VITRIUM.COM

Vitrium Security Administrator Manual

Version 9.x.x
June 2021

Table of Contents

About Vitrium Security

Vitrium Security is a content protection and digital rights management (DRM) software solution. Trusted by companies around the world, and accessed by over a million users, Vitrium Security limits the risk of your content being copied, leaked, shared, or stolen.

Supported Formats

IMPORTANT NOTE: Vitrium Security is designed to protect content, therefore, content cannot be edited.

SUPPORTED INPUT FORMATS

Upload and protect files directly within the application or via APIs (requires Enterprise Edition):

Documents	**Images**	**Videos**[1]	**Audio**[1]
PDF	JPG	MOV	WAV
Word	PNG	MP4	MP3
Excel	GIF *(except animated GIFs)*	WMV	AAC
PowerPoint	TIFF	AVI	FLAC
CSV	BMP	FLV	AC3
RTF		MKV	AIFF
TXT			OGG
OpenOffice formats			M4A

SECURED FILE FORMATS

Vitrium then converts these original formats into two different secured output formats:

1. **Secure Web Viewer** format that can be opened in a web browser on any device

2. **Protected PDF File** that can be opened with Adobe Acrobat Reader, Adobe Acrobat Pro, or Adobe PDF-XChange (desktop versions only)

Distribution Methods

Depending on which edition is selected, Vitrium has a variety of different options for you to choose from:

- Via email with web links and/or PDF attachments
- Via your website
- Via a file sharing program
- Via secure client portal
- Via a third-party system[2]

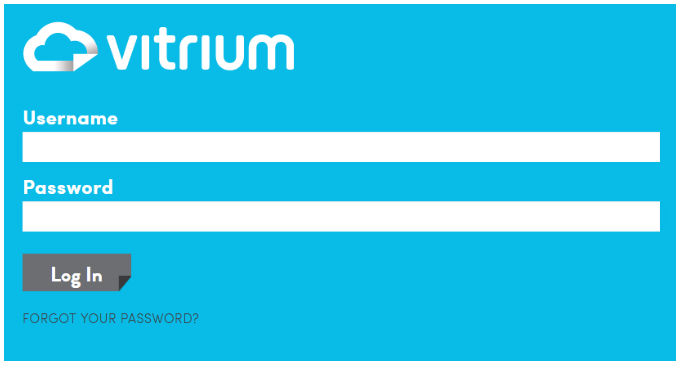
[1] To protect video or formats, you will need to have video and audio enabled on your account. If it is not enabled, please contact a Vitrium representative as there is an additional cost to add video or audio protection to your account.

[2] Third-party systems can include a content management system (CMS), document management system (DMS), customer relationship management (CRM) system, learning management system (LMS), association management system (AMS), eCommerce system, or more.

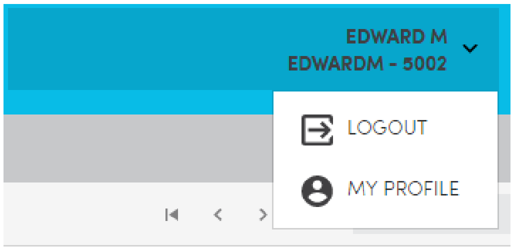
Logging In and Out of Vitrium

You will require Internet access on a Windows or Mac operating system.

1. **To LOG IN**, open a web browser (Chrome, Firefox, Edge, Safari, Internet Explorer) and bookmark this URL:
    a. For US-hosted customers: https://security.vitrium.com/
    b. For Canadian-hosted customers: https://security-ca.vitrium.com/
    c. For Installed customers: you will have a custom domain to log into and will need to check with your Vitrium system administrator
2. Enter your Username and Password, then click Log In

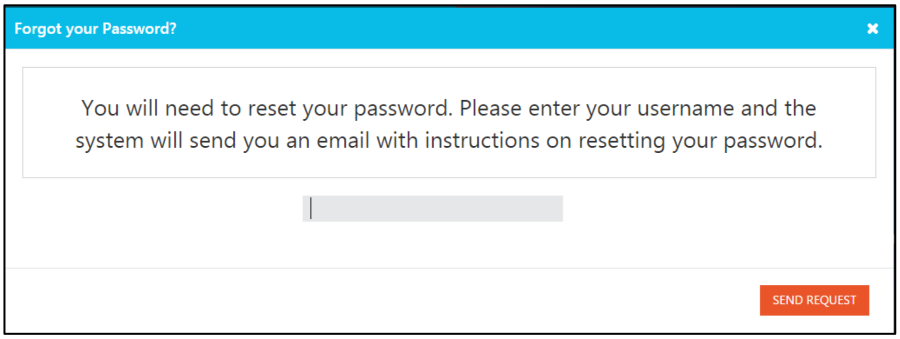


3. **To LOG OUT**, click on the arrow beside your name at the top right corner of your screen and click *LOGOUT*



If you have **forgotten your password:**

1. From the login screen, click 'Forgot Password?' and this window will open:



You will need to reset your password. Please enter your username and the system will send you an email with instructions on resetting your password.

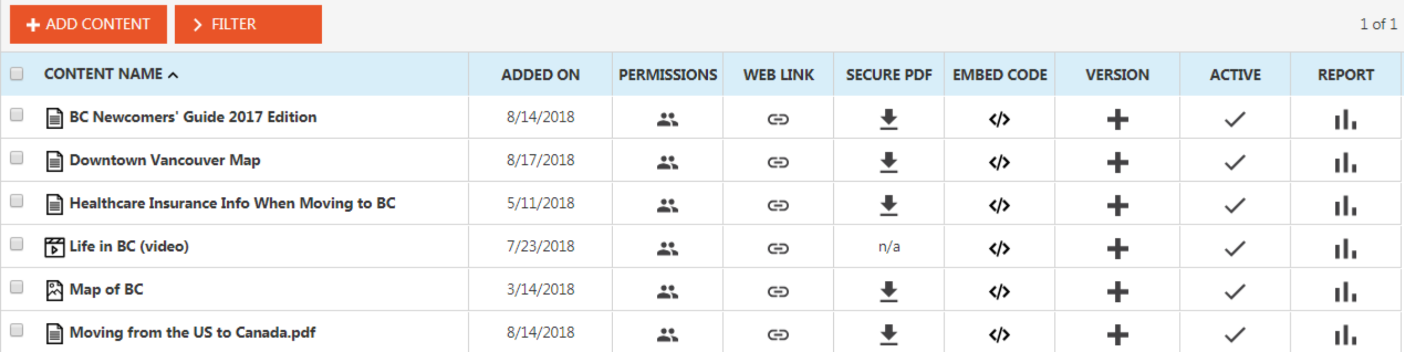
2. Enter your Username and click the 'Send Request' button
3. Check your email and click the password reset link in that email
4. Type in your new password and again to confirm, then click 'Set New Password' to save your changes
5. Log in with your new password

1.0 CONTENT TAB

1.1 Overview

The Content tab is the primary place where you will manage your files and folders. This tab has 3 main sections:

1. **FILES** (or **CONTENT**) section in the middle

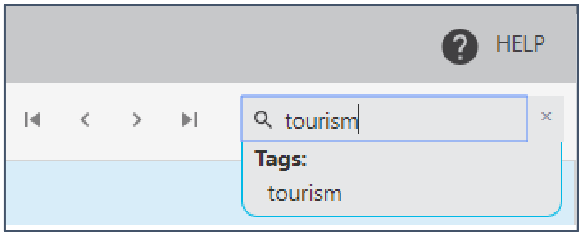


□	CONTENT NAME ^	ADDED ON	PERMISSIONS	WEB LINK	SECURE PDF	EMBED CODE	VERSION	ACTIVE	REPORT
□	BC Newcomers' Guide 2017 Edition	8/14/2018	👥	🔗	⬇	</>	+	✓	📊
□	Downtown Vancouver Map	8/17/2018	👥	🔗	⬇	</>	+	✓	📊
□	Healthcare Insurance Info When Moving to BC	5/11/2018	👥	🔗	⬇	</>	+	✓	📊
□	Life in BC (video)	7/23/2018	👥	🔗	n/a	</>	+	✓	📊
□	Map of BC	3/14/2018	👥	🔗	⬇	</>	+	✓	📊
□	Moving from the US to Canada.pdf	8/14/2018	👥	🔗	⬇	</>	+	✓	📊

2. **FOLDERS** section on the left-hand side – refer to *Section 1.8 Using Folders* for more details but one important note to be aware of is the Search bar in this section is folder searches, not file searches.

3. **ADD CONTENT, SEARCH** and **FILTER** section along the top – the ADD CONTENT function is described in the following section.

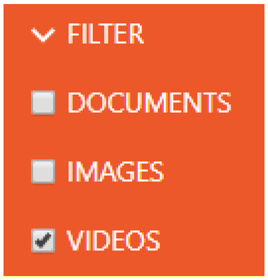
   The SEARCH function at the top right-hand side allows you to search for a FILE NAME or a TAG. A 'tag' is a meta keyword that you would add when uploading and protecting your content.



🔍 tourism

Tags:
tourism

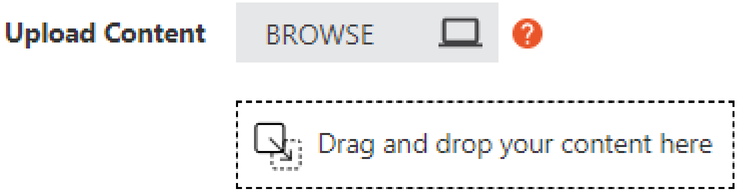
The FILTER function at the top left-hand side allows you to filter the content by their type – DOCUMENT or IMAGE or VIDEO (if video is enabled on your account).



⌄ FILTER
□ DOCUMENTS
□ IMAGES
☑ VIDEOS

1.2 Protecting Content

1. Click the **+ ADD CONTENT** button and the “Add Content” box appears
2. ***Upload Content:*** you can upload content (as a single file or multiple files) via two methods:
    a. Click BROWSE and select your file(s) from your computer or a network
    b. Drag and drop your files from anywhere onto this screen



IMPORTANT NOTE: if you select multiple files to upload, they must be all documents, or all images, or all videos. You cannot mix different types of content since they have different Content Settings that apply. Click here to view the list of supported input formats.

3. ***Content Settings:*** choose the default setting or another Content Setting that you have set up (refer to section 5.2 for more details on creating Content Settings)
4. ***Tags:*** enter any Tags that you wish to apply to the content – tags are keywords or other meta data you wish to use to define your content so you can search for it more easily in the Content tab, or users can search for tags in the user portal (if the ‘Portal’ has been enabled)
5. You may complete the process here by clicking on *Save & Exit*, or continue to the Advanced Options and Permissions.

ADVANCED OPTIONS TAB

6. There are additional advanced options that you may wish to apply to your content such as:

For Documents & Images:

a. ***Content Name:*** you can enter a different file name if you wish to change it from the original
b. ***Pages to Leave Unprotected:*** this applies to the protected PDF file only (not the web version); it allows you to leave specific pages in your document unprotected – for example, the title page and table of contents or an executive summary
c. ***Disable Web Viewer:*** allow you to disable the access to the secured web link, and instead, focus on the secured PDF version of your secured document(s).
d. ***Notify User When New Version is Available:*** the default is always checked so end users will always be notified when there is a new version (or even an update made) to the original file that was uploaded
e. ***External Key:*** this option is available to Enterprise customers only; it allows you to store your own ID for your own document management, content management, CRM or other system

For Videos:

a. ***Content Name:*** you can enter a different file name if you wish to change it from the original
b. ***Upload Thumbnail:*** you can add a thumbnail image as the preview image in the video player.
c. ***External Key:*** It allows you to store your own ID for your own content management system.

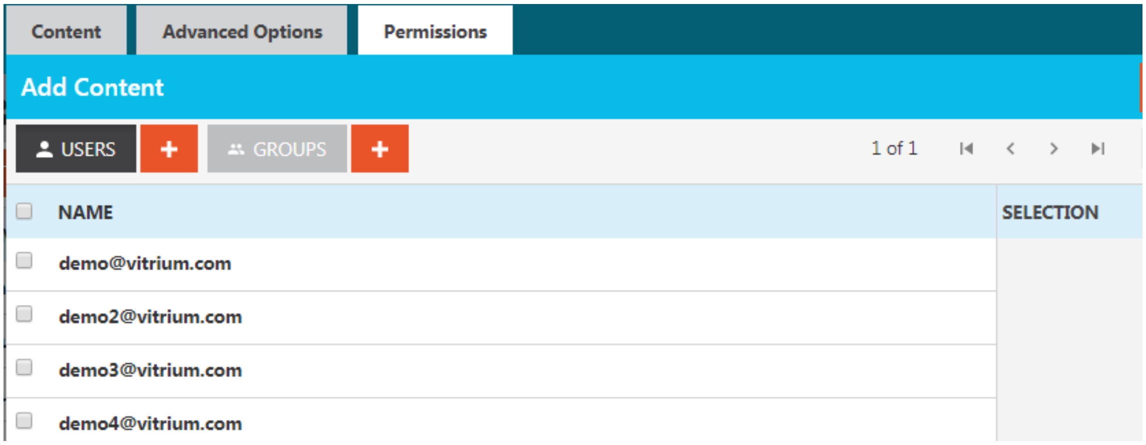
d. ***Notify User When New Version is Available:*** the default is always checked so end users will always be notified when there is a new version (or even an update made) to the original file that was uploaded

For Audio:

a. ***Content Name:*** you can enter a different file name if you wish to change it from the original
b. ***Upload Thumbnail:*** you can add a thumbnail image as the preview image in the audio player.
c. ***External Key:*** It allows you to store your own ID for your own content management system.
d. ***Notify User When New Version is Available:*** the default is always checked so end users will always be notified when there is a new version (or even an update made) to the original file that was uploaded

PERMISSIONS TAB

7. This is where you assign USERS or GROUPS to have access to your secured content:

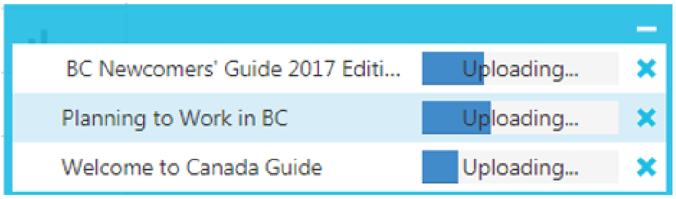


□ NAME	SELECTION
□ demo@vitrium.com	
□ demo2@vitrium.com	
□ demo3@vitrium.com	
□ demo4@vitrium.com	

a. ***Add Users or Groups:*** check the box beside any of the users or groups you wish to assign permissions to this file; the selected users and/or groups will appear in the right-hand side. If you haven't already set up any Users or Groups, you can always come back to add the Permissions later
b. ***DRM Policy:*** you may select a DRM Policy from the drop-down menu if you wish to apply one at this level (see the DRM Policy section for more details about other places you can apply a DRM policy)

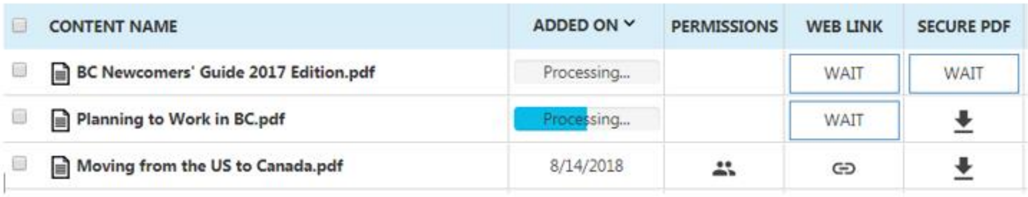
8. Click **Save & Exit** and your content will go through an uploading and processing stage.

UPLOADING STAGE



BC Newcomers' Guide 2017 Editi...	Uploading...	✕
Planning to Work in BC	Uploading...	✕
Welcome to Canada Guide	Uploading...	✕

PROCESSING STAGE



□	CONTENT NAME	ADDED ON ⌄	PERMISSIONS	WEB LINK	SECURE PDF
□	BC Newcomers' Guide 2017 Edition.pdf	Processing...		WAIT	WAIT
□	Planning to Work in BC.pdf	Processing...		WAIT	⬇
□	Moving from the US to Canada.pdf	8/14/2018	👥	🔗	⬇

IMPORTANT NOTE: For video uploads or larger file uploads, the processing stage may take some time as the files are being converted into their protected formats. You will only see the protected file links when this processing has completed.

1.3 Opening Protected Content

Vitrium offers 2 types of protected content:

1. **SECURE WEB LINK** (available for documents, images and video content) – this is an HTML5 web version of your content. Your original file has been converted to a web-friendly format with 256-bit AES encryption and can be opened on any web browser on any device. The content cannot be downloaded but there is an 'offline access' feature available for documents and images.

   Supported Browsers: all currently supported versions of Chrome, Firefox, Safari, Edge, Internet Explorer, Opera

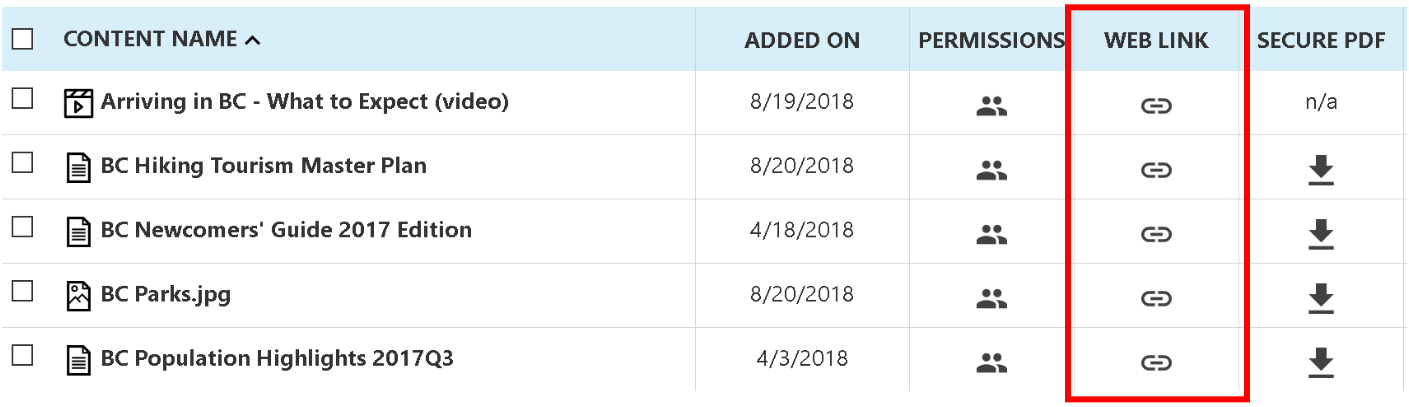
2. **SECURE PDF FILE** (available for documents and images) – this is a protected PDF file with 128-bit AES encryption that your users can download to their own computer. The file can be opened with Adobe Reader or Acrobat on a PC or Mac desktop environment. Although the file can be downloaded, it will remain encrypted and protected no matter where it travels.

   Supported Applications: all currently supported versions of Adobe Acrobat Reader DC or Adobe Acrobat Pro DC or Foxit Reader

SECURE WEB LINK

To copy and share the secure web link with your users, you can do this in one of two ways:

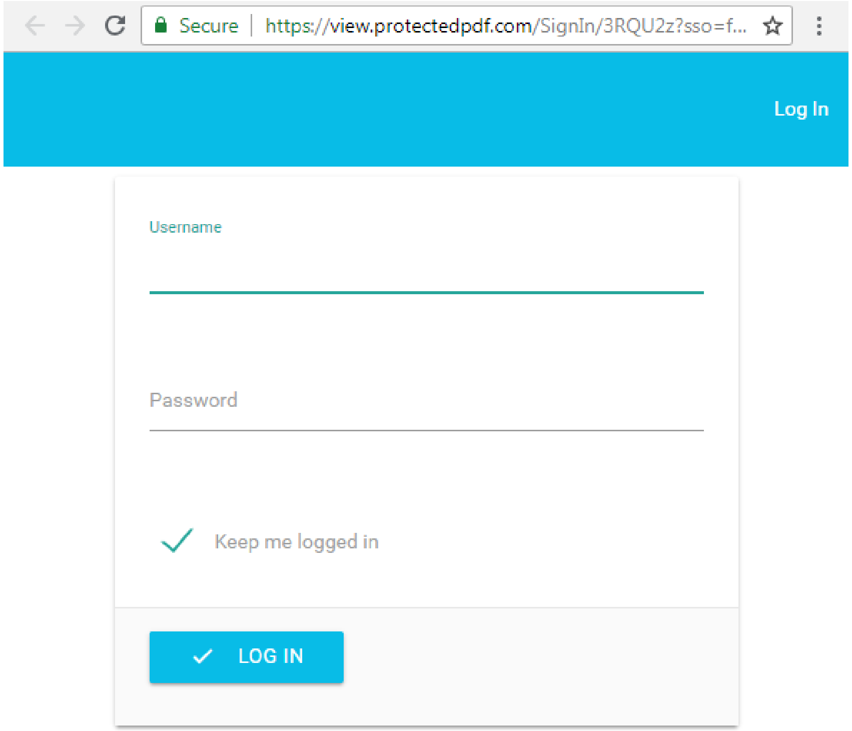
1. Click the web link and, once it opens in a web browser, copy the URL address,
   -OR-
2. Right-click on the link and select "Copy Link Location" and then paste the URL link in an email, your website, or any other method of distribution you are using.



□	CONTENT NAME ^	ADDED ON	PERMISSIONS	WEB LINK	SECURE PDF
□	Arriving in BC - What to Expect (video)	8/19/2018	👥	🔗	n/a
□	BC Hiking Tourism Master Plan	8/20/2018	👥	🔗	⬇
□	BC Newcomers' Guide 2017 Edition	4/18/2018	👥	🔗	⬇
□	BC Parks.jpg	8/20/2018	👥	🔗	⬇
□	BC Population Highlights 2017Q3	4/3/2018	👥	🔗	⬇

To open the secure web link:

1. First, ensure you set yourself up as a test user and assign yourself with permissions to view the content:
   a. Click the Permissions icon
   b. Click Add, then click the + symbol beside USERS
   c. Enter your test username and password, then click SAVE & EXIT (you can learn more about the other user fields in Section 2 Users)
   d. Select a DRM policy from the drop-down menu, then click ADD PERMISSIONS
   e. Click SAVE & EXIT one more time
2. Once you're assigned permission to access the content, click the web link icon and log in with your test username and password – you'll see this login page:



Secure | https://view.protectedpdf.com/SignIn/3RQU2z?sso=f...

