Security Model в QP7.Framework

Общее описание

При разработке QP7.Framework за основу взята модель Security Windows NT. В данной модели есть Security Objects, на которые могут быть назначены права доступа и Security Subjects (пользователи и группы пользователей, причем группы могут быть вложенными), которым назначаются эти права. По использованию объекты Security можно разделить на 3 основные группы:

1) Права на использование функциональности
    - Права доступа на страницы Backend(вкладки)
2) Основные права на модификацию данных
    - Права доступа на сайты
    - Права доступа на контенты
    - Права доступа на статьи
3) Дополнительные права на модификацию данных
    - Права доступа на Workflow
    - Права доступа на Site Library

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

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

Права доступа на страницы Backend

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 дной из корневых страниц, так как единой корневой страницы в Backend нет).

Так как для страниц поддерживается иерархия, то для того, чтобы быстро настроить редакторские права доступа, достаточно дать пользователю право Read на страницу Sites (а значит, на всю иерархию Sites) и Modify на Article Info. С другой стороны, если нужно закрыть от пользователя нежелательные дочерние страницы, то придется явно прописывать право доступа Deny.

Общие правила соответствия функций и необходимого уровня доступа приведены в табл. 1

Таблица 1.

Функции	Минимальный уровень доступа
1) Remove 2) Assemble 3) Restore Backup, Import, Synchronize	Full Access
1) Add New, Save, Update, Create Like 2) Archive, Restore 3) Export, Backup	Modify
1) Properties 2) Preview 3) Cancel 4) OnScreen	Read

Права доступа на данные

Общий принцип

В отличие от прав доступа на страницы, эффективные права доступа на данные не вычисляются иерархически, поэтому на каждый объект Security они должны быть заданы явно. Из этого правила есть единственное исключение: если для контента сброшена опция 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 Security, автоматически получает Full Access на него. Существует модификация данного правила для статей: если создатель статьи входит в группу с установленной опцией Shared Ownership, то все члены данной группы получают Full Access на данную статью.

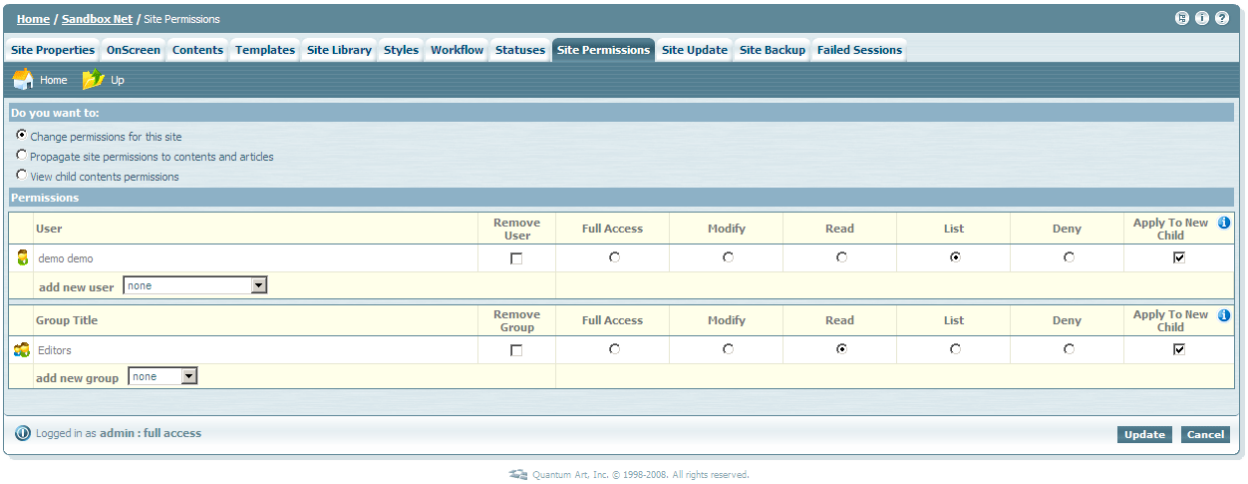
Кроме того, для контентов и статей предусмотрен механизм копирования правил доступа с верхнего уровня (сайта и контента, соответственно). Для его реализации предусмотрена специальная опция Apply To New Child. Она задается для конкретного правила доступа. Если она установлена, то соответствующее правило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

При создании новой папки в Site Library права на нее автоматически копируются с сайта. При создании новой папки в 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

