Creatio Academy

Security settings

Version 7.17

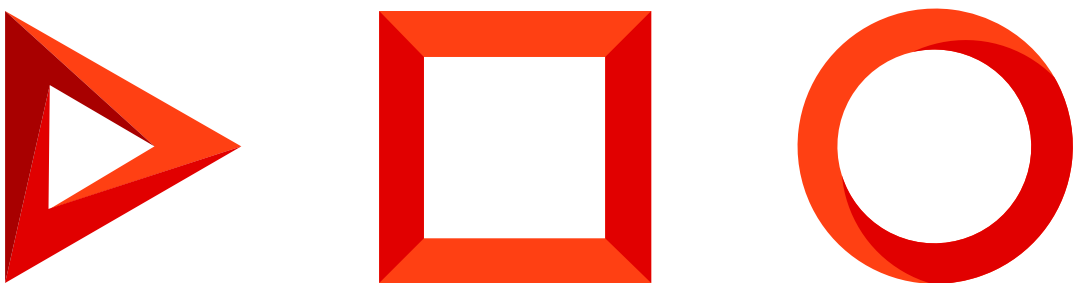


Table of Contents

Secure file upload

PRODUCTS: ALL CREATIO PRODUCTS

Restrict the types of files uploaded to Creatio to improve application security. The security restrictions apply to both users and integrations such as third-party web services.

With the secure file upload enabled, Creatio checks the type of the files uploaded via the [*Attachments and notes*] detail. If the file type is not restricted, the file will be uploaded successfully. Otherwise, the file will not be uploaded, and the user will receive a notification that uploading the file is not allowed for security reasons. The security restrictions do not apply to files that have been added to Creatio earlier.

The restrictions only apply to the upload of new files to Creatio. Any users can download a file of a restricted type if they have sufficient permissions to access the file.

Creatio supports the following file security modes:

- File extensions **AllowList**. Only files with explicitly specified extensions are allowed for upload.
- File extensions **DenyList**. Files with any extensions not explicitly restricted are allowed for upload.
- **Unknown file types** are restricted. Allow or disallow uploading files without an extension when the type of the file cannot be determined by its content.

Secure file upload is managed by system administrators. The general procedure for **secure file upload** is as follows:

1. Select the preferable file security mode for uploading files.
2. Set up the file extensions allow list or deny list.
3. Define Creatio behavior upon uploading a file of an unknown type.
4. Set up security exceptions for web services if required.

