ArtistScope Site Protection System (ASPS)

ArtisFilter Installation & ASPS Page Design

Revised July 2020

About ASPS

The ArtistScope Site Protection System (ASPS) is basically comprised of two (2) components to provide an encrypted stream for html from web server to web client. On the client end a custom web browser known as the ArtisBrowser is used to request, decrypt and display encrypted content delivered by the ArtisFilter that is installed on the web server.

ArtistScope Site Protection System (ASPS) is able to detect whether the request originated from the ArtisBrowser or a standard browser. If the request originated from the ArtisBrowser and the page includes the ASPS tag, the requested content is encrypted and delivered so that only the ArtisBrowser can decrypt and display the page. Any page that includes the ASPS tag will always be encrypted so that only the ArtisBrowser can display it. Otherwise the page is delivered as a normal page, viewable by any web browser.

Unless activated by ASPS the ArtisBrowser will operate as a normal web browser. However when CopySafe is detected on a web page it will switch to protection mode but most options will depend on the CopySafe parameters rather than ASPS meta-tags.

Licensing

ArtistScope Site Protection System (ASPS) can be used on any website by installing the ASPS Server Filter (ArtisFilter) on the server hosting the site. A dedicated or virtual server with admin rights to install software at system level is required.

Licensing for the ASPS Server Filter is per server and can include several website domains when nominated at the time of installation. Server licenses are not transferable as licensing is locked to the server's machine ID. License files can be updated/extended to cater for hard drive failure or host relocation by special arrangement and payment of a service fee.

In all cases the ASPS Server Filter is installed by the ArtistScope support team to ensure that the ArtisFilter matches the server platform and version, that configuration caters for changes that some Control Panel software makes to HTTP modules, and that the license key matches your server. Consequently self install is not an option. Remote access to the server with administrator rights will be required for all installations/updates of ASPS Server Filter and license keys.

ASPS Server Filter Installation

The ASPS server filter software (ArtisFilter) is available for most server types including:

- Linux/Apache (Redhat/Centos 5.8+)
- Windows Server 2003 (all Windows OS since XP running IIS)
- Windows Server 2008/2012/2016 and Windows 7/8/10 Pro versions

Installation and file resources are different for each type of server and version, especially with Linux. Different Control Panel systems provided by web hosts usually alter HTTP daemons and their configuration which can require adjustments made to the ArtisFilter and/or HTTP settings.

So self install cannot be an option. The ArtistScope support team needs to install your ASPS ArtisFilter so that you can be assured that the software suits your server and that it is properly configured.

Control Panel Software

While Control Panel (CP) software can enable one to set up and configure websites with little to no experience, doing without a CP provided by a webhost is strongly recommended.

On Windows servers, a Remote Desktop Connection can provide admin access to the server's desktop and all admin tasks just as if your were working directly on a workstation.

On Linux servers, you can install Webmin by SSH and command line. Webmin will provide a web interface for managing all admin tasks and configurations including the installation of additional software and services. While Webmin is a CP, it does not alter the server's core or daemons to be able to manage their settings.

If you are setting up a virtual server for the first time, and not confident with server configuration, go for the "bare-bones" option (without a CP) and let our support team configure your website for you. In such cases we can create the website, setup ASPS and then all you have to do is add your content to the site folder.

Server Licenses

The ASPS ArtisFilter is licensed per server. While that license enables the server to provide ASPS services on an unlimited number of domains, each license is limited to one server and that is governed by the unique ComputerID of the server. That ID is encrypted into your license file and license files are not transferable or usable on other servers or computers.

The only way that ASPS can be licensed for your server is to allow access to ArtistScope for the creation of your license file and the proper installation of the ArtisFilter for your server type.

Configuring web pages for ASPS

Unless the *ArtisReader* tag (shown below) is added to the first line of HTML on a web page, that page will be delivered by the server as normal HTML and viewable by all web browsers. So to invoke ASPS protection options and encrypt so that only the ArtisBrowser can display them, simply add the following tag to appear before any other HTML on the page…

`<!-- ArtisReader -->`

Note: please observe the space before and after the word "ArtisReader" (the ASPS tag). If this tag is not found exactly as it appears here, it will not be recognized by the server.

Anything appearing after the *ArtisReader* tag will be encrypted prior to delivery. This tag must appear foremost on the page that is delivered to the browser. If you are using server languages like ASP or PHP where their initialization tag must always be the first line on a page, that is OK because *server side* scripting is performed before assembly of the HTML that is delivered. JavaScript and other *client-side* scripting languages performed by the browser after download cannot be used to add the *ArtisReader* tag.

