



ArtistScope

Web Access Rights Management

INTRODUCTION

ArtistScope Web Access Rights Management (WARM) can be used to control access to your web pages. Permissions to view select web pages can be assigned to individuals or members of groups (such as students in a particular class). If a user/student does not have permission to access those pages then they cannot be accessed directly or indirectly (by using site grabbers/downloaders), ensuring that your information/lessons are for your target audience only.

Web page encryption

With WARM you have the option of adding access rights permissions to existing web pages (and new pages) by adding a top and bottom protect tag to the web pages html. Or you can use the Article Manager to create new web pages that are not only WARM protected but are encrypted and stored in your database for delivery on the fly.

Web access security

This solution is much more secured than password protection because passwords can be passed onto friends and anyone with a password can gain free access. However with WARM a user's access is governed by their computer's footprint and no two computers can have the same footprint. Also, because each user has a unique ID, their account settings can be changed at any time from your end for immediate effect, enabling you to suspend their account, extend their subscription period and add/remove new entitlements as they become available.

Online web page creation

The screenshot displays the 'Web Access Control' interface. At the top, there is a navigation bar with 'ARTICLE EDIT' and a menu: 'Add new article | Articles | Users | Groups | Pages | Insert code | Newsletter | Help'. Below this, the article details are shown: Title: 'What is Digital Rights Management (DRM)', Active: 'Yes', Group: '00 all', Windows: checked, Mac: checked, Linux: checked, Expiry: '8' (days), 'March' (month), and '2011' (year). A rich text editor toolbar is visible with various icons for text formatting and insertion. The main content area shows a preview of the article with the title 'Digital Rights Management (DRM)' in blue. The preview includes a photo of a man at a laptop and the following text: 'Digital Rights Management (DRM) covers a variety of technologies employed in the control of access rights to information and various media such as e-books, music, movies, software and digital documents. Access Rights Management solutions typically consist of security measures applied according to authorized group level governed by database records that determine the correct policy to apply to each file and individual user. The security mechanizations and rights [database records](#) are typically protected by a cryptographic layer usually comprised of the most secure encryption methods of the day.' Below this is a section titled 'Portability and support' with the text: 'A common misunderstanding is that any document can be converted to DRM. Why this can never be true is that any document in its natural file format, while being viewable in its [natural viewer](#) (ie: Word for .doc, Excel for .xls, etc) cannot be protected. The document needs to have policy added and then needs to be encrypted to maintain that policy remains intact. So for each and every document type one needs to use a custom viewer (ie: .doc files cannot be opened in Adobe Reader)'

Using the inbuilt page maker you can create new web pages with full control over the html format. You can upload images, embed Flash and video and set individual security preferences for each page such group access, restrict to Windows, Mac or Linux computers only, set expiration dates and more. When your page is saved it is encrypted and added to your database.

Web Access Control													
USERS													
Add new user Users Articles Groups Pages Insert code Newsletters Help													
ID	Firstname	Lastname	P	Key	Group	Credits	Start	Renewal	Expiry	Last login	IP	Email	Active
<input type="checkbox"/>	100019	Susan	Anderson		<input type="checkbox"/>	00 all		2010-06-04			2010-06-06 02:43		<input type="checkbox"/>
<input type="checkbox"/>	100010	Andrew	McDonald		<input type="checkbox"/>	01 student		2010-06-01	2010-06-03	2010-06-03	2010-06-04 16:42		<input checked="" type="checkbox"/>
<input type="checkbox"/>	100007	Ken	Douglas		<input checked="" type="checkbox"/>	03 student	0	2010-04-23			2010-06-06 15:44	124.254.82.220	<input checked="" type="checkbox"/>
<input type="checkbox"/>	100000	William	Kent		<input checked="" type="checkbox"/>	00 all	100	2010-02-02			2010-06-08 01:03	124.254.82.220	<input checked="" type="checkbox"/>

Users and groups

The creation and management of user accounts can be managed online from any computer in the world. Create new users, update document permissions or suspend document availability at any time. Access can be assigned to individual users or groups. For example if you have pages for level 2 students only, then create a group for “Level 2” and then assign your users to the Level 2 group.

To cater for the maximum possibility of variations the following rules apply:

- Every account must have a unique username (email address) per computer
- Each database is limited to 999,999 users
- Each database is limited to 999,999 groups
- Each database is limited to 999,999 documents
- Each database is limited to 999,999 web pages

The same web site can host an unlimited number of databases, for example one database for each author account who may have up to 999,999 users each, extending the scope of your WARM solution to cater for every one in the world from a single domain.