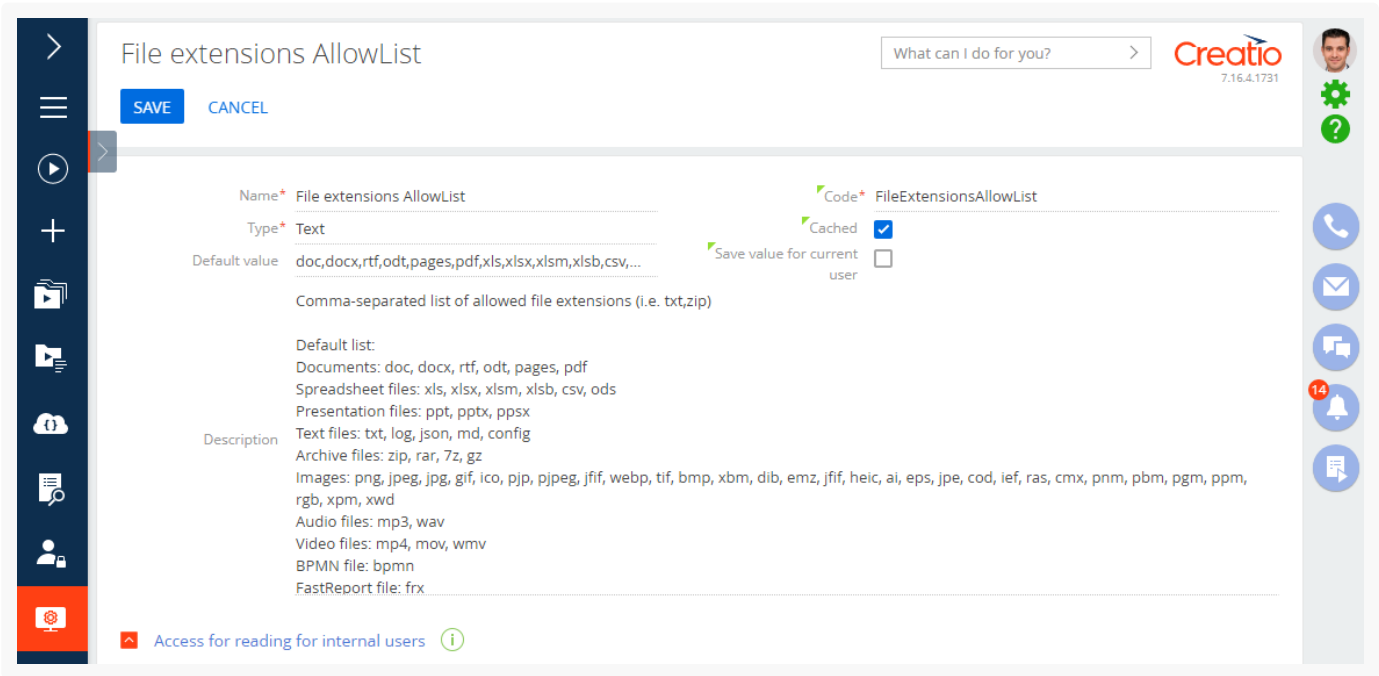
Select file security mode

1. Click to open the **System Designer**.
2. Open the **System settings** section.
3. Open the **File Security Mode** (FileSecurityMode) system setting.
4. Select the required restriction type in the **Default value** field:
   a. “**Disable file security**” – disable all restrictions on file upload.
   b. “**File extensions DenyList**” – disallow uploading files with specific file types.
   c. “**File extensions AllowList**” – only allow uploading files with specific file types.
5. Click **Save**.

Set up the file type list

1. Click to open the **System Designer**.
2. Open the **System settings** section.
3. Open one of the following system settings:
   a. **File extensions AllowList** (FileExtensionsAllowList) – to set up a list of allowed file extensions. By default, this setting contains the most frequently used file extensions.
   b. **File extensions DenyList** (FileExtensionsDenyList) – to set up a list of restricted file extensions. By default, this setting contains extensions associated with potentially malicious file types.
4. Enter **file extensions** as a comma-separated list without whitespace characters in the **Default value** field (Fig. 1) and verify the entered data.

Fig. 1 Setting up the [*File extensions AllowList*]



5. Click **Save**.

Set up restrictions for files of unknown types

Creatio determines the type of a file type by its extension. If the file extension is not available, Creatio uses the content of the file to determine the file type. By default, uploading files of unknown types is allowed. Denying such files from uploading will make working with Creatio more secure. However, this mode requires setting up a file extension allow list or deny list.

To **deny uploading** files of unknown types to Creatio:

1. Click to open the **System Designer**.
2. Open the **System settings** section.
3. Open the **Allow processing files of unknown type** (AllowFilesWithUnknownType) system setting.
4. Clear the **Default value** checkbox.
5. Click **Save**.

Set up web services excluded from file security

File security restrictions apply to all Creatio web services, including services added during customization, in project solutions, and Marketplace applications. **Add web services to the list of file security exclusions** to allow them to upload files of the restricted file types. To do this:

1. Click to open the **System Designer**.
2. Open the **Lookups** section.
3. Open the **List of file security excluded Uris** lookup.
4. Click **New**.
5. In the **Name** field, specify the **URI** of the web service to exclude from restrictions. The record will be saved automatically.
   a. A **.NET Framework** example: /0/rest/[*Custom service name*]/[*Custom service endpoint*], without specifying the application domain.
   b. A **.NET CORE** example: /rest/[*Custom service name*]/[*Custom service endpoint*], without specifying the application domain.
6. **Repeat** for other web services to enable them to upload files to the application without restrictions.