Controlling the Protection Options

Without any meta-tags added to a page, the default setting will apply all options:

- Prevent PrintScreen and screen capture (including screen recording)
- Disable use of the keyboard
- Disable printing
- Disable saving of linked files for download
- Disable right click menu options
- Disable access by computers running virtual desktops
- Disable access to Mac* computers

Any of the above options can be disabled by adding a meta-tag like:

`<meta name="artis-allowcapture" value="true" />`	enable PrintScreen and screen capture
`<meta name="artis-allowkeys" value="true" />`	enable use of the keyboard
`<meta name="artis-allowprint" value="true" />`	enable printing
`<meta name="artis-allowsave" value="true" />`	enable save as
`<meta name="artis-allowremote" value="true" />`	enable remote (virtual) viewing
`<meta name="artis-allowmac" value="true" />`	enable access to Mac computers

Anything that is not "true" (or = 1) is assumed to be false.

Controlling Browser Window Size

Each page can be set to display a nominated size that you can include in your meta-tags.

- Control width and height of the browser window
- Use Kiosk mode to open fullscreen without a toolbar

These options can be controlled by adding meta-tags like:

<meta name="artis-width" value="800" />   set width in pixels
<meta name="artis-height" value="600" />   set height in pixels
or…
<meta name="artis-kioskmode" value="true" />   open fullscreen (without toolbar)

Note: that setting the windows size is not necessary if you want to leave it to the user's preference as any window opening from a previous window will maintain the same window size. So you only need to add these size tags on windows that you do want to be a specific size.

To move from a normal window to 'Kiosk Mode" which uses fullscreen without a toolbar, you only need to set the size tag on the pages to be displayed at fullscreen. So them to return from full screen to a smaller window, simply link to a page that has tags for the new window size.

NOTE: that the active window will govern the size setting for all tabs, but only on first load. Swapping between different tabs will not change the size once it is set by a new window/tab.

Custom error pages and screen messages

ArtisFilter provides its own unique error messages suitable for ArtisBrowser usage.

Customizing your web pages for smooth transition

When the ASPS tag is added to web pages delivered from an ASPS Server, normal web browsers will not be able to display those pages. So for doorway pages such as your home page and user indexes some careful editing can cater for both protected and unprotected mode.

These notes cover all tags that can be added manually to (hard-coded) web pages.

ASPS Tag Management

To manage websites that use dynamic page assembly provided by CMS like DNN, Drupal, Joomla, Moodle and WordPress, ArtistScope provides free plugin add-ons for "ASPS Tag Management" that enable site owners to nominate which pages are protected from a settings page within the CMS.

See https://artistscope.com/asps_web_site_protection.asp#tag

The ASPS Tag Management plugins enable one to nominate which page is to be protected by ASPS by simply listing their full URL or a keyword found in the URLs. For example nominating "lessons" will apply ASPS protection to all web pages like http://example.com/**lessons**/view.php?id=*

ArtisBrowser Information

The ArtisBrowser user-agent provides additional information for web designers to work with:

Mozilla/5.0 (windows ***) Gecko/****** ArtisReader/**.*.*) Firefox/** ArtisBrowser/**.*.*

The additional **server variables** can be found in the request header:

- HTTP_ARTISDRM
- HTTP_ARTISDATE
- HTTP_ARTISWIDTH
- HTTP_ARTISHEIGHT

HTTP_ARTISDRM gives the client Computer ID for use in DRM. This number is unique to each computer and can be used to verify a user's identity by comparing to a record of it in your user database.

HTTP_ARTISDATE gives the date on the client computer in YYYYMMDD format – useful for checking if the client date is different from the server date indicating if they rolled their clock back to bypass expiries and usage restrictions.

HTTP_ARTISWIDTH gives the user's screen width in pixels.

HTTP_ARTISHEIGHT gives the user's screen height in pixels.