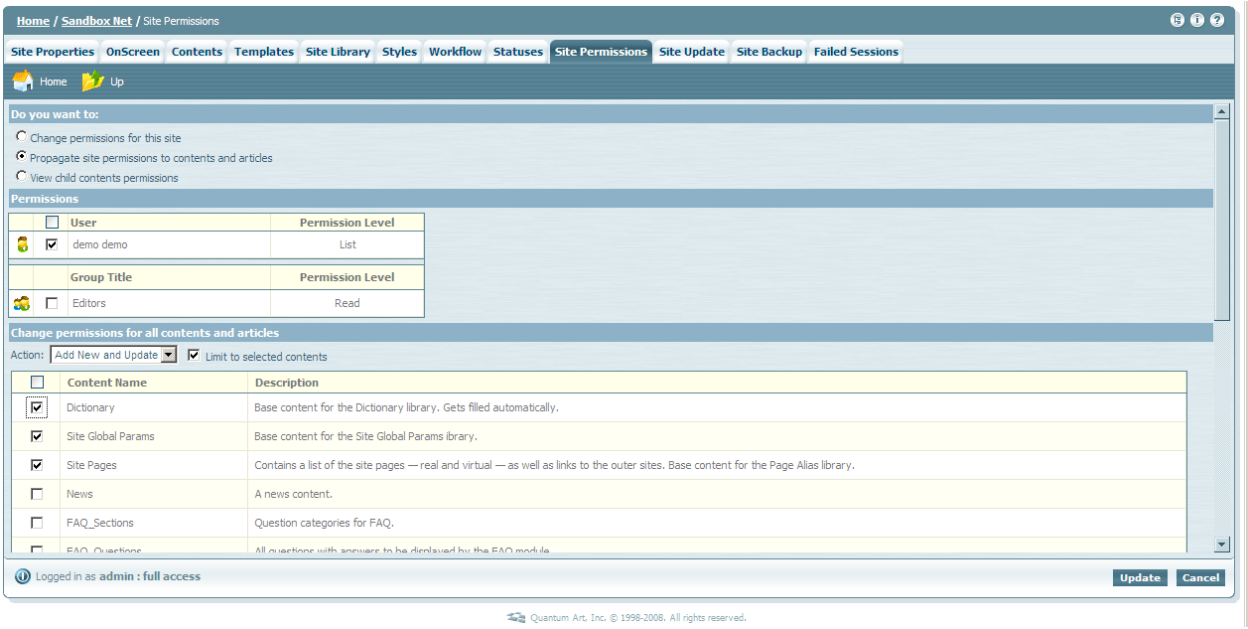
Стандартный функционал является общим для всех объектов Security. Он достаточно прост и самоочевиден (рис. 1). Стоит только отметить галочку Aapply To New Child для контентов и сайтов (про нее говорилось в предыдущем разделе) и то, что в данном интерфейсе не отображаются встроенный пользователь Administrator и встроенная группа Administrators, так как они всегда имеют полный доступ на все объекты Security.

Рис. 1. Стандартный интерфейс Security



Так как права доступа на данные должны быть заданы явно на каждом уровне иерархии, то в Backend предусмотрены функции, облегчающие такую настройку. Это механизмы Propagate site permissions to contents и Propagate content permissions to articles (рис. 2). 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 (галочка Limit to Selected Articles, Limit to Selected Contents).

Рис. 2. Интерфейс копирования правил Security на нижний уровень



Есть несколько режимов переноса информации. Режим по умолчанию – Add New and Update. В этом режиме Add New означает, что если для дочерних сущностей не существует настроенных прав доступа для данного пользовтеля или группы, то эти правила будут скопированы. Смысл же Update – 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 Security в общем случае. Режимы копирования Add New и Update доступны также по отдельности. Кроме этого существует режим Remove позволяющий удалить права доступа у дочерних сущностей для выбранных пользователей или групп. Следует отдавать предпочтение этому методу по сравнению

