



Drumlin Publisher

Secure PDF Publisher and Administration Program
for the Drumlin Digital Rights Management (DRM) Service



Overview and getting started

DrumlinPublisher is a free MS Windows program that provides facilities for the creation of encrypted (secure) versions of PDF files in formats suitable for use with our Javelin and Javelin3 PDF readers and associated Drumlin Digital Rights Management (DRM) service. Files created using DrumlinPublisher are protected against copy/paste, saving to other file formats, or sending to other users for them to view without separate authorization. [Technical notes](#) relating to the publishing process are provided at the end of this document. DrumlinPublisher also

includes service administration functionality, including facilities for creating access codes and document license files, and for tracking usage. DrumlinPublisher can also be run from the command line, enabling automation of secure file and code generation.

Source PDF files can be converted using DrumlinPublisher to our proprietary 256-bit encrypted formats, which have file extensions .drmz (for cross-platform usage) and .drmx for desktop/laptop usage only. Files created using DrumlinPublisher can only be opened using our free [Javelin PDF readers](#) which are available for Windows, OSX, iOS and Android operating systems. When using this facility your PDFs remain on your PC - there are never transmitted to our servers unless you ask us to convert and host files on your behalf. For web browser-based PDF secure distribution, which we also offer, please see our website page: <https://www.drumlinsecurity.com/online.php> or [contact us](#) for more details.

Access control to secured files is provided using **authorization codes** or document-and-device specific **license files**, managed via our DRM Server(s). For files that do not require authorization see the Permissions tab section. Permission controls that can be specified using DrumlinPublisher include Date expiry, Number of views permitted, Number of printouts permitted (if any), On-screen and On-print intelligent watermarking and screen capture protection for Windows PCs. A special “personalization” option is also available, that generates multiple “personalized” copies of the secured file, one for each target end user, with their full details included in the filename, tracked activity and as a watermark on-screen and on-print (where printing is permitted). DrumlinPublisher can be downloaded from the Drumlin downloads page: <https://www.drumlinsecurity.com/publisherdownloads.php>

Video demos of the basics on how to use the software are available at: <https://www.drumlinsecurity.com/demos-mp4.php>

DrumlinPublisher can be installed on any modern Windows platform, including all modern 32- and 64-bit MS Windows versions with current dotNet installation included, including those installed on top of Mac OSX using virtualization facilities such as Parallels. It can also be installed on multiple PCs - in this way multiple people in an organization can act as Editor/Publishers and Administrators. Special facilities exist to provided restricted use of DrumlinPublisher facilities for “sub-administrators/support staff”.

This manual is primarily in the form of screen shots of the main functions provided by the program - each of which is largely self-explanatory, with text provided for each of the main forms and fields. Several of the buttons on the application provide direct links to the main Drumlin Security website - these include the Help, Order Services, View License and Check for Updates buttons. Other buttons are described in the text and/or are self-explanatory. Command-line operation is described separately at the end of this document.

Registered users are prompted to login to the service via a pop-up dialog box, with their username and password, as shown below. Registration is described on the next page, and is usually a self-registration process, although we can register you directly if required. Note the servername on the login dialog - this is usually set as the main DRM server although the setting can be changed by clicking on the servername if we provide you with details for a different server to be used. See further details in the Technical Notes section at the end of this Guide.

The screenshot shows the Drumlin Publisher application window. The title bar reads "Drumlin Publisher". The main window header contains the application logo (a stylized figure in green and red) and the text "Drumlin Publisher: PDF Security Software". Below the header is a navigation menu with tabs: Home, Select Files, Set Permissions, Add Watermarks, Event History, Published Files, Codes, Code List, and Personalized Files. The main content area is partially obscured by a "Login" dialog box. The dialog box has a title "Login" and contains two input fields for "Username:" and "Password:". Below the fields is the URL "https://www.drumlinsecurity.co.uk/Service.asmx" and two buttons: "OK" and "Cancel". At the bottom of the dialog box, it says "Drumlin Publisher [2020-06-30]". In the background, the main window shows a "Login" button and the text "Currently not logged in". At the bottom of the main window, there is a status bar with "Software version: 1.00.079 [2020-06-30]", "View License", and "Check for Updates" buttons. A footer bar contains "Help", "Change Password", "Save Settings", "Order Services", "Create Secure PDFs", and "Quit" buttons. The footer also includes copyright information "(c) Drumlin Security Ltd, 2020", the website URL "https://www.drumlinsecurity.com", and the email address "info@drumlinsecurity.com".

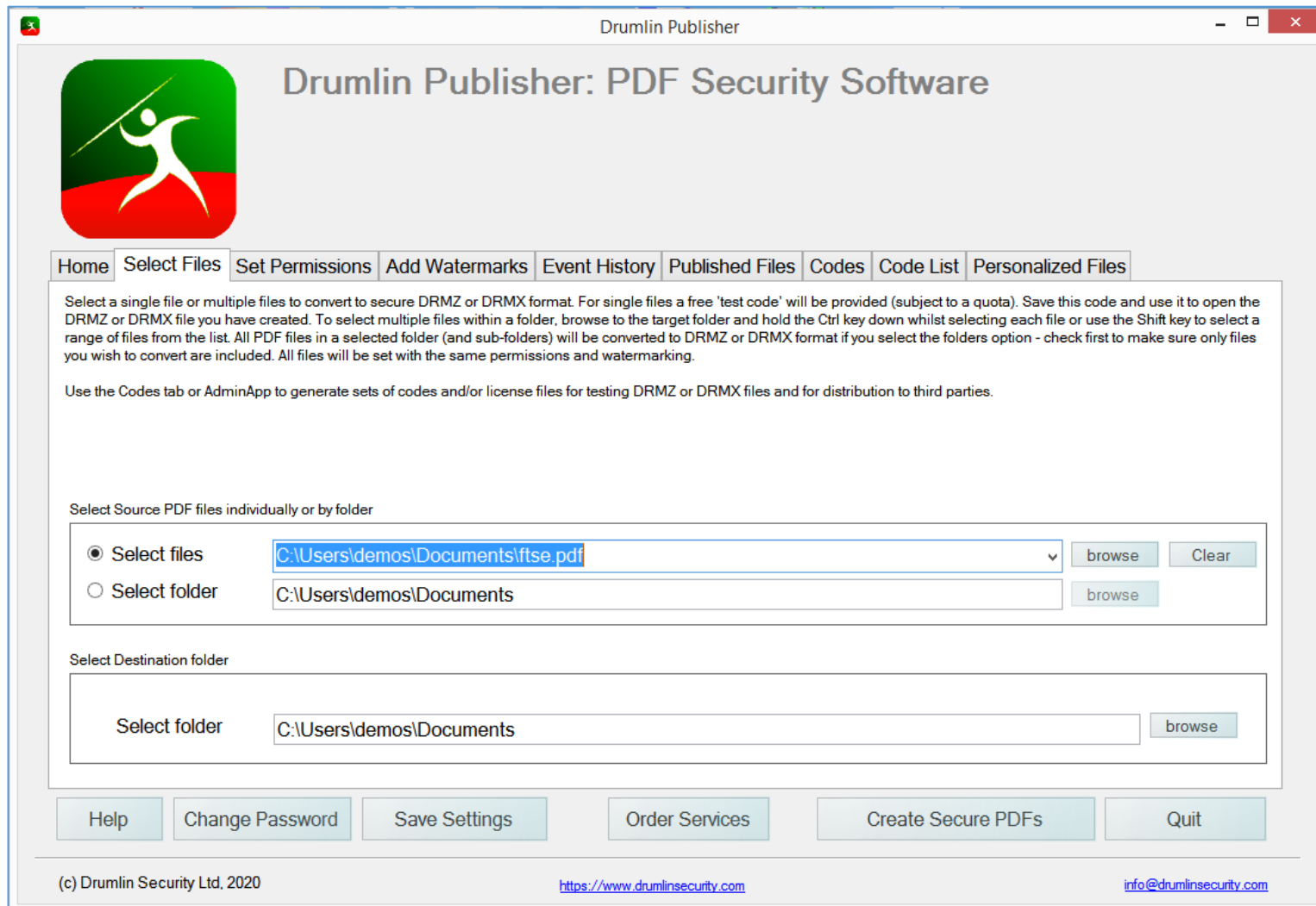
Home screen

Tab 1 provides the facilities for logging into the DRM service. To create secure versions of PDFs Login is required - this can use an existing username/password for currently registered Drumlin users, or for new users, simply use the Register button to create your own user registration details, including your chosen username and password. Once registered you can then login and use the program. The registration screen includes DRM server selection (as per the login screen). Only select an alternative server to the default if we advise it.



