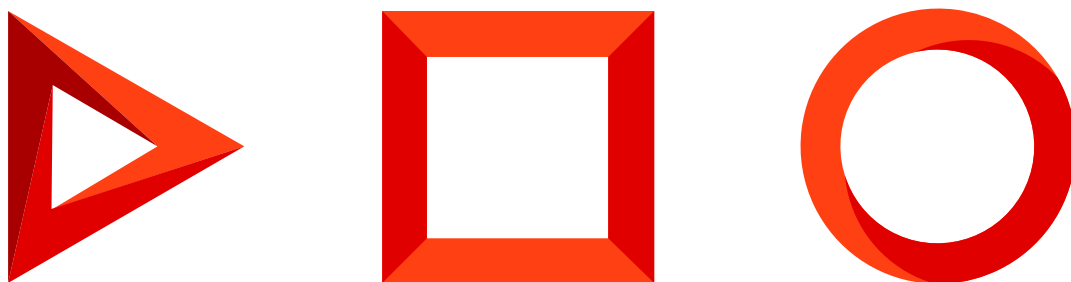


Настройки безопасности

Безопасная загрузка файлов

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

Безопасная загрузка файлов	4
Выбрать режим проверки файлов	4
Настроить список типов файлов	4
Настроить ограничения для неизвестных типов файлов	5
Настроить исключение веб-сервисов из ограничений загрузки файлов	6

Безопасная загрузка файлов

ПРОДУКТЫ: **ВСЕ ПРОДУКТЫ**

Для повышения безопасности работы в Creatio вы можете настроить ограничения форматов загружаемых в приложение сторонних файлов. Ограничения на загрузку файлов действуют как для пользователей, так и для интеграций, например, внешних веб-сервисов.


При настроенных ограничениях Creatio проверяет формат файлов, которые загружаются на деталь [*Файлы и ссылки*]. В случае соответствия настройкам файл будет успешно загружен. В другом случае файл загружен не будет, а пользователь получит уведомление, что загрузка данного файла запрещена настройками безопасности. Для файлов, загруженных в систему до включения ограничений, настройки не применяются.

Ограничения действуют только на загрузку файлов в Creatio, скачивать файлы могут все пользователи, имеющие к ним доступ.

В системе предусмотрены следующие способы ограничения загрузки файлов:

- Ограничения для файлов **определенных типов** — вы можете настроить список **разрешенных расширений** или список **запрещенных расширений** файлов. В этом случае можно установить разрешение или запрет на загрузку в приложение файлов определенных типов.
- Ограничения для файлов **неизвестных типов**. В этом случае можно установить разрешение или запрет на загрузку в приложение файлов, у которых не указано расширение и невозможно определить тип по содержимому.

Выбрать режим проверки файлов

1. Перейдите в **дизайнер системы** по кнопке .
2. Перейдите в раздел [**Системные настройки**].
3. Откройте системную настройку **“Режим проверки файлов”** (код “FileSecurityMode”).
4. В поле [**Значение по умолчанию**] выберите необходимый тип ограничения:
 - **“Проверка файлов отключена”** — чтобы отменить все ограничения на загрузку файлов в приложение.
 - **“Список запрещенных расширений”** — чтобы запретить загрузку в приложение файлов определенных типов.
 - **“Список разрешенных расширений”** — чтобы разрешить загрузку в приложение только файлов определенных типов.
5. **Сохраните** изменения.

