Drupal 8 Module for CopySafe Web

About this Module and CopySafe Web

This Drupal module enables websites using Drupal CMS to upload, display and manage pages and posts that show encrypted images created by the CopySafe Web software.

When CopySafe Web encrypted images load, they activate the CopySafe Web browser plugin to prevent Print Screen and screen capture. Thus, the addition of even a small encrypted image can be used to add copy-protection to your Drupal pages and protect any media displayed on that page, including Flash and video. CopySafe Web software is a separate application to this Drupal module and a license is required to use it per website. Otherwise, this Drupal module is provided as a free add-on.

Domain Lock

CopySafe Web software encrypts images and embeds Domain Lock inside the image, so that they can only be displayed from your website. The images are useless to anyone saving a copy of the file itself. CopySafe Web encrypted images stored on a web server are even safe from your web master.

Using CopySafe Web in Drupal Web Pages

CMS solutions like Drupal, WordPress and others make it easy for non-technical people to create and manage sophisticated websites. But adding new functions requires complex programming that can be beyond most web designers. For this reason, a module like this one is provided as an add-on, so that new functions like the display of CopySafe Web encrypted images and the invoking of copy protection is made as easy as point-and-click with a mouse.

Drupal 8 Changes

Note that use of this module has changed between Drupal version 7 and 8. Whereas media could be uploaded and added from the editor in Drupal 7, in Drupal 8 that has changed. Now you are required to upload all media from the module's setting's page, from where you can generate the shortcode to use on your pages, by simply copy-n-paste.

Installation

1. Download drupal_copysafe_web_8.zip to your local machine as a zip file package.
2. Unzip the drupal_copysafe_web_8.zip to extract:
   - the **drupal_copysafe_web** folder
   - Readme in text and PDF
   - a sample encrypted image (.class) that can be uploded and viewed from http://localhost
3. Upload the **drupal_copysafe_web** folder to the /modules/contrib/ folder.
4. Go to Administration » Modules, then enable CopySafe Web module.
5. Go to Configuration page. Under "CONTENT AUTHORING" section click "Text Formats". Click "configure" button against Full HTML (important) under "Operations" column
6. Enable "Enable CopySafeWeb tag replacement" filter and Drag it to first in the processing order.

Using the CopySafe Web Drupal Module

1. Go to Configuration » CopySafe Web screen.
2. Here, you can upload and embed a CopySafe Web protected image. After uploading you can the select the "Embed Options" which will create the shortcode to add to your page. Copy that shortcode to the clipboard.
3. To add the protected image to a web page, edit/create a page and paste the shortcode in teh text area where you want it to be displayed. make sure that you select the "Full HTML" option at the bottom of the editor window.
4. You can upload new image class files or select from a list of already uploaded class files.
5. The protection settings (which will apply to all pages) can be edited at Configuration » CopySafe Web Settings page for such things as:
   - Enable or disable protection from PrintScreen and screen capture.
   - Enable or disable the viewing by computers using remote or virtual connections.
   - Enable or disable use of browser menus.
   - Enable or disable use of the keyboard.

*Note: that you can only upload protected image that have a [.class] file extension.

Until you have a CopySafe Web software license and real encrypted images, or if you just want to use this module in demo mode to add protection from right-mouse click and drag-and-drop, you can use the encrypted image included with the download or this one. While this 20 x 20 pixel image may not be registered for your website on the Internet, it will function on any test server running at localhost. When prompted to upload or select your first image, you use this one to get started.

CopySafe Web encrypted images can be displayed at their original size (calculated from the file name) or they can be rescaled by setting width and height in the shortcode.
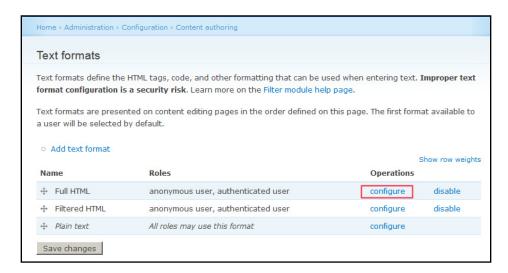
Testing at localhost

Included in your module's zip fie is an encrypted image (icon_0020_0020_C.class) that can be uploaded and viewed on sites running at http://localhost (your local test server). The image represents a 20 x 20 pixel image of a padlock.
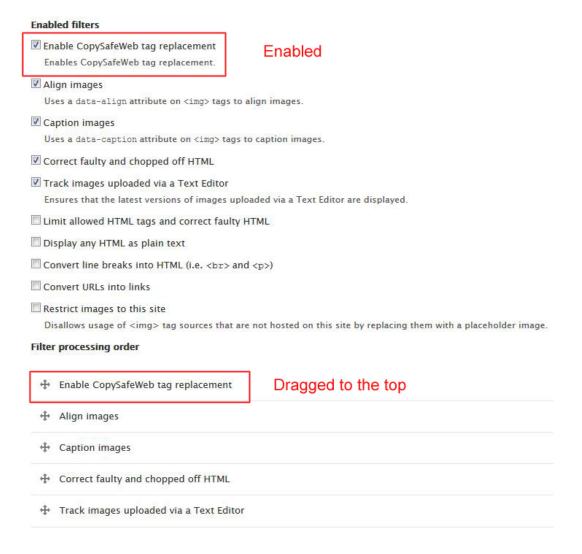
Configuration

