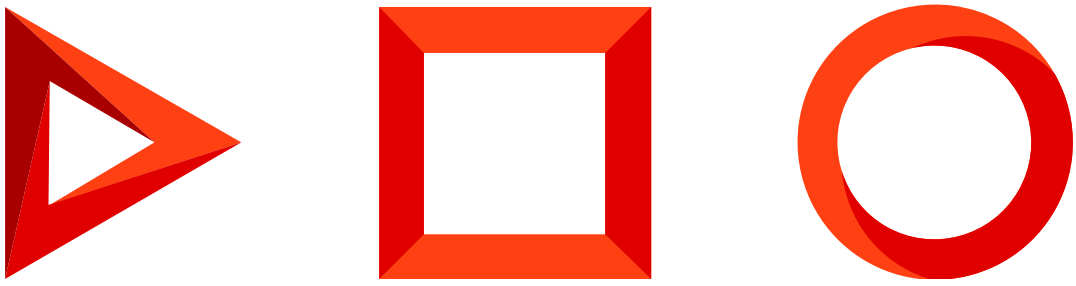
Creatio Academy

Информационная безопасность

Рекомендуемые настройки информационной безопасности

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.

© 2022 Terrasoft. Все права защищены.

Содержание

© 2022 Terrasoft. Все права защищены.

Рекомендуемые настройки информационной безопасности

ПРОДУКТЫ: ВСЕ ПРОДУКТЫ

Статья содержит лучшие практики настроек информационной безопасности Creatio.

Внедрить политику паролей организации

Убедитесь в том, что настройки логина и пароля соответствуют политике безопасности компании. Вы можете использовать рекомендованные значения, если не определены точные требования.

Длина пароля. Рекомендуем использовать пароли, состоящие из 8 и более символов. Установить сложность пароля вы можете в следующих системных настройках:

- “Сложность пароля: Минимальная длина” (код “MinPasswordLength”);
- “Сложность пароля: Минимальное количество символов нижнего регистра” (код “MinPasswordLowercaseCharCount”);
- “Сложность пароля Минимальное количество символов верхнего регистра” (код “MinPasswordUppercaseCharCount”);
- “Сложность пароля Минимальное количество цифр” (код “MinPasswordNumericCharCount”);
- “Сложность пароля Минимальное количество специальных символов” (код “MinPasswordSpecialCharCount”).

История паролей. Creatio сравнивает предыдущий пароль пользователя с новым, чтобы убедиться, что они не совпадают. Количество предыдущих паролей, которые необходимо сравнить с новым, вы можете указать в системной настройке “Количество анализируемых паролей” (код “PasswordHistoryRecordCount”).

Количество **попыток входа до предупреждающего сообщения** и **время блокировки пользователя**. Рекомендуем установить 5 попыток входа до предупреждающего сообщения и 15 минут в качестве времени блокировки пользователя. Вы можете отрегулировать поведение блокировки в следующих системных настройках:

- “Количество попыток входа“ (код “LoginAttemptCount”) — допустимое количество неудачных попыток ввода логина или пароля.
- “Количество попыток входа до предупреждающего сообщения“ (код “LoginAttemptCount”) — порядковый номер неудачной попытки ввода логина или пароля, после которого отобразится сообщение о возможности дальнейшей блокировки учетной записи пользователя.
- “Время блокировки пользователя“ (код “UserLockoutDuration”) — время блокировки (в минутах) учетной записи пользователя после указанного количества неудачных попыток ввода логина или пароля.

Подробнее: Разблокировать учетную запись пользователя.

Сообщения о неверном пароле и **блокировке** при попытке входа. Рекомендуем отображать

© 2022 Terrasoft. Все права защищены.

сообщение с общей информацией без уточнения конкретной проблемы. Для этого убедитесь, что у следующих системных настроек снят признак в значениях по умолчанию:

- “Отображать информацию о блокировке учетной записи при входе” (код “DisplayAccountLockoutMessageAtLogin”);
- “Отображать информацию о неверном пароле при входе” (код “DisplayIncorrectPasswordMessageAtLogin”).

