ASPS Tag Management for Drupal

About this Module and Drupal

This module enables websites using Drupal to manage pages intended for display via the ArtistScope Site Protection System (ASPS), by nominating which pages are to be protected and which are not, thus enabling access to the public via generic doorway pages and only copy protecting those pages or sections that require protection.

By using a CMS web designers can have a difficult time tagging which pages are to be delivered via ASPS. In fact the means to do so will be beyond most web developers who today are more accustomed to using ready-made "modules" to customize their sites without having to touch code.

This module has been provided to greatly simplify that task.

What triggers ASPS Protection?

The ASPS server filter can be installed server side (for both Windows and Linux servers). Which sites can use ASPS then depends on the filter's configuration. When ASPS is configured for a web site the ASPS filter lies dormant until invoked by the inclusion of a tag that precedes any HTML on the page. Note that including the ASPS tag anywhere else in the HTML will crash the page.

How it works

This module enables you to nominate which pages need to be protected, by simply listing the pages or a keyword that might be found in their URL. For example if you have a URL like http://mysite.com/lessons/part1etc then nominating "lessons" will tag all pages that include that keyword in its URL. In the module's settings, you can also nominate which meta-tags to apply for the different protection options.

Browser Behavior

The ArtisBrowser is the only web browser that can decrypt the HTML delivered by the ASPS filter. The ArtisBrowser is a most functional web browser and provides similar support to the popular web browsers when displaying generic content. However when a web page is tagged for ASPS (or CopySafe is found used on the page) it switches to protection mode by disabling all of the features that common browsers provide for saving, copying and generally plagiarizing intellectual data.

ArtisBrowser on its own will not copy protect anything. But it does provide the most secure web viewing experience when used in conjunction with ASPS or one of the CopySafe solutions.

ASPS Meta-tags

These options will apply to all ASPS tagged pages:

- AllowCapture - allow all copy by disable screen capture protection.
- AllowKeys - allow use of the keyboard.
- AllowPrint - allow printing.
- AllowRemote - allow access from virtual devices running remote view software.
- AllowSave - allow save.
- ArtisWidth - set browser window width in pixels.
- ArtisHeight - set browser window height in pixels.
- ArtisKiosk - display fullscreen kiosk window without menu bar.

Best Policy

The best policy is to apply ASP to only those pages that need protecting, leaving your home pages and generic info pages such contact forms intact. Otherwise you will not benefit from search engines.

The Alternative

The ASPS Tag Management module sets meta-tags that apply to all pages where a trigger word is found in its url.

Installation

1. Install is simple. Unzip ASPS_Tag_Magement_Drupal.zip to retrieve:

- asps-tag-management.zip
- ASPS_Tag_Management_Drupal.pdf

2. Then upload and unpack asps-tag-management.zip to your web site into the /modules/contrib/ folder.

3. Then, go to Extensions and scroll down to ASPS Tag Management, check the box and click the Install button at the bottom of the page:

4. Go to Configuration > ASPS Tag Management and click the Settings link:

ASPS Tag Management Settings ☆

Home » Administration » Configuration » ASPS Tag Management

✓ The plugin is active

Mode

- (•) Active
- ( ) Disabled
- ( ) Debug

[ ] Exempt Admin from ASPS tags?

URL KEYWORD TRIGGERS

Keywords

test

Separated by Commas e.g. lesson,course,download

Enforce ASPS

- (•) To all in the above list
- ( ) To all except in the above list

SELECT OPTIONS TO ALLOW

- [ ] Allow Capture
- [x] Allow Keyboard
- [ ] Allow Save
- [x] Allow Remote
- [ ] Allow Print

BROWSER WINDOW

Height (in px)

Width (in px)

[ ] Kiosk Mode

Height and Width are not applicable if Kiosk mode is selected.

Save configuration

- Set Mode to Active
- Add keywords or full urls to use as URL triggers, separated by comma.
- Select "Enforce ASPS to all in the above list".
- Select "Allow Remote" if want to allow virtual computers.

Browser Window settings are optional. If window size is set, all browser windows will use that size. However Kiosk Mode over-rides windows size.

The inserted tags will not have any effect on your pages until the ASPS server filter is installed and enabled. Tag insertion can be disabled at anytime by disabling Mode (first line).

Configuring Settings

First thing to do is nominate the keywords to trigger ASPS. For example if you have a section for lessons that you want to protect, create those pages so that "lesson" appears on their url as either folder or page name. Then simply add "lesson" as a keyword on your ASPS Tag settings page.

Next, set the meta-tags for protection settings, noting that the same settings are applied to all ASPS protected pages.

It is that easy to use.

Troubleshooting

If the ASPS Tag Management module has been installed before the ArtisFilter is installed on the server, you can easily check your protected page by viewing source code. The prime requirement is that the <!-- ArtisReader --> tag appears before any other HTML.

However if the ArtisFilter has been installed and if you are getting an error when requesting your test page, the most likely problem is that other code has been added before placement of the <!-- ArtisReader --> tag, but because the ArtisFilter is active, you can no longer see HML when viewing source code.

The extra code is probably added in Debug mode of your Theme. Drupal 8 sites are have 2 modes, Development and Production. Our module will work perfectly in Production mode.

As per Drupal 8 standard, debug mode should be disabled in production environments as default.

Please follow below steps to disable theme's debug mode:

1. Go to root folder of Drupal code.
2. Go to sites/default folder.
3. Make sure that permission of file "services.yml" is not "read-only". Open "services.yml" file in text editor.
4. Go to line number 58 of "services.yml" file. You should see "debug: true" on line number 58.
5. Change it to "debug: false". Save the file and revert the file permission back to "read-only".
6. Now login as Administrator user, and go to, admin/config/development/performance. Click "Clear all caches" button. 7)

7. That's it! Drupal theme debug mode is disabled and ArtisReader tag should appear on the first line of page's HTML.

If Drupal's debug mode has been disabled then there should be no HTML conflict. However Drupal coding is far from perfect. For example, adding extra information for "Description" meta-tags can create BAD HTML that will break the ASPS decryption. So you need to check all meta-tags on the protected page, and if you see a "description" tag with 2 lines of text separated by a line return, you have found the problem. Line returns should never appear in meta-tags!

Debug Mode

Debug mode will replace the ArtisReader tag with a non-effective Debug tag that will not activate ASPS and thus enable you to check the HTML of your page.

Licensing

This module is free. However, you will need a license to use the ArtistScope Site Protection System (ASPS) on your web site. The installation of the ASPS server filter will require server admin privileges to install, so you will need a dedicated or virtual server.

To purchase ASPS for your web site see – https://www.artistscope.net/ssl/order/order_asps_software.asp