3. Once logged in, you should see Vitrium’s web viewer:

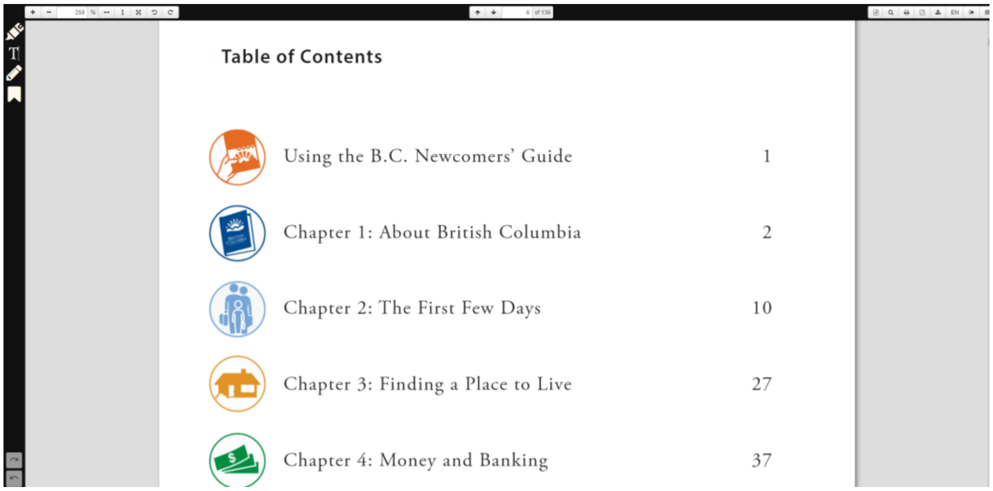


Table of Contents

Using the B.C. Newcomers’ Guide 1

Chapter 1: About British Columbia 2

Chapter 2: The First Few Days 10

Chapter 3: Finding a Place to Live 27

Chapter 4: Money and Banking 37

SECURE PDF / PROTECTED PDF FILE

Vitrium’s protected PDF file can be opened with Adobe Reader or Acrobat or Foxit Reader, on a PC or Mac desktop environment only. Your end user does not require a plug-in to access the protected content but the user may be prompted with some messages in Adobe and Foxit Reader: (1) to allow the communication to occur with the Vitrium server for authentication, or your server if you have Vitrium installed on your environment, and in Adobe (2) to disable the Adobe global object security policy.

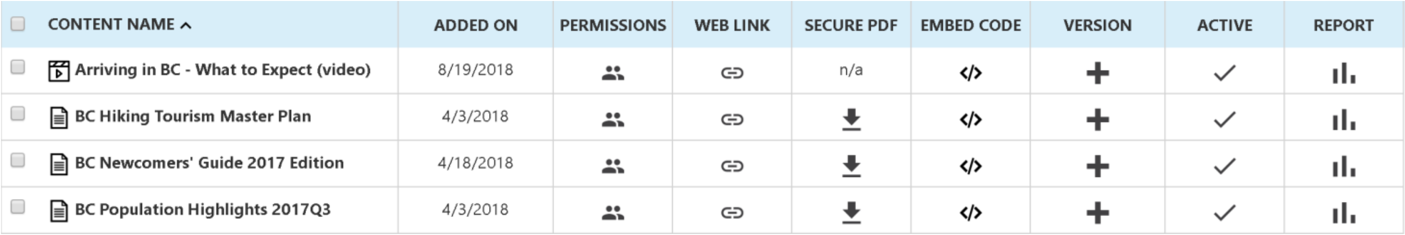
<u>To DOWNOAD the protected PDF file</u> to send to your customers or upload it to your website or other system:

1. In the Content tab, find your file and click the download icon under the Secure PDF column ⬇
2. Depending on which browser you’re using will depend on how the download occurs
3. If you save the file, browsers like Chrome will automatically save it your Downloads folder on your computer and the file will have your original file name, along with the extension –*protected* (i.e. Your File Name-protected.pdf)
4. You can now send this protected PDF file to your users or upload it to your website or another system

<u>To OPEN the protected PDF file:</u>

1. Unless you have Adobe Reader or Foxit Reader installed as the default PDF viewer on your computer, when you open the protected PDF file, it may open automatically in Chrome’s built-in PDF viewer – this will NOT work and you should set Adobe as your default viewer
2. In your downloads folder (or wherever you saved the file), right-click on the file and select “Open With”, then select Adobe Reader / Foxit Reader from the menu (check the box “Make this my default”), then click Open

1.4 Understanding Column Functions



□	CONTENT NAME ^	ADDED ON	PERMISSIONS	WEB LINK	SECURE PDF	EMBED CODE	VERSION	ACTIVE	REPORT
□	Arriving in BC - What to Expect (video)	8/19/2018	👥	🔗	n/a	</>	+	✓	📊
□	BC Hiking Tourism Master Plan	4/3/2018	👥	🔗	⬇	</>	+	✓	📊
□	BC Newcomers' Guide 2017 Edition	4/18/2018	👥	🔗	⬇	</>	+	✓	📊
□	BC Population Highlights 2017Q3	4/3/2018	👥	🔗	⬇	</>	+	✓	📊

CONTENT NAME
This is the name of the file you uploaded. You can change this in the Advanced Options tab when you upload or edit content.

ADDED ON
This is the date when the file was uploaded into Vitrium.

PERMISSIONS
This is where you can add or change permissions (add users or groups) to the file.

WEB LINK
This is one of the protected file outputs, the secure web link that you can send to your end users to unlock or view the protected content. They can open this link using any web browser, from any type of web-enabled device.

SECURE PDF
This is the other protected file outputs, the downloadable protected PDF file (available for documents and images only) that you can send to your end users to unlock or view the protected content. They can open this with Adobe Reader or Acrobat or Foxit Reader, on a PC or Mac desktop environment only, without the need to download a plug-in.

ACTIVE
This is where you can de-activate a file if you no longer wish to allow end users to access it. You can later re-activate the file or delete it entirely from the system.

REPORT
This is where you can access a ‘User Activity Log’ report for the file you click on. You will be redirected to the Reports section and you will see who has opened the file, on what date and time, from which IP address, from what type of application or browser, and more.

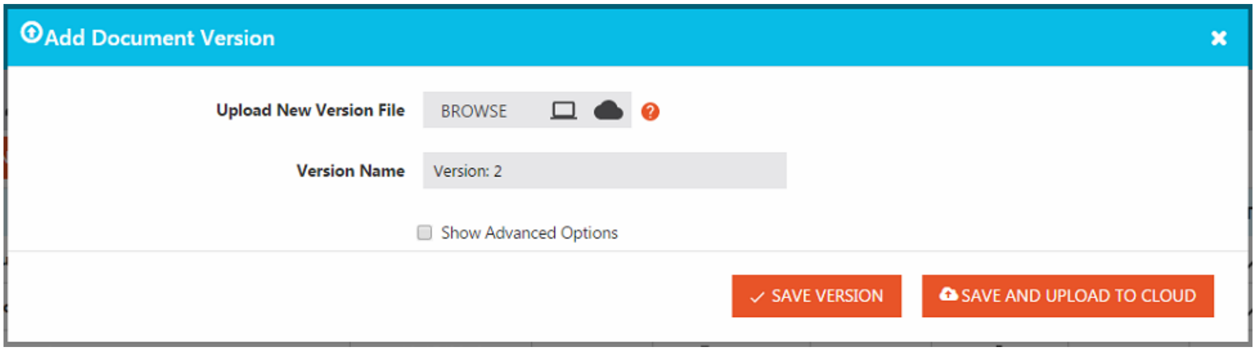
EMBED CODE
This is an iFrame code that you can use to embed the protected web version of your file onto your website, portal or other 3rd party application.

VERSION (ENTERPRISE ONLY)

This allows you to manage and control the different versions of files you might have. All customers (including Standard and Professional accounts) can replace content but the 'version' functionality allows you to keep previous versions while adding new ones.

a) Add a New Version

To add a version, click the + icon and a pop-up window will appear.



Add Document Version ✖

Upload New Version File: BROWSE

Version Name: Version: 2

□ Show Advanced Options

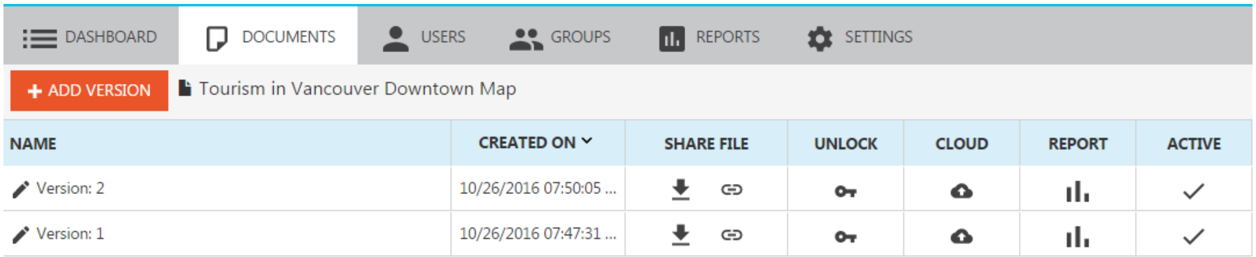
✓ SAVE VERSION

SAVE AND UPLOAD TO CLOUD

Click BROWSE to find the newer version of your file, change the name if you wish, then click 'Save Version'.

b) Manage Versions

Once you have more than 1 version set in place, the icon will change to MANAGE 2 which would also indicate how many versions of the original document have added or changed (in this case, 2 versions). If you click the 'Manage' button, you will be redirected to a new page where you will see the different versions:

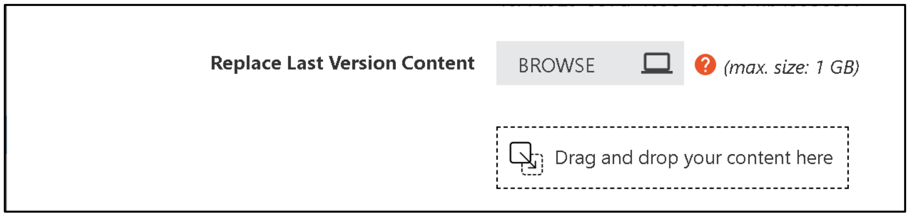


Tourism in Vancouver Downtown Map

NAME	CREATED ON	SHARE FILE	UNLOCK	CLOUD	REPORT	ACTIVE
Version: 2	10/26/2016 07:50:05 ...					✓
Version: 1	10/26/2016 07:47:31 ...					✓

1.5 Replacing Content

If you accidentally uploaded the wrong file or you want to change an existing file, you can click on the file to replace the content. Beside the 'Replace Last Version Content' field, click BROWSE or drag and drop the new file into this window. If you don't require any other changes, click *Save & Exit* and this will re-process your file.



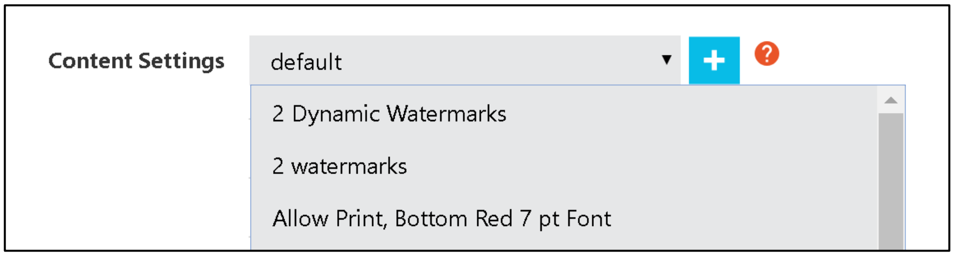
Replace Last Version Content: BROWSE (max. size: 1 GB)

Drag and drop your content here

IMPORTANT NOTE: When replacing content, these changes will appear immediately for the web viewer content, but for the protected PDF version, you will need to re-download it and re-send the updated version to your end users.

1.6 Changing Content Settings

If you wish to change the Content Settings for a file because you decided to allow printing after not allowing printing, or you wanted to use a different watermark, you can do this easily in the Edit Content pop-up box by and selecting a different Content Settings (assuming you already created it) or clicking the + symbol to create a new Content Settings. Once you have the new Content Settings you wish to apply, click *Save & Exit* and this will re-process your file.



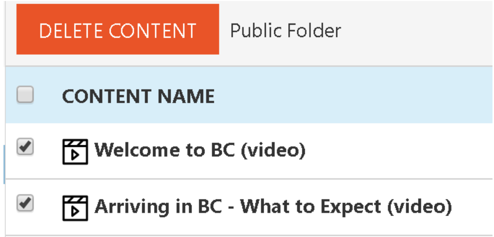
Content Settings: default

- 2 Dynamic Watermarks
- 2 watermarks
- Allow Print, Bottom Red 7 pt Font

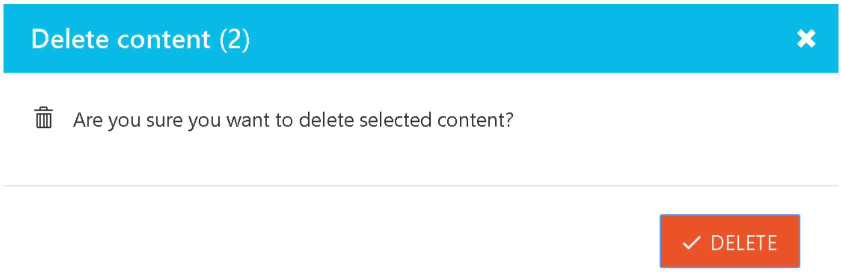
IMPORTANT NOTE: When changing Content Settings, these changes will appear immediately for the web viewer content, but for the protected PDF version, you will need to re-download it and re-send the updated version to your end users.

1.7 Deleting Content

You can delete a single file or multiple files from within the Content tab. Select the file(s) that you wish to delete, then the ADD CONTENT button will change to DELETE CONTENT. Click this Delete Content button and you will see another prompt confirming your deletion as these files will be permanently deleted from the Vitrium system and you cannot get them back. If you are absolutely certain you want to delete them, then you can click DELETE.



	CONTENT NAME
☑	**Welcome to BC (video)**
☑	**Arriving in BC - What to Expect (video)**



Delete content (2)

Are you sure you want to delete selected content?

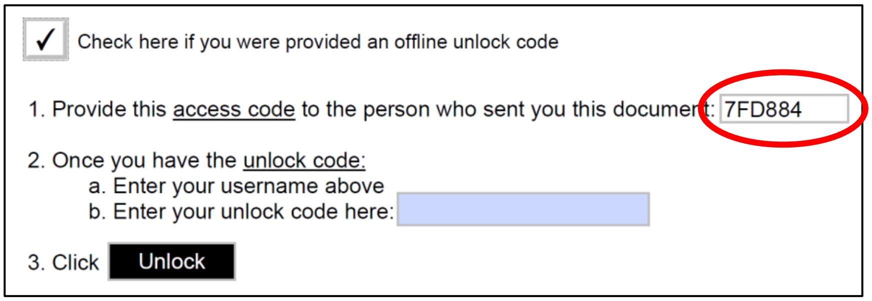
1.8 Understanding Offline Unlock

If you have a customer who is in a location with no access to Internet but they need to unlock a protected PDF file, you can do this via the 'Offline Unlock' feature, either at the file level or user level.

IMPORTANT NOTE: The 'offline unlock' feature only works with the protected PDF file, not the web viewer version of the file.

End User Steps – STAGE 1

1. The user should open the protected PDF file using Adobe Reader or Foxit Reader
2. Near the bottom of the login page, they should check the 'offline unlock' statement and, once clicked, the user should see an access code that they will need to provide to the Vitrium administrator



☑ Check here if you were provided an offline unlock code

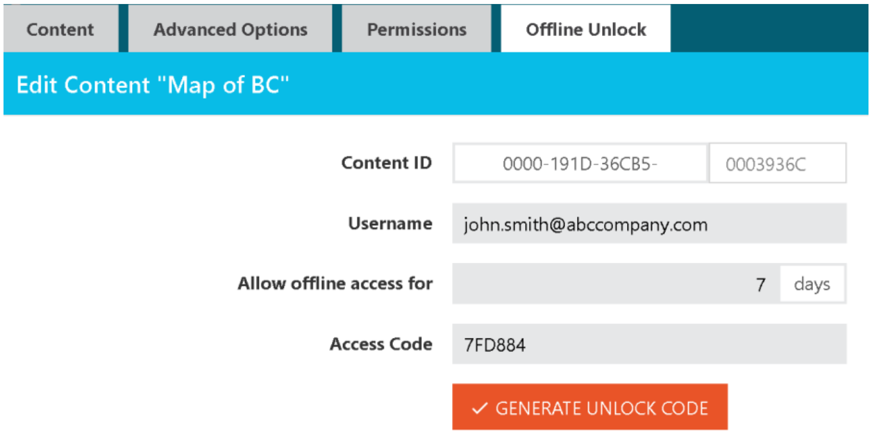
1. Provide this access code to the person who sent you this document: 7FD884

2. Once you have the unlock code:
   a. Enter your username above
   b. Enter your unlock code here:

3. Click

Vitrium Administrator Steps

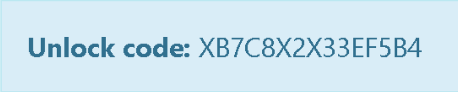
1. In the Vitrium Content tab, click the file in question and go to the Offline Unlock tab
2. Enter the following information:
   a. Username = enter the person's username that needs the offline unlock
   b. Allow offline access for = enter however many days you feel comfortable in providing
   c. Access code = enter the access code that the user has provided to you (see steps above)
   d. Click the GENERATE UNLOCK CODE button



Edit Content "Map of BC"

Content ID	0000-191D-36CB5- 0003936C
Username	john.smith@abccompany.com
Allow offline access for	7 days
Access Code	7FD884

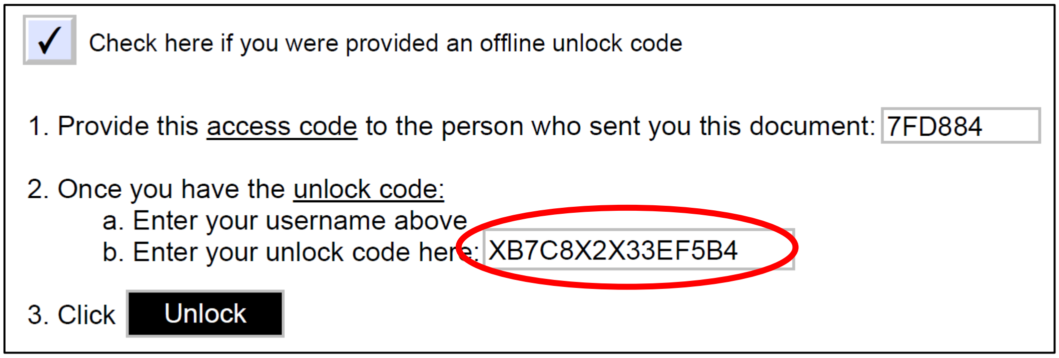
3. You should then see an unlock code that you can provide to the end user



Unlock code: XB7C8X2X33EF5B4

End User Steps – STAGE 2

1. The end user should then enter the unlock code provided to them in their protected PDF file at step 2 indicated below, then click UNLOCK and the file should open successfully



☑ Check here if you were provided an offline unlock code

1. Provide this access code to the person who sent you this document: 7FD884

2. Once you have the unlock code:
   a. Enter your username above
   b. Enter your unlock code here: XB7C8X2X33EF5B4

3. Click Unlock

1.9 Using Folders

This is the area where you can sort and organize your files and content into different folders.

ADD A NEW FOLDER

1. Click on the Add Folder button
2. Enter the Folder Name and click *Save & Exit*
3. For Enterprise Customers, if you wish to add an external key to your folder, you can click on the *Advanced Options* tab and enter one there.

MOVING CONTENT TO A DIFFERENT FOLDER

1. You can drag and drop a file from one folder to another folder

RENAME FOLDER

1. Click the arrow beside the folder you wish to rename and select *Edit folder*
2. Rename the folder, then click *Save & Exit*

DOWNLOAD FOLDER

1. Click the arrow beside the folder you wish to download and select *Download Folder*
2. This bundles and zips into a file the selected folder and all its subfolders and protected files

PERMISSIONS (FOLDER LEVEL)

If you wish to set Permissions and a DRM policy at the folder level, follow these instructions:

1. Click the arrow beside the folder you wish to assign Permissions to and select *Permissions*
2. Add the appropriate Permissions, then click *Save & Exit*

DELETE A FOLDER

1. Click the arrow beside the folder you wish to delete and select *Delete Folder*
2. A pop-up window will open asking if you wish to delete the folder; click OK if you agree

IMPORTANT NOTE: you can only delete subfolders and not the root folders.

2.0 USERS TAB

It is very important to understand that there are two types of “Users” in Vitrium which are defined here:

- **End Users:** those who you wish to grant access (permissions) to view your protected content. These could be your customers, clients, students, subscribers, members, or even your internal staff. Add these types of users in the USERS tab.
- **Staff Users:** those who can log into Vitrium and perform certain ‘administrative functions’ such as adding content, adding users, assigning permissions, viewing reports, and so on. Add these types of users in the SETTINGS tab. Refer to Section 5.5 for more details about Staff Users.

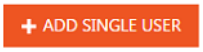
IMPORTANT NOTE: if you are planning to use Vitrium with your internal staff only, then you will need to ensure you are clear about where to add these users: as end users in the USERS tab, or as staff users in the SETTINGS tab. If the primary function for the user is to access protected content, then add them as an end user in the USERS tab. If the primary function for the user is to add content or perform other administrative functions in Vitrium, then add them as a staff user in the SETTINGS tab.

This section deals with END USERS – how to add them, edit them, activate or de-activate them, assign them permissions, view their activity, and more.

2.1 Adding Users & Understanding Column Functions

To add End Users in Vitrium Security, you can do this in one of two ways: (1) one at a time; or (2) as a batch upload using the multi-line window or CSV import tool.