Select Files

Tab 2 (Select Files) enables one or more PDF files to be selected for conversion, or optionally an entire folder within which all PDF files will be included for conversion (**Source PDFs**). When files are converted, the new secure versions are saved to the **Destination** folder that you specify.



Set Permissions

Tab 3 is the place where you specify the main permissions/security controls you want to be applied to the encrypted file. In most cases this will be for no printing, unlimited viewing, an end date in the distant future and .drmz file format. Press the SAVE SETTINGS button after selecting your options, so that these are available next time you use the program. See below and the [video demos](#) for more details.

The screenshot shows the 'Set Permissions' tab in the Drumlin Publisher software. The window title is 'Drumlin Publisher'. The main title is 'Drumlin Publisher: PDF Security Software'. The interface includes a logo on the left and a navigation bar with tabs: Home, Select Files, Set Permissions (active), Add Watermarks, Event History, Published Files, Codes, Code List, and Personalized Files.

The 'Set Permissions' tab contains the following sections:

- Date selection:** Specify an absolute start and end date, or the number of days that the file can be viewed once it has been authorized.
 - Start/End dates: Start date: 01/01/2020, End date: 31/12/2050.
 - Expires after
- Document printing permissions:** If printing is permitted it is recommended that the Printing count is kept at Unlimited, and control of printing is set by specifying the total number of pages that are permitted to be printed.
 - Printing count: 0 (dropdown), Enable printing button.
 - Total pages count: 0 (dropdown), Disable printing button.
- Secured file type:** Choose DRMZ for most applications (standard encryption). Choose DRMX for desktop/laptop only usage with strongest possible encryption.
 - Secured file type:
 - DRMZ files (for cross platform working)
 - DRMX files (for PC/Mac only)
 - Disable screen capture
 - Self-authorizing DRMZ file
- Document viewing (count of views):** Number of views: <unlimited> (dropdown).

Notes: After creating DRMZ or DRMX files you will need to run our free Javelin for Windows software, and/or versions of Javelin for other platforms (obtainable from the main App Stores). When prompted for an authorization code use the free test code provided or a code or license file (for JavelinPro) created using the Codes tab or AdminApp. Always test files using Javelin or JavelinPro on Windows first. If you re-generate a DRMZ or DRMX file, having edited the source PDF or having changed the permission settings above, open the file in Javelin, select the Tools menu, Remove authorization option, and this will ensure your previous settings are cleared.

Buttons at the bottom: Help, Change Password, Save Settings, Order Services, Create Secure PDFs, Quit.

Footer: (c) Drumlin Security Ltd, 2020. <https://www.drumlinsecurity.com> info@drumlinsecurity.com

Set permissions – more details

Date controls - Start and end dates/Expires after: In most cases the Start Date will be today and the end date will be a date long off into the future (e.g. 1/1/2030), but any suitable start and end dates can be specified - there is now an option to specify NO EXPIRY DATE in which case the expiry date is automatically set 200 years forward! Files that have an absolute expiry date cannot be re-enabled - a new file must be issued with a later expiry date. The “Expires after” option allows you to specify that a document can be read for a specified number of days (for example, up to 999 days maximum) from the date the file is authorized, and then it will expire. This is effectively like a document loan or rental - it provides a means of allowing an end user a fixed amount of time to view the file. A file that has expired as a result of an “Expires after nnn days” can be renewed simply by provision of a new, or re-enabled, authorization code for that file, or a multiple usage code. Authorization codes do not control the expiry dates, but for Corporate/Pro users License files can be used to take precedence over the start/end date settings. **IMPORTANT NOTE:** The Javelin readers incorporate a number of checks to ensure that the system date on the end user device has not been tampered with (e.g. set back and then reset forwards).

Document viewing control - Number of Views: Set to unlimited viewing in most cases. Set to a number, e.g. 2, to permit viewing 2 times. Can be reset by re-authorizing a file after the available count has been used up.

Printing Controls - Printing Count: To disable all printing set to 0 or select the option selector Disable printing. In most cases set this value to 0 or to unlimited (which is then subject to the page count setting, **Total Print count**). **Total print count (Pages):** This option only applies if Printing Count is not set to 0 or disabled. It specifies the number of pages that may be printed overall (i.e. across all sessions of printing that are permitted). We recommend specifying this value as the number of pages in the document (or a little more) or a multiple of the number of pages for multiple copies or “unlimited”. See also the [Technical Notes](#) section.

Disable screen capture: Copying to the MS Windows clipboard is disabled as the default in Javelin for Windows and JavelinPro for Windows. Use of screen grabbing programs under MS Windows is disabled when the Disable screen capture option is selected - note that this can result in frustration for end users running standard Windows software, like OneNote, Evernote or similar packages, as these keep a screen capture module in the background even after the programs themselves have been closed. For additional protection use of Intelligent Watermarking is recommended, as this is the only protection available against misuse on most devices, especially those with hardware-based screen capture (e.g. most tablets and mobile phones).

Self-authorizing DRMZ file: this facility is only enabled for publishers who have chosen this licensed service option. It enables drmz files to be created that do not require authorization. As such it provides a mechanism to distribute secured files that cannot be saved in alternative formats, the contents cannot be copied, optionally time-expired (recommended), with or without watermarks and/or with or without printing enabled. The files can be duplicated as they do not have the added protection of online authorization, but are ideal for selected corporate, fieldworker and education sector environments.

Add Watermarks

Tab 4 is where optional dynamic watermarks can be specified. These can be on-screen (always in a fixed location at the foot of the viewable window) and/or on-print (with a number of selectable font attributes and position relative to the PDF page top left corner), or no such special watermark. Fields available for inclusion are shown on this form - e.g. %a (authcode), %l (device information) and %u (user details). See also the [Personalization](#) and [Advanced Watermarking](#) sections later in this document.

Drumlin Publisher

Drumlin Publisher: PDF Security Software

Home | Select Files | Set Permissions | **Add Watermarks** | Event History | Published Files | Codes | Code List | Personalized Files

Static (page-based text) watermarking: If required add static watermarks to your source PDFs prior to creating secure DRMZ or DRMX files. Note that such watermarks will appear on-screen and on-print (where printing is permitted).

Dynamic watermarking: Use this section to define the content of on-screen and on-print dynamic watermarks. This single line watermark can include static text and numbers, and dynamically loaded data (fields). Dynamic content is loaded when the document is viewed or printed. Dynamic fields are denoted by a % character followed by a letter, e.g. %a for the authorization code. On-screen window display of dynamic watermarks are placed on every screen window or page at the foot of the currently zoomed view. Recommended minimum format (c) %a %u - Available fields: %F filename, %M machine name, %C documentID, %U username, %l machineID, %D date, %T time, %a authorization code; and for Javelin3Pro only %N firstname, %L Lastname and %E email address. Tick the On-Screen and/or On-Print selectors below to enable these features.

Dynamic Watermark

Printing: Settings in this section only apply to on-print dynamic watermarks. On-print watermarks are positioned relative to the top left corner of the page (approximately), based on the page size of page 1 in the document. Specify the font size, color, opacity and position of on-print dynamic watermarks below.