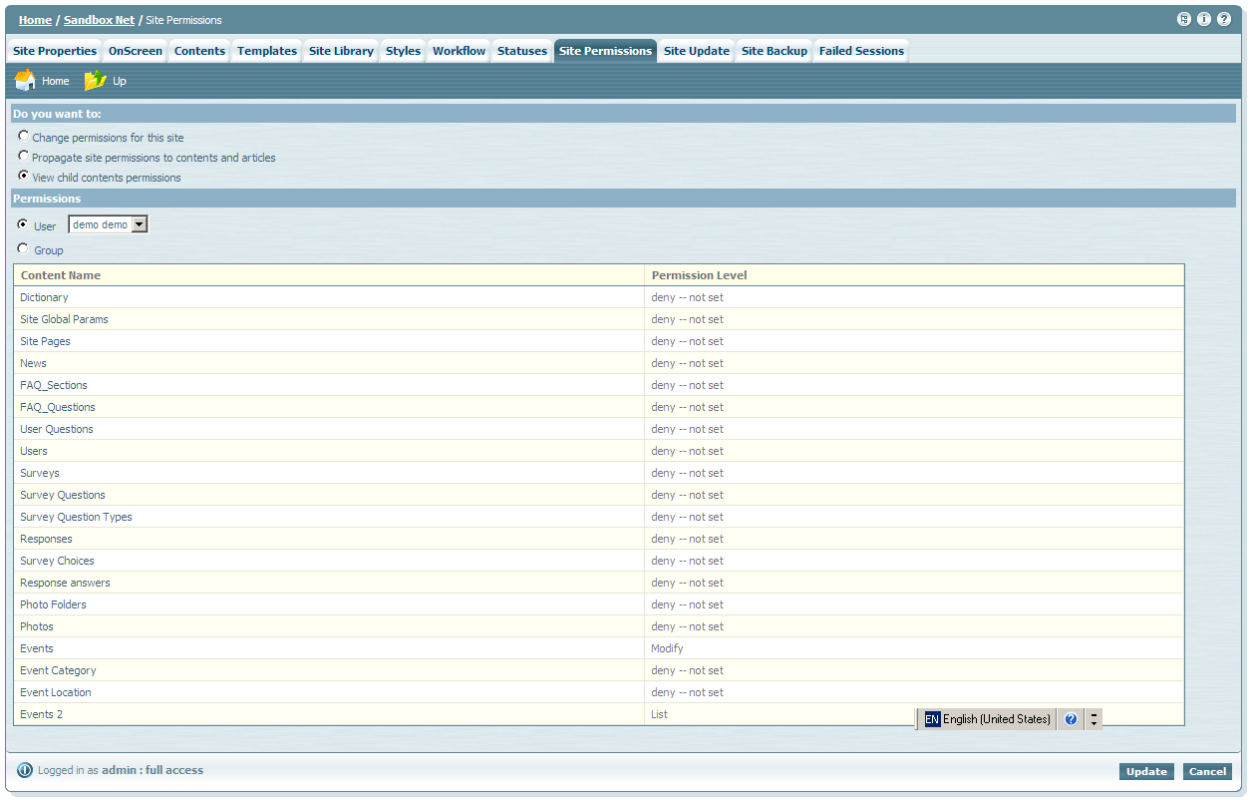
с массовой установкой Deny, так как логика – такая же, а дополнительных записей в базе данных не требуется.

Например, редактору нужно дать право изменять все контенты сайта, при этом свойства сайта модифицировать он не должен. Для этого нужно сначала дать право доступа Modify на сайт, затем выполнить операцию Propagate site permissions to contents (при этом галочку 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 задчачи 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 View child permissions (рис. 3).

Рис. 3. Интерфейс просмотра правил Security нижнего уровня



Алгоритм вычисления эффективных прав доступа на объект

1) Если пользователь – администратор, то результат – Full Access
2) Если ищутся права для статьи, а для контента отключена опция Allow Article Permissions, 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 – 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 в Article Workflow для статей выставлен режим Inherits - наследование от контента. Этот режим используется по умолчанию.
2) Статьи, на которые назначен собственный Workflow

Кроме основных правил Security, общих для всех объектов Backend, 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 удялять 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

1) Настройка прав доступа к страницам
    a. Дать пользователю право List на вкладку Sites
    b. Закрыть пользователю доступ ко всем дочерним вкладкам Sites, кроме Contents
    c. Закрыть пользователю доступ к дочерним вкладкам Contents: Content Info, Fields, Notifications. Решение об остальынх вкладках этого уровнея принимается на основании конкретной логики использования функционала
    d. Закрыть пользователю доступ к дочерним вкладкам Articles: Article Permissions, Article Workflow
2) Настройка прав доступа к сайту и контентам
    a. Настройка контентов, которые пользователь может просматривать (пользователь должен иметь право доступа List на связанные через поля Relation контенты, чтобы он имел право просматривать содержимое полей типа Relation в редактируемых статьях и выбирать нужные значения).
        i. Дать пользователю право доступа Read на сайт
        ii. Выполнить операцию Propagate to selected contents для нужных контентов (или для всех контентов)

    b. Настройка контентов, которые пользователь может редактировать
        i. Дать пользователю временно право доступа Modify (Full Access) на сайт
        ii. Выполнить операцию Propagate to selected contents для нужных контентов
    c. Дать пользователю право доступа List на сайт.
3) Настройка прав доступа к статьям

a. Если для каких-то контентов выставлена опция Use article permissions, то возможно для них потребуется более тонкая настройка прав доступа. Она выполняется аналогично предыдущему пункту, только на уровне контента.