ADD SINGLE USER

1. From the Users Tab, click 

2. Enter the following information:

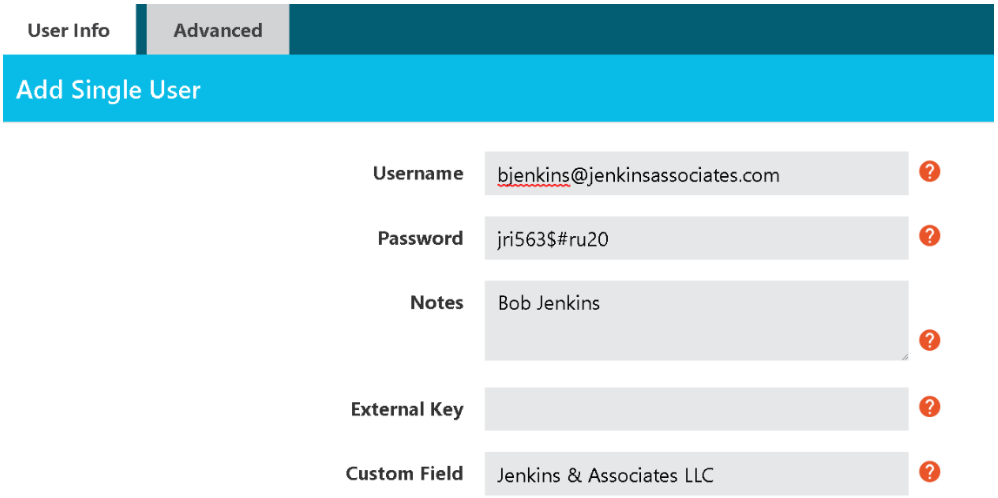
   Username: this is a mandatory field and we recommend using an email address for username as that can be used later for the password recovery feature

   Password: this is a mandatory field and we recommend adding a strong password with a combination of letters, numbers and characters

   Notes: this is an optional field that can be used for any number of reasons – to add the person’s full name, a company name, a division or department name, etc.

   Custom Field: this is another optional field that can be used for any of the same reasons as above

External Key: this is an optional field for Enterprise customers if they wish to enter their corresponding 3rd party ID to associate this user with that system



Add Single User

Username	bjenkins@jenkinsassociates.com
Password	jri563$#ru20
Notes	Bob Jenkins
External Key	
Custom Field	Jenkins & Associates LLC

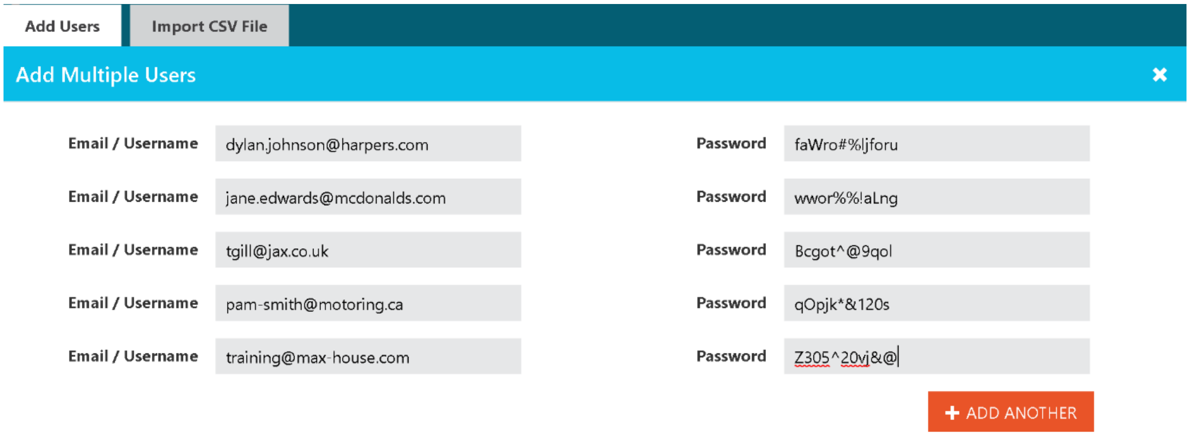
3. Click the Advanced tab ONLY if you wish to set a DRM policy at the User level. We generally do not recommend setting the DRM policy here as we recommend setting it at the File level or Group level. Refer to Section 5.4 for more details about DRM Policy Settings.
4. Click *Save & Exit* when you're done and start the process again with other Users

ADD MULTIPLE USERS

There are two ways to add multiple users: (1) via manual input but you can only enter the username and password fields, or (2) via the CSV import tool but you need to ensure you follow the sample CSV file structure.

Via Manual Input:

2. From the Users Tab, click ADD MULTIPLE USERS
3. Enter the Usernames and Passwords of the users you wish to add manually



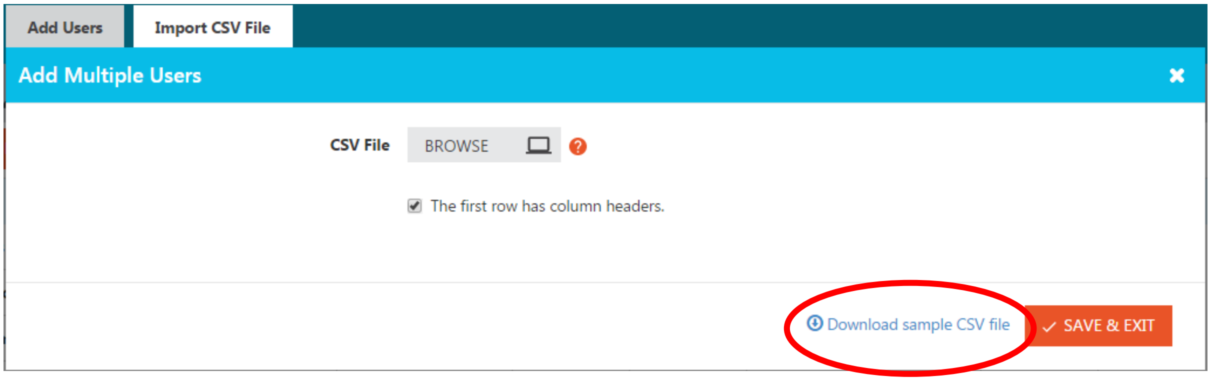
Add Multiple Users

Email / Username	dylan.johnson@harpers.com	Password	faWro#%ljforu
Email / Username	jane.edwards@mcdonalds.com	Password	wwor%%!aLng
Email / Username	tgill@jax.co.uk	Password	Bcgot^@9qol
Email / Username	pam-smith@motoring.ca	Password	qOpjk*&120s
Email / Username	training@max-house.com	Password	Z305^20vj&@

4. Although only 5 lines show by default, you can click the + ADD ANOTHER button to add more
5. Click *Save & Exit* when you are done

Via CSV Import:

1. From the Users Tab, click ADD MULTIPLE USERS
2. Select the Import CSV File tab
3. We strongly recommend you click on the “Download sample CSV file” and use the same row headings as this file



Add Users | Import CSV File

Add Multiple Users ✖

CSV File BROWSE

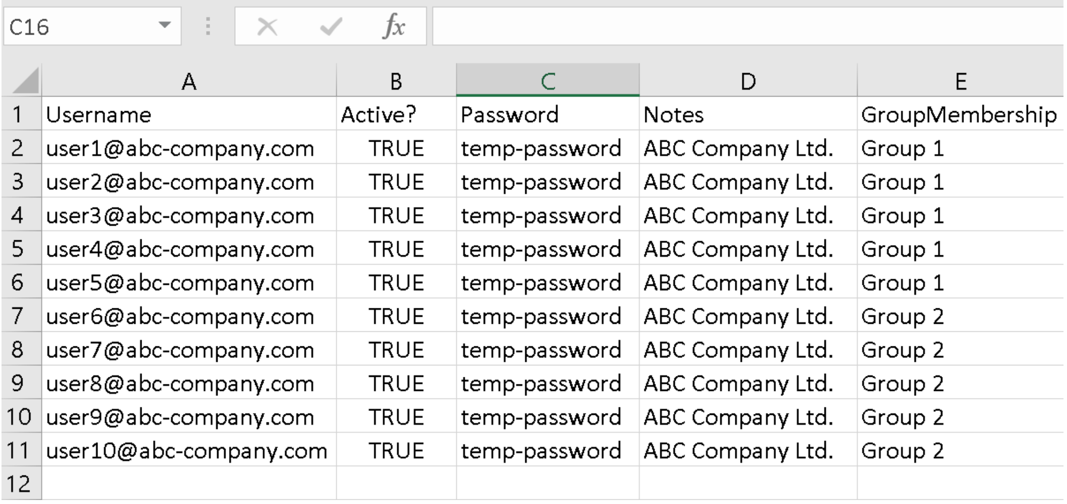
☑ The first row has column headers.

Download sample CSV file ✓ SAVE & EXIT

4. In the CSV file, ensure you enter at least the following 3 columns of information:

   Username: enter all your usernames (again we strongly recommend entering email addresses)
   Active: enter TRUE for an *active* user, FALSE for *inactive*
   Password: enter any password that you wish although we recommend using strong passwords; you can enter a temporary password and then activate the ‘forgot password’ feature in the user portal later
   All other fields in the CSV file are optional to enter.

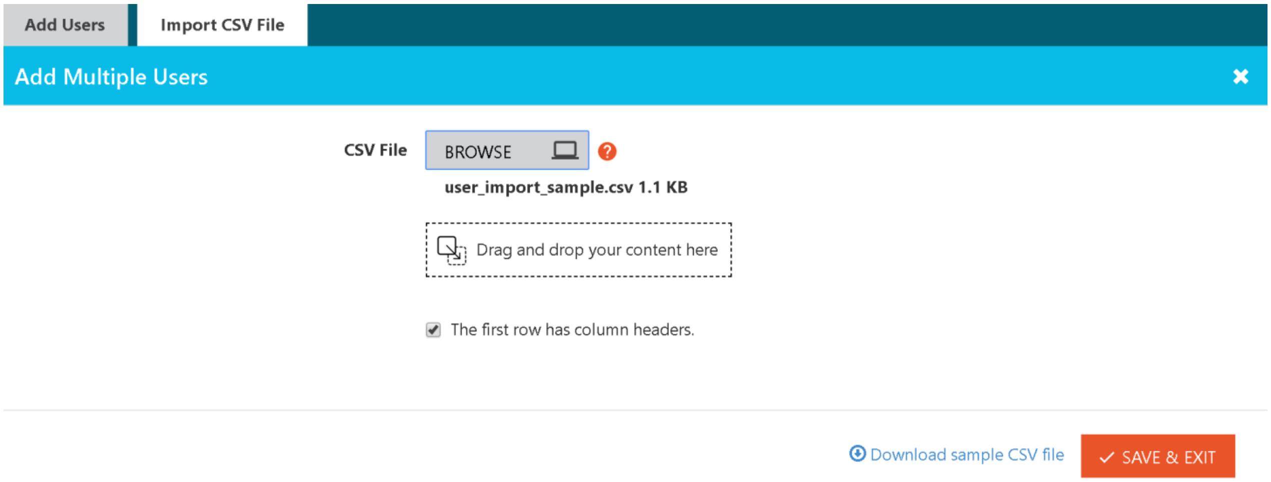
IMPORTANT NOTE: when entering a Group in the CSV file, that Group name must already exist in your Vitrium account, otherwise the user will not get added to the Group.



C16

	A	B	C	D	E
1	Username	Active?	Password	Notes	GroupMembership
2	user1@abc-company.com	TRUE	temp-password	ABC Company Ltd.	Group 1
3	user2@abc-company.com	TRUE	temp-password	ABC Company Ltd.	Group 1
4	user3@abc-company.com	TRUE	temp-password	ABC Company Ltd.	Group 1
5	user4@abc-company.com	TRUE	temp-password	ABC Company Ltd.	Group 1
6	user5@abc-company.com	TRUE	temp-password	ABC Company Ltd.	Group 1
7	user6@abc-company.com	TRUE	temp-password	ABC Company Ltd.	Group 2
8	user7@abc-company.com	TRUE	temp-password	ABC Company Ltd.	Group 2
9	user8@abc-company.com	TRUE	temp-password	ABC Company Ltd.	Group 2
10	user9@abc-company.com	TRUE	temp-password	ABC Company Ltd.	Group 2
11	user10@abc-company.com	TRUE	temp-password	ABC Company Ltd.	Group 2
12					

5. Once completed, save the CSV file, then go back into Vitrium, and upload the file here, ensuring the “first row has column headers” statement is checked (which is the default), then click *Save & Exit*



Add Users | Import CSV File

Add Multiple Users ✖

CSV File BROWSE ?

user_import_sample.csv 1.1 KB

Drag and drop your content here

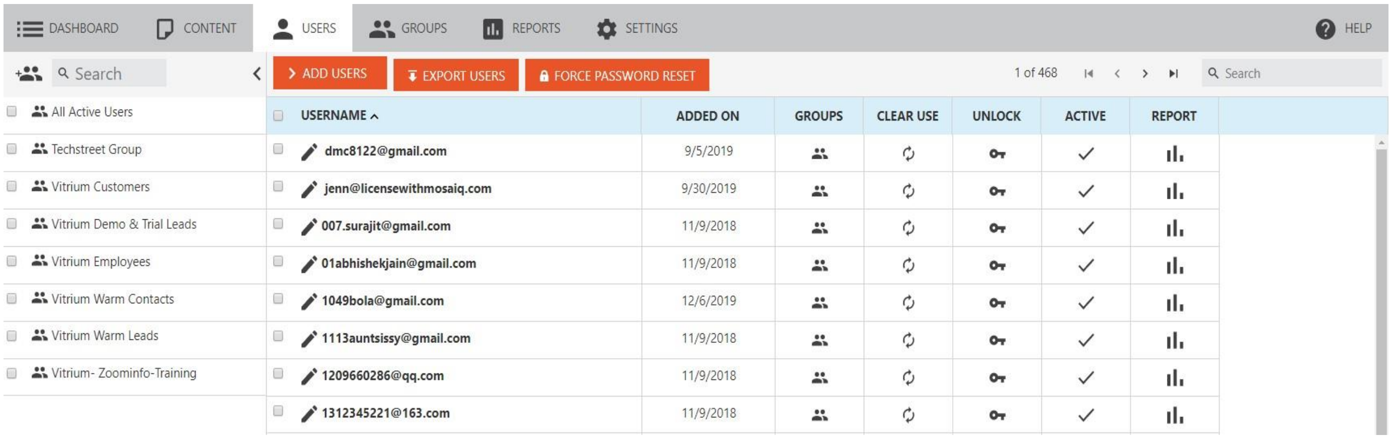
☑ The first row has column headers.

Download sample CSV file

✓ SAVE & EXIT

6. Your users should get added instantly to your Vitrium account. You may need to click on the ‘Added On’ column to sort by date to see all the newly added users.

UNDERSTANDING COLUMN FUNCTIONS

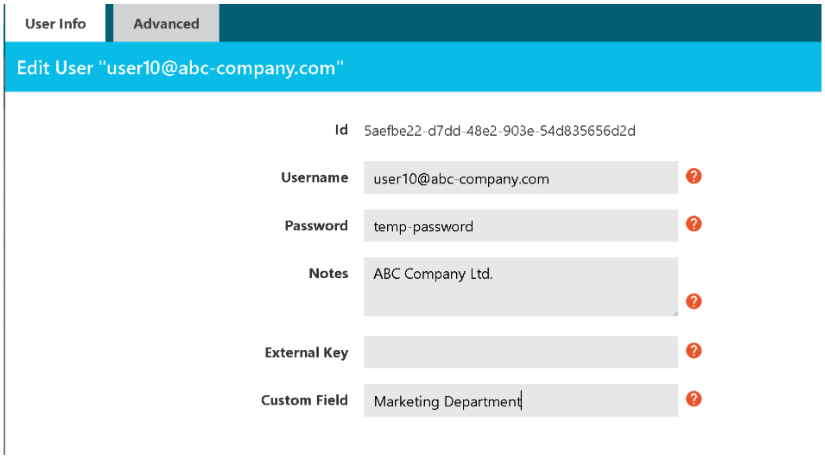


□ All Active Users
□ Techstreet Group
□ Vitrium Customers
□ Vitrium Demo & Trial Leads
□ Vitrium Employees
□ Vitrium Warm Contacts
□ Vitrium Warm Leads
□ Vitrium- Zoominfo-Training

□	USERNAME ^	ADDED ON	GROUPS	CLEAR USE	UNLOCK	ACTIVE	REPORT
□	dmc8122@gmail.com	9/5/2019	👥	↻	🔑	✓	📊
□	jenn@licensewithmosaiq.com	9/30/2019	👥	↻	🔑	✓	📊
□	007.surajit@gmail.com	11/9/2018	👥	↻	🔑	✓	📊
□	01abhishekjain@gmail.com	11/9/2018	👥	↻	🔑	✓	📊
□	1049bola@gmail.com	12/6/2019	👥	↻	🔑	✓	📊
□	1113auntsissy@gmail.com	11/9/2018	👥	↻	🔑	✓	📊
□	1209660286@qq.com	11/9/2018	👥	↻	🔑	✓	📊
□	1312345221@163.com	11/9/2018	👥	↻	🔑	✓	📊

EDIT USER

Click on any username in your column list to edit their details. The same pop-up window that you used to add a single user will appear and you can add or change any details that you want, then click *Save & Exit*.



User Info | Advanced

Edit User "user10@abc-company.com"

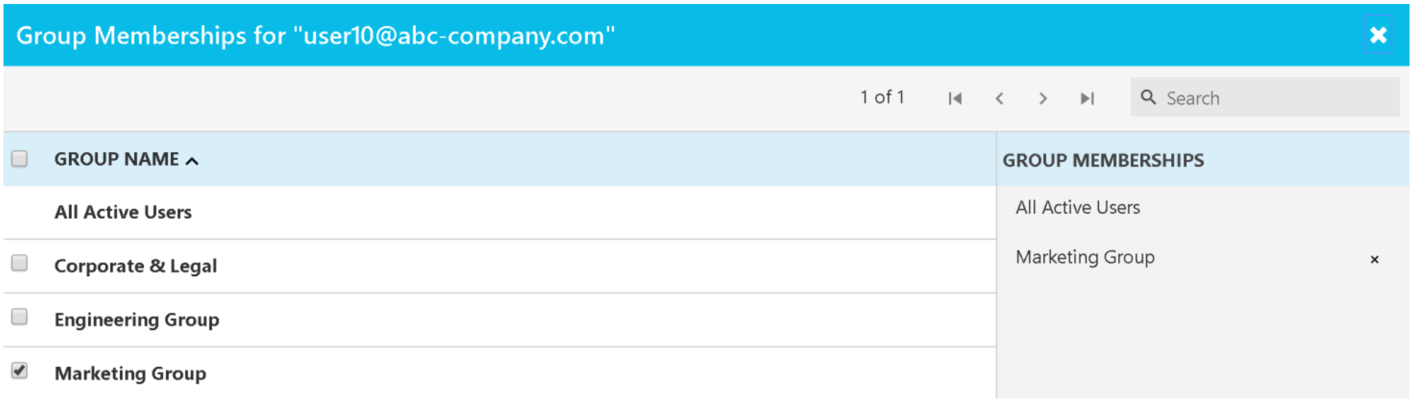
Id	5aefbe22-d7dd-48e2-903e-54d835656d2d
Username	user10@abc-company.com
Password	temp-password
Notes	ABC Company Ltd.
External Key	
Custom Field	Marketing Department

ADDED ON

This is the date that the user got added to Vitrium. You can click on this column to sort in ascending or descending date order.

GROUPS

Click the Groups icon to check which groups the user belongs to. You can also assign the user to a group or multiple groups through this window.



Group Memberships for "user10@abc-company.com"

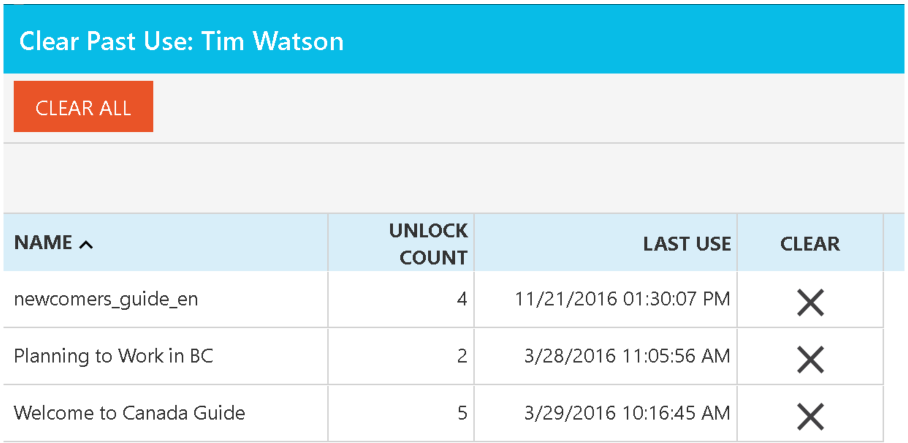
GROUP NAME	GROUP MEMBERSHIPS
All Active Users	All Active Users
□ Corporate & Legal	Marketing Group ×
□ Engineering Group	
☑ Marketing Group	

CLEAR USE

This is a very useful feature if you wish to clear a person's use. When you are applying DRM policies to users to restrict their access to content (to prevent file sharing and so on), sometimes a legitimate user may get caught up in this if they happen to upgrade their computer or tablet or phone, and they reach their PDF/browser limit, or some other limit.

<u>If you do not suspect fraud or malicious use of any kind</u>, you can 'clear the person's use' by clicking this icon ↻ then, depending on which edition you subscribe to, one of the following windows will pop up.