Getting the User's Computer ID using ASP:

Request.ServerVariables("HTTP_ARTISDRM")

Getting the User's Computer ID using PHP:

$_SERVER['HTTP_ARTISDRM]

Getting generic server variables using ASP:

```
strCheckReferrer =      Request.ServerVariables("HTTP_REFERER")
strCheckIPnumber =      Request.ServerVariables("REMOTE_ADDR")
strServer =             Request.ServerVariables("SERVER_NAME")
strUrl =                Request.ServerVariables("URL")
strUserLanguage =       Lcase(request.servervariables("HTTP_ACCEPT_LANGUAGE"))
```

Getting generic server variables using PHP:

```
$checkreferrer =        $_SERVER['HTTP_REFERER'];
$checkipnumber =        $_SERVER['REMOTE_ADDR '];
$server =               $_SERVER['SERVER_NAME '];
$url =                  $_SERVER['QUERY_STRING'];
$userlanguage =         $_SERVER['HTTP_ACCEPT_LANGUAGE '];
```

General Browser Information

Getting generic server variables using ASP:

```
strCheckReferrer =        Request.ServerVariables("HTTP_REFERER")
strCheckIPnumber =        Request.ServerVariables("REMOTE_ADDR")
strServer =               Request.ServerVariables("SERVER_NAME")
strUrl =                  Request.ServerVariables("URL")
strUserLanguage =         Lcase(request.servervariables("HTTP_ACCEPT_LANGUAGE"))
```

Getting generic server variables using PHP:

```
$checkreferrer =          $_SERVER['HTTP_REFERER'];
$checkipnumber =          $_SERVER['REMOTE_ADDR '];
$server =                 $_SERVER['SERVER_NAME '];
$url =                    $_SERVER['QUERY_STRING'];
$userlanguage =           $_SERVER['HTTP_ACCEPT_LANGUAGE '];
```

Document Rights Management (DRM)

The ArtisBrowser has been optimized to enhance DRM for web projects, by identifying each user by unique Computer ID which it reports as a server variable in all page requests.

Web designers can update any existing CMS to lock user accounts to the user's computer by recording that Computer ID and subsequently validating future access. In CMS like WordPress one can add a new column for ComputerID to the user table and add some code to their login script.

However, when updating any CMS like WordPress which is prone to want to update itself, precautions are needed to prevent that update from overwriting whatever modifications that were made. In such case it may be better to create a custom plugin that will remain intact even after core upgrades.

Customization and Branding

We no longer recommend custom branding because thorough renaming can confuse users who need to be using the latest version when available. Also, due to the system level interaction of this application, code-signing and reputation play a major art in acceptance by modern anti-virus software.

If all of your users are within a corporate intranet, branding may not cause problems. But if there is a chance that your users might visit other websites that use ASPS, then we strongly recommend leaving the ArtisBrowser as is.

However we may be able to cater for branded installers and custom start pages. If interested, please contact us giving a description of your requirements and your project.

Troubleshooting

Logging can be unnecessary overhead and only recommended for debugging errors that may be encountered until it is configured properly. Once it is running it is most recommended to disable logging by removing <add key="LogPath" value="C:\Temp" /> from web.config.

Directly Linking to Media

Providing hyperlinks that are direct links to media is not recommended unless you want to force the visitor to open that media in another application and not the ArtisBrowser. That is because opening any media outside of the ArtisBrowser will escape the realm of ASPS protection.
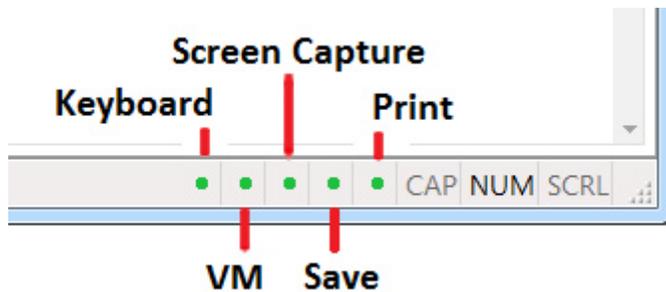
Protecting All Media

While ASPS and the ArtisBrowser can most securely protect all data and media that can be duisplayed on a web page, that does not apply to PDF.

That is because while most unencrypted and unprotected media such as images, Flash, Java applets, MP4 video, HTML5 video, etc can be displayed in ArtisBrowser by the browser or ancillary plugins, raw PDF displayed on web pages use Adobe Reader resources which will always provide save, copy and print options in its menu bar. There was a time that those menu options could be disabled in the object tag parameters, but Adobe changed that to enhance sales of their own extremely expensive DRM solutions.

So to display PDF embedded on any web page and copy protect it, you need to use CopySafe PDF Protection. All CopySafe solutions are supported by ArtisBrowser.

Status Bar Indicator

At bottom-right of the browser window you can see a series of red/green dots. Those dots indicate the current protection status.

Red = disabled
Green = enabled