Font size: Opacity [%]: Colour:

On-Print text direction: Vertical Horizontal Diagonal Angle in degrees:

Apply to pages: All Page range From: To:

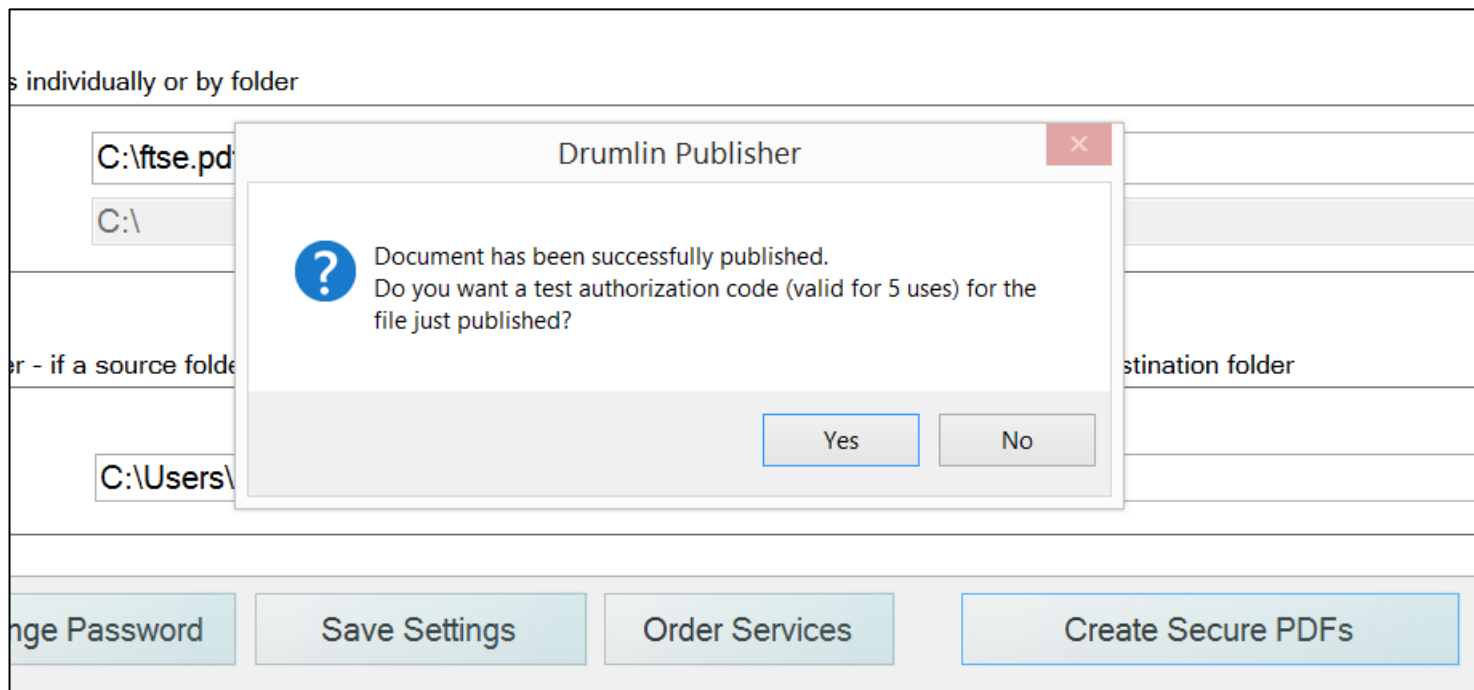
Offset on page from top left [mm]: Horizontal offset: Vertical offset:

Print watermark Screen watermark

(c) Drumlin Security Ltd, 2020 <https://www.drumlinsecurity.com> info@drumlinsecurity.com

Create Secure PDFs

Once the selection of file(s), permissions and any watermarking have been specified, the final steps in the process is to press the Create Secure PDFs button. If a single file has been selected for conversion the file will be created and saved in the Destination directory you specified earlier, and a free authorization code (for use on up to 5 devices) is provided in case you need this for testing. The screenshot below shows this - in general select the YES option and save the file to your local disk - it will simply be a text string that is specific to that file (defined by its DocID which is automatically assigned to it by our DRM service). If you have chosen multiple files or an entire folder of files for conversion, a free code will not be offered and you will need to use the Codes tab in DrumlinPublisher in order to create codes for testing and onward distribution to users/customers.



At this point the secure file creation process has been completed, and the files will be available in your Destination folder where they should be tested using Javelin3 for Windows (or Javelin3Pro for Windows) using an authorization code or license file - see the [Codes](#) section below for more details. If files are in .drmz format they can be viewed on multiple platforms, and again we strongly recommend that generated files are tested on all the target platforms before they are distributed.

Event History

This tab provides a sortable list of all file events generated using this application on this PC. To sort the list, click on the fieldname at the top of each column. Use the scroll bar at the foot of the grid to see additional details relating to the Event. Note that the initial default sort order is on the source PDF file name (Name column). For more details see the [Technical Notes](#) section.

Publ.Date	DocID	Files
11/05/2016 21:26	26664	C:\Users\michaeldesmith\Documents\WEEK 1 - 01.dmz
11/05/2016 21:26	26665	C:\Users\michaeldesmith\Documents\WEEK 1 - 02.dmz
11/05/2016 21:30	26664	C:\Users\michaeldesmith\Documents\WEEK 1 - 01.dmz
11/05/2016 21:30	26665	C:\Users\michaeldesmith\Documents\WEEK 1 - 02.dmz
11/05/2016 21:30	26666	C:\Users\michaeldesmith\Documents\WEEK 2 - 01.dmz
11/05/2016 21:30	26667	C:\Users\michaeldesmith\Documents\WEEK 2 - 02.dmz
11/05/2016 21:30	26668	C:\Users\michaeldesmith\Documents\WEEK 3 - 01.dmz
11/05/2016 21:30	26669	C:\Users\michaeldesmith\Documents\WEEK 3 - 02.dmz
11/05/2016 21:30	26670	C:\Users\michaeldesmith\Documents\WEEK 3 - 03.dmz
11/05/2016 21:30	26671	C:\Users\michaeldesmith\Documents\WEEK 4 - 01.dmz
11/05/2016 21:30	26672	C:\Users\michaeldesmith\Documents\WEEK 4 - 02.dmz
11/05/2016 21:30	26673	C:\Users\michaeldesmith\Documents\WEEK 5 - 01.dmz
11/05/2016 21:30	26674	C:\Users\michaeldesmith\Documents\WEEK 5 - 02.dmz
11/05/2016 21:30	26675	C:\Users\michaeldesmith\Documents\WEEK 6.dmz
12/05/2016 11:42	26679	C:\Users\michaeldesmith\Documents\vtse.dmz

Published Files

Note - this tab is updated from our DRM server whenever it is selected to ensure the latest data is displayed. When PDF files are published as secure versions in our drmz or drmx formats, data (not the files themselves) is exchanged with our DRM server and stored for future use. The Documents database table on our server holds this information and the current state of your available files on our DRM server can be viewed via the Published Files tab. The screenshot below shows a sample record which has been selected (highlighted in blue) by clicking on the record selector at the left-hand end of the record or double-clicking the record. A double-click or right-button mouse click will display four options: DRM Properties (displays details about the file permissioning etc.); Archive (removes record from list); change owner (if permitted); and Change Document Description (from the default which is the full file specification including directory location when published). The pop-up menu is illustrated below:

Home Select Files Set Permissions Add Watermarks Event History **Published Files** Codes

This section lists all PDFs published by currently logged-in user as stored within the Digital Rights Management (DRM) server. Items listed in the grid, and then use right mouse click on the record itself to view: DRM Properties - to view additional details; Archive - re-assigns owners change owner - re-assigns the document to another owner (if enabled). All columns in the table below can be sorted up or down by clicking edge.