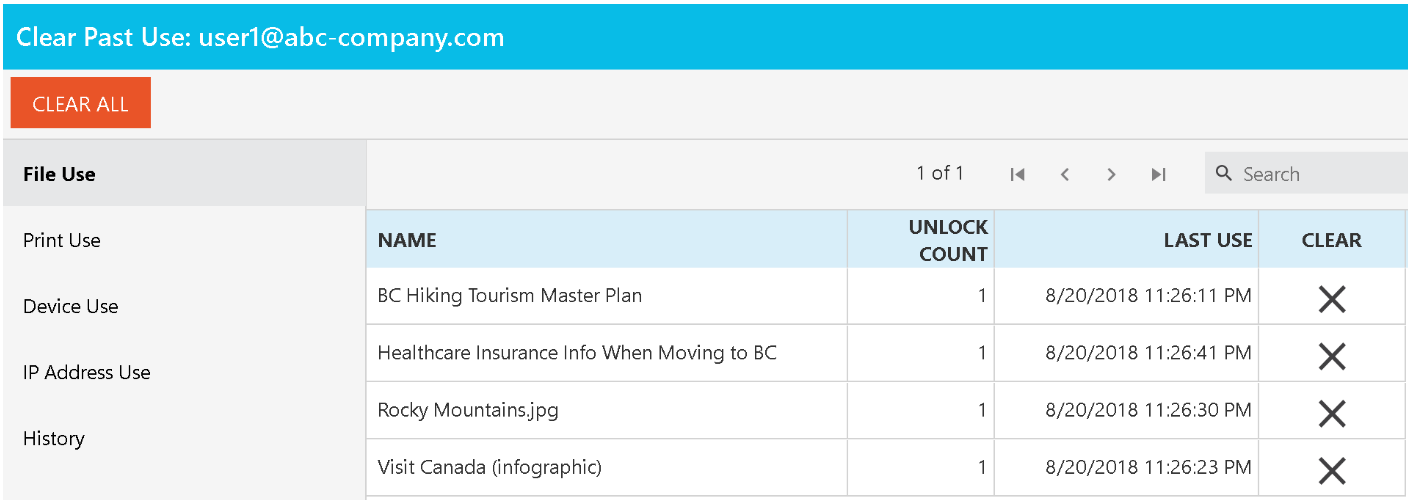
Standard & Professional accounts will be able to clear the use for a <u>specific file only</u>:



Clear Past Use: Tim Watson

NAME ^	UNLOCK COUNT	LAST USE	CLEAR
newcomers_guide_en	4	11/21/2016 01:30:07 PM	✕
Planning to Work in BC	2	3/28/2016 11:05:56 AM	✕
Welcome to Canada Guide	5	3/29/2016 10:16:45 AM	✕

Enterprise accounts will be able to clear use by different means – for a specific file or all files, for print use, device use, or IP address use. They will also be able to see a history of how many times the clear use function was used:



Clear Past Use: user1@abc-company.com

NAME	UNLOCK COUNT	LAST USE	CLEAR
BC Hiking Tourism Master Plan	1	8/20/2018 11:26:11 PM	✕
Healthcare Insurance Info When Moving to BC	1	8/20/2018 11:26:41 PM	✕
Rocky Mountains.jpg	1	8/20/2018 11:26:30 PM	✕
Visit Canada (infographic)	1	8/20/2018 11:26:23 PM	✕

UNLOCK 🔑

If you wish to provide access to a protected PDF file to someone that is not connected to the Internet, you can click this icon 🔑 to access the offline unlock functionality. This feature can also be useful for users who are behind restrictive proxy servers or firewalls that may be preventing their content from opening. To understand how to use this feature, refer to the steps in *Section 1.7 Understanding Offline Unlock*.

ACTIVE ✓

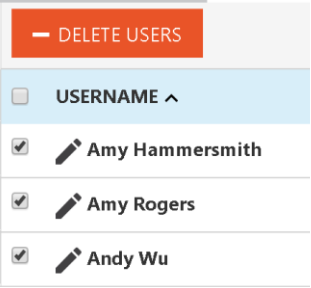
The checkmark ✓ means that the User is active and the X means they are not active. You can toggle this feature very easily to activate or de-activate a user in your account.

REPORT 📊

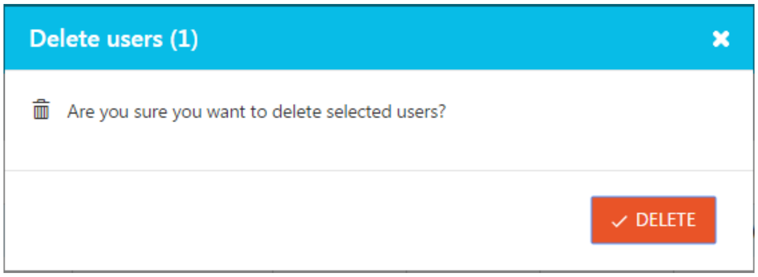
Click the Report icon if you wish to view the 'User Activity Log' report for a particular user. It will pull up all the activity associated with that user included what files they opened, when, from which IP address, what browser or application was used, what operating system they used, and so on.

2.2 Deleting Users

If you wish to delete a User or Users entirely from Vitrium (and not just de-activate them by clicking the checkmark icon under the Active column), you can select the users you wish to delete, then the ADD USERS button will change to DELETE USERS and you can click this button.



You will then be prompted with a message confirming that you are okay to delete the selected users. If you are, click DELETE again.



Are you sure you want to delete selected users?

Once the user or users are deleted from Vitrium, this will effectively revoke any and all access they previously had access to and you will not be able to get back the users' information.

Delete or Deactivate?

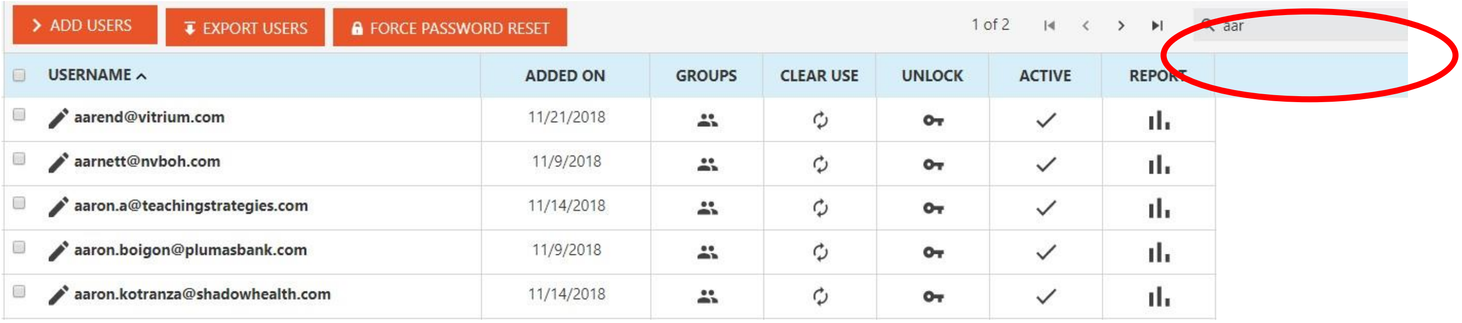
If you do not wish to delete the users entirely and lose all their information, you can choose to de-activate them instead by clicking the checkmark icon under the Active column and an 'X' will appear instead indicating that they have been de-activated. This will still revoke their access to any and all files they previously had access to but it will keep all the users' information in Vitrium.

IMPORTANT NOTE: If you are using plain text names as usernames and you previously had a user named Bob (Reyes) that you deleted (and you only entered 'Bob' as the username, not his full name), then later you added a new user with the name Bob (Walter) but again didn't enter his last name, Bob Reyes' previous history and report will show under the new Bob, even after the original Bob was deleted. This is another reason why we strongly recommend using email addresses as usernames to avoid these potential conflicts.

2.3 Searching Users

By Username, Notes, Custom Field or External Key

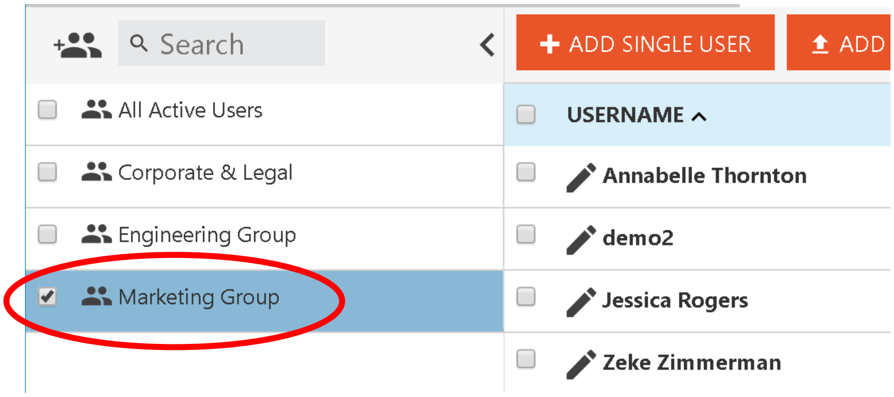
You can search for users in the Search bar at the top right-hand side of the screen by their Username, Notes, Custom Field, or External Field making this a very powerful search function in Vitrium and allowing you to only export a specific group of users instead of the entire list if you need to.



☐	USERNAME ^	ADDED ON	GROUPS	CLEAR USE	UNLOCK	ACTIVE	REPORT
☐	aarend@vitrium.com	11/21/2018				✓	
☐	aarnett@nvboh.com	11/9/2018				✓	
☐	aaron.a@teachingstrategies.com	11/14/2018				✓	
☐	aaron.boigon@plumasbank.com	11/9/2018				✓	
☐	aaron.kotranza@shadowhealth.com	11/14/2018				✓	

By Group

You can also search for users by their Group by selecting the Group Name on the left-hand side of the screen.



☐ All Active Users
☐ Corporate & Legal
☐ Engineering Group
☑ Marketing Group

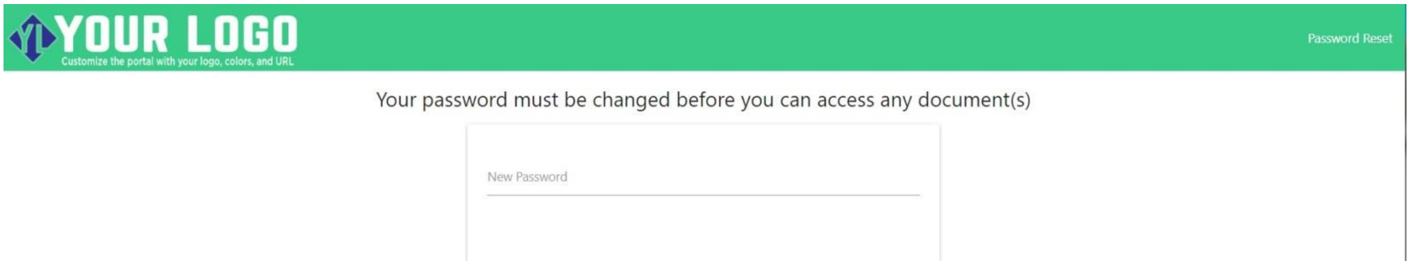
☐	USERNAME ^
☐	Annabelle Thornton
☐	demo2
☐	Jessica Rogers
☐	Zeke Zimmerman

2.4 Exporting Users

You can export all users or a group of users that you have searched on by clicking the EXPORT USERS button at the top of the Users window and you will receive a CSV file of the export.

2.5 Force Password Reset

You can force your users to reset their password. This is a useful security feature when you add new users and you want them to change their password before they can unlock the document.



Your password must be changed before you can access any document(s)

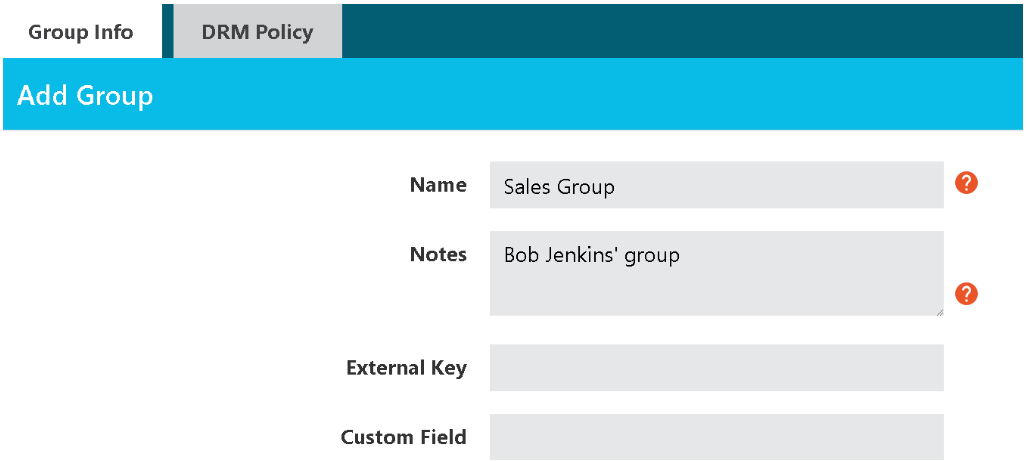
New Password

3.0 GROUPS TAB

This section is for adding, editing, or deleting groups, and for adding, editing, or removing users to and from groups.

3.1 Adding a Group & Understanding Column Functions

To add a group, click the + ADD GROUP button and enter all the relevant information you wish to add. Only the **Name** field is mandatory. All other fields are optional.



Name	Sales Group
Notes	Bob Jenkins' group
External Key	
Custom Field	

You may wish to add a DRM Policy at the Group level and if you do, click the DRM Policy tab for the Group and update the following fields. Be sure to review Section 5.4 DRM Policy Settings to learn more.

UNDERSTANDING COLUMN FUNCTIONS

Once there are group/groups established in your User account, the Group List will automatically get generated for customization purposes.

EDITING A GROUP

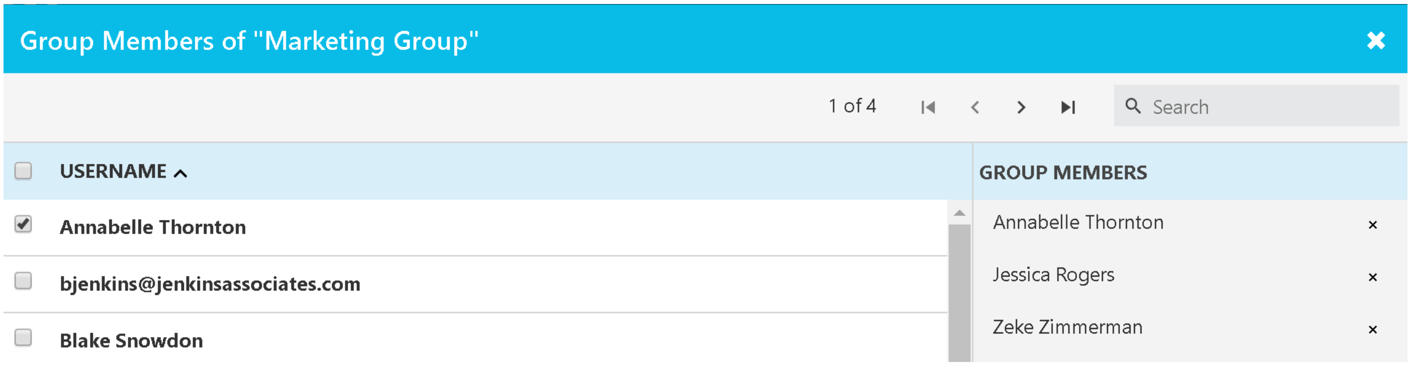
You can click on any Group once it's added to edit the information about that Group including its Name, Notes, External Key, or the DRM policy information.

ADDED ON

Much like the 'Added On' column in the Content tab and Users tab, this is the same. It will show the date when the Group was created (added) in Vitrium. You can also sort data by this column.

USERS

Click the Users icon to view, add, edit or remove Users (or ‘Group Members’) from the selected Group.



Group Members of "Marketing Group" ✖

1 of 4 Search

☐	USERNAME ^
☑	Annabelle Thornton
☐	bjenkins@jenkinsassociates.com
☐	Blake Snowdon

GROUP MEMBERS	
Annabelle Thornton	×
Jessica Rogers	×
Zeke Zimmerman	×

On the left-hand side, you can select Users to add to the Group. On the right-hand side, you can view Users (or ‘Group Members’) that are in the Group. You can also remove Users from this Group by clicking the small ‘x’ beside the username.

ACTIVE

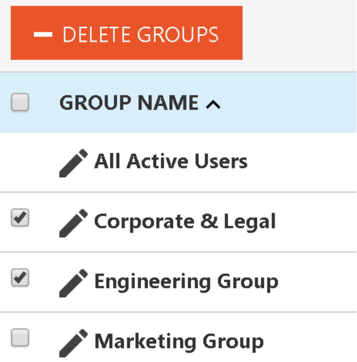
Much like the ‘Active’ column in the Content tab and Users tab, the checkmark indicates that the Group is active and an ‘X’ indicates it is not active. To deactivate a Group, simply click the checkmark and all Users within that Group will no longer have access to any content that the Group had access to.

REPORT

Clicking the Report icon will direct you to the ‘User Activity Log’ report showing you unlock and viewing activity for that specific Group. From there, you can also export the Group’s activity level for a specific time period.

3.2 Deleting Groups

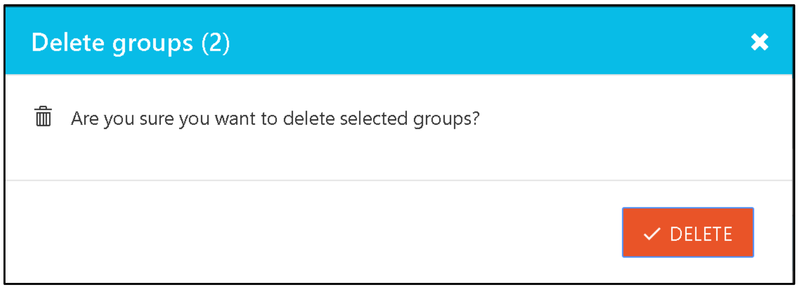
You can delete a Group or multiple Groups by selecting them and clicking the DELETE GROUPS button.



− DELETE GROUPS

☐	GROUP NAME ^
	All Active Users
☑	Corporate & Legal
☑	Engineering Group
☐	Marketing Group

You will then be prompted with a message confirming that you are okay to delete the selected users. If you are, click DELETE again.


Delete groups (2)

Are you sure you want to delete selected groups?

Once the Group(s) are deleted from Vitrium, this will effectively revoke all access that any User had as part of this Group (if the Permissions were assigned to the Group) and you will not be able to get back the Groups' information.

Delete or Deactivate?
If you do not wish to delete the Group entirely and lose all its information, you can choose to de-activate it instead by clicking the checkmark icon under the Active column and an 'X' will appear instead indicating that the Group has been de-activated. This will still revoke the Users' access to any and all files they had access to as this Group but it will keep all the Group's information in Vitrium.

4.0 DASHBOARD & REPORTS

Every Vitrium Security account comes equipped with a rich set of content analytics, available as a graphical dashboard in the DASHBOARD tab or as detailed, exportable reports in the REPORTS tab.

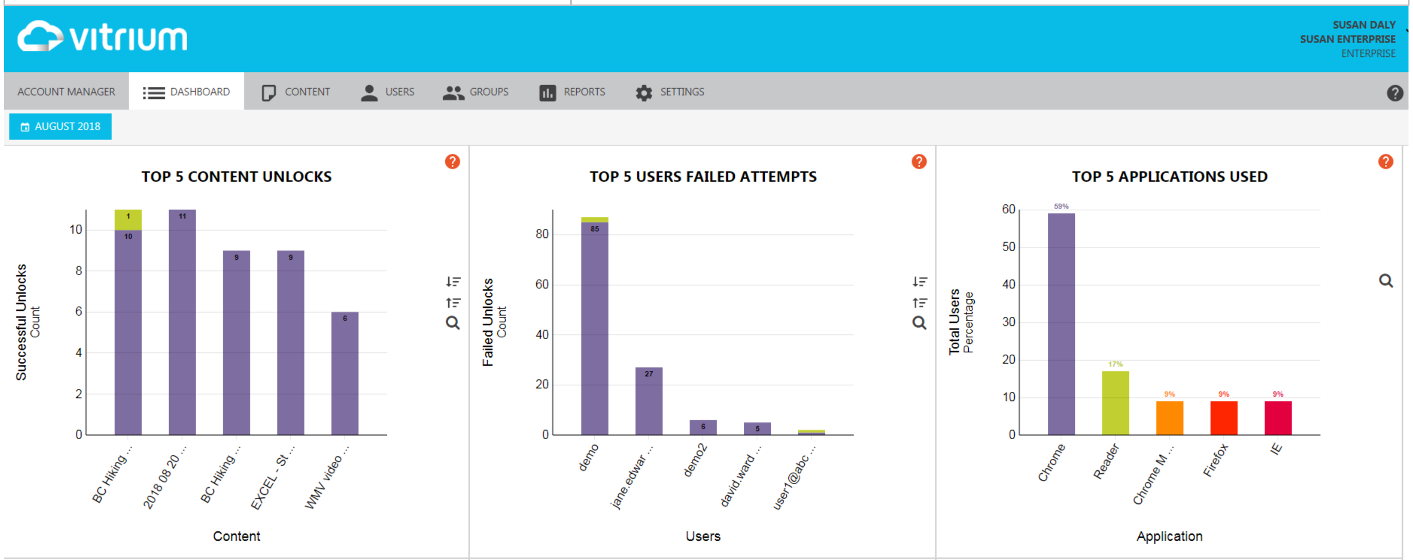
4.1 Dashboard

The dashboard is a graphical representation of the top 5 or bottom 5 of something (content, users, applications, and so on) within a given time period. You can drill in on any graph to show all the data in the report, or you can drill in on a specific file or user to only show data for that particular file or user.

DASHBOARD GRAPHS
Depending on which Vitrium Security edition you subscribe to will determine which graphs you have access to. Furthermore, some of the graphs with page-level or time-detailed information only shows data for the secured web version of the content, not the protected PDF version. This is due to limitations in PDF Reader's and how analytical data is collected over the web. The graphs that only show data with the web viewer content are indicated with an * Asterix below.

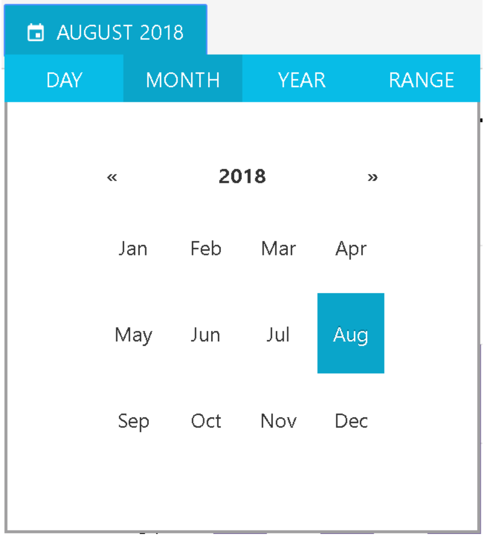
Standard accounts will see:	**Professional & Enterprise accounts will see:**
• Top 5 Content Unlocks • Top 5 Users Failed Attempts • Top 5 Applications Used • User Locations by Country	• Top 5 Content Unlocks • Top 5 Users Failed Attempts • Top 5 Applications Users • User Locations by Country • 5 Most Read Content* • 5 Most Read Users* • 5 Most Accessed Content* • 5 Most Content Spent Time On*

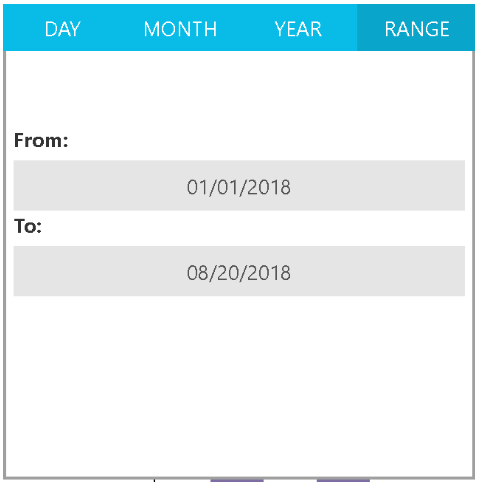
	• 5 Most Active Users* • Top 5 Users Spent Time on Content*



DATE RANGE

By default, the date range shows the current month but you can click on the Date button to change this to a specific DAY, MONTH, YEAR or a RANGE of time.





