Creatio Academy

Information security settings

Recommended information security settings

Version 7.18

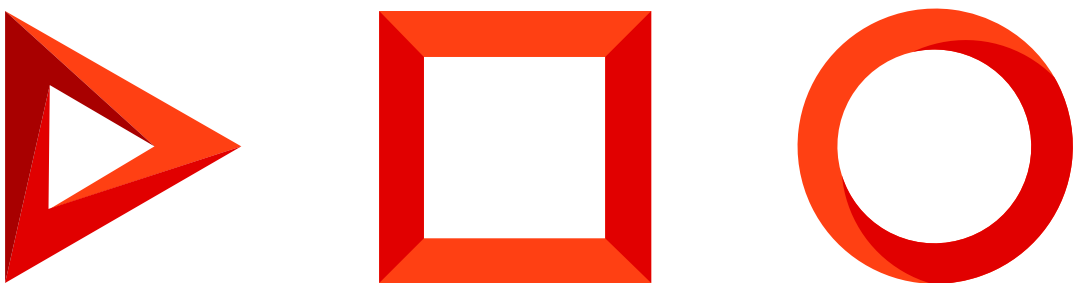

Table of Contents

Recommended information security settings

PRODUCTS: ALL CREATIO PRODUCTS

This article covers best practices for Creatio settings related to information security.

Implement the password policy of your organization

Make sure the password and login settings comply with your company's security policy. You can use the recommended values if the policy does not specify the exact requirements.

Password strength. We recommend using passwords that are at least 8 characters long. Set up the desired password complexity in the following system settings:

- “Password complexity: Minimum length” (the “MinPasswordLength” code)
- “Password complexity: Minimum quantity of lower case characters” (the “MinPasswordLowercaseCharCount” code)
- “Password complexity: Minimum quantity of upper case characters” (the “MinPasswordUppercaseCharCount” code)
- “Password complexity: Minimum quantity of digits” (the “MinPasswordNumericCharCount” code)
- “Password complexity: Minimum quantity of special characters” (the “MinPasswordSpecialCharCount” code)

Password history. Creatio compares previous user passwords to the new password to ensure they do not match. Specify how many previous passwords to compare in the “Quantity of analyzed passwords” (the “PasswordHistoryRecordCount” code) system setting.

The number of **permitted login attempts** and **user lockout time**. We recommend permitting 5 login attempts and setting the lockout time to 15 minutes. Configure the lockout behavior in the following system settings:

- “Number of logon attempts” (the “LoginAttemptCount” code). Sets the number of permitted login attempts.
- “Quantity of login attempts for warning message” (the “LoginAttemptBeforeWarningCount” code). Sets the number of failed login attempts after which the lockout warning message is displayed.
- “User locking time” (the “UserLockoutDuration” code). Sets the period in minutes during which the user cannot log in to Creatio if they run out of login attempts.

Learn more in a separate article: Unblock a user.

Incorrect password and **user lockout messages** on login attempts. We recommend displaying a unified message that does not specify the exact issue. To do this, make sure the values of the following system settings are “false:”

- “Show message about locking account during logging in” (the “DisplayAccountLockoutMessageAtLogin” code)
- “Show message about incorrect password during logging in” (the “DisplayIncorrectPasswordMessageAtLogin” code)

Configure the session expiration time

Set up the period in minutes after which to close the session in the “User session timeout” (the “UserSessionTimeout” code) system setting. The default value is “60.”

TLS protocol (Creatio on-site)

Creatio supports TLS 1.2 protocol out-of-the-box. Deprecated TLS 1.0 and 1.1 protocols are a security vulnerability.

Secure header configurations (Creatio on-site)

Ensure browsers are not susceptible to preventable vulnerabilities. To do this, enable the following headers that comply with OWASP Secure Headers Project:

HTTP Strict Transport Security (HSTS). Enable the `Strict-Transport-Security` header and set the time to store the parameter in browser memory to 1 year:

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

Clickjacking protection. Enable the `X-Frame-Options` header and set it to allow pages to be embedded only on addresses that have the same location as your Creatio application:

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

Cross-site-scripting attack (XSS) protection. Enable the `X-XSS-Protection` header and set it to block the XSS attack attempts:

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

MIME-sniffing protection. Enable the `X-Content-Type-Options` header and set it to nosniff mode. The mode prevents the browser from trying to determine the content type of a resource different from the declared content type:

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

Referrer Policy. Enable the `Referrer-Policy` header and set it to origin-when-cross-origin. The header specifies how much referrer information (sent with the Referrer header) to include in requests:

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

Attention. Before you implement the **Content Security Policy** settings, review the existing and planned browser-level integrations, such as CTI connectors. Include the corresponding domains in the Content Security Policy list. Otherwise, the browser-level integrations will stop working.

Content Security Policy. Enable the `Content Security Policy` header and configure it as follows:

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

Limit the information shared in responses (Creatio on-site)

Limit the amount and type of information available in responses. To do this, modify the Web.config file in Creatio root directory as follows:

Disable `X-Powered-By`.

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

Disable `X-AspNet-Version`.

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

Disable `Server Header` (available for IIS version 10 and later).

```
<system.webServer>
<security>
```

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

Set up Redis (Creatio on-site)

We recommend using a combination of stable Debian and up-to-date Redis versions.

Password protect access to Redis as well. To do this, modify configuration files in Redis and Creatio.

For **simple Redis configuration**:

1. Add the following string to the redis.conf file in Redis config:

```
requirepass ${redis_password}
```

2. Add the following string to the ConnectionStrings.config file in Creatio:

```
${redis_password} host=${master_ip};port=${master_port};db=;password=${redis_password}
```

For **Redis Cluster configuration**:

1. Add the following strings to the redis.conf file in each node:

```
requirepass ${redis_password}
masterauth ${redis_password}
```

2. Add the following string to the ConnectionStrings.config file in Creatio:

```
clusterHosts={node1_ip}:{node1_port},{node2_ip}:{node2_port},{node3_ip}:{node3_port},{node4_i
```