут скопированы с текущего уровня, также есть возможность ограничить набор дочерних записей, к которым это правило будет применено (галочки **Ограничить выбранными статьями (Limit to Selected Articles)**, **Ограничить выбранными контентами (Limit to Selected Contents)**)).

Домой / Sandbox Net / Доступ к сайту

Свойства сайта OnScreen Контенты Шаблоны Библиотека сайта Стили Workflow Статусы **Доступ к сайту** Обновление сайта Резервная копия сайта

Домой Вверх

Вы хотите:

- ☐ Изменить разрешения для этого сайта
- ☒ Перенести разрешения сайта на контенты и статьи
- ☐ Посмотреть разрешения дочерних контентов

Права доступа

<input type="checkbox"/> Пользователь	Уровень доступа
<input checked="" type="checkbox"/> demo demo	Список

<input type="checkbox"/> Название группы	Уровень доступа
<input type="checkbox"/> Editors	Чтение

Изменить разрешения на все контенты и статьи

Действие: **Добавить и обновить** ☒ Ограничить выбранными контентами

<input type="checkbox"/> Название контента	Описание
<input checked="" type="checkbox"/> Dictionary	Base content for the Dictionary library. Gets filled automatically.
<input checked="" type="checkbox"/> Site Global Params	Base content for the Site Global Params library.
<input checked="" type="checkbox"/> Структура разделов	Contains a list of the site pages — real and virtual — as well as links to the outer sites. Base content for the Page Alias library.
<input type="checkbox"/> News	A news content.
<input type="checkbox"/> FAQ_Sections	Question categories for FAQ.
<input type="checkbox"/> FAQ_Questions	All questions with answers to be displayed by the FAQ module.

Вошёл в систему как admin : Полный доступ

Обновить Отменить

Есть несколько режимов переноса прав доступа на нижний уровень иерархии. Режим по умолчанию – **Добавить и обновить (Add New and Update)**. В этом режиме *Добавить* означает, что если для дочерних сущностей не существует настроенных прав доступа для данного пользователя или группы, то эти правила будут скопированы. Смысл же *Обновить* – такой, что если эти правила для дочерних сущностей существуют, то они будут заменены. Этот режим является основным, и именно его нужно использовать для переноса правил доступа в общем случае. Режимы копирования **Добавить (Add New)** и **Обновить (Update)** доступны также по отдельности. Кроме этого существует режим **Удалить (Remove)** позволяющий удалить права доступа у дочерних сущностей для выбранных пользователей или групп. Следует отдавать предпочтение этому методу по сравнению с массовой установкой уровня доступа **Запретить (Deny)**, так как логика – такая же, а дополнительных записей в базе данных не требуется.

Например, редактору нужно дать право изменять все контенты сайта, при этом свойства сайта модифицировать он не должен. Для этого нужно сначала дать право доступа **Изменение (Modify)** на сайт, затем выполнить операцию **Перенести разрешения сайта на контенты и статьи (Propagate site permissions to contents and articles)** (при этом галочку **Ограничить выбранными контентом (Limit to Selected Contents)** мы не используем).

Данные механизмы, кроме непосредственного копирования прав доступа с верхнего уровня на нижний позволяют еще решать задачу групповой настройки прав. При решении задачи групповой настройки прав часто бывает необходимо просмотреть существующие права перед внесением изменений или наоборот, взглянуть на результаты этих изменений. Для этой цели существует дополнительный режим работы **Посмотреть разрешения дочерних контентов (View child permissions)**

Домой / Sandbox Net / Доступ к сайту

Свойства сайта OnScreen Контенты Шаблоны Библиотека сайта Стили Workflow Статусы **Доступ к сайту**

Домой Вверх

Вы хотите:

- ☐ Изменить разрешения для этого сайта
- ☐ Перенести разрешения сайта на контенты и статьи
- ☒ Посмотреть разрешения дочерних контентов

Права доступа

☐ Пользователь

☒ Группа

Название контента	Уровень доступа
Dictionary	Не установлено (Запретить)
Site Global Params	Не установлено (Запретить)
Site Pages	Изменение
News	Изменение
FAQ_Sections	Чтение
FAQ_Questions	Изменение
User Questions	Чтение
Users	Чтение
Surveys	Не установлено (Запретить)
Survey Questions	Не установлено (Запретить)
Survey Question Types	Не установлено (Запретить)
Responses	Не установлено (Запретить)
Survey Choices	Не установлено (Запретить)

Вошёл в систему как **admin** : Полный доступ

Обновить Отменить

Интерфейсы

Настроить доступ к объектам QP7 можно в следующих интерфейсах:

- Права доступа на сайты – вкладка **Доступ к сайту (Site Permissions)** на уровне сайта
- Права доступа на контенты – вкладка **Доступ к контенту (Content Permissions)** на уровне контента
- Права доступа на статьи – вкладка **Доступ к статье (Article Permissions)** на уровне статьи
- Права доступа на Workflow – вкладка **Права workflow (Workflow Permissions)** на уровне workflow
- Права доступа на папки библиотеки сайта – интерфейс, вызываемый кнопкой **Права доступа (Permissions)** на вкладке **Библиотека сайта (Site Library)** на уровне сайта

Вычисление эффективных прав доступа на объект QP7

1. Если пользователь – администратор, то результат – **Полный доступ (Full Access)**
2. Если ищутся права для статьи, а для контента отключена опция **Использовать права доступа статей**, то запрос переадресуется на уровень контента.
3. Ищутся явные права для данного пользователя

4. Если ничего не найдено, то ищутся явные права для групп, в которые входит данный пользователь. Если права доступа найдены сразу для нескольких групп, то учитывается максимальный уровень доступа.
5. Если ничего не найдено, то продвигаемся вверх по иерархии групп, при этом ранее рассмотренные группы уже не учитываются. Процесс заканчивается при нахождении результата (явных прав доступа), либо при достижении корня по всем цепочкам поиска.
6. Если на одном из 3 предыдущих шагов найдены явные права доступа, то они и являются результатом вычисления. Если ничего не найдено, то результирующий уровень доступа – **Запретить (Deny)**.

Модификация алгоритма вычисления прав доступа при использовании Workflow

Здесь и далее под статьями, находящейся в Workflow называются следующие статьи:

1. Статьи, находящиеся в контенте, на который назначен Workflow. При этом на странице **Workflow статьи** для статей выставлен режим **Наследуется (Inherits)** - наследование от контента. Этот режим используется по умолчанию.
2. Статьи, на которые назначен собственный Workflow

Кроме основных правил безопасности, общих для всех объектов QP7, на статьи, находящиеся в Workflow, действуют некоторые дополнительные правила:

1. Если пользователь не входит в Workflow (как лично, так и в составе группы), то он не может удалять или модифицировать статьи, находящиеся в Workflow.
2. Пользователь, входящий в Workflow, может удалить статью, находящуюся в Workflow, только если он явно или в составе группы назначен на последний этап Workflow.

Типовая последовательность настройки доступа для редакторов

Настройка прав доступа к страницам

1. Дать пользователю право **Список (List)** на вкладку **Сайты (Sites)**.
2. Закрыть пользователю доступ ко всем дочерним вкладкам **Сайтов (Sites)**, кроме вкладки **Контенты (Contents)**.
3. Закрыть пользователю доступ к дочерним вкладкам **Контентов (Contents)**: **Свойства контента (Content Info)**, **Поля (Fields)**, **Уведомления (Notifications)**. Решение об остальных вкладках этого уровня принимается на основании конкретной логики использования функционала.
4. Закрыть пользователю доступ к дочерним вкладкам **Статей (Articles)**: **Доступ к статье (Article Permissions)**, **Workflow статьи (Article Workflow)**

Настройка прав доступа к сайту и контентам

1. Настройка контентов, которые пользователь может просматривать (пользователь должен иметь право доступа **Список** на связанные контенты, чтобы он имел право просматривать содержимое полей типа **Связь (Relation)** в редактируемых статьях и

выбирать нужные значения).

2. Дать пользователю право доступа **Чтение (Read)** на конкретный сайт (вкладка **Доступ к сайту (Site Permissions)**)
3. Выполнить операцию **Перенести разрешения сайта на контент и статьи (Propagate to selected contents and articles)** для нужных контентов (или для всех контентов)

Настройка контентов, которые пользователь может редактировать

1. Дать пользователю временно право доступа **Изменение (Modify)** или **Полный доступ (Full Access)** на сайт
2. Выполнить операцию **Перенести разрешения сайта на контент и статьи (Propagate to selected contents and articles)** для нужных контентов
3. Дать пользователю право доступа **Список (List)** на сайт.

Настройка прав доступа к статьям

1. Если для каких-то контентов выставлена опция **Использовать права доступа статей (Use article permissions)**, то возможно для них потребуется более тонкая настройка прав доступа. Она выполняется аналогично предыдущему пункту, только на уровне контента.

From:

<http://wiki.qpublishing.ru/> - QP7.Framework Docs

Permanent link:

http://wiki.qpublishing.ru/doku.php?id=permissions_users_groups

Last update: **2009/08/27 13:23**