From: 01/01/2018

To: 08/20/2018

MENU ICONS

There several different icons that you'll see on each graph, each with their own unique function.

↓≡	Arranges Data from Most to Least
↑≡	Arranges Data from Least to Most
#	Shows Data by Count (# of Files or # of Users)
🕘	Shows Data by Time
🔍	Drill in to Show All Data in the Reports Tab

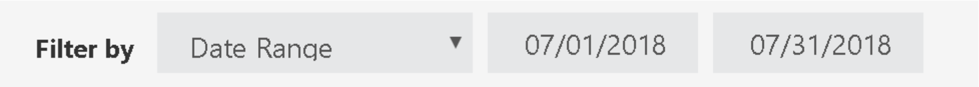
4.2 Reports

There is a wealth information collected from users accessing your protected content. The Dashboard shows the top 5 or least 5 of something, whereas the Reports show all the applicable data, in the given time period that is selected. Depending on which Vitrium Security edition you subscribe to will determine which reports you have access to. Much like the dashboard graphs, some of the reports with page-level or time-detailed information only shows data for the secured web version of the content, not the protected PDF version. This is due to limitations in PDF readers and how analytical data is collected over the web. The reports that only show data with the web viewer content are indicated with an * asterisk below:

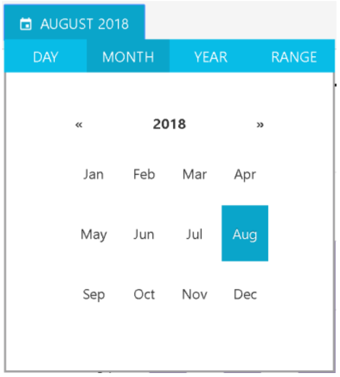
Standard accounts will see:	**Professional & Enterprise accounts will see:**
• User Activity Log	• User Activity Log
• Successful Unlocks by Content	• Successful Unlocks by Content
• Failed Unlocks by User	• Failed Unlocks by User
• User Applications	• User Applications
• User Locations by Country	• User Locations by Country
	• Read-Through-Rate by Content*
	• Read-Through-Rate by Users*
	• Views by Content*
	• Views by Users*
	• Time Spent by Content*
	• Time Spent by User*
	• View-Rate by User* (for accounts with video enabled)
	• View-Rate by User* (for accounts with video enabled)

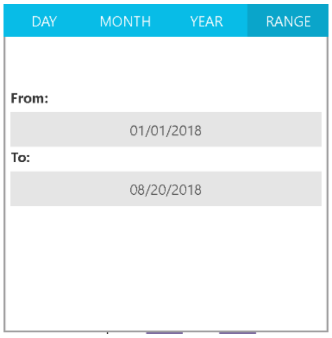
DATE RANGE

The date range for the **User Activity Log** appears differently than the other reports. You can find it as one of the drop-down options in the 'Filter by' button:



The date range for **all other Reports** appears the same as in the Dashboard with a large blue button that shows the current month but if you click on the Date button, you can change this to a specific DAY, MONTH, YEAR or a RANGE.



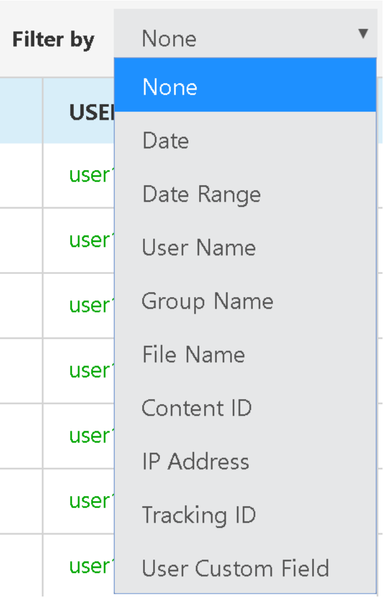


From: 01/01/2018

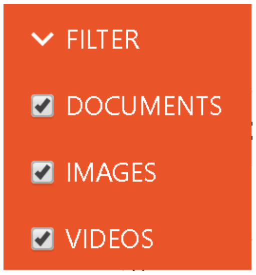
To: 08/20/2018

FILTER

The filter feature for the **User Activity Log** appears differently than the other reports but it has a lot of options to choose from including:



For **other Reports,** a different type of Filter button appears where you can filter by content type: Documents or Images or Videos (if video is enabled on your account).

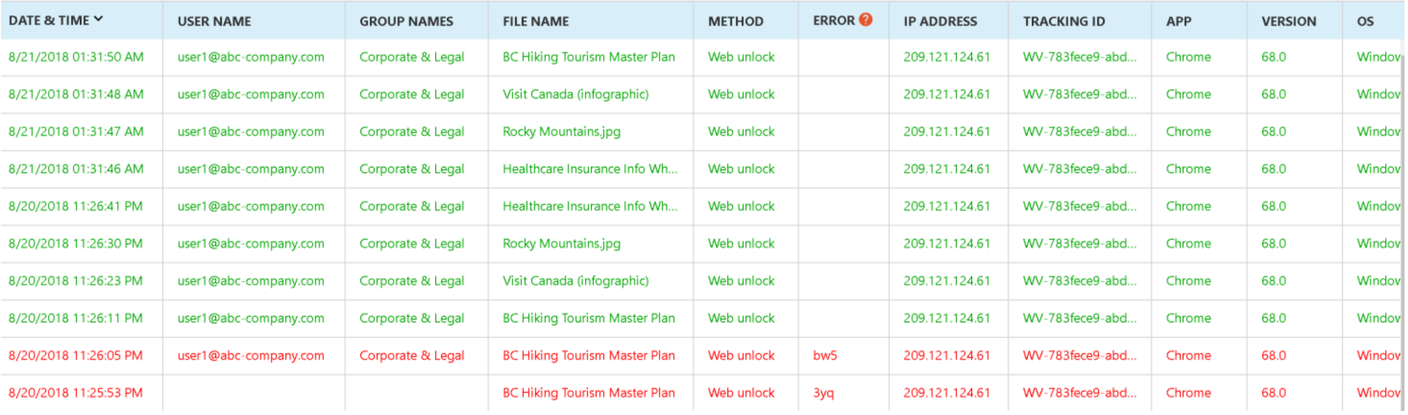


EXPORT

You can **EXPORT any report** in Vitrium. Ensure that you have the right date range selected before you export the report especially for the User Activity Log since the default view shows all activity in the report. Once ready, click the large EXPORT button and a CSV file will download.

USER ACTIVITY LOG

The *User Activity Log* report shows ALL user activity including for both web viewer unlocks/views and PDF unlocks/views. The report shows the date and time when a file was accessed, what the file name is, which user accessed the file, which group the user belongs to, which method they used to unlock the file (web or PDF), which IP address they used to unlock from, what their tracking ID is (a specific ID from their application or browser's cookie), and also which application or browser was used, what version, and what operating system they used. If there was an error, an error code would show in the error column and the whole activity would appear in red. Successful unlocks would appear in green, failed unlocks in red, and user activity that has been cleared by the Clear Use function would appear in a light gray color.

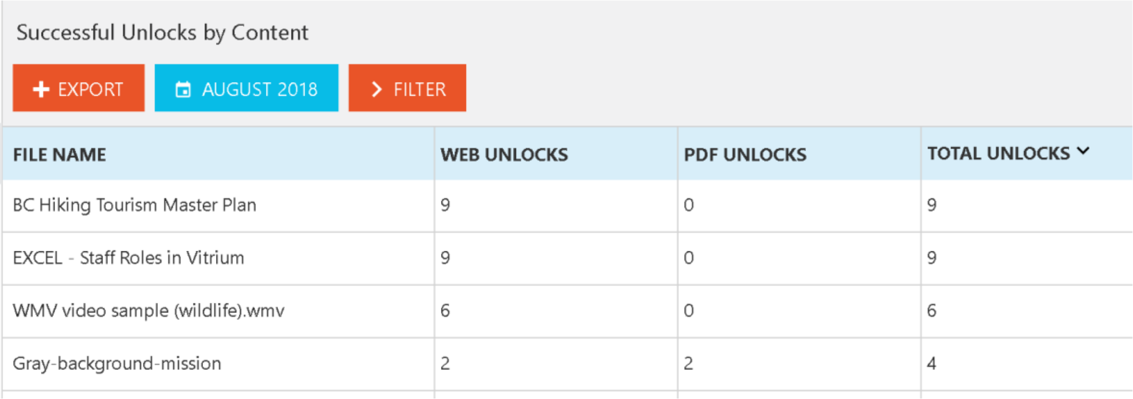


DATE & TIME ⌄	USER NAME	GROUP NAMES	FILE NAME	METHOD	ERROR ❓	IP ADDRESS	TRACKING ID	APP	VERSION	OS
8/21/2018 01:31:50 AM	user1@abc-company.com	Corporate & Legal	BC Hiking Tourism Master Plan	Web unlock		209.121.124.61	WV-783fece9-abd...	Chrome	68.0	Window
8/21/2018 01:31:48 AM	user1@abc-company.com	Corporate & Legal	Visit Canada (infographic)	Web unlock		209.121.124.61	WV-783fece9-abd...	Chrome	68.0	Window
8/21/2018 01:31:47 AM	user1@abc-company.com	Corporate & Legal	Rocky Mountains.jpg	Web unlock		209.121.124.61	WV-783fece9-abd...	Chrome	68.0	Window
8/21/2018 01:31:46 AM	user1@abc-company.com	Corporate & Legal	Healthcare Insurance Info Wh...	Web unlock		209.121.124.61	WV-783fece9-abd...	Chrome	68.0	Window
8/20/2018 11:26:41 PM	user1@abc-company.com	Corporate & Legal	Healthcare Insurance Info Wh...	Web unlock		209.121.124.61	WV-783fece9-abd...	Chrome	68.0	Window
8/20/2018 11:26:30 PM	user1@abc-company.com	Corporate & Legal	Rocky Mountains.jpg	Web unlock		209.121.124.61	WV-783fece9-abd...	Chrome	68.0	Window
8/20/2018 11:26:23 PM	user1@abc-company.com	Corporate & Legal	Visit Canada (infographic)	Web unlock		209.121.124.61	WV-783fece9-abd...	Chrome	68.0	Window
8/20/2018 11:26:11 PM	user1@abc-company.com	Corporate & Legal	BC Hiking Tourism Master Plan	Web unlock		209.121.124.61	WV-783fece9-abd...	Chrome	68.0	Window
8/20/2018 11:26:05 PM	user1@abc-company.com	Corporate & Legal	BC Hiking Tourism Master Plan	Web unlock	bw5	209.121.124.61	WV-783fece9-abd...	Chrome	68.0	Window
8/20/2018 11:25:53 PM			BC Hiking Tourism Master Plan	Web unlock	3yq	209.121.124.61	WV-783fece9-abd...	Chrome	68.0	Window

SUCCESSFUL UNLOCKS BY CONTENT

<u>Report (below)</u>

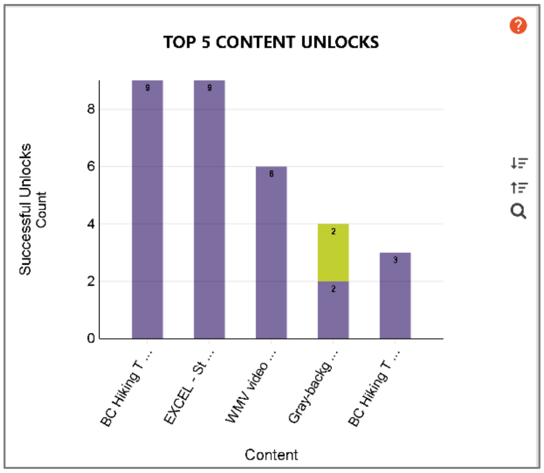
This report shows the number of times your content has been unlocked or viewed by end users, including the web and PDF unlocks, and total unlocks. For Enterprise accounts that utilize single sign-on (SSO), you can consider 'unlocks' the same as 'views'.



FILE NAME	WEB UNLOCKS	PDF UNLOCKS	TOTAL UNLOCKS ⌄
BC Hiking Tourism Master Plan	9	0	9
EXCEL - Staff Roles in Vitrium	9	0	9
WMV video sample (wildlife).wmv	6	0	6
Gray-background-mission	2	2	4

Graph (right)

The associated dashboard graph *Top 5 Most Content Unlocks* is the same representative of the Successful Unlocks report except that it shows only the top 5 files. The color will appear purple to represent web unlocks and green to represent the PDF unlocks.



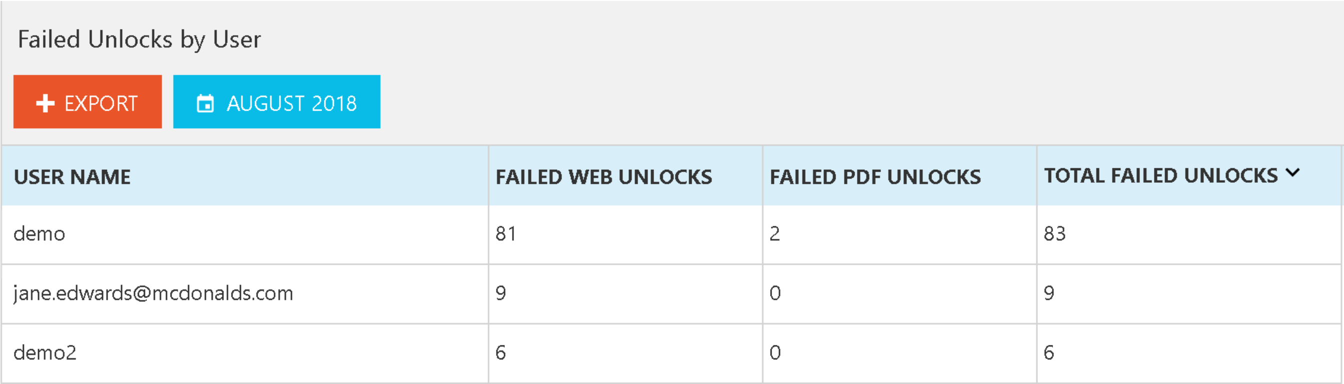
Drill-In Functionality

If you drill down on a specific file, you'll see the full list of users that have unlocked or viewed this content.

FAILED UNLOCKS BY USER

Report (below)

This report shows which of your end users is having the most 'difficulty' in accessing your protected content. This allows you, as the Vitrium administrator, to determine who to reach out to and what type of assistance you can provide. For example, if you see a particular user has numerous failed attempts and they all relate to error code 'bw5' which indicates they're using the wrong login credentials, you can reach out to the user and remind them of what the correct username and password they should be using.

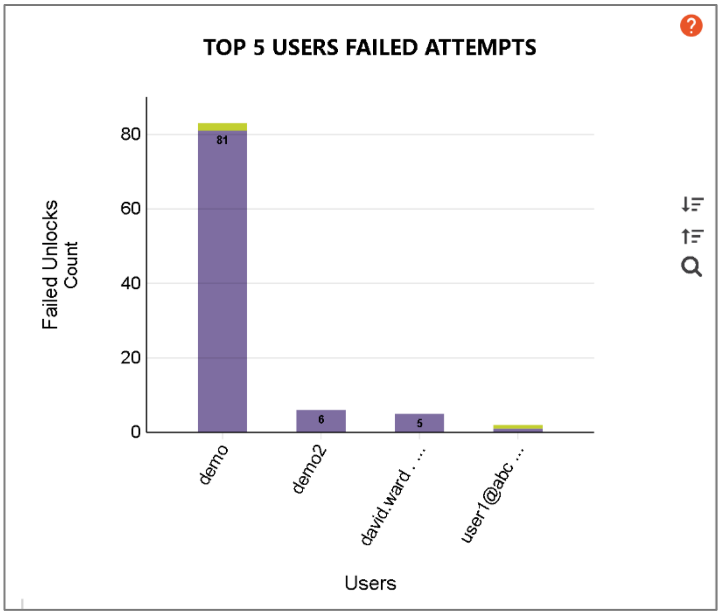


Failed Unlocks by User

USER NAME	FAILED WEB UNLOCKS	FAILED PDF UNLOCKS	TOTAL FAILED UNLOCKS ⌄
demo	81	2	83
jane.edwards@mcdonalds.com	9	0	9
demo2	6	0	6

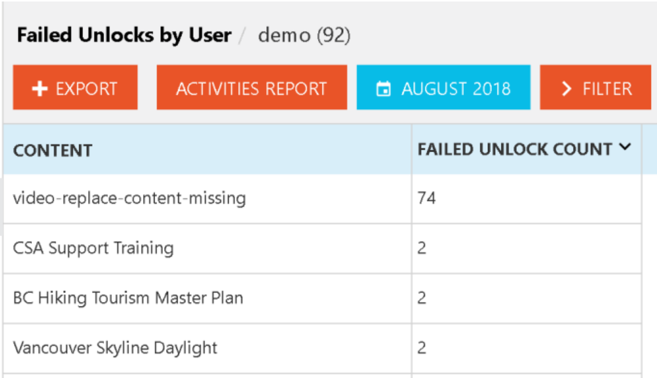
Graph (right)

The associated dashboard graph *Top 5 Users Failed Attempts* is the same representative of the Failed Unlocks report except that it shows only the top 5 users whereas the report will show all the users. The color will appear purple to represent failed web unlocks and green to represent failed PDF unlocks.



Drill-In Functionality

If you drill down on a specific user, you'll see the full list of content that the user has failed to unlock.



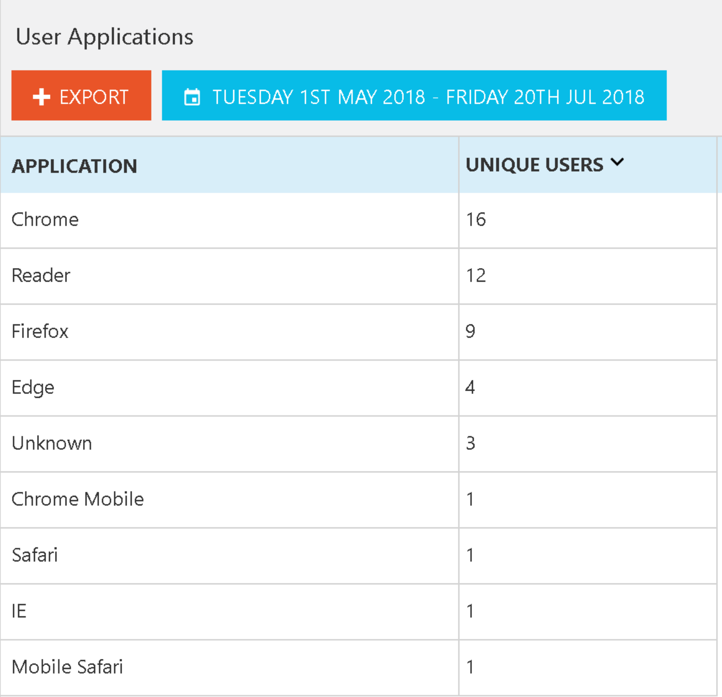
Failed Unlocks by User / demo (92)

CONTENT	FAILED UNLOCK COUNT
video-replace-content-missing	74
CSA Support Training	2
BC Hiking Tourism Master Plan	2
Vancouver Skyline Daylight	2

USER APPLICATIONS

Report (right)

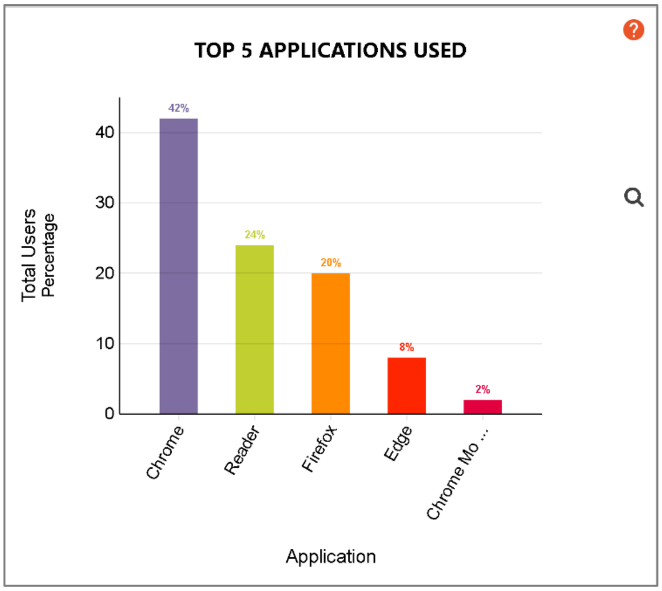
This report shows which applications or browsers your end users used to unlock or access your content from, whether it was Chrome, Firefox, IE, Edge, Safari, Chrome Mobile, Safari Mobile (as some of the more popular web browsers), or Adobe Reader or Acrobat or Foxit Reader (as the PDF viewing application).


User Applications

APPLICATION	UNIQUE USERS
Chrome	16
Reader	12
Firefox	9
Edge	4
Unknown	3
Chrome Mobile	1
Safari	1
IE	1
Mobile Safari	1

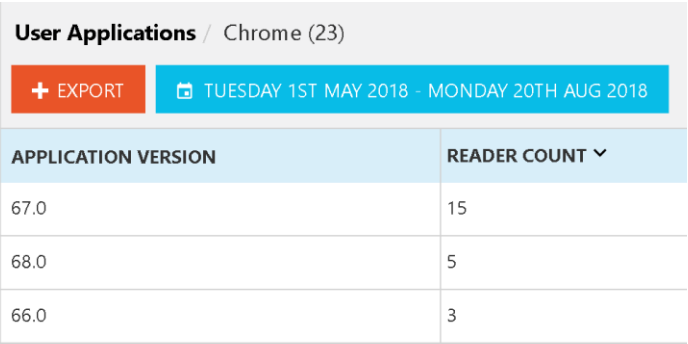
Graph (left)

The associated dashboard graph *Top 5 Applications Used* is the same representative of this report except that it shows only the top 5 applications whereas the report will show all applications.