DocID	DocName	DocDescription	PubDate
26784	ftse.pdf	C:\User\michaeldecsmith\Desktop\Drumlin\Testfiles\ftse.pdf	23/05/2016 12:44
26859	Invoice 2.pdf	C:\Use	2016\Invoice 2.pdf
26858	InvoicesDec2014 2.pdf	C:\Use	14 2.pdf
26857	InvoicesDec2014 3.pdf	C:\Use	14 3.pdf
26778	preview.pdf	C:\Use	LeighMartin\preview.pdf

Context menu options: DRM Properties, Archive, Change Owner, Change Document Description

The Archive option re-assigns the file to a special userID (it is not deleted from the database), with the result that it will no longer appear in your list of (active) documents. Archive files can be restored on request to our support team. Likewise, the Change Owner option is only available to publishers requesting this facility and who have multiple “publisher” registrations within their company. For example, a customer may have multiple editors/publishers, but may wish to re-assign all such files to a common userID for convenience. Finally, the Change Document Description option allows the default description (the file location) to be amended if required.

The DRM Properties option displays the basic DRM data stored relating to that particular file and is the same as the information displayed via the DRM Properties option within the Javelin readers. A sample screenshot for DocID 26772 is shown below

DocID	DocName	PubDate	CreatorID	OwnerID	StartDate	ExpiryDate
26772	Cells-HT-Assessment-GDL-update.pdf	19/05/2016 09:04	7150	7150	01/01/2016	01/01/2020
26771	Vide				01/01/2016	01/09/2016
26770	Sup				01/01/2016	01/09/2016
26769	Sup				01/01/2016	01/09/2016
26768	Star				01/01/2016	01/09/2016
26767	Star				01/01/2016	01/09/2016
26766	Neb				01/01/2016	01/09/2016
26765	Neb				01/01/2016	01/09/2016
26746	ABM				01/01/2016	01/01/2020
26745	ABM				01/01/2016	01/01/2020
26737	Digi				01/01/2016	01/09/2016
26735	Pair				01/01/2016	01/09/2016
26734	Mod				01/01/2016	01/09/2016
26730	3D Modeling and Printing 2016.ppt	15/05/2016 10:00	7150	7150	01/01/2016	01/09/2016
26729	Chefology DD and IE.pdf	15/05/2016 10:00	7150	7150	01/01/2016	01/09/2016

Properties ✕

Document ID

Start date

Expires after

Number of views

Printing count

Total print count

Disable screen capture

In the example illustrated the document selected (DocID 26772) has a start date of 1st Jan 2016, an overall end date of 1st Jan 2020, but is set to expire after 45 days from the date at which the user authorizes the file on their device - i.e. they have 6 weeks to view the document before it expires. The document in question is set with no limit on the number of times it can be viewed and no limit on the number of times or pages that can be printed.

Codes, Licenses and Usage Tracking

The Codes tab provides a range of functionality. For users of DrumlinPublisher who are not service subscribers or “bundle pack” customers, i.e. are simply using the software after initial registration, the functionality in the Codes tab is disabled. The screenshot below shows the Codes tab when accessed by a typical subscriber. You can now also specify No Expiry Date for codes in which case they are pre-set to expire in 200 years!

The screenshot shows the 'Codes' tab in the Drumlin Publisher software. The interface includes a navigation menu with tabs: Home, Select Files, Set Permissions, Add Watermarks, Event History, Published Files, Codes (selected), Code List, and Personalized Files. The 'Codes' tab displays a table of generated codes and a control panel on the left.

ID	Title	Description
26859	Invoice 2.pdf	C:\Users\michaeldesmith\Documents\Accounts\May20
26858	InvoicesDec2014 2.pdf	C:\Users\michaeldesmith\Documents\InvoicesDec2014
26857	InvoicesDec2014 3.pdf	C:\Users\michaeldesmith\Documents\InvoicesDec2014
26784	ftse.pdf	C:\Users\michaeldesmith\Desktop\Drumlin\Testfiles\fts
26778	preview.pdf	C:\Users\michaeldesmith\Documents\ClientProjects\Le

The control panel on the left includes the following options:

- Select Documents: Owned By: demo2016 [8029] (dropdown), Title From: (text box), To: (text box), Refresh (button), All (button)
- Select by document ID: Document ID: (text box), Find Document (button)
- Number of Generated Codes: 1 (spinner), Code Counter: 10 (spinner)
- Code(s) Expiration Date: 24/10/2025 (calendar icon)
- Generate AuthCodes for Selected Document(s) (button)
- Create License Files for Users (button)
- Manage Pro Users (button)

At the bottom of the window, there are buttons for Help, Change Password, Save Settings, Order Services, Create Secure PDFs, and Quit. The footer contains the copyright information: (c) Drumlin Security Ltd, 2020, the website URL <https://www.drumlinsecurity.com>, and the email address info@drumlinsecurity.com.

Select documents

Starting on the left-hand side are selectors that enable the list of documents in the grid shown to the right to be filtered if required. When first opened no documents are displayed in the grid. If the **Refresh** button is pressed then grid is populated with all the documents owned by the currently logged-in user. As with similar grids, the entries can be sorted by clicking on the title fields at the top of each column. Alternatively enter a specific DocID and press **Find document** to filter the results for that specific item, or select a title range (e.g. from A To C) and press the **Refresh** button to update the list in the grid. Use the **All** button to re-display all entries.

Generate Authorization codes

The button **Generate Authcodes for Select Document(s)** will create a text file containing a list of authorization codes for the currently selected document or documents (highlighted in blue in the grid) with the number of codes generated and usage count (Code counter) and code expiry date that you specify. Typically, you will generate a block of codes, e.g. 10 or 50 with a usage count of 1 (one device) or 2 (two devices) for one or more selected files. An example is shown below for 1 file selected, 5 codes each with at most 2 usages.

The screenshot shows the 'Codes' tab in the DrumlinPublisher application. The interface includes a navigation bar with tabs: Home, Select Files, Set Permissions, Add Watermarks, Event History, Published Files, Codes, and Personalized Files. Below the navigation bar, there are several input fields for document selection: 'Select Documents:', 'Owned By: demo2016 [8029]', 'Title From:', 'To:', 'Select by document ID:', and 'Document ID: 26784'. A 'Number of Generated Codes' spinner is set to 5, and a 'Code Counter' spinner is set to 2. The 'Code(s) Expiration Date' is set to 18/01/2022. A large button at the bottom reads 'Generate AuthCodes for Selected Document(s)'. On the right, a table displays document information:

DocID	DocName	DocDescription	PubDate	CreatorID
26784	ftse.pdf	C:\Users\michael...	23/05/2016 12:44	8029

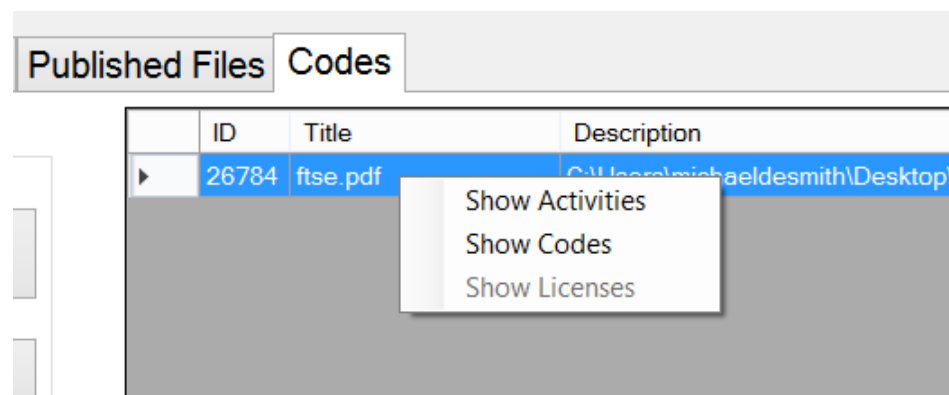
A 'CodeType' dialog box is open, asking 'You are about to generate 5 codes for 1 selected documents?'. It has two checkboxes: 'Generate DRMZ code(s)?' (checked) and 'Common Codes?' (unchecked). There are 'Cancel' and 'Generate TXT files' buttons.