Настроить список типов файлов


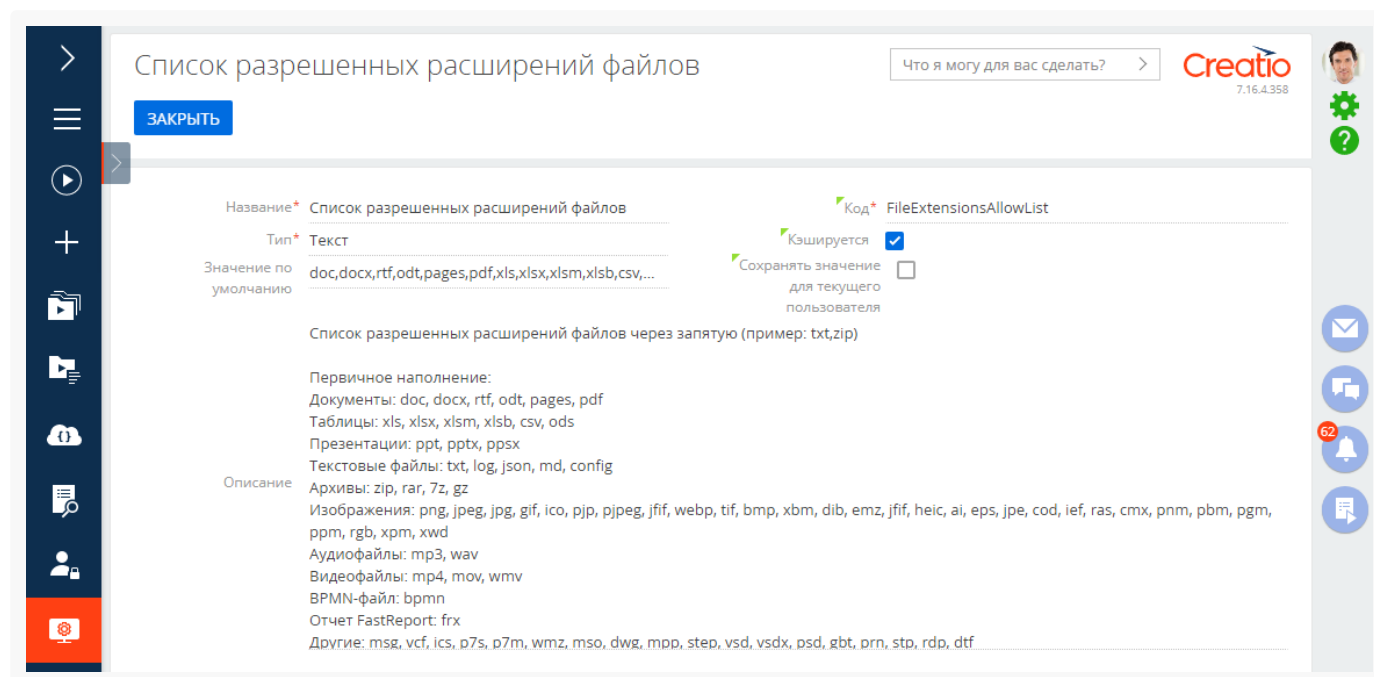
1. Перейдите в **дизайнер системы** по кнопке .
2. Перейдите в раздел [**Системные настройки**].
3. Откройте системную настройку
 - **“Список разрешенных расширений файлов”** (код “FileExtensionsAllowList”), чтобы настроить список разрешенных к загрузке типов файлов. По умолчанию в настройке приведены наиболее часто используемые типы файлов.
 - **“Список запрещенных расширений файлов”** (код “FileExtensionsDenyList”), чтобы настроить список запрещенных к загрузке типов файлов. По умолчанию в настройке приведены типы файлов, которые могут являться вредоносными.
4. В поле [**Значение по умолчанию**] через запятую без пробела укажите **расширения файлов** ([Рис. 1](#)) и проверьте корректность ввода.

Рис. 1 — Пример заполнения системной настройки “Список разрешенных расширений файлов”



5. **Сохраните** изменения.

Настроить ограничения для неизвестных типов файлов

Creatio определяет типы загружаемых файлов по их расширению. В случае если расширение не указано, система определяет тип файла на основании его содержимого. По умолчанию в систему разрешено загружать файлы неизвестных типов. Запрет загрузки таких файлов повысит безопасность работы в приложении, но в этом случае обязательно потребуется настроить список разрешенных или запрещенных расширений.


Чтобы **запретить загрузку** в Creatio файлов неизвестных типов:

1. Перейдите в **дизайнер системы** по кнопке .

2. Перейдите в раздел [**Системные настройки**].
3. Откройте системную настройку “**Разрешить работу с неизвестными типами файлов**” (код “AllowFilesWithUnknownType”).
4. Снимите признак [**Значение по умолчанию**].
5. **Сохраните** изменения.

Настроить исключение веб-сервисов из ограничений загрузки файлов

Ограничение загрузки файлов применяется для всех используемых в системе веб-сервисов, включая те, которые были добавлены в процессе кастомизации системы, в проектных решениях и приложениях Marketplace. Чтобы веб-сервисы могли добавлять в Creatio файлы тех типов, которые не разрешены пользователям, их необходимо **добавить в список исключений**. Для этого:

1. Перейдите в **дизайнер системы** по кнопке .
2. Перейдите в раздел [**Справочники**].
3. Откройте справочник [**Список исключений из проверки безопасности файлов**].
4. Нажмите [**Добавить**].
5. В поле [**Название**] укажите **URI** веб-сервиса, который необходимо добавить в исключения. Запись сохраняется автоматически.
 - Пример для приложений на **.NET Framework**: /0/rest/[*Название пользовательского сервиса*]/[*Конечная точка пользовательского сервиса*], без указания [*Адреса приложения*].
 - Пример для приложений на **.NET CORE**: /rest/[*Название пользовательского сервиса*]/[*Конечная точка пользовательского сервиса*], без указания [*Адреса приложения*].
6. **Повторите** для всех веб-сервисов, которым необходимо разрешить загрузку файлов в приложение.