Drill-In Functionality

If you drill down on a specific application, you'll see the various versions of that application used.

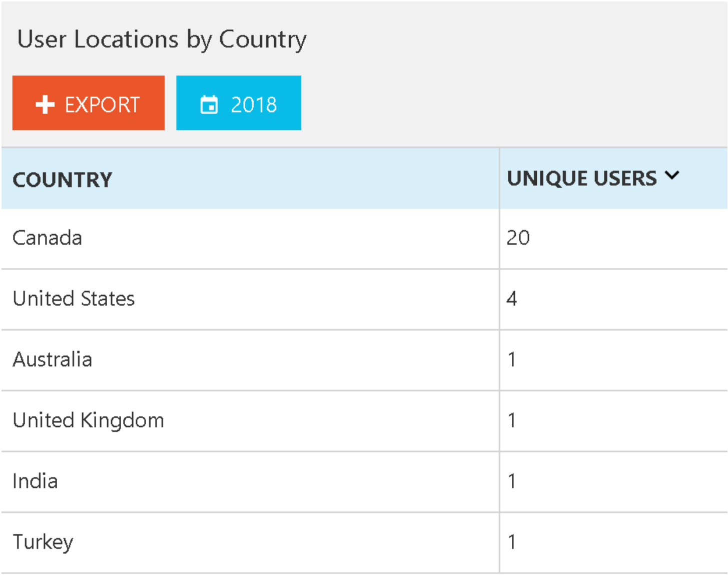

User Applications / Chrome (23)

APPLICATION VERSION	READER COUNT
67.0	15
68.0	5
66.0	3

USER LOCATIONS BY COUNTRY

Report (right)

This report shows which country your users have been accessing your protected content from. This information is based on the user's IP address.

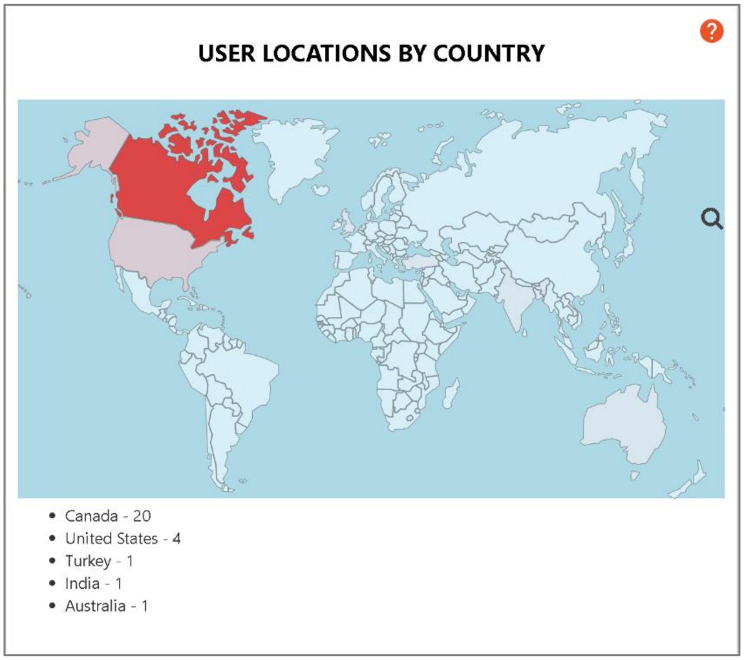


User Locations by Country

COUNTRY	UNIQUE USERS
Canada	20
United States	4
Australia	1
United Kingdom	1
India	1
Turkey	1

Graph (left)

The associated dashboard graph *User Locations by Country* is the same representative of this report except that it shows only the top 5 countries whereas the report will show all countries.

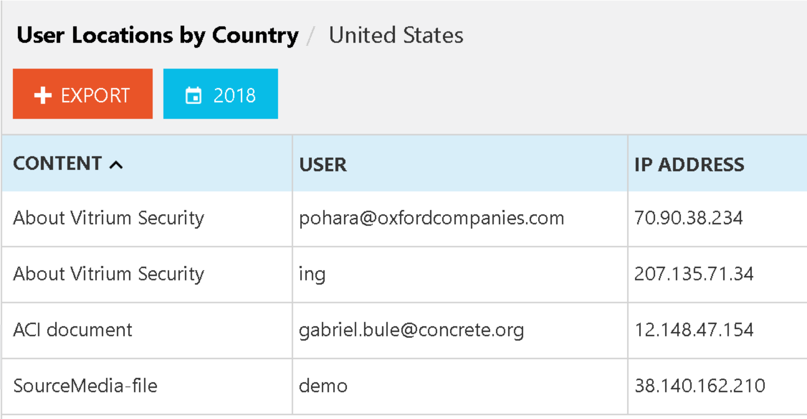


USER LOCATIONS BY COUNTRY

- Canada - 20
- United States - 4
- Turkey - 1
- India - 1
- Australia - 1

Drill-In Functionality

If you drill down on a specific country, you'll see the various content accessed and users from that country.



User Locations by Country / United States

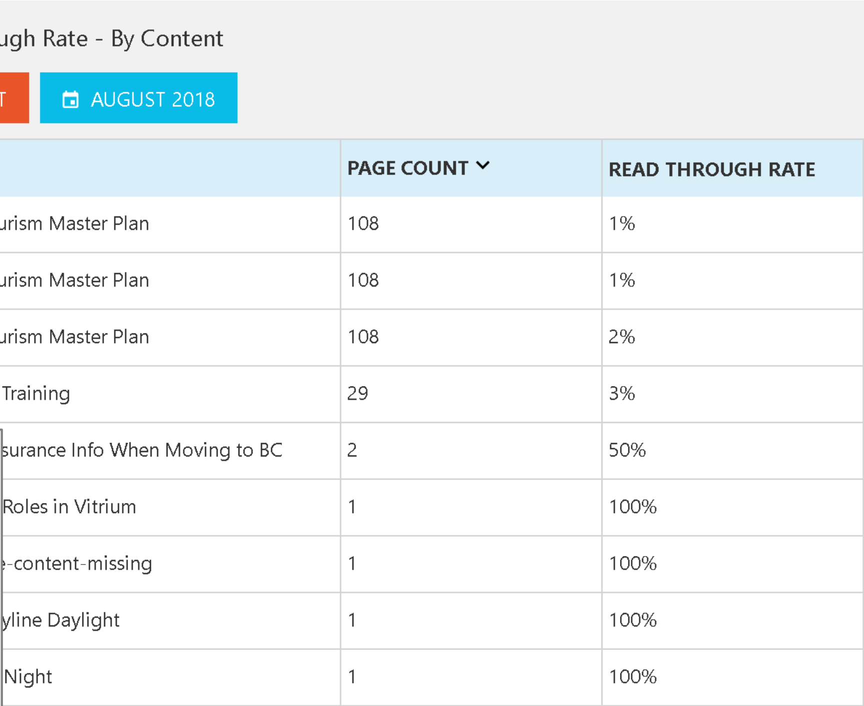
CONTENT	USER	IP ADDRESS
About Vitrium Security	pohara@oxfordcompanies.com	70.90.38.234
About Vitrium Security	ing	207.135.71.34
ACI document	gabriel.bule@concrete.org	12.148.47.154
SourceMedia-file	demo	38.140.162.210

READ-THROUGH-RATE BY CONTENT

(Available in Professional & Enterprise accounts only)

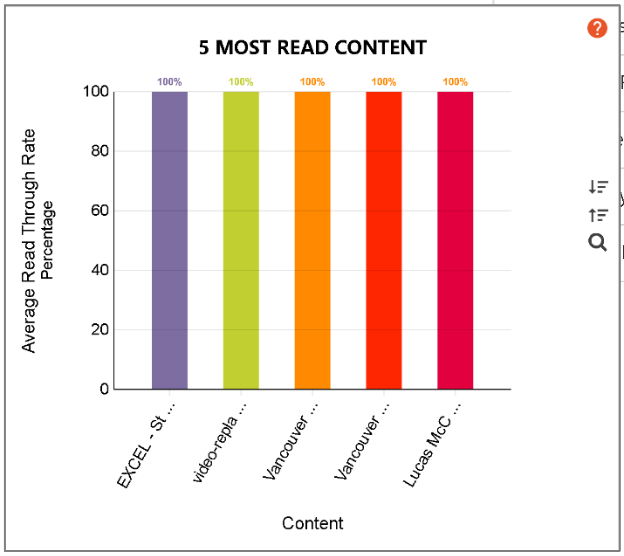
Report (right)

This report shows the average read-through-rate (RTR) among all users who viewed the file within the selected date range. RTR is the percentage of all pages in a document that all users have read cumulatively.



Read Through Rate - By Content

FILE NAME	PAGE COUNT ⌄	READ THROUGH RATE
BC Hiking Tourism Master Plan	108	1%
BC Hiking Tourism Master Plan	108	1%
BC Hiking Tourism Master Plan	108	2%
CSA Support Training	29	3%
surance Info When Moving to BC	2	50%
Roles in Vitrium	1	100%
-content-missing	1	100%
yline Daylight	1	100%
Night	1	100%

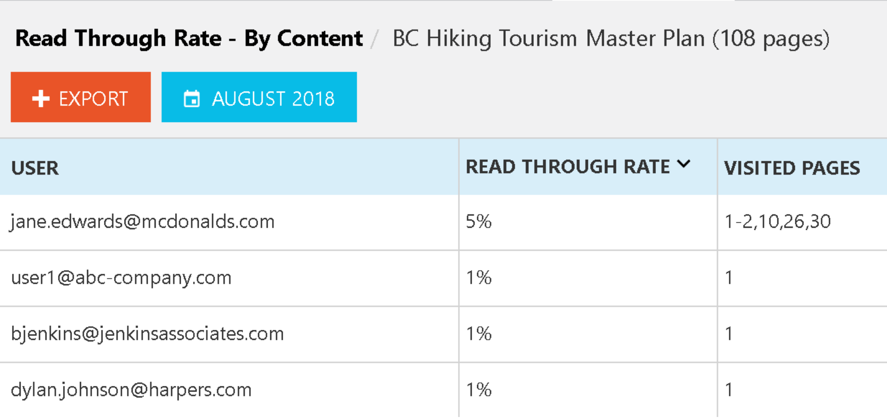


Graph (left)

The associated dashboard graph *Top 5 Most Read Content* is the same representative of this report except that it shows only the top 5 content whereas the report will show all content.

Drill-In Functionality

If you drill down on a specific file, you'll see the various users that have accessed and read that content.



Read Through Rate - By Content / BC Hiking Tourism Master Plan (108 pages)

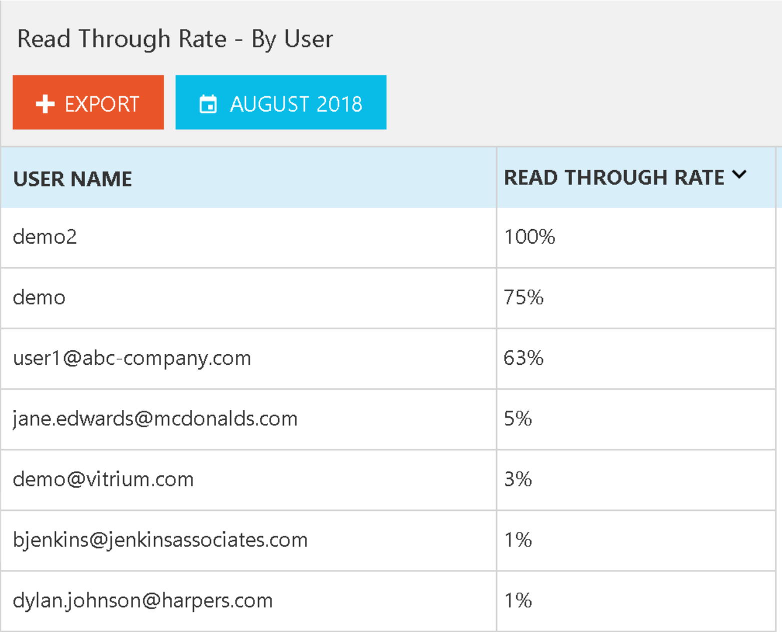
USER	READ THROUGH RATE ⌄	VISITED PAGES
jane.edwards@mcdonalds.com	5%	1-2,10,26,30
user1@abc-company.com	1%	1
bjenkins@jenkinsassociates.com	1%	1
dylan.johnson@harpers.com	1%	1

READ-THROUGH-RATE BY USER

(Available in Professional & Enterprise accounts only)

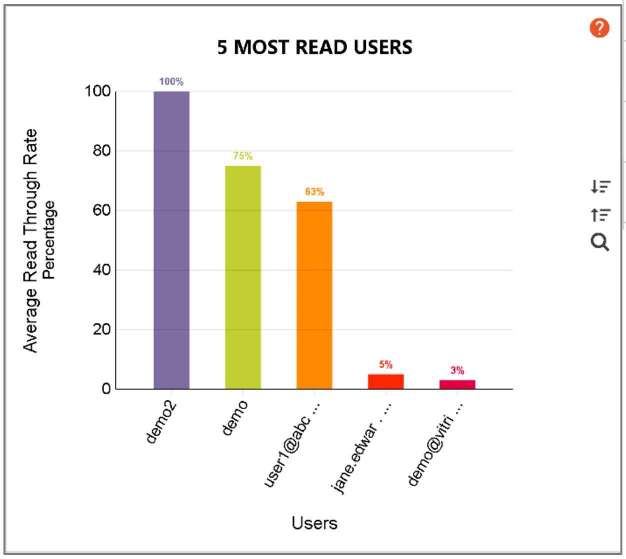
Report (right)

This report shows the average read-through-rate (RTR) for a user among all the files they viewed within the selected date range. RTR by user is the percentage of the reading intensity of each respective user.



Read Through Rate - By User

USER NAME	READ THROUGH RATE ⌄
demo2	100%
demo	75%
user1@abc-company.com	63%
jane.edwards@mcdonalds.com	5%
demo@vitrium.com	3%
bjenkins@jenkinsassociates.com	1%
dylan.johnson@harpers.com	1%

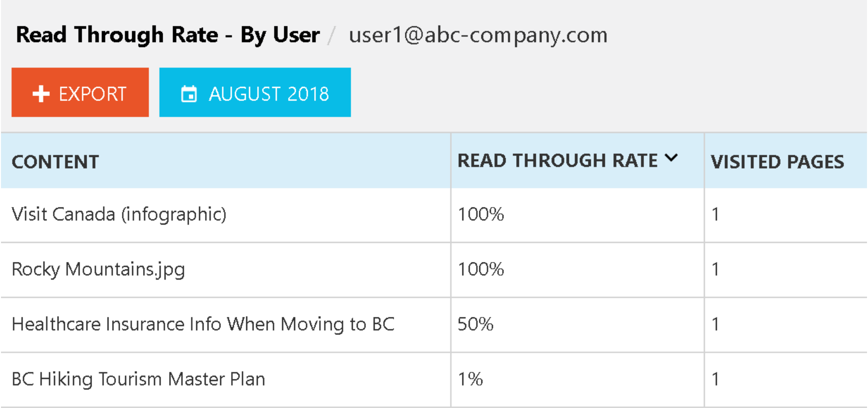


Graph (left)

The associated dashboard graph *Top 5 Most Read Users* is the same representative of this report except that it shows only the top 5 users whereas the report will show all users.

Drill-In Functionality

If you drill down on a specific user, you'll see the various files that the user has accessed and read.



Read Through Rate - By User / user1@abc-company.com

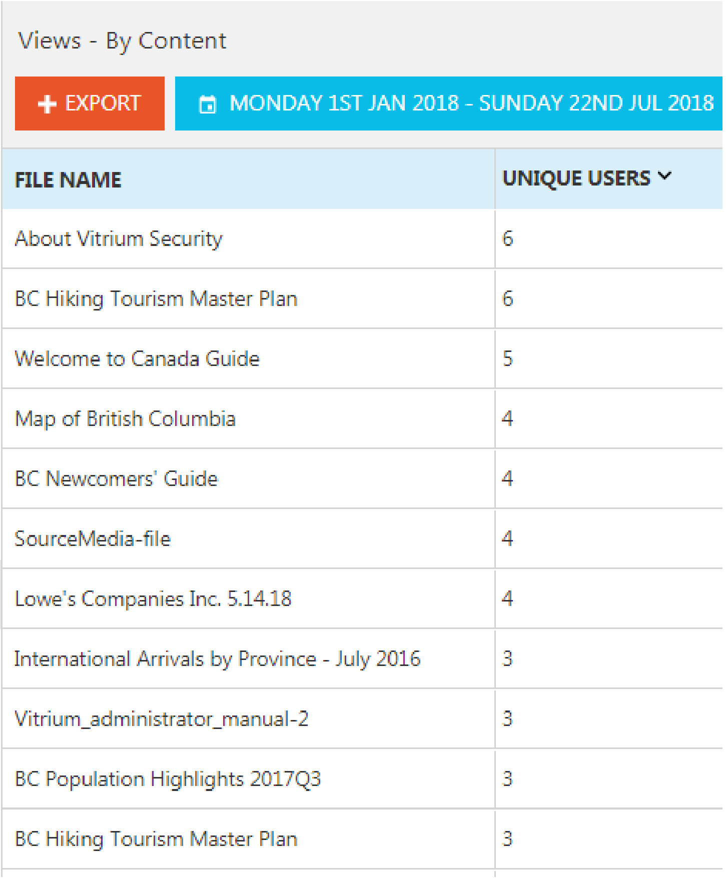
CONTENT	READ THROUGH RATE ⌄	VISITED PAGES
Visit Canada (infographic)	100%	1
Rocky Mountains.jpg	100%	1
Healthcare Insurance Info When Moving to BC	50%	1
BC Hiking Tourism Master Plan	1%	1

VIEWS BY CONTENT

(Available in Professional & Enterprise accounts only)

Report (right)

This report shows the total number of unique users who have viewed and accessed all the files within the selected date range.

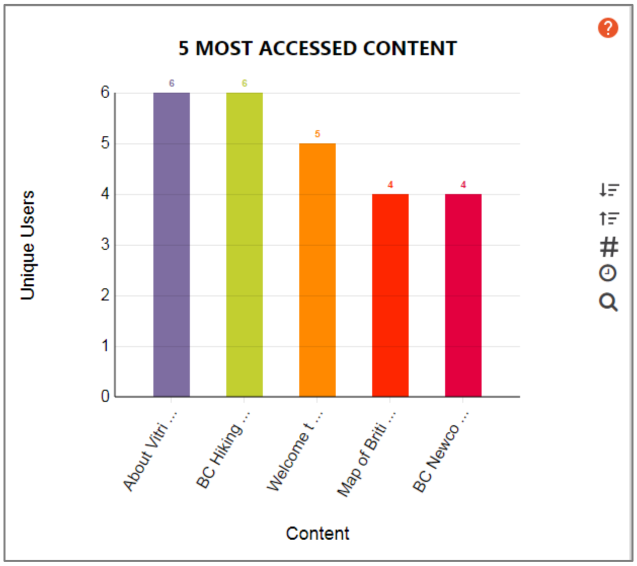


Views - By Content

FILE NAME	UNIQUE USERS
About Vitrium Security	6
BC Hiking Tourism Master Plan	6
Welcome to Canada Guide	5
Map of British Columbia	4
BC Newcomers' Guide	4
SourceMedia-file	4
Lowe's Companies Inc. 5.14.18	4
International Arrivals by Province - July 2016	3
Vitrium_administrator_manual-2	3
BC Population Highlights 2017Q3	3
BC Hiking Tourism Master Plan	3

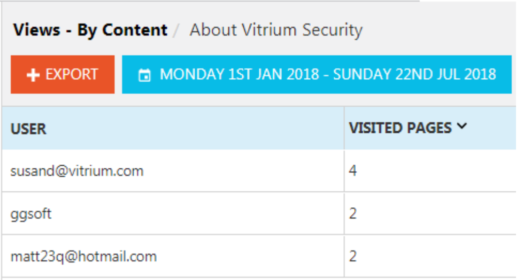
Graph (below)

The associated dashboard graph *Top 5 Most Accessed Content* is the same representative of this report except that it shows only the top 5 files whereas the report will show all files for the time period you have selected.



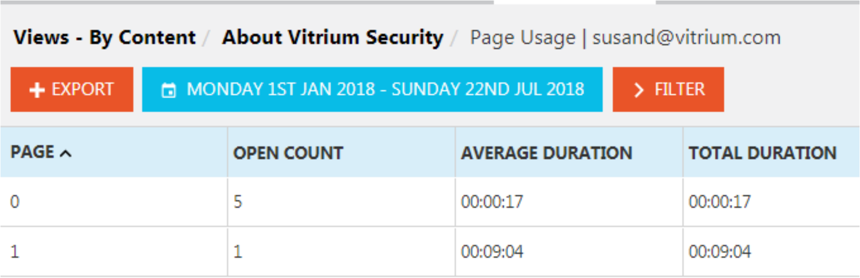
Drill-In Functionality

If you drill down on a specific file, you'll see the users that have accessed that file and what pages they've viewed (screenshot below on left), and if you drill in one more step by clicking on a particular user, you will see more details about how much time they spent on each page (screenshot below on right).