Common codes

DrumlinPublisher supports the generation of "common codes" where it is desirable to issue a single code string to end users who will be using multiple documents (e.g. several modules that form part of a training course). For example, suppose that 4 secured documents are selected from the Documents list in the Codes tab, and each of these 4 files are to be issued with codes to 10 students. When generating the codes required, 10 would be selected in the field "Number of codes to be generated". Then when the codes are created a total of 40 codes will be generated, 10 for each of the 4 documents. Normally this would mean that each student would receive 4 code strings, all of which were different, one for each file they receive. However, if the option to generate "common codes" is ticked, 40 codes would still be generated but the code string for all 4 documents for the first student would all be the same, e.g. *abcdefghi* and likewise a different set for the second student, e.g. *hijklmnop* etc. - only one text string is needed to be sent to each student and this will work for all 4 documents they receive. When there are 30 students and 40 documents, 1200 codes would be generated but only 30 different codes would need to be issued, simplifying the end user experience greatly.

Tracking and reporting

The Codes tab provides access to additional information for a selected document. For example, if you right click or double-click a document in the list a pop-up menu is displayed, as illustrated below. From this you can then select to view the Activity history associated with that document, or the list of codes generated for that document with associated status information. For Corporate/Pro customers there may also be license files that have been issued for the selected document, in which case details of the licenses issued will be displayed. Examples of the first two items are shown in the subsequent screen shots. For quick searching and cross-document code listings, use the new [Codes List](#) tab.



Activities

Activity log data provides the main usage tracking facility - the extract below for the selected FTSE document illustrates the kind of information provided. Activity log data can be exported to a csv file for further analysis if so required. We can also provide special (bespoke) data queries on multiple documents by request. As with other grid displays, each column in the grid can be sorted, up or down, by clicking on the top bar of the grid - in the current example it is sorted by ActivityDate and the downward facing arrow on this field shows that is sorted with the most recent items first, going backward in time.

Activities for document 26784

ID	Description	ActivityDate	UserID	DocID	ActivityID	IPAddr	ProUserID	OrgID
438679	Authorization successful - UserID:-1 DocID:26784 Code:123456789 JM_1.00.90 [10.10.5 (14F1808)] MacBookPro11,1 SN:C2QPP006G971	11/08/2016 22:20	-1	26784	150	187.254.147.129	-1	-1
431245	Authorization successful - UserID:-1 DocID:26784 Code:123456789 JW_2.029 []	21/07/2016 10:37	-1	26784	150	101.160.0.108	-1	-1
421800	Authorization successful - ProUserID:403 OrgID:6 DocID:26784 Code:123456789 JW_2.030 []	29/06/2016 04:35	-1	26784	151	202.174.120.2	403	6
421798	Authorization - ProUserID:403 DocID:26784 Code:12345 (Wrong Authorization Code! -1) JW_2.030 []	29/06/2016 04:34	-1	26784	151	202.174.120.2	403	6
421797	AR - successfully removed authorization DocID:26784 Code:123456789	29/06/2016 04:33	-1	26784	157	202.174.120.2	-1	-1

Activities for document 21347

Activities for document 21347

ID	Description	ActivityDate	UserID
442759	Authorization successful - UserID:-1 DocID:21347 Code:123456789 JW_2.029 []	22/08/2016 20:44	2
440325	Authorization successful - UserID:-1 DocID:21347 Code:123456789 JIPAD_v02.000.000	18/08/2016 09:10	-1
395034	Authorization successful - UserID:-1 DocID:21347 Code:123456789 JW_2.029 []	28/04/2016 16:17	-1
392774	License generated by UserID:50 for 131. DocID:21347	22/04/2016 17:45	50
392773	AR - successfully removed authorization DocID:21347 Code:123456789	22/04/2016 17:44	-1
392765	Authorization successful - UserID:-1 DocID:21347 Code:123456789 JW_2.024 [v6.2.9200 [2]]	22/04/2016 17:35	-1
391272	Authorization successful - UserID:-1 DocID:21347 Code:123456789 JW_2.029 []	19/04/2016 17:48	-1
386121	Authorization successful - UserID:-1 DocID:21347 Code:123456789 JA v.1.00.55 [armeabi-v7a gtelwfi samsung SM-T560 gtelwifoo]	11/04/2016 15:45	-1
385948	Authorization successful - UserID:-1 DocID:21347 Code:123456789 JA v.1.00.54 [armeabi-v7a gtelwfi samsung SM-T560 gtelwifoo]	11/04/2016 11:25	-1
385946	Authorization - UserID:-1 DocID:21347 Code:123456 (Wrong Authorization Code! -1) JA v.1.00.54 [armeabi-v7a gtelwfi samsung SM-T560 gtelwifoo]	11/04/2016 11:25	-1
385887	Authorization successful - UserID:-1 DocID:21347 Code:123456789 JW_2.029 []	11/04/2016 09:41	-1
385885	AR - successfully removed authorization DocID:21347 Code:123456789	11/04/2016 09:41	-1
385881	Authorization successful - UserID:-1 DocID:21347 Code:123456789 JW_2.029 []	11/04/2016 09:29	-1
385879	AR - successfully removed authorization DocID:21347 Code:123456789	11/04/2016 09:29	-1
385877	Authorization successful - UserID:-1 DocID:21347 Code:123456789 JW_2.029 []	11/04/2016 09:23	-1
384135	Authorization successful - UserID:-1 DocID:21347 Code:123456789 JW_2.029 [Windows 7 (x64)]	05/04/2016 14:12	-1
370857	Authorization successful - UserID:-1 DocID:21347 Code:123456789 JW_2.003 [v6.2.9200 [2]]	07/03/2016 16:37	-1
363504	Authorization successful - UserID:-1 DocID:21347 Code:123456789 JW_2.024 [v6.2.9200 [2]]	24/02/2016 05:06	-1
363409	Authorization successful - UserID:-1 DocID:21347 Code:123456789 JW_2.024 [v6.2.9200 [2]]	24/02/2016 01:12	-1
362778	Authorization successful - UserID:-1 DocID:21347 Code:123456789 JW_2.024 [v6.2.9200 [2]]	23/02/2016 09:05	-1
354925	License generated by UserID:50 for 244. DocID:21347	08/02/2016 09:51	50
354924	License generated by UserID:50 for 244. DocID:21347	08/02/2016 09:50	50
352454	Authorization successful - UserID:-1 DocID:21347 Code:123456789 JW_2.024 [v6.2.9200 [2]]	31/01/2016 22:30	-1

However, sometimes it is useful to be able to search through the main Description field, for example looking for all activity that has occurred for a particular code, or maybe for a particular type of end user device. This can now be achieved simply and speedily using the Filter Description: field at the foot of the form, as illustrated below. Simply enter the text you would like the software to use to filter the Description field and press the Filter button and the relevant subset of records will be displayed. Use the Display All button to reset this filter. A similar facility is provided on the Codes Summary form (see next sub-section).

Export to CSV Filter Description: Filter Display All OK

Codes and license files

If the Show Codes option is selected a list of the codes for the selected document is displayed - in the first example below two such codes are shown. Where an initial usage count is included, it indicates that the code was generated with that usage count and the UsedStatus column shows the currently available count. In the first entry below the initial count was 5 (it was a free “test” code) and the current UsedStatus is 3, so we can tell it has been used on two devices/twice in total. The second entry is the code we use for demos and was created manually. It has a current usage count of 492 and a code of 123456789. The Valid For field can be ignored; the Expiry Date field refers to the date at which the code will no longer be usable, unless that date is reset, even if there are still usage available in the UsedStatus field. This field is set for 3 years from the date the code was created by default, but you can specify your own preferred expiry period or No Expiry Date.

