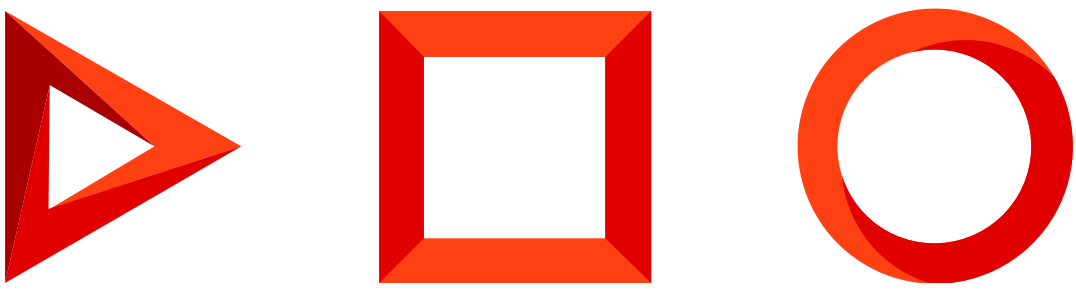
Creatio Academy

Доступ по системным операциям

Настроить права доступа на системные операции

Версия 8.0



Эта документация предоставляется с ограничениями на использование и защищена законами об интеллектуальной собственности. За исключением случаев, прямо разрешенных в вашем лицензионном соглашении или разрешенных законом, вы не можете использовать, копировать, воспроизводить, переводить, транслировать, изменять, лицензировать, передавать, распространять, демонстрировать, выполнять, публиковать или отображать любую часть в любой форме или посредством любые значения. Обратный инжиниринг, дизассемблирование или декомпиляция этой документации, если это не требуется по закону для взаимодействия, запрещены.

Информация, содержащаяся в данном документе, может быть изменена без предварительного уведомления и не может гарантировать отсутствие ошибок. Если вы обнаружите какие-либо ошибки, сообщите нам о них в письменной форме.

Содержание

Настроить права доступа на системные операции 4

Настроить права доступа на системные операции

ПРОДУКТЫ: ВСЕ ПРОДУКТЫ

В этой статье рассмотрена настройка прав **доступа к действиям системы**. Примеры таких действий: импорт и экспорт данных, создание бизнес-процессов, настройка рабочих мест, изменение содержимого справочников, конфигурирование системы и т. д.

Действия системы не относятся к конкретному объекту и права на них не могут настраиваться на уровне операций чтения, редактирования и удаления данных в объекте. Для настройки прав доступа к действиям системы используются **системные операции**. Они имеют два уровня доступа: у пользователя либо роли есть право на выполнение системной операции, или его нет. Например, если вы разрешите роли “Все сотрудники компании” выполнять операцию “Экспорт реестра” (код “Export list records”), то все без исключения пользователи смогут экспортировать данные реестра раздела в Excel.

Управление доступом к системным операциям доступно в дизайнере системы, по ссылке **“Права доступа на операции”**. Работа с группами в реестре системных операций не предусмотрена, но вы можете воспользоваться стандартным или расширенным фильтром.

Доступ к бизнес-данным подразумевает выполнение CRUD-операций с данными (создание, чтение, редактирование и удаление) и выполняется через настройку прав доступа к соответствующим объектам системы. Подробнее читайте в статье Настроить доступ по операциям.

Если вы только начинаете знакомство с Creatio, то рекомендуем ознакомиться с концепцией прав доступа на объекты в Creatio в онлайн-курсе Управление пользователями и ролями. Права доступа.