Enable CopySafe Web in Configuration » Content Authoring » Text Formats » Full HTML.
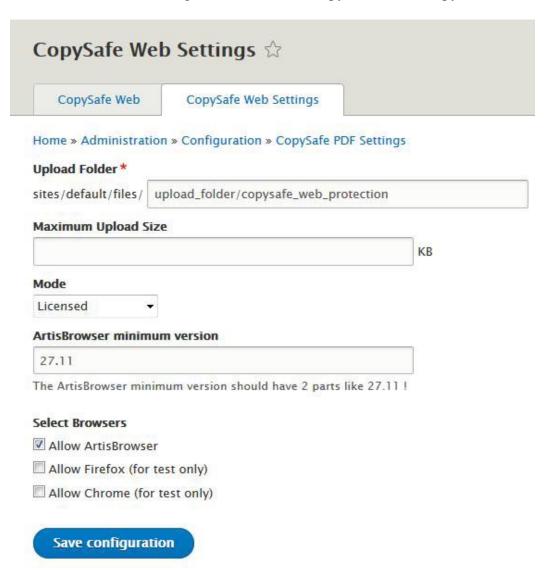

Enable "Enable CopySafeWeb tag replacement" filter and Drag it to first in the processing order.

Settings

See Administration » Configuration » Media » CopySafe Web » CopySafe Web Settings:

These settings are applied to all CopySafe Web pages.

Upload folder

Leave the upload folder as is, as the default is set to be included in the normal Drupal upload folder and it will be created automatically with the correct permissions. If you are having problems with uploading, you may want to check that folder to ensure that everyone has write permissions.

Mode

You can set the Mode and change it at any time for debugging purposes:

1. Demo Mode - displays a placeholder image.
2. Licensed Mode - displays encrypted images and activates the CopySafe Web browser plugin.
3. Debugging Mode - displays the html used in the object tag in a text area form object.

Select Browsers

ArtisBrowser is the only web browser that can display these encrypted files and the only web browser suitable for copy protection. However Firefox and Chrome may be used by admin for checking the shortcode and redirection for downloads, etc. But only for testing as only ArtisBrowser can display the protected content.

ArtisBrowser Minimum Version

ArtisBrowser is updated regularly to improve security and sometimes CopySafe plugins can be updated which may not be compatible with earlier versions. So to ensure that your users have the latest version or the version that supports your CopySafe files, you can set the minimum version of ArtisBrowser that will be allowed. An earlier versions than what you nominate will be redirected to download the latest version of ArtisBrowser.

CopySafe Web Plugin Installation

Viewing protected images displayed on a web page using a web browser requires a browser plugin. By installing the ArtisBrowser the CopySafe Web browser plugin will be included. In fact, the ArtisBrowser includes support for all CopySafe solutions.
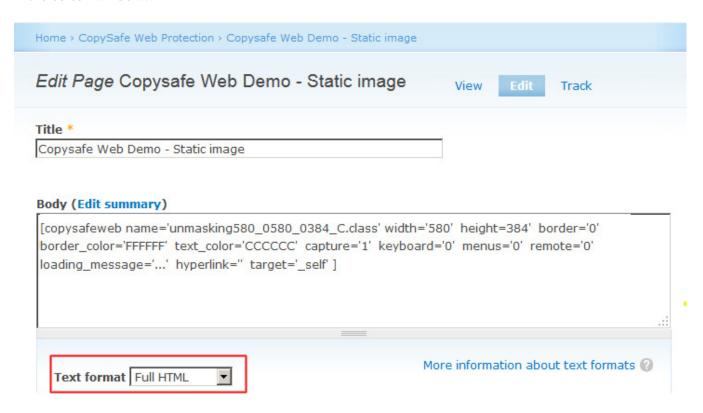
Customizing the Download Pages

Any files found in the CopySafe Web folder pertaining to "download" can be safely edited without affecting this module's functions.

Licensing

This Drupal module is free. However, you will need a license to use the CopySafe Web image encryption software. See – https://www.artistscope.net/ssl/order/order_web.asp

Using the Drupal Module for CopySafe Web

After copying the shortcode that you created using the Embed option, paste to where you want it placed in the editor window.

Note that you must be using "Full HTML" as seen above. The code that you see in the text area is what we call "shortcode" and it is used to store the settings that you nominate for this image display. When embedding encrypted images you select these options from a web form. But you can edit this shortcode at any time.

width is the width of the image in pixels and **height** is the height in pixels.

border_color and **text_color** govern the image background and loading message colors. **border** can be used to add a frame around the image, ie: border = 10 will add a 10 pixel border.

capture means what it says. If this option is enabled then users can use Print Screen and screen capture software to copy your web pages. The default setting is 0 which also activates scripting to disable right-click mouse options and drag-drop of images to the desktop.

keyboard and **menus** can be enabled or disabled however the effect of this option varies between different web browsers.

remote can enable access from remote or virtual partitions such as when Mac users run Bootcamp or install Parallels to run Windows on their Mac. Remote viewing enables screenshots and is not recommended.