Codes for document 26784

	ID	CreateDate	PublisherID	DocID	UsedStatus	StatusChangeDate	AuthCode	ValidFor	ExpiryDate	InitialUsageCount
▶	530037	23/05/2016 12:44	8029	26784	3	23/05/2016 15:17	gcae27xd7	0	23/05/2019 12:44	5
	530280	25/05/2016 21:54	8029	26784	492	11/08/2016 22:20	123456789	0	25/05/2019 21:54	

If you select a particular record using the record selector at the left-hand end of an entry and then right click with the mouse (double-clicking an entry will have the same effect), a pop-up menu is displayed to allow you to reset a code (Set Counter from any value to 0 or from any value to the maximum value enabled for you, typically 5) or to delete a code. You can also reset the expiration date and copy the selected code to the clipboard. In general, we recommend that to disable a code simple reset it to 0 for its UsedStatus, as this will keep the code but make it unavailable for further use, e.g. to disable further use of a code. This step is slightly different from the Enable codes/Disable codes facility shown, as discussed below. A new facility is provided to allow you to amend an existing code to a different/preferred text string, for example an easily remembered or personalized string.

Codes for document 26784

	ID	CreateDate	PublisherID	DocID	UsedStatus	StatusChangeDate	AuthCode	ValidFor	ExpiryDate	InitialUsageCount	Status
▶	560962	28/06/2016 12:18	7150	26784	0	28/06/2016 12:22	12345-StudentID	0	28/06/2019 12:18		1
	530037	23/05/2016				23/05/2016 15:17	gcae27xd7	0	23/05/2019 12:44	5	1
	572489	30/08/2016				30/08/2016 09:20	zsj2x2fzu	0	30/08/2019 09:20	3	1
	572490	30/08/2016				30/08/2016 09:20	bz3rgdwht	0	30/08/2019 09:20	3	1
	572491	30/08/2016				30/08/2016 09:20	hdfmxutp	0	30/08/2019 09:20	3	1
	572492	30/08/2016				30/08/2016 09:20	76j9b6q3u	0	30/08/2019 09:20	3	1
	572496	30/08/2016				30/08/2016 09:52	w2dx6ah86	0	30/08/2019 09:52	2	1
	530280	25/05/2016				07/03/2021 10:07	123456789	0	25/05/2019 21:54		1

Controlling code and document usage

Codes have a usage count (also referred to as a counter value or UsedStatus), as noted above. If a code is selected and the Set Counter option is used to change its value to 0, the UsedStatus of the code will show a zero value, and the code cannot be used again. However, if the option Disable Code(s) is used, the code details will remain unchanged but its “Status” will change from 1, as shown on the right-hand end of the above screenshot, to 0, meaning that the code is now marked as disabled. When an end user runs Javelin3 readers (current versions) and tries to use the code or tries to open a file for which the code has been used to authorize access to the file, the reader software will automatically disable access and warn the user that the code has been disabled - use this facility with care! Log entries are made to the Activity Log so that the publisher is aware of the events. A disabled code can be Enabled, so for example, this could be a temporary hold on access pending a review of usage or for a subscription service (pending renewal). After a code has been disabled, the end user will only be able to view the document again if the code is re-enabled and has a UsedStatus of 1 or more, or if they are provided with a new code for that document. Special facilities also exist for Javelin3Pro “corporate” services to enable/disable documents and registered users.

Code search

DrumlinPublisher includes a code search facility on the Codes list form, so that specific codes can be quickly located for a document where large numbers of codes for that document have been created. Sub-strings of a code can be entered, e.g. to see all codes with 9tk in them for example. For quick searching and cross-document code listings, use the new [Codes List](#) tab.

License files

Licences are special files that accompany secured PDF documents and allow the file to be opened without requiring an online connection. Licences currently only apply to JavelinPro registered users as they include encoded details of the end user registration data. They are created by publishers who have the necessary privilege for such license creation. In the example above for user demo2016, this facility is disabled, so no button is provided for License file creation. License files can also be generated by special arrangement for standard DRM service subscribers on request (contact us for more details). If a publisher has permission to create and view License files, details of license files that have been created for specific documents can be displayed. A sample is shown below:

Licenses for document 26580

	ID	StartDate	EndDate	UserID	DateCreated	CreatorID	DocName	FirstName	LastName	DocID	deviceId
▶	76	23/08/2016	31/12/2016 23:59	131	23/08/2016 17:01	50	SalesReportSummary.pdf	mike	de Smith	26580	00260-00405-10

Code List tab

A new facility in v1.00.77 and later is the Code List tab. This provides a cross-document code search and list facility. If the selection/search fields are left blank and the Display All Codes button is pressed, all codes generated by the current user will be listed (up to 15000 max). As with other grid listings, the grid column titles can be clicked to sort on that column, and the entries can be double-clicked to change the entries, e.g. for code resetting or disabling. Individual codes may be searched for, and all codes for a specific DocID can be listed and/or filtered and details exported if required.

Drumlin Publisher: PDF Security Software

Home Select Files Set Permissions Add Watermarks Event History Published Files Codes Code List Personalized Files

Code Search Display All Codes

Document ID Search

ID	CreateDate	PublisherID	DocID	UsedStatus	StatusChangeDate	AuthCode	ValidFor	ExpiryDate	InitialUsageCount	Status
867519	01/06/2020 09:48	50	68591	981	12/06/2020 07:16	abcabcabc	0	01/06/2030 09:48	5	1

Export to CSV Code Filter: Filter Display All Count: 1

Personalization (stamping)

Personalization is a special facility that creates multiple secure copies of a single input PDF file, each uniquely dynamically watermarked and each uniquely named. This facility is a licensed option and is only enabled for subscribers with the appropriate permissioning. The personalization procedure is quick, flexible and can generate a large number of personalized files from a single input PDF. The screenshot below shows the Personalization tab. It becomes “active” when the Enable personalized files option is ticked. When this option is ticked, the Browse button can be used to select a text file containing details for personalizing the output secured files. As soon as a suitable file of names is selected it is loaded into a grid for review and/or editing. Full details of using this facility are provided on the next page.

Drumlin Publisher: PDF Security Software

Home | Select Files | Set Permissions | Add Watermarks | Event History | Published Files | Codes | **Personalized Files**

Use this tab to create a set of DRMZ files, each personalized with watermark text based on an input comma separated value (CSV) text file. This CSV file can contain multiple lines (one per output document) of up to three separate fields. These fields can be included in the dynamic watermark when the file is viewed and/or printed. The fields are defined using the identifiers %1, %2, %3. These fields can be combined in the watermark with standard dynamic fields such as %a and %F using the Watermark tab.

The steps are as follows:

1. Check the enable personalized file creation option is ticked
2. Select a single file to convert to secure DRMZ or DRMX format on the Select Files tab
3. Select the destination folder for the personalized output files on the Select Files tab
4. Specify your dynamic stamping watermark, e.g. (c) %1 %2 %3 %a on the Add Watermarks tab
5. Select the CSV file, below, containing the data to be used for each of the personalized output files

Enable Personalized Files Select CSV File: C:\Users\michaeldesmith\Desktop\DrumlinTestfiles\name.csv **Browse** New Save CSV File

Field 1	Field 2	Field 3
James cameron	james@cameron.com	ABC Ltd
Bob Hope	bob@hope.com	DEF Ltd
Keith Floyd	keith.floyd@kfloyd.com	Chef
Test user	joh@john.com	Porcupine
*		

Create Code List Usage Count: 1

Help | Change Password | Save Settings | Order Services | Create Secure PDFs | Quit

(c) Drumlin Security Ltd, 2017 <https://www.drumlinsecurity.com> info@drumlinsecurity.com

Select CSV file (list of names)

This is a list containing up to three, comma separated, text entries per line, e.g. names.txt or names.csv - the first entry (Field 1) on each line should be the target user name, and in the example shown the user's email address and company name provide Fields 2 and 3, of the format as shown below:

```
James cameron, james@cameron.com,ABC Ltd  
Bob Hope, bob@hope.com,DEF Ltd  
... etc.
```

The resulting generated secured PDF files will use these fields to create personalized versions of the source PDF file. For example, if the source PDF was the file ftse.pdf, the first two output secured files would be [ftse_James cameron.drmz](#) and [ftse_Bob Hope.drmz](#). Each file will include an on-screen and/or on-print watermark, identifying the individual based on the details in this list. The watermarks are included using the Watermark tab, with fields 1, 2 and 3 being identified using the placeholders %1, %2 and %3. More details on specifying the watermarks is provided further down in this section. The %| (percent symbol and vertical bar) can be used within a watermark to force a new line, so that a long watermark can be split across more than one line.