Views - By Content / About Vitrium Security

USER	VISITED PAGES
susand@vitrium.com	4
ggsoft	2
matt23q@hotmail.com	2

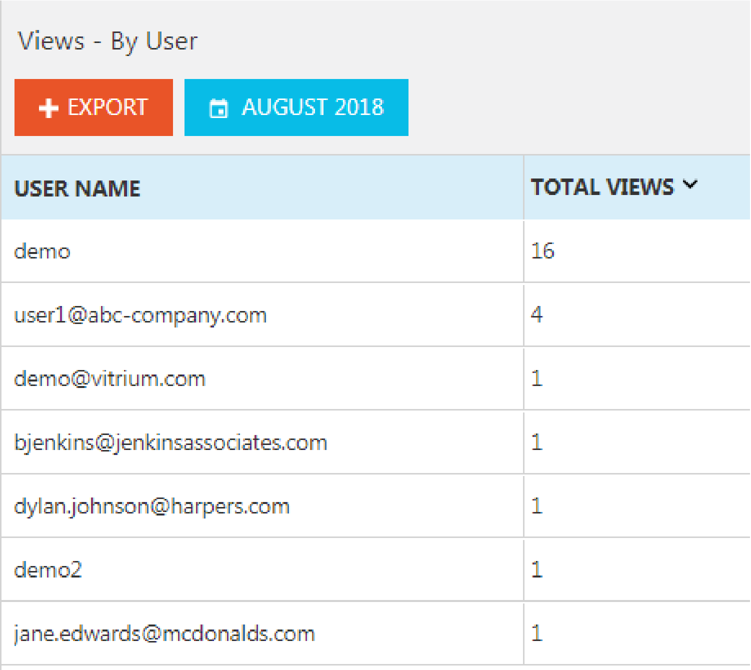


Views - By Content / **About Vitrium Security** / Page Usage | susand@vitrium.com

PAGE	OPEN COUNT	AVERAGE DURATION	TOTAL DURATION
0	5	00:00:17	00:00:17
1	1	00:09:04	00:09:04

VIEWS BY USERS

(Available in Professional & Enterprise accounts only)



Views - By User

+ EXPORT | AUGUST 2018

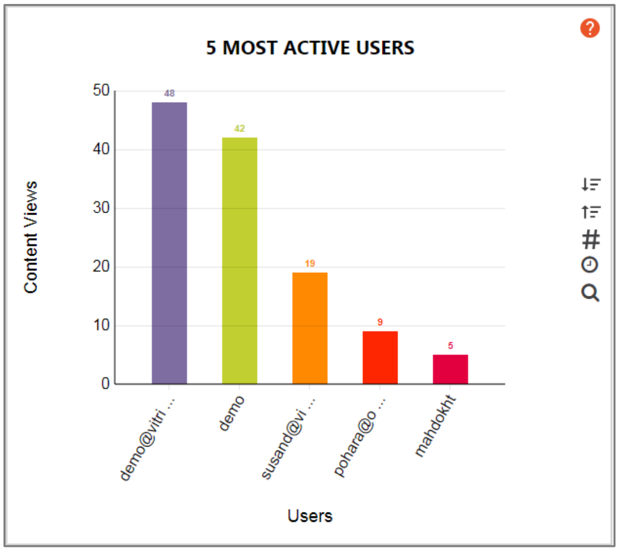
USER NAME	TOTAL VIEWS ˅
demo	16
user1@abc-company.com	4
demo@vitrium.com	1
bjenkins@jenkinsassociates.com	1
dylan.johnson@harpers.com	1
demo2	1
jane.edwards@mcdonalds.com	1

Report (right)

This report shows the total views by each user within the selected date range.

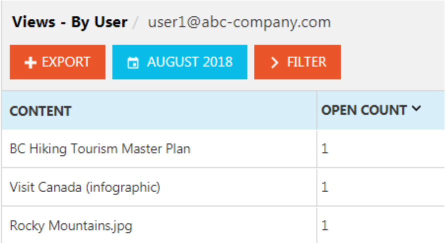
Graph (below)

The associated dashboard graph *Top 5 Most Active Users* is the same representative of this report except that it shows only the top 5 users whereas the report will show all users for the time period you have selected.



Drill-In Functionality

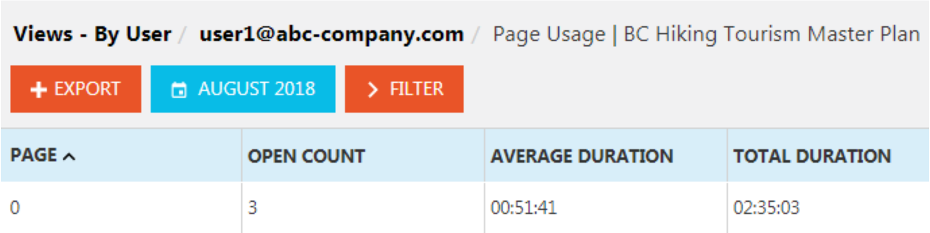
If you drill down on a specific user, you'll see all the files that user has accessed and how many times they opened the file (screenshot below on left), and if you drill in further on a particular file, you will see more details about what pages were viewed and how much time was spent on each page (screenshot below on right).



Views - By User / user1@abc-company.com

+ EXPORT | AUGUST 2018 | > FILTER

CONTENT	OPEN COUNT ˅
BC Hiking Tourism Master Plan	1
Visit Canada (infographic)	1
Rocky Mountains.jpg	1



Views - By User / **user1@abc-company.com** / Page Usage | BC Hiking Tourism Master Plan

+ EXPORT | AUGUST 2018 | > FILTER

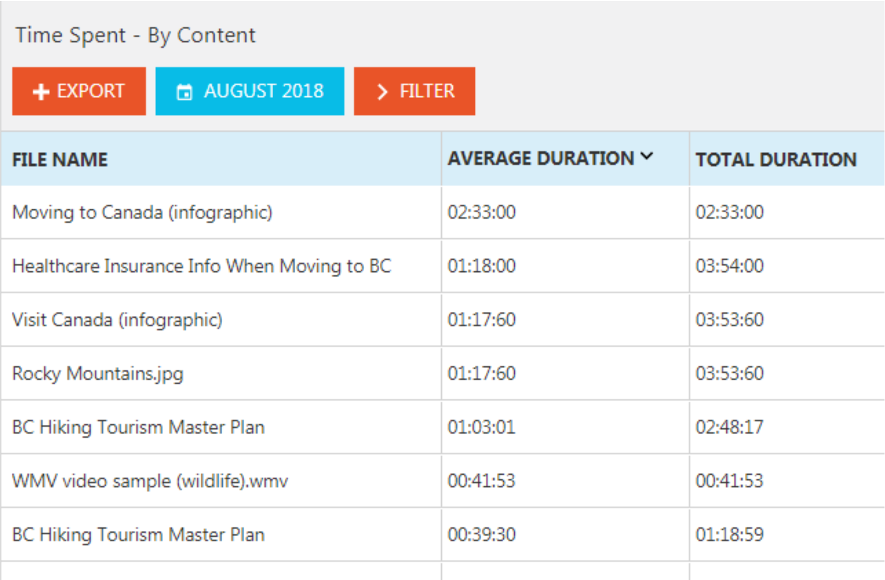
PAGE ˄	OPEN COUNT	AVERAGE DURATION	TOTAL DURATION
0	3	00:51:41	02:35:03

TIME SPENT BY CONTENT

(Available in Professional & Enterprise accounts only)

Report (right)

This report shows the time spent (by all users) for a particular file, as an average duration of all the users and as the total duration spent by all the users. The data shown is based on the selected date range.

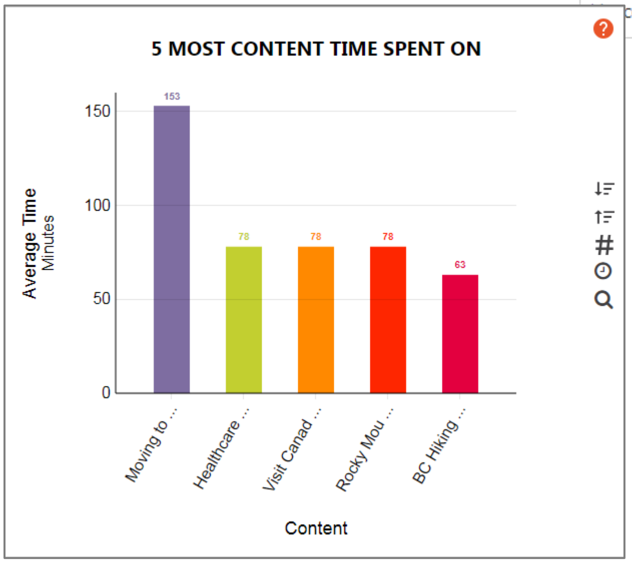


Time Spent - By Content

FILE NAME	AVERAGE DURATION	TOTAL DURATION
Moving to Canada (infographic)	02:33:00	02:33:00
Healthcare Insurance Info When Moving to BC	01:18:00	03:54:00
Visit Canada (infographic)	01:17:60	03:53:60
Rocky Mountains.jpg	01:17:60	03:53:60
BC Hiking Tourism Master Plan	01:03:01	02:48:17
WMV video sample (wildlife).wmv	00:41:53	00:41:53
BC Hiking Tourism Master Plan	00:39:30	01:18:59
couver at Night	00:38:30	01:16:60

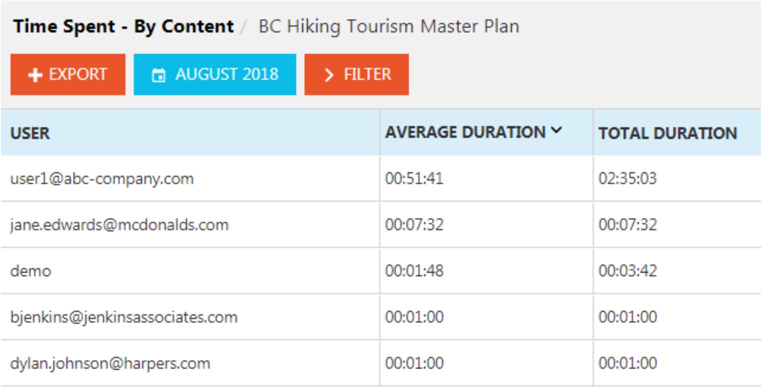
Graph (below)

The associated dashboard graph *Top 5 Most Content Time Spent On* is the same representative of this report except that it shows only the top 5 files whereas the report will show all files for the time period selected.



Drill-In Functionality (screenshot below)

If you drill down on a specific file, you'll see all the users that have accessed that file and what their average and total duration of time spent on the file was.



Time Spent - By Content / BC Hiking Tourism Master Plan

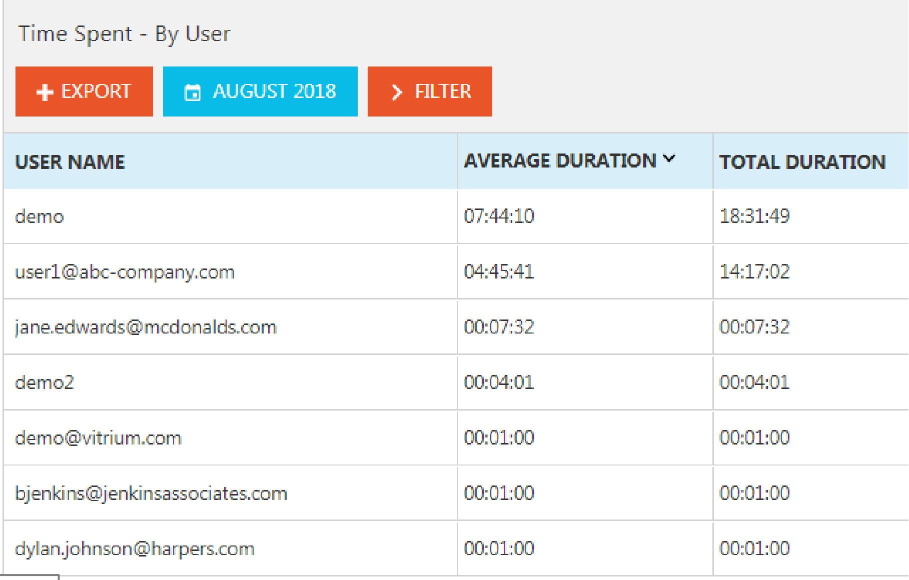
USER	AVERAGE DURATION	TOTAL DURATION
user1@abc-company.com	00:51:41	02:35:03
jane.edwards@mcdonalds.com	00:07:32	00:07:32
demo	00:01:48	00:03:42
bjenkins@jenkinsassociates.com	00:01:00	00:01:00
dylan.johnson@harpers.com	00:01:00	00:01:00

TIME SPENT BY USER

(Available in Professional & Enterprise accounts only)

Report (right)

This report shows the time spent (on all files) for a particular user, as an average duration for all the files and as the total duration spent on all the files. The data shown is based on the selected date range.

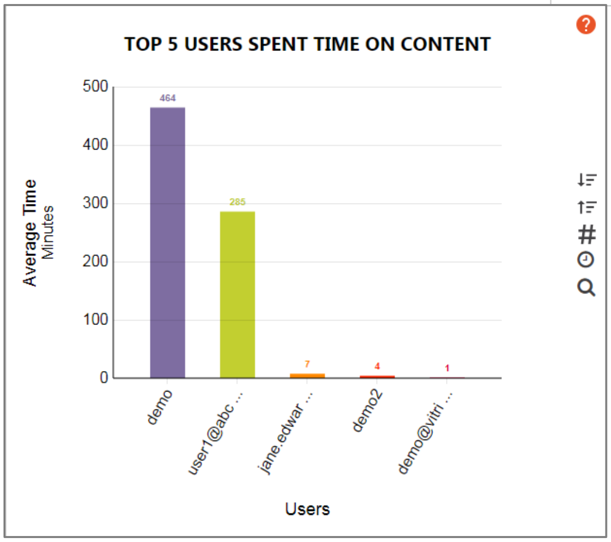


Time Spent - By User

USER NAME	AVERAGE DURATION	TOTAL DURATION
demo	07:44:10	18:31:49
user1@abc-company.com	04:45:41	14:17:02
jane.edwards@mcdonalds.com	00:07:32	00:07:32
demo2	00:04:01	00:04:01
demo@vitrium.com	00:01:00	00:01:00
bjenkins@jenkinsassociates.com	00:01:00	00:01:00
dylan.johnson@harpers.com	00:01:00	00:01:00

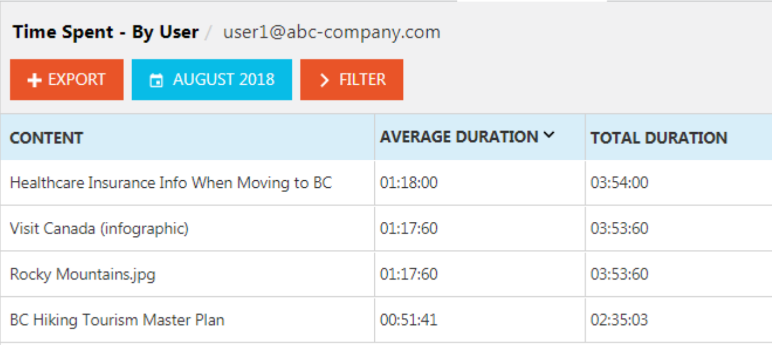
Graph (below)

The associated dashboard graph *Top 5 Users Spent Time on Content* is the same representative of this report except that it shows only the top 5 users whereas the report will show all users for the time period selected.



Drill-In Functionality (screenshot below)

If you drill down on a specific user, you'll see all the file that user has accessed and what their average and total duration of time spent on the file was.



Time Spent - By User / user1@abc-company.com

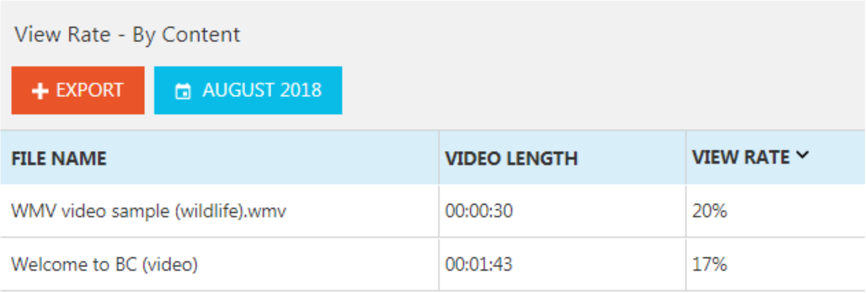
CONTENT	AVERAGE DURATION	TOTAL DURATION
Healthcare Insurance Info When Moving to BC	01:18:00	03:54:00
Visit Canada (infographic)	01:17:60	03:53:60
Rocky Mountains.jpg	01:17:60	03:53:60
BC Hiking Tourism Master Plan	00:51:41	02:35:03

VIEW-RATE BY CONTENT

(Available in Professional & Enterprise accounts only and requires video to be enabled on the account)

Report (right)

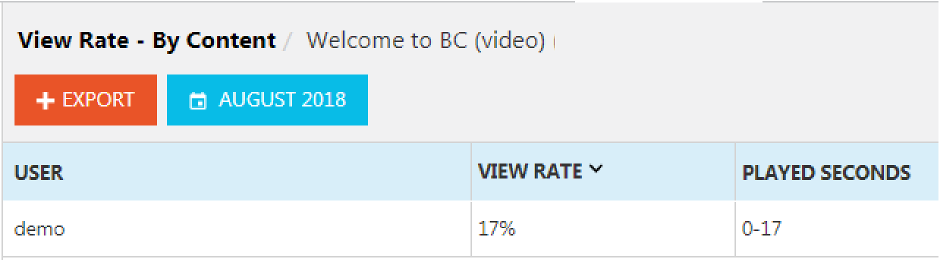
This report shows the percentage of time that all users spent on watching a particular video, within the time period selected.



FILE NAME	VIDEO LENGTH	VIEW RATE
WMV video sample (wildlife).wmv	00:00:30	20%
Welcome to BC (video)	00:01:43	17%

Drill-In Functionality (below)

If you drill down on a specific video, you'll see all the users that have watched the video and what their percentage of time was spent viewing the video.



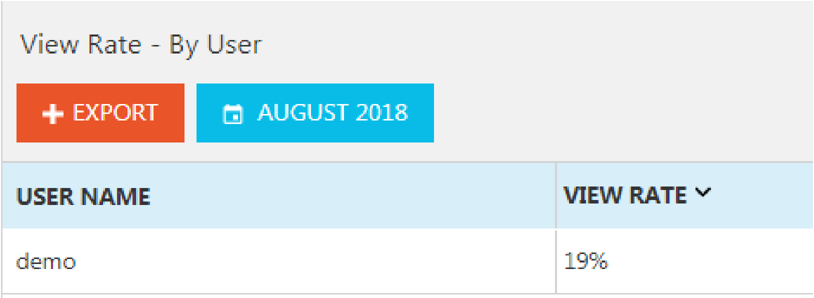
USER	VIEW RATE	PLAYED SECONDS
demo	17%	0-17

VIEW-RATE BY USER

(Available in Professional & Enterprise accounts only and requires video to be enabled on the account)

Report (right)

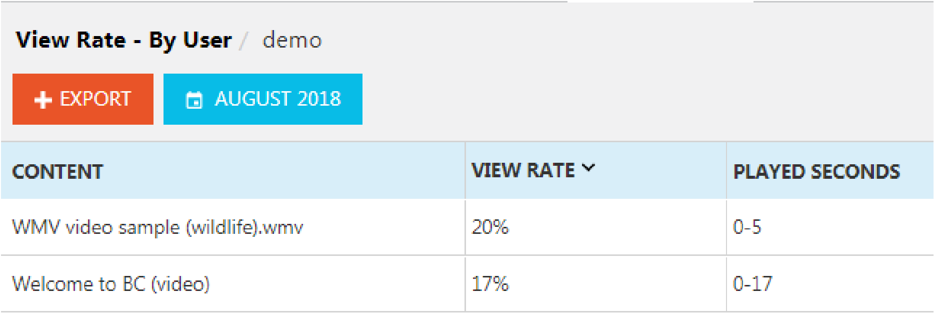
This report shows the percentage of time that each user spent watching all the videos, within the time period selected.



USER NAME	VIEW RATE
demo	19%

Drill-In Functionality (below)

If you drill down on a specific user, you'll see all the videos that user has watched and what their percentage of time was spent viewing each video.



CONTENT	VIEW RATE	PLAYED SECONDS
WMV video sample (wildlife).wmv	20%	0-5
Welcome to BC (video)	17%	0-17

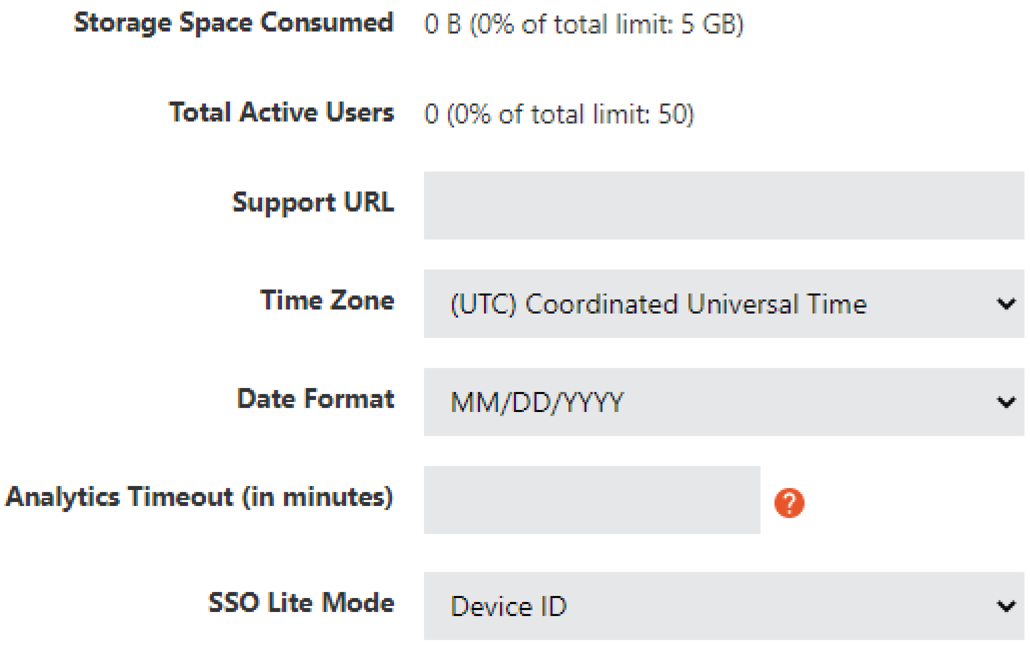
5.0 SETTINGS TAB

This tab allows you to set up a variety of settings related to your Vitrium Security account including Watermark Settings, Content Settings, DRM Policy Settings, as well as adding Staff Users, setting up a User Portal, and viewing your Account Settings and My Profile.