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
```

Remote access for Creatio support

PRODUCTS: ALL CREATIO PRODUCTS

Creatio cloud users can set up secure remote access for Creatio technical support specialists to troubleshoot and resolve cases faster. Remote access sessions will not compromise your personal and commercial data security since you do not have to share your login credentials with support.

> **Note.** Remote support sessions use the following system settings: “Default external access client id” (DefaultExternalAccessClientId), “Identity server client secret” (IdentityServerClientSecret), Identity server Url (IdentityServerUrl), “Identity server client id” (IdentityServerClientId). The values in these system settings are populated automatically.

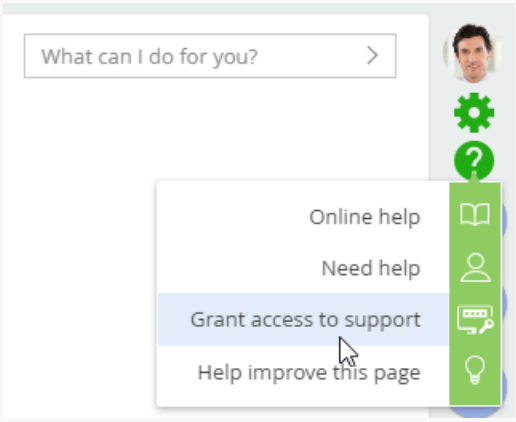
- To hide section record data from the technical support specialists, use the **data isolation mode**.
- To restrict technical support specialists from modifying configuration settings, use the **configuration restriction mode**. The support specialists will still have permission to read configuration settings needed to resolve the customer’s case.

To enable remote support access, a user must have system administrator privileges (have the “System administrators” role). Technical support specialists can connect remotely under the administrator account or the account of any other application user. All remote support session data are logged and can be retrieved later. Logged connection data include the time of the connection and information on which data were modified during the session.

Set up remote sessions

1. Click → “Grant access to support” in the upper right corner of the application window. (Fig. 1)

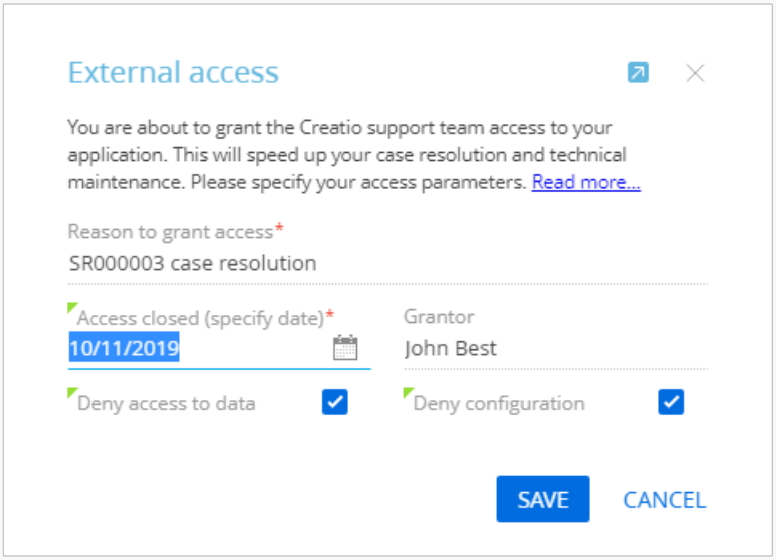
Fig. 1 Locating remote sessions set up in the help menu



Note. To grant access to support, you need permissions to read and add records in the “External access” object. Users with the “System administrators” role have these permissions by default. Learn more about object operation permissions in the “Managing object operation permissions” article.

2. Fill out the displayed mini page (Fig. 2):

Fig. 2 Remote session parameters



1. In the [***Reason to grant access***] field, specify what problem requires granting access to support, the request number, or the list of services a technical support specialist has to provide.
2. In the [***Access close date***] field, specify the date when the granted access expires. Granted access will expire at 11:59 PM on the specified date.