As soon as the CSV file is selected the entries are loaded into the grid area, for checking. This is actually an editable grid, so minor errors can be edited in the grid and then the **Save csv** file button will be available so the entries can be saved in their amended form. Indeed, a suitable file can be directly entered into the grid by using the **New** button, and then saving the file, so it provides for direct entry of the details if required. Any additions/changes must be saved in order to be sure they will be used. Finally, below the grid there are options to automatically create authorization codes and to set the counter for these codes. So the steps are:

- Login to DrumlinPublisher as a user enabled for access to the personalization facility
- Select a single file from the Select Files tab to be used as the source PDF when personalized files are generated and specify your output folder on this Select Files tab
- Specify the watermark required, including at least the %1 place marker entry (see further below)
- Select the personalization tab and tick the boxes for creating such files and the codes for these
- Select the file of NN names required - note that if held in an Excel spreadsheet or database etc. then these can just be exported to a csv file ready for loading into this tab. Files should ideally have an extension of .csv or .txt
- Check the names and other settings, and if all is OK, press the Create Secured PDFs button

A set of NN files will then be generated and output to your selected output folder, together with a list of codes with associated details of which document each relates to. A sample output codes list is shown below:

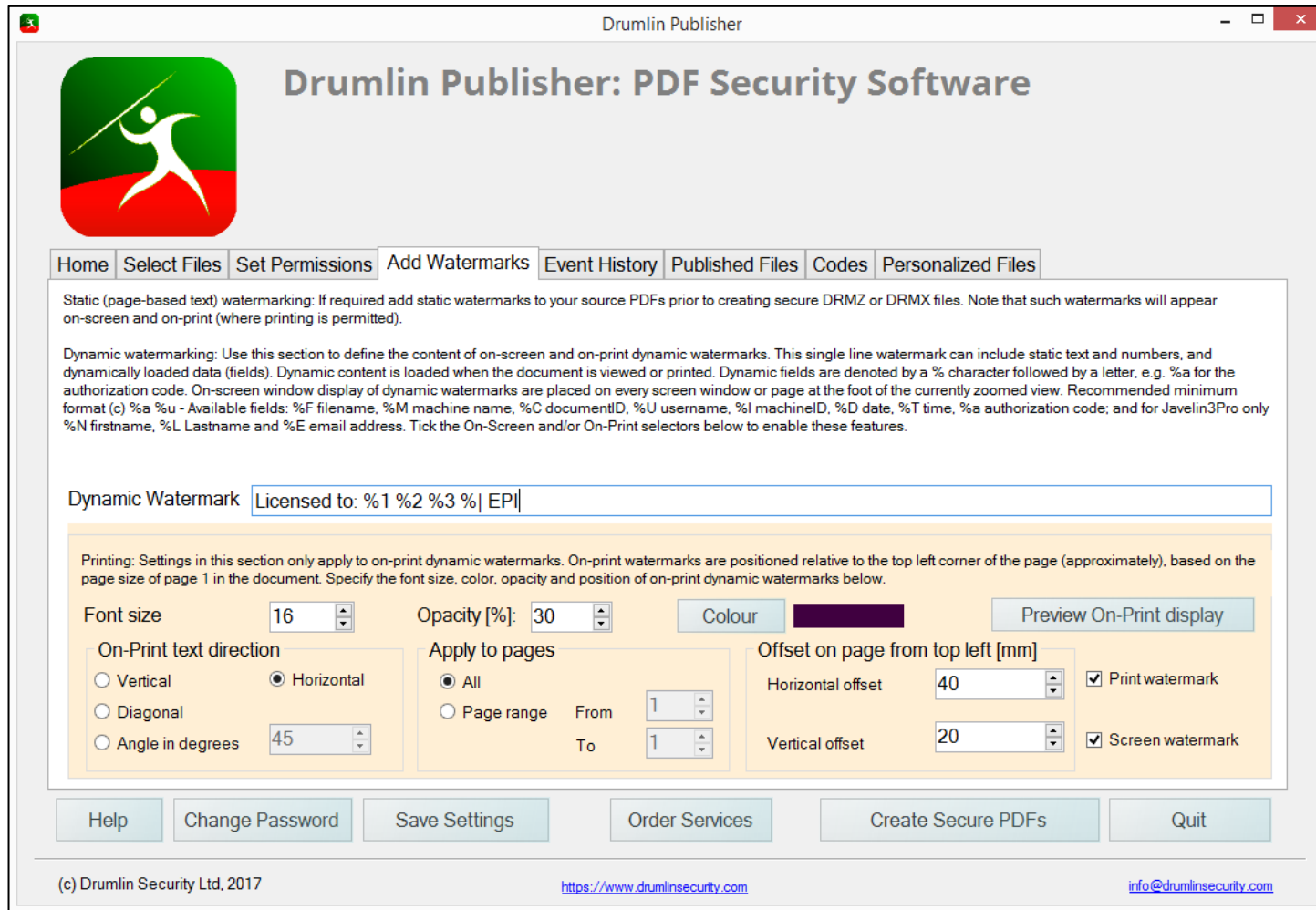
```
James cameron, ftse_James cameron.drmz, gj82b6xx9  
Bob Hope, ftse_Bob Hope.drmz, h386ezmpm  
... etc.
```

As can be seen, it is again in csv format for easy loading into Excel etc. it identifies the person, the file that has been generated specifically for them, plus the code created uniquely for them (the counter for the code has been pre-defined). The resulting files generated automatically consists of one file for each customer/end user/student in the list plus a text file of codes for these individuals.

The output files all have the same DocID, so each retains the same DocID as any file generated from that particular source PDF. The way it works is by replacing the placeholder fields, i.e. fields like %1, %2 etc. with the text in the list of names, so in a sense the result is essentially a static watermark element, just as if the name had been manually typed into the dynamic watermark in the same way as, for example, one might include the text: "Licensed to:" as part of the dynamic watermark. Because the personalization is implemented in this way it in this way it will work on all technology platforms, whatever the version of Javelin or JavelinPro is used. Furthermore, because each file is uniquely named, activity log data that is available via the DRM server identifies the activities of the named individual at each step of the process.

Advanced Watermarking

The watermark screenshot below illustrates the kind of entry that would be included in the watermark when generating personalized files. In this example it includes four new elements: three are “placeholders”: %1 %2 and %3 - these correspond to the 3 fields in the list of names in the Personalization csv file. Also shown in the watermark example is an entry of the form: %| (% and vertical bar). This is a new special entry that indicates that there should be a new line at this point, i.e. Javelin3/Javelin3Pro software supports two line watermarks if required.



