TOTAL CONTROL
Document Rights Management
Control user rights to view and print documents and images
with the option of changing permissions at any time.

www.artistscope.com

ArtistScope DRM for PDF documents

ArtistScope DRM for PDF is a total control solution for the Access Rights Management of documents and eBooks where an author can assign different permissions per user or group of users. When copy protection and DRM rights are assigned the document becomes for "their eyes only" and any copies forwarded on cannot be viewed by others unless the recipient also has rights to view.

Total control over access rights managed from anywhere

The creation of user accounts, document conversion and distribution can be managed online from any computer in the world. Create new users, assign administrators and other special users permitted to submit publications, update document permissions or suspend document availability at any time.

Copy protect intellectual property, photos, plans and drawings

Upload and protect Word and Excel documents for distribution as documents that cannot be copied or printed unless you allow the privilege. Publish using a variable combination of DRM or copy protection rules or none at all.

Protect financial data and other sensitive information

Provide financial data and statistics to valued clients. ArtistScope provides the most secure DRM solution imaginable where documents can be made capture safe at the click of a button and permissions to use a document cannot be foiled in any way.

Manage access rights and permissions with total control at all times

- o Restrict which users or groups can view a document
- o Set expiration on a document validated by time server
- o Allow or limit the number of views of documents per user or group
- o Allow or limit the number of prints of documents per user or group
- o Allow or limit access to documents by IP number or network
- o Allow or limit a user to add/edit documents for shared distribution
- o Create member accounts for authoring documents
- o Encrypt and copy protect from all saving and copy methods
- o Prevent Printscreen, screen capture and remote viewing
- o Stop forwarding and unauthorized redistribution in its tracks!

Uploading

While access rights to view a document (Document Rights Management) can be restricted per unique computer, access to your management pages can be gained from any computer in the world, even from an internet cafe.

The CopySafe PDF Protector software provides a Universal Document Converter for converting most file types to PDF for encryption as a .ENC file. When converted for DRM protection, it is those ENC files that need to be uploaded for registration in your online DRM management system

Copy protected PDF

CopySafe PDF Protector can encrypt PDF for protection from all copy methods including Printscreen and screen capture. This option enables distribution to anyone with CopySafe PDF Reader installed which is a free download to the public.

DRM protected PDF

DRM protected PDFs are automatically copy protected plus they are protected from unauthorized redistribution by ensuring that on the persons with your permission can open the document. You can limit the number of times it can be viewed or how many times it is printed. And you can change these permissions at any time with immediate effect that also applies to documents that have already been downloaded.

Document types

The most secure method for copy protecting documents for distribution is by encrypting them for use with our proprietary reader. Copy protected documents are output as a custom file type:

  o **.ENC** format are lightweight library files that can be read with the CopySafe PDF Reader.

Setting document permissions

Each registered author can set user access permissions on document for:

  - Expiry date
  - Password
  - Number of views or prints allowed

Authors with admin permissions can set all of the above plus:

  - Edit all documents including those of their members
  - Add new members and edit
  - Add new groups and edit

Admin rights

Admin rights vary according to user status and group. For example a **demo** account can:

  - Add and edit new user accounts but cannot make them active
  - Upload and create documents and web pages for their own group
  - Edit their own documents and pages
  - Send test emails to their own email address
  - View their own gallery and documents
  - View all documents and pages assigned to their group

Any **author** with admin permissions (but not a demo account) can:

  - Create their own group
  - Add and edit users belonging to any groups which they are a member of
  - Set access levels to users, groups and documents that belong to their groups
  - View, add and edit all documents where they are author
  - View and edit all documents that are active in their groups
  - Send newsletter emails to all groups and users which they author
  - View statistics on their documents and reset their users' hit counts
  - Set expiration and renew subscription dates for all users in their groups

Expiry date

When setting expiration on a protected PDF for public distribution, the expiry date is embedded in the encrypted document and is final... it cannot be changed without uploading the original and re-converting. However when setting expiration for a DRM document, the expiry date is stored on record and can be changed at any time.

When you set an expiry date the document will expire at midnight of that day according to GMT.

IP ban and networks allowed

Users can be banned by IP number or network and exceptions to the rule can be set. For example you can ban a network but permit an individual IP number. Likewise you can allow a network and ban a single IP from it. For example to ban an ISP you can set 100.100.100 or 100.100. You can also set 100. but be warned that you will also ban any IP numbers or networks that contain "100". In the main settings file for the DRM site you can set to allow all networks except those listed, or deny all networks except those listed.

Password

Setting a password for a document only applies if it's not converted for DRM options, because with DRM a password is no advantage to the protection already in place.

Users and groups

Permissions can be assigned to groups and/or users. Documents can be assigned to a single group and multiple users. Web pages can be assigned per group only so that they can get a menu of all pages assigned to their group.

Print limitation

When converting a document for DRM the number of prints allowed per user or group can be limited. DRM print limits can be varied at any time.

Document quality

The quality of your copy protected PDF will depend on its content and the PDF converter that was used in its creation. While some converters may be able to produce a file that behaves as a PDF it may not survive encryption. To maintain consistency and conformity a Universal Document Converter is provided with the CopySafe PDF Protector that will convert most file types to PDF for import and encryption as a DRM document.

Image quality

For the best quality do not use compressed images or images of low resolution. It's also best to avoid using GIF images in documents because when viewed at smaller or higher percentages of the actual document size, the images may not look so good. JPG and PNG are good but BMP will look better all round when the page is varied in size.

Email distribution

From your document menu you can select a file to send to your readers by email as a newsletter. You have the option to select which users or groups to send to and which file format to send.

File update and overwrite

Modification to existing documents is not recommended especially after distribution to your readers.

Statistics and usage counts

Each time a document is validated the hit is recorded so that Authors can monitor usage and the popularity of their content. Registered authors can view the hits on their documents and if needed reset usage counts for individual users. If an account is regulated by credits for validation hits then the Author's Preferences will show the current balance of hits in credit.

How hit counts work

Each time one of your users requests permission to open a DRM protected document their ID and access rights are checked against the database. Each request that is unique in any given session is recorded as a hit against the author's account. For example if a user requests authorization for 3 documents in the one session then the total of hits recorded will be 3. If the same user loads and reloads the same document several times the recorded hits will still be 3.

The exception to the rule is if the visitor is either the site administrator, an admin for the Group that the document belongs to, or is the author of that Group or document, then the total hit count will be 0... enabling authors and administrators to check, edit and test their deliverables without being penalised.

Statistics and usage counts

Each time a web page is validated the hit is recorded so that Authors can monitor usage and the popularity of their content. Registered authors can view the hits on their web pages and if needed reset usage counts for individual users. If an account is regulated by credits for validation hits then the Author's Preferences will show the current balance of hits in credit.