5.1 Account Settings

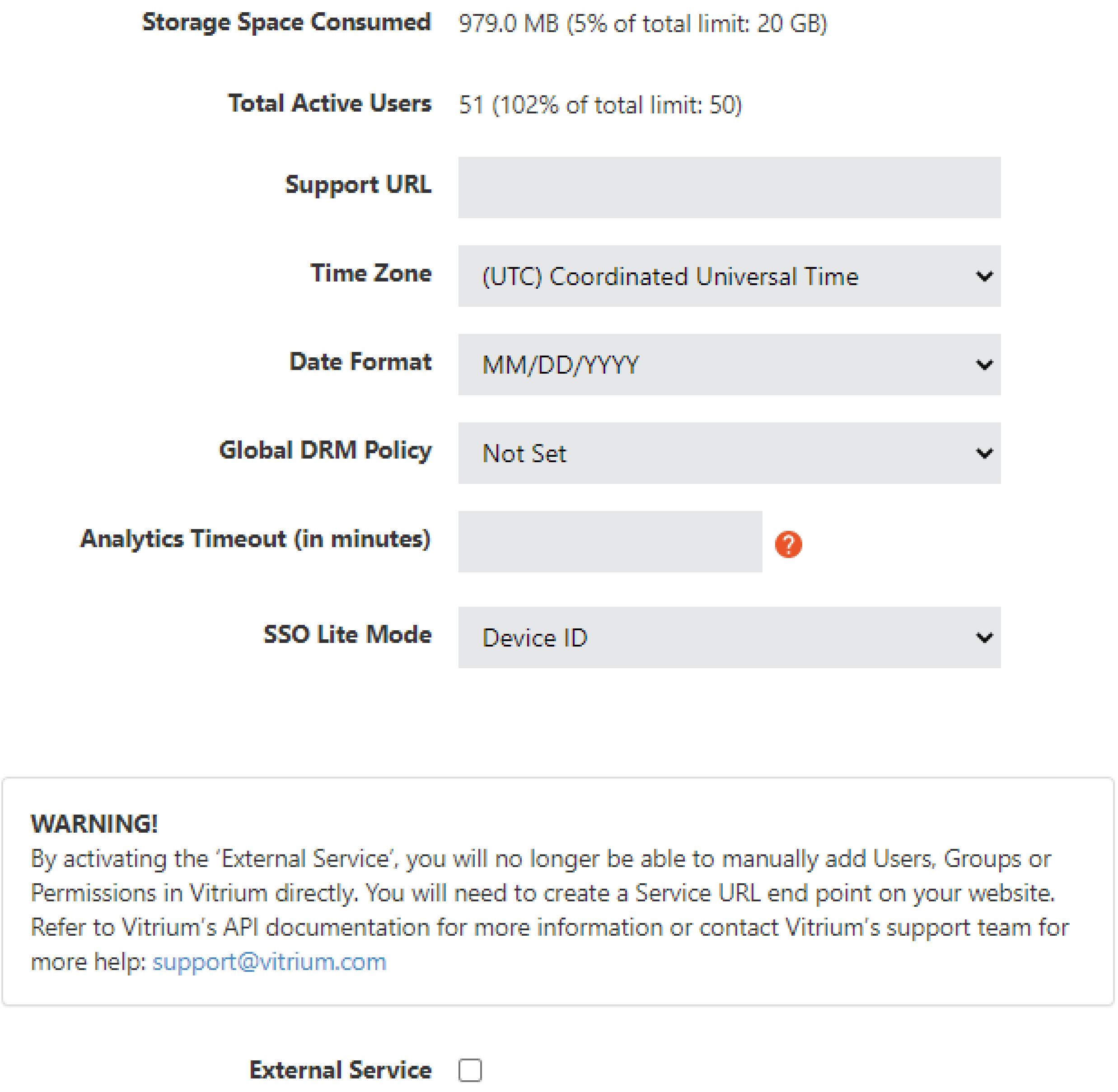
Depending on which edition of Vitrium Security you subscribe to, you may see different fields in your Account Settings.

What Standard & Professional accounts will see:



Storage Space Consumed	0 B (0% of total limit: 5 GB)
Total Active Users	0 (0% of total limit: 50)
Support URL	
Time Zone	(UTC) Coordinated Universal Time
Date Format	MM/DD/YYYY
Analytics Timeout (in minutes)	
SSO Lite Mode	Device ID

<u>What enterprise accounts will see:</u>



Storage Space Consumed	979.0 MB (5% of total limit: 20 GB)
Total Active Users	51 (102% of total limit: 50)
Support URL	
Time Zone	(UTC) Coordinated Universal Time
Date Format	MM/DD/YYYY
Global DRM Policy	Not Set
Analytics Timeout (in minutes)	
SSO Lite Mode	Device ID

WARNING!
By activating the 'External Service', you will no longer be able to manually add Users, Groups or Permissions in Vitrium directly. You will need to create a Service URL end point on your website. Refer to Vitrium's API documentation for more information or contact Vitrium's support team for more help: support@vitrium.com

External Service ☐

STORAGE SPACE CONSUMED
This is the total storage space being consumed by this account on Vitrium's servers (if you are hosted with Vitrium) or on your company's servers (if you have Vitrium installed on your environment). <u>The limit shown here is the Storage Limit</u> which is different than the File Limit. These are defined here:

File Limit: the total size limit of your original files
Storage Limit: the total size limit of the storage space being consumed on Vitrium's servers (this will often be 3-5x more than your original files for the reasons listed below)

<u>What Vitrium stores on its server:</u>

For every 1 document or image (original file) uploaded into Vitrium, Vitrium stores 3 different copies:

- 1 copy of the original file
- 1 copy of the protected PDF file
- 1 copy of the web viewer file

For every 1 video (original file) uploaded into Vitrium, Vitrium will store 4 different copies:

- 1 copy of the original video
- Up to 4 additional copies of the web viewer file at various bitrates

SUPPORT URL

This is an optional field. If you would like to direct your users to a particular support page, this URL will show up in some of the error messages that the user may encounter when trying to unlock or view their content. The support URL may not appear in all error messages since the error may be related to a server connection issue or a single sign-on (SSO) issue which is generated from the customer's side, not Vitrium's side.

TIME ZONE

This is the time zone that is associated with your Vitrium account in the reports section. We recommend you change it to your local time zone as the default is UTC.

ANALYRICS TIMEOUT (IN MINUTES)

Our Web Viewer collects analytics to capture how long a user "reads" or remains on a page and which page(s) the user has navigated to. If a user does not move to a new page within the default 10 minutes, the system will assume the user is not actively reading the page and stop collecting statistics until they move to a new page.

The default internal value of 10 is an arbitrary number that assumes that a user will only require 10 minutes to read an average page in your content. Without this "timeout", should a user leave the browser and go away from their computer for an extended period, the system would continue to collect and log that the user has been reading the page for a very long time which causes the analytical data to be unrealistic.

If you need, you can shorten the default value of 10 or increase it if you know that most of your content requires more or less time for an average user to read an average page.

GLOBAL DRM POLICY *(applicable to Enterprise accounts)*

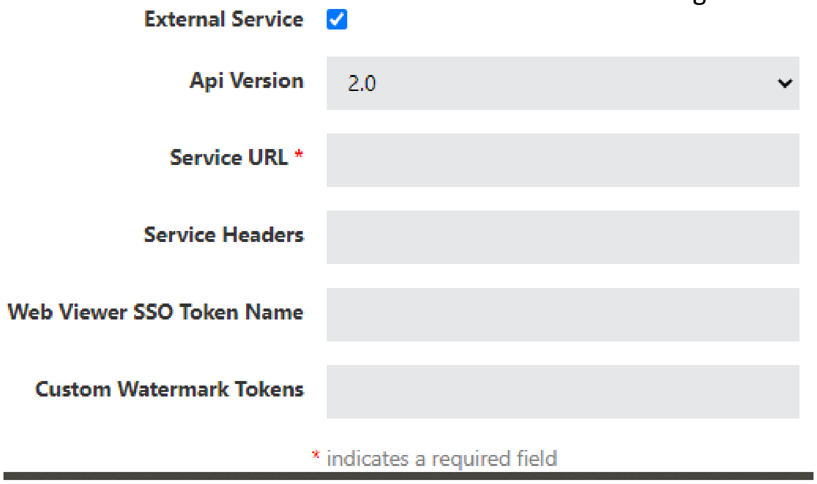
If you only have 1 DRM policy that would apply across your entire business, then you could set your Global DRM policy here, however, we strongly recommend that you DO NOT set anything here as you may encounter conflicts if you are also setting a DRM policy at the file level or group level. Refer to section 5.4 for more details about DRM Policy Settings.

SSO LITE MODE *(applicable to Enterprise accounts)*

This is a convenient feature that allows a User to login to a file once, and afterward, they are automatically granted access to other files you provide to them. When this field is set to Device ID (the default), the user is identified by the web viewer cookie or Adobe Reader/Foxit reader profile. When set to IP address, the user is identified by their IP address.

EXTERNAL SERVICE *(applicable to Enterprise accounts)*

If you will be connecting Vitrium to a 3rd party system for user authentication via a JSON API server, then you will need to enable the External Service and fill in the following fields:



External Service	☑
Api Version	2.0
Service URL *	
Service Headers	
Web Viewer SSO Token Name	
Custom Watermark Tokens	

* indicates a required field

API Version: Please contact our customer service team by emailing success@vitrium.com

Service URL: this is where you will add your JSON API Service URL

- Ensure you enter a secured site with "https" and an SSL certificate is highly recommended that
- Be sure to suffix your server with "/api/2.0/"

Service Headers: this is optional if you wish to provide any header key value pairs

- Separate each header key/value pair with semicolons
- Separate each key and value with an equal sign
- Example: key1=value1; key2=value2

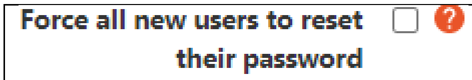
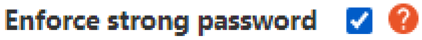
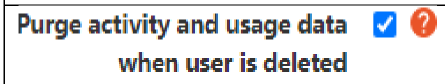
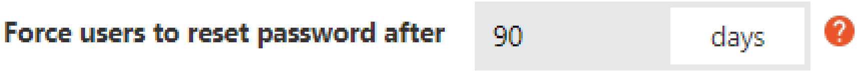
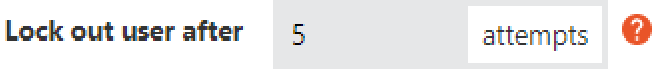
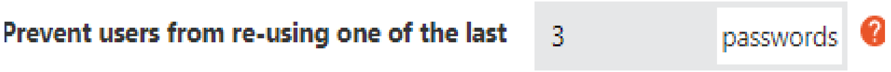
Web Viewer SSO Token Name: this is an optional field

Custom Watermark Tokens: Please contact our customer service team by emailing success@vitrium.com

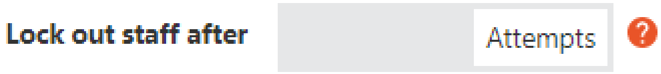
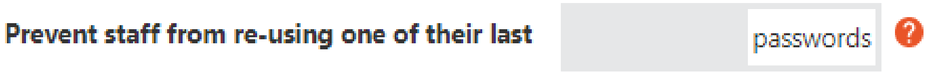
IMPORTANT NOTE: You should also refer to the Vitrium API Guide when enabling an External Service or reach out to the Vitrium Customer Success team at success@vitrium.com.

5.2 Security Settings

END USER SETTINGS:

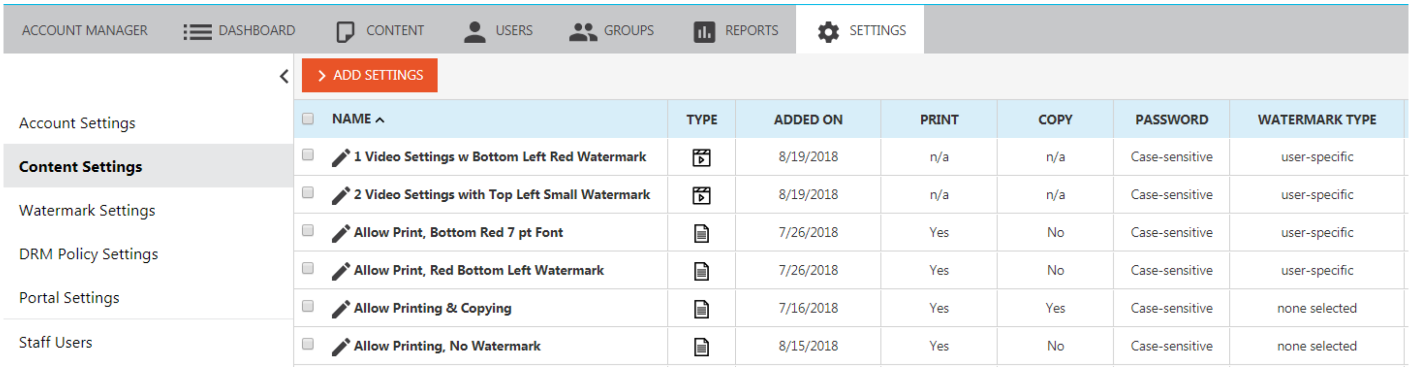
 Force all new users to reset their password ☐	Selecting this will force all new users top change their passwords.
 Enforce strong password ☑	Select this to force all users to use a password that is a minimum of 8 characters and must contain at least one uppercase letter, one number and a symbol, if deselected, users can have any (or blank) passwords.
 Purge activity and usage data when user is deleted ☑	Selecting this will, upon deletion of a user, delete all records used in analytics and reports, as well as the user details. It will also delete old analytic information that belonged to previously deleted users. If deselected, on deleting a user, report and analytic data remains.
 Force users to reset password after 90 days	Enter a number for days before a user is forced to reset their password. Blank or 0 disables this functionality.
 Lock out user after 5 attempts	Enter a number for retries before a user's account is deactivated. It will be reactivated in 15 minutes. Or to reset sooner, activate the user in the users tab. Blank or 0 disables this functionality.
 Prevent users from re-using one of the last 3 passwords	Enter a number for old passwords (excluding current password) a user is not allowed to reuse when changing password. Blank or 0 disables this functionality.

STAFF USER SETTINGS:

Enforce strong password for staff ☐ ?	Select this to force all staff users to use a password that is a minimum of 8 characters, and must contain at least one upper case, one number and a symbol. If deselected, users can have any (or blank) passwords.
Force staff to reset password after days ?	Enter a number for days before staff user is forced to reset their password. Blank or 0 disables this functionality.
 Lock out staff after Attempts ?	Enter a number for retries before a staff user's account is deactivated. to reset, activate the user in the users tab. Blank or 0 disables this functionality.
 Prevent staff from re-using one of their last passwords ?	Enter a number for old passwords (excluding current password) a staff user is not allowed to reuse when changing password. Blank or 0 disables this functionality.

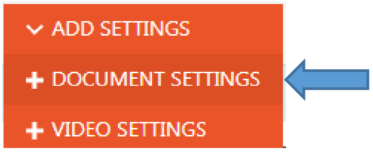
5.3 Content Settings

Content Settings are the protection settings that you apply at the file level – allow printing or copying, allow highlights or annotations, insert a watermark, and so on. Content Settings for documents and images will be different for video since they are different content types.



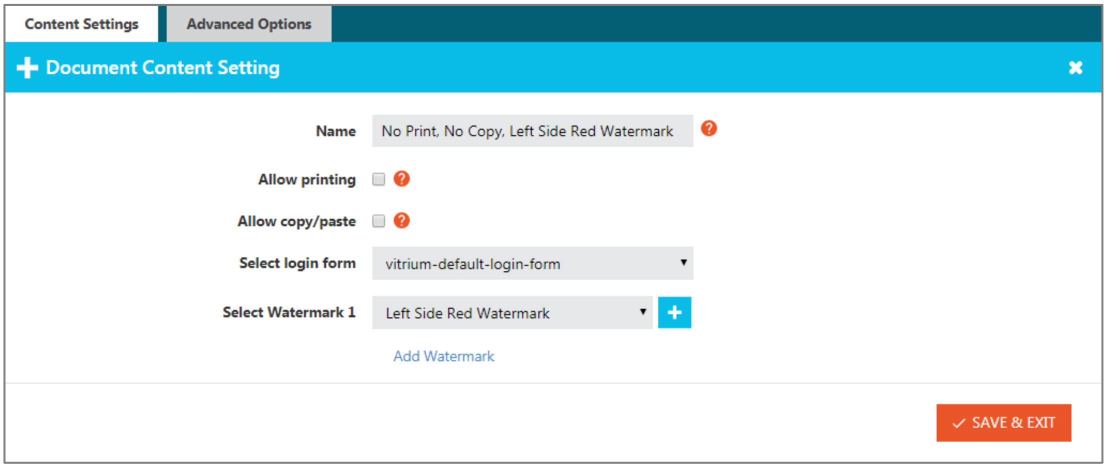
NAME	TYPE	ADDED ON	PRINT	COPY	PASSWORD	WATERMARK TYPE
1 Video Settings w Bottom Left Red Watermark		8/19/2018	n/a	n/a	Case-sensitive	user-specific
2 Video Settings with Top Left Small Watermark		8/19/2018	n/a	n/a	Case-sensitive	user-specific
Allow Print, Bottom Red 7 pt Font		7/26/2018	Yes	No	Case-sensitive	user-specific
Allow Print, Red Bottom Left Watermark		7/26/2018	Yes	No	Case-sensitive	user-specific
Allow Printing & Copying		7/16/2018	Yes	Yes	Case-sensitive	none selected
Allow Printing, No Watermark		8/15/2018	Yes	No	Case-sensitive	none selected

FOR DOCUMENTS & IMAGES



To add a new Content Setting, click Add Settings, then select DOCUMENT SETTINGS from the drop-down menu.

Content Settings tab



Name: No Print, No Copy, Left Side Red Watermark

Allow printing: □

Allow copy/paste: □

Select login form: vitrium-default-login-form

Select Watermark 1: Left Side Red Watermark

Name: enter a name for your Content Setting (we recommend one that includes details such as "No Print, No Copy, Left side Red Watermark")

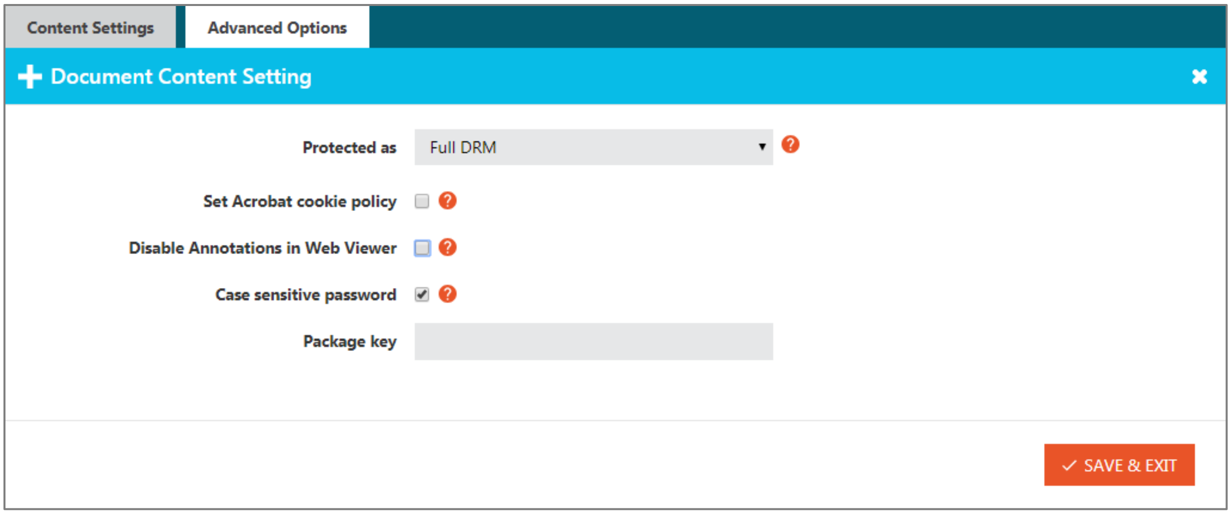
Allow printing: check the box to allow your content to be printed or leave it blank to block printing

Allow copy/paste: check the box to allow content to be copied or leave it blank to block copying

Select login form: this field will only show for Enterprise accounts that use different PDF login forms (not web viewer login forms) with their content

Select Watermark 1: you can select an existing watermark from the drop-down list or create a new one by clicking the + symbol; to add a 2nd or 3rd watermark, click the 'Add Watermark' link and select from the list again

Advanced Options



Protected as: Full DRM

Set Acrobat cookie policy: □

Disable Annotations in Web Viewer: □

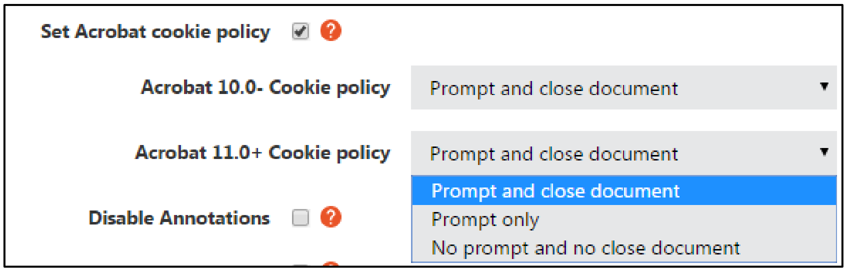
Case sensitive password: ☑

Package key:

Protected as: there are two options to choose from:

> **Full DRM:** this is the default option and will provide you the fullest extent of DRM for your content including the ability to control settings at the user level (user authentication, password-control, expiry date control, device limit control, and so on)
>
> **Social DRM:** this option removes all user DRM controls and there is no login or authentication mechanism required for accessing content, but it will still allow you to retain control over your content such as allowing or blocking printing and copying, and you can apply watermarks to your content

Set Acrobat cookie policy: this allows you to change the behavior of the Adobe global object security policy (GOSP) pop-up that appears in the protected PDF file which relates to how Vitrium tracks and counts 'device limit' or 'application limit' for the user:



Set Acrobat cookie policy ☑

Acrobat 10.0- Cookie policy: Prompt and close document

Acrobat 11.0+ Cookie policy: Prompt and close document

- Prompt and close document
- Prompt only
- No prompt and no close document

Disable Annotations □

> **PromptAndCloseDocument:** this is the default selection where the Adobe GOSP pop-up message will appear and the user will need to close the prompt, make the required change (disable the GOSP by going to Preferences > JavaScript and unchecking the GOSP field), then re-open the file to unlock it
>
> **PromptOnly**: if this option is selected, the Adobe GOSP pop-up message will appear with the instructions for disabling the GOSP but the user can just close it and continue on with unlocking their document but no cookie gets stored, so you run the risk of the user reaching their PDF limit very quickly if they did not follow the instructions
>
> **NoPromptAndNoClose:** if this option is selected, the Adobe GOSP message will NOT appear at all and is only recommended in scenarios where you DO NOT require setting a PDF limit for users

Disable Annotations in web viewer: this option allows you to disable both the highlighting and notes feature in the web viewer (note, this feature cannot be disabled for the protected PDF version)

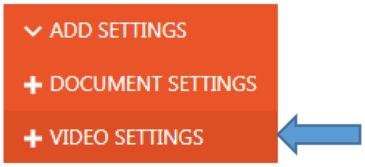
Case sensitive password: this option allows you to force login credentials to be case-sensitive