Command line (CLI) operation – automation

For many publishers interactive use of DrumlinPublisher provides all the functionality that is needed. However, there are situations where it is desirable to generate a secure file and a code or codes for that file, without running DrumlinPublisher in interactive mode - for example, in order to create a secure file and code for that file dynamically, in response to an order or as part of an automated document processing operation. To enable this, DrumlinPublisher provides a command line interface. This can be driven from a batch file or programmatically. In order to use the facility, you will need to run DrumlinPublisher interactively to start with: select the various default settings you require (those relating to permissions, Watermarks and file type) and use the Save Settings option to save these details. The saved settings are read as part of the command line processing and used to define the permissions, watermarking and type of file (drmz or drmx) that is generated. Optionally some of the settings may be specified in the command line, as explained below:

The command line takes parameters in the format `drumlinpublisher <command letter>:details` where the parameters are as shown below - note that filenames and watermark strings should be enclosed within quote marks:

U:username
 P:password
 I:input PDF file
 O:output protected file (optional – it must be possible to write to the output folder specified otherwise an error message is issued)
 C:code file (optional)
 N:number of codes
 G:code usage
 X run in “silent” mode (no console messages issued - all text will be redirected to DrumlinSilent.log file in %APPDATA%\DrumlinSecurity\DrumlinPublisher\logs directory)
 S: start date, e.g. S:2020-06-25 or S:06/25/2020
 E: end date
 A: expires after (overrides end date)
 W: watermark text

Examples

```
drumlinpublisher U:harry P:mypass "I:c:\my folder\myfile.pdf" N:8 G:2
```

will generate 8 codes for protected file "myfile.drmz" or "myfile.drmx" (depending on the saved settings within DrumlinPublisher). Each code will have a usage count of 2, i.e. codes provided to the end user for two devices. Codes will be in file C:\my folder\myfile-code.txt"

```
drumlinpublisher U:drumlinsecurity P:xxxxxxx I:C:\Users\ drumlinsecurity\Desktop\Drumlin\Testfiles\ftse.pdf  

O:C:\Users\drumlinsecurity\Desktop\Drumlin\Testfiles\ftse-testing N:2 G:2
```


will generate 2 codes with 2 usages for the file ftse.pdf and name the output file ftse-testing.drmz (assuming the default filetype has been set as drmz).

When the program is run in this way, for example via a batch file, it opens a console window and issues responses as it logs in, generates the output file and creates the codes file. Note that if exactly the same command is run a second time it will create a backup copy of the drmz or drmx file and the codes file in the same directory and generate a new drmz or drmx file and code file, as appropriate.

Technical notes

- DrumlinPublisher provides a means of encrypting and controlling access to standard PDF files. By “standard” we refer to PDF files that comply with PDF 1.6 specification or earlier, and do not include embedded media or special code (e.g. Adobe-specific facilities such as embedded video or audio or 3D models). PDF files should not have Adobe-style security enabled and ideally should ensure that all hyperlinks are explicit (i.e. a link to an external website or email address are specified explicitly rather than simply displaying a text string, as these will not result in a link be activated - most PDF creation software will ensure such links are correctly specified, but tools exist in Adobe Acrobat etc. to convert implicit URLs to explicit URLs if required). For larger documents we also recommend that they include a navigation tree - also referred to as a contents list, bookmark list or “outline” (the latter is the terminology used by Apple). Navigation trees can be generated automatically when the PDF file is created from applications such as Word and InDesign. Ideally filenames should avoid using spaces or special characters, as these may cause problems when hosted on web servers for downloading
- The username/password login connects via a secure https:// connection to our default DRM server, <https://www.drumlinsecurity.co.uk> so this login process requires internet access to the server. Logged in users can create secure files, and a limited number of free codes for testing will be made available, even if you are not a subscriber to the DRM service. To obtain more codes or to create codes and track document usage, you will need to subscribe to the DRM service. For bespoke projects and dedicated private DRM server licensees the selected DRM server may be amended - selection is by clicking on the default servername in the registration and/or login forms. The server details are stored in the Appdata folder for DrumlinPublisher, settings.cfg file, so may be edited here if required. Note that all encrypted PDF files will be server-specific, and likewise for all aspects of the DRM service (user registrations, codes, licenses, tracking data etc.)
- The buttons labelled Check for updates, Order services, Help and View License all currently link to our main website. Updating is currently a manual process - simply download the latest kit and run the installation process to update the software version. The Software Version and Date are provided on the Home screen, lower left
- Select files tab: when using the select files facility you can select single or multiple files. To select multiple files uses the Windows standard multi-file selection facilities enabled using the Ctrl key + mouse or the SHIFT key plus mouse. Free test codes are only issued

when a single file is selected and secure file created, and a quota applies to these free test codes. If your quota expires no free code will be offered - you can contact us to re-enable this facility if you are a current service customer (e.g. a subscriber to the DRM service)

- Set permissions tab: if you enable printing we recommend you leave the number of times to print as “unlimited” and specify the total number of pages that can be printed, e.g. for a 100 page document, printable 2x, specify this is 200 or 250 pages (the higher amount allows for a few printing errors, e.g. paper outage, ink outage, paper jams etc.). Note that all printing is restricted to a pre-defined list of valid printers/manufacturers (specified as “relaxed printing” in earlier versions of the Drumlin software) and printing to non-physical devices such as PDF writers and Image writers is not permitted. Printing is only supported for MS Windows and Mac OSX, not for mobile devices
- Event history: The event history file is kept locally in the APPDATA folder on your PC, typically somewhere like: C:\Users\\AppData\Roaming\DrumlinSecurity\DrumlinPublisher in a file called PublishingHistory.csv - you can open this file in Excel or a text editor if you wish, to remove old entries and/or search for items. If you have logged in with more than one username/password then all events will be included here, whereas in the Published files tab only those files recorded on the central DRM database for the currently logged in user are displayed. The event log file shows both the source PDF filename and the name you used to save the drmz or drmx file. Note also - if you re-generate a drmz file from the same source PDF (even if you have updated the contents of the PDF file) the software will re-use the same DocID as in the original publication, even if you rename the output file. If you want to ensure the output file has a different DocID then rename the source PDF, e.g. from myfile.pdf to myfile1.pdf
- The APPDATA folder mentioned above also contains a settings.cfg file and a detailed log file in the sub-directory \log
- Once a secured file has been created, use a test code (free) to test the file or files using Javelin3 for Windows, and ideally using Javelin3 for Mac, Javelin for iOS and Javelin3 for Android if cross-platform use is planned. To check how a file will look within Javelin readers you can also simply open the original PDF using Javelin/Javelin3, i.e. it is not necessary to create a secure file first - the display and core functionality available is the same for both standard PDFs and our encrypted format PDFs. To check the security settings for a file when open in Javelin, select the File menu, Properties option, and view the PDF and DRM properties tabs. You can also check the Published files tab in DrumlinPublisher to see what information relating to a file is stored on our server (see the Published files section above for details)
- If you re-publish an existing PDF using the same source PDF filename and the same logged in username, DrumlinPublisher will generate the updated file with the same DocID as was used previously. If you have tested the earlier file using Javelin for Windows or Javelin for Mac, open it and use the Remove authorization option to ensure that stored information on the PC or Mac are removed before you re-test. Occasionally it is useful to ask end users to do this, for example if you update the permissions on a file you have already issued and wish them to have the changed details (e.g. a new end date or different print settings). After using the Remove authorization facility the file will need to be re-authorized using a new code or the same code as before if enabled (usage count/counter value >0).

- DRMX files involve a different encryption process from DRMZ files. If you re-generate a DRMX file with the same source filename and same username logged in, it will overwrite the previous encryption data relating to that file on our DRM server. This means that anyone trying to authorize a PREVIOUS version of the file will not be able to do so and will need the latest version in order to view the file. If they have already authorized the previous version this is not a problem. This highlights the need for care when updating DRMX files, especially if large numbers of these files have been pre-generated and issued on portable media such as USB drives or SD cards or CDs etc. If this is the case, then we recommend you rename the source file, e.g. as <sourcefilename>1.pdf and generate the new updated file from the new filename, as this will definitely have a new DocID and not interfere with any previously generated version