ASPS Tag Management for WordPress

About this Plugin and WordPress

This plugin enables WordPress sites to manage pages intended for ArtistScope Site Protection System (ASPS). ASPS can be applied to nominated pages only, 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. This plugin has been provided to greatly simplify that task.

What triggers ASPS Protection?

The ASPS server filter can be installed server side (for Windows, Linux and Nginx 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 cause an error.

How it works

This plugin 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 plugin'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 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.

Best Policy

The best policy is to apply ASPS to only those pages that need protecting, leaving your home pages and generic info pages such as contact forms intact. Otherwise you will not benefit from search engines and even lock yourself out of your admin section to be able to restore the mistake.

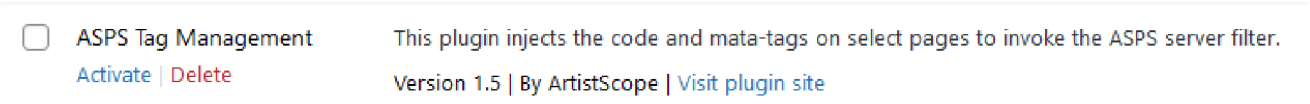
Installation

Install is simple. Unzip ASPS_Tag_Magement_WordPress.zip to retrieve:

- wp-asps-tag-management.zip
- ASPS_Tag_Management_WordPress.pdf

NEXT: upload and unpack wp-asps-tag-management.zip to the /wp-content/plugins/ folder.

NEXT: on your Plugins page, click to Activate ASPS Tag Management.



Then, go to Settings > ASPS Tag Management

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

ASPS Meta-tags

These options will apply to all ASPS tagged pages:

- AllowKeys - allow use of the keyboard (Windows only).
- AllowRemote - allow access from virtual devices running remote view software.
- AllowWindows - allow Windows computers.
- AllowMac - allow Mac OSX computers.
- AllowiOS – allow iPhone and iPad devices.
- AllowAndroid – allow Android mobile phones.
- ArtisWidth - set browser window width in pixels.
- ArtisHeight - set browser window height in pixels.
- ArtisKiosk - display fullscreen kiosk window without menu bar.

Remote View

Remote viewing enables use in VMs that allow capture from the host computer and not recommended except for testing. Note that other browsers can now view remote desktops, so other browsers will be shut down while viewing ASPS protected pages. AllowRemote will enable other browsers to run.

Keyword Triggers

You can nominate Keywords, page names or full urls. Nominating a keyword like “exam” will trigger all urls containing that word. But if you only want to trigger a folder name, then use “/exam/”.

ASPS Tag Management Settings

The plugin is active.

Mode : (●) Active ( ) Disabled

Debug Mode : ( ) Enabled (●) Disabled

URL Keyword Triggers (Separated by Commas e.g. lesson,course,download)

lessons, course-video, login

(●) Enforce ASPS to all in the above list ( ) Enforce ASPS to all except in the above list

Select Options to Allow

- [x] Allow Keyboard
- [x] Allow Remote

ArtisBrowser and Versions to Allow:

Windows	[x]	34.2	Min. Version
Mac OSX	[x]	32.1	Min. Version
IOS	[x]	33.0	Min. Version
Android	[x]	34.0	Min. Version

Browser Window

Height (in px) : 600 Width (in px) : 400

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

- [ ] Kiosk Mode

Save Changes

Browser Support

ArtisBrowser is available for all Windows OS, Mac OSX, Android phones and iOS (IPhone and iPad) devices. However they must be specifically allowed. For example, to allow Mac using ArtisBrowser, the AllowMac meta-tag must be found in between the head tags of the page, so set to allow in plugin settings.

Minimum ArtisBrowser Version

Use this setting to specify minimum version that will be allowed access. It is most recommended to use the latest version so that the latest security and protections are used. Note: browser version must be entered using only one decimal point like **34.0**

Configuring Settings

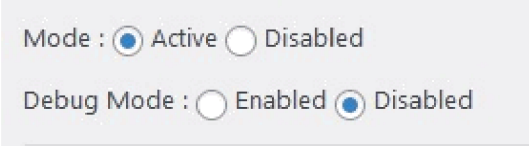
First thing to do is nominate the keywords to trigger ASPS. For example if you have a section for lessons that you want to protect, create those pages so that "lesson" appears in their url as either folder or page name. Then simply add "lesson" as a keyword on your ASPS Tag settings page (see image above).

Languages

You are welcome to translate the download pages in this plugin's folder at:
/wp-content/plugins/wp-asps-tag-management/

Debugging

When Debug Mode is Enabled, you can access ASPS pages using a normal browser to view page source.



In Debug Mode the <!—ArtisReader → Tag is replaced with <!—Debug → so be sure to Disable Debug to continue running ASPS when done testing. Note that ASPS Mode should always be Active.

If this tag is missing or does not appear as the first line of HTML and on a line of its own, then you have a problem with page compression caused by PageSpeed filters/plugins or services like Litespeed or Cloudfare. How they cause a problem is because they think that by removing page comments from HTML that they will actually increase download speed. Cloudfare does provide options in their settings to disable "page compression" but other services may need to be investigated/educated.

Licensing

ASPS can be installed for all versions of Apache, Nginx and Windows IIS servers. However they do require different modules so be sure to specify your requirements before installation commences.

Copyright © 1998-2023 ArtistScope. All Rights Reserved - www.artistscope.com