Время завершения сессии

Задайте интервал в минутах, по истечении которого сессия будет закрыта, в системной настройке “Таймаут сеанса пользователя” (код “UserSessionTimeout”). Значение по умолчанию: “60”.

Протокол TLS для Creatio on-site

В Creatio реализована поддержка протокола TLS 1.2. Устаревшие версии протокола TLS 1.0 и 1.1 делают систему безопасности уязвимой.

Безопасные конфигурации заголовков для Creatio on-site

Примите необходимые меры для того, чтобы браузеры не поддавались уязвимостям, которые можно предотвратить. Для этого включите следующие заголовки, которые соответствуют OWASP Secure Headers Project (открытый проект обеспечения безопасности веб-приложений):

HTTP Strict Transport Security (HSTS). Включите заголовок `Strict-Transport-Security` и установите значение хранения параметра в памяти браузера, соответствующее одному году:

```
Strict-Transport-Security: max-age=3153600
```

Защита от кликджекинга (clickjacking). Включите заголовок `X-Frame-Options` и разрешите встраивание веб-страниц только на тех же адресах, что и у вашего приложения Creatio:

```
X-Frame-Options: sameorigin
```

Защита от атак межсайтового скриптинга (XSS). Включите заголовок `X-Frame-Options` и установите блокировку попыток XSS-атак:

```
X-XSS-Protection: 1; mode=block
```

Защита от MIME-сниффинга. Включите заголовок `X-Content-Type-Options` и установите режим “nosniff”. Этот режим предотвращает попытку браузера переопределить тип контента ресурса, если он отличается от объявленного типа контента:

© 2022 Terrasoft. Все права защищены.

```
X-Content-Type-Options: nosniff
```

Политика референта (referrer policy). Включите заголовок `Referrer-Policy` и установите значение “origin-when-cross-origin”. Заголовок определяет, какой объем информации о референте (отправленной с заголовком “Referer”) будет включен в запросы:

```
Referrer-Policy: origin-when-cross-origin
```

Безопасность контента. Включите заголовок `Content Security Policy` и настройте его следующим образом:

```
Content-Security-Policy: default-src 'self'; script-src 'unsafe-inline' 'unsafe-eval'; script-sr
```

Ответы на запросы для Creatio on-site

Ограничьте количество и тип информации, доступной в ответах на запросы. Для этого измените файл Web.config в корневом каталоге Creatio следующим образом:

Отключите `X-Powered-By`.

```
<system.webServer> <httpProtocol> <customHeaders> <remove name="X-Powered-By" /> </customHeaders
```

Отключите `X-AspNet-Version`.

```
<httpRuntime enableVersionHeader="false" />
```

Отключите `Server Header` (доступно для IIS версии 10 и выше).

```
<system.webServer> <security> <requestFiltering removeServerHeader ="true" /> </security> </syst
```

Запрет одновременных сеансов для Creatio on-site

Начиная с версии Creatio 7.13.3, вы можете запретить несколько одновременных входов в систему под одним пользователем. Creatio автоматически закроет старую сессию на другом устройстве, если пользователь откроет новую. Чтобы включить ограничение сессии, установите для параметра web.config **Feature-AllowOnlyOneSessionPerUser** значение "true":

© 2022 Terrasoft. Все права защищены.

```
<add key=""Feature-AllowOnlyOneSessionPerUser"" value=""true"" />
```

Функциональность доступна в режиме бета-тестирования. Не поддерживаются следующие функции:

- мобильное приложение;
- сквозная аутентификация Windows (UsePathThroughAuthentication);
- SSO (SAML).

Кроме того, для каждой интеграции необходима отдельная учетная запись Creatio, которая не используется пользователями.

© 2022 Terrasoft. Все права защищены.