3. In the [***Grantor***] field, the user who is granting access is specified by default. You can specify a different user account to use by technical support specialists for accessing your application.
4. Select or clear the [***Deny access to data***] and [***Deny configuration***] checkboxes to enable or disable the data isolation mode and configuration restriction mode respectively. By default, both checkboxes are selected. This means that a technical support specialist will not be able to see your section record data or configure the system.

- If you need the technical support specialist to have the same permissions as the user under whose account remote access is granted, clear both of the checkboxes.
- If you need the technical support specialist to modify the current configuration without being able to see your records, only clear the [*Deny configuration*] checkbox. The technical support specialist will also be able to access the System designer functions required for updating configuration (for instance, the [*Lookups*], [*Advanced settings*], [*Process library*] sections and more). The record data in the main sections will remain unavailable to the Creatio support.
- If you need the technical support specialist to be able to access your records without being able to modify the configuration of the system, you should only clear the [*Deny access to data*] checkbox. In this case, Creatio support will be able to access the system configuration in the read-only mode.

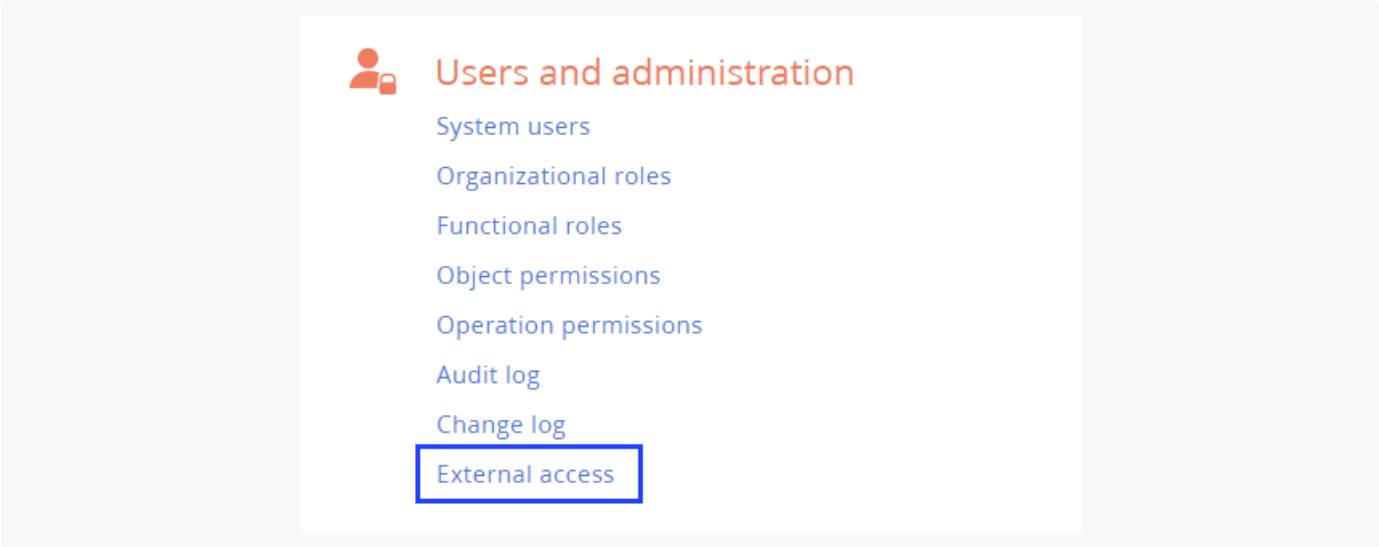
5. Save the record.

   As a result, a new record will be added in the [*External access*] section. Technical support specialists will be able to log in under the user account specified as the [*Grantor*]. Support specialists will not need login credentials. The specialists will have access to the corresponding permissions not otherwise restricted in the sessions settings. The remote access session will expire on the specified date at 11:59 PM.

View remote access logs

1. Open the System designer and click [*External access*] (Fig. 1).

Fig. 1 The [*External access*] section



2. Open the required record in the section list. On the record page, you can view all access parameters (Fig. 2). After the support session is over, the [*Sessions*] tab will display the session data.

Fig. 2 An example record with remote access parameters in the [*External access*] section