Features and functions

- Visitor access request registration
- New registration email validation
- Anti-spam Captcha protection
- User password retrieval
- User friendly error messages for login failures
- Safeguard to prevent account duplication
- New account approval by admin before enabling access
- Admin add new users with email address only
- New users are emailed instructions for validating their computer ID
- Admin can approve or suspend an account for immediate effect at any time
- Admin can manage user subscription by number of hits, expiry date or no limitation
- Admin can manage user and group level permissions
- Admin can send newsletters with attachment to users sorted by group
- Existing web pages can be protected by adding 2 lines of code
- New web pages can be created using an online HTML editor and image uploader
- Web pages can remain as static html or be encrypted for database delivery
- Protected web pages are accessible to users according to group policy
- Computer ID plugins available for Windows, Mac and Linux web browsers
- Fully supported on all web sites with ASP and Access database support

Platform support and web site requirements

For your students, all commonly used web browsers on Windows, Mac and Linux computers are supported. Users can log in to update their contact details and computer ID at any time.

WARM does not require DLLs to be installed on the web or the server. For your installation and management all that you need is a web site on a Windows web server with ASP support. For example, a FrontPage web site will be most adequate. Database support can be either Access or MS-SQL.

Statistics and usage counts

Each time one of your users requests permission to view a WARM protected page their access rights are checked against the database. Each unique request in any given session is recorded as a hit against the user's account.

Expiry dates

When setting expiration for a web page, the expiry date is stored on record and can be changed at any time. Expiry dates will expire at midnight of that day according to GMT. If no expiry is to be set, leave this field blank.

Email newsletters

Newsletters can be sent from your control panel advising all or select users of new publications, etc.

INSTALLATION

Web Site Requirements

For your installation and management all that you need is a web site on a Windows web server with ASP support. For example, a FrontPage web site will be most adequate. Database support can be either Access or MS-SQL.

To install WARM to your web site

1. Unzip the install package
2. Upload the "drm" folder to the root of your web site
3. Set read/write permissions on the "dbase" folder if the Access database is used.
4. For MS-SQL create a new database and import the tables and data.
5. If modify your database path and default settings in *inc_warm_dbconnection.asp*
6. Set read/write permissions on the upload folders named "classin" and "attachments".

Now point your web browser to <http://yoursite.com/drm/>

PROTECT EXISTING WEB PAGES

All you need to do is add the following code to the top of your page:

```
<%@LANGUAGE="VBSCRIPT"%>
<% option explicit %>
<% response.buffer = true %>
<!--#include file="inc_protect_top.asp" -->
<!--#include file="inc_protect_bottom.asp" -->
```

To use these insert tags it is assumed that you have already established a database connection.

Database connection strings

If your web pages have not already included an appropriate connection string and opening instructions for your database they will need to be added. If you are adding this WARM to existing web pages that already have connection strings for another database, you can proceed to add these because the code inserts have been designed to be unique and thus not interfere with any existing calls. Another option is to graft the database databases tables onto your existing database.

Grafting tables to an existing database

Whether you are using MS-SQL or an Access database the database tables for your Web Access protection can be added to an existing database. For Access databases simply open each database and copy'n'paste the Web Access tables to your existing database taking care to ensure that the table names are the same. In the case of a table graft, note that all of the WARM ASP pages will need to be modified to reflect the change, although if done properly only the connection string (for the different database name/path) should need to be changed.

Using the WARM database as provided

Regardless of whether your web pages are already accessing a database or not, using WARM straight out of the box is the easiest to install and should be compatible.

ASP rules

Whether converting existing html to ASP or adding WARM to existing ASP pages some fundamental rules will always apply. The first line must be as follows:

```
<%@LANGUAGE="VBSCRIPT"%>  
<% option explicit %>
```

The *option explicit* statement, if used, must be next and all string variables will need to be declared. WARM already has a list of declarations in *inc_dim_statements.asp* which should suffice unless you add new strings. The top insert tag includes the database connection and dim statements.

```
<!--#include file="inc_protect_top.asp "-->
```

If the user is authorized to view the page then everything between the top and bottom WARM tags will display, otherwise a warning message will be displayed with further instructions for the visitor.

```
<!--#include file="inc_protect_bottom.asp "-->
```

If the user doesn't have a WARM plugin installed to validate their computer ID then they will be redirected for download with further instructions.

Copyright © 1998-2010 ArtistScope. All Rights Reserved.

www.artistscope.com