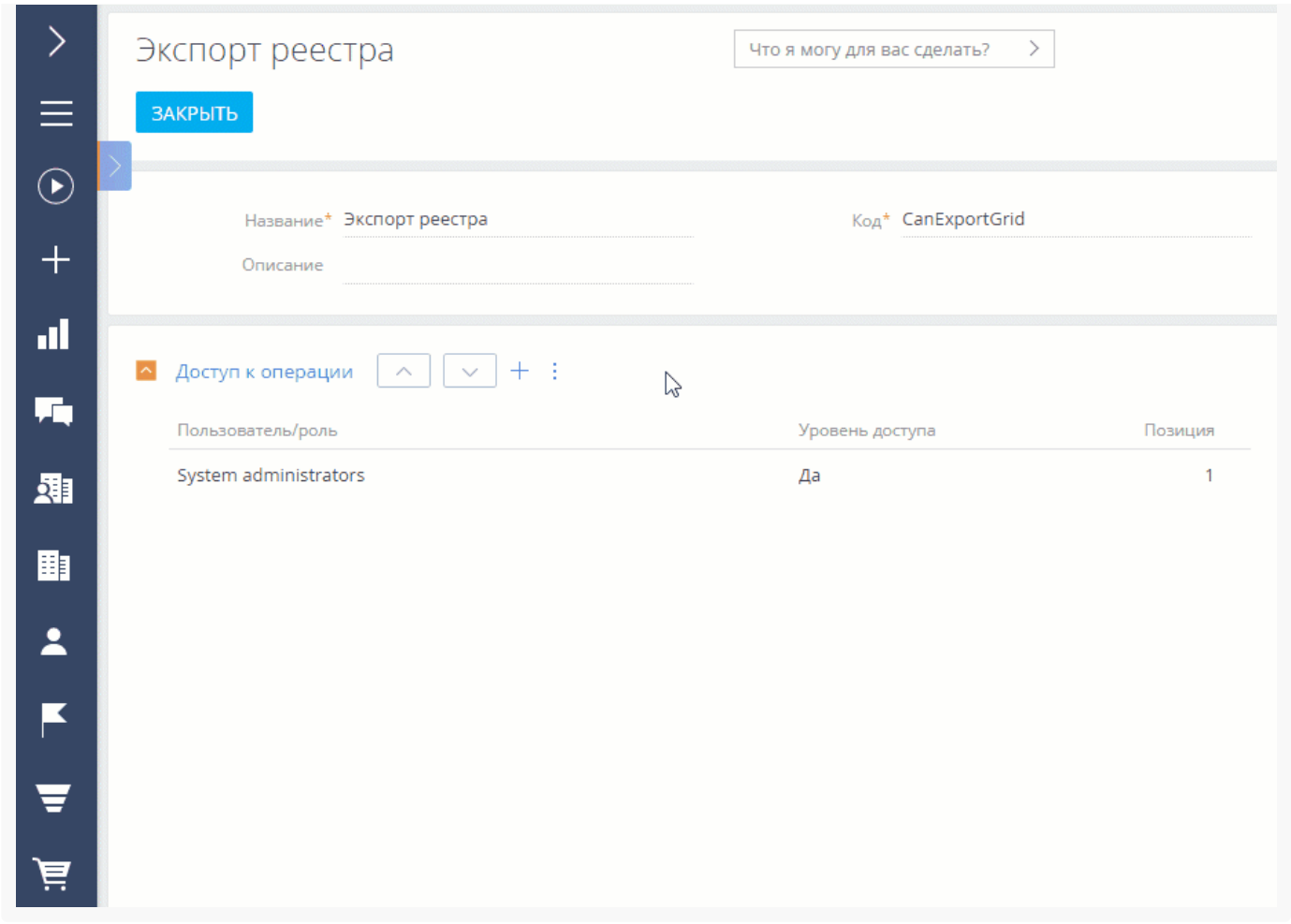
Обратите внимание, что право на выполнение системной операции не отменяет других прав доступа. Например, пользователи смогут экспортировать только те данные, к которым у них есть доступ.

По умолчанию доступ к основным системным операциям есть только у администраторов системы. Вы можете настроить права доступа к системным операциям для определенных пользователей или групп пользователей.

Пример. Дать доступ на экспорт реестра для руководителей менеджеров по продажам.

1. Нажмите ⚙ —> Дизайнер системы —> **“Права доступа на операции”**.
2. Установите фильтр “Название = Экспорт реестра” (или “Код = CanExportGrid”). **Кликните по заголовку** системной операции или выделите ее в реестре и нажмите кнопку [*Открыть*].
3. На детали [*Доступ к операции*] нажмите кнопку + —> **укажите получателя прав**. В нашем примере это роль “Менеджеры по продажам. Группа руководителей”. Запись появится на детали со значением “Да” в колонке “Уровень доступа”. В результате пользователи, входящие в роль “Менеджеры по продажам. Группа руководителей” получат доступ к системной операции [*Экспорт реестра*] (Рис. 1).

Рис. 1 — Добавление прав доступа на системную операцию



На заметку. Чтобы запретить доступ, установите в колонке [*Уровень доступа*] значение “Нет”. Для этого выберите пользователя или роль в списке. Значение в колонке “Уровень доступа” отобразится в виде признака. Снимите признак, чтобы запретить доступ для выбранного пользователя или роли. Сохраните запись.

Когда вы настраиваете ограничения на доступ к системной операции для определенных пользователей или ролей, возможны случаи, что уровни доступа противоречат друг другу, т. к. роли пересекаются. Настройте приоритетность прав доступа на операцию, чтобы для всех ролей они отрабатывали корректно. Для этого воспользуйтесь кнопками и на детали [*Доступ к операции*]. Если пользователь будет входить в несколько ролей, добавленных на деталь, то для него будут применен уровень доступа той роли, которая расположена выше в списке. Например, если вы хотели бы запретить всем пользователям, кроме руководителей менеджеров по продажам, экспорт реестра, расположите роль “Все сотрудники компании” ниже, а роль “Менеджеры по продажам. Группа руководителей” — выше.

На заметку. Пользователи или роли, которые не добавлены на деталь, не получают права доступа к операции. При этом они не участвуют в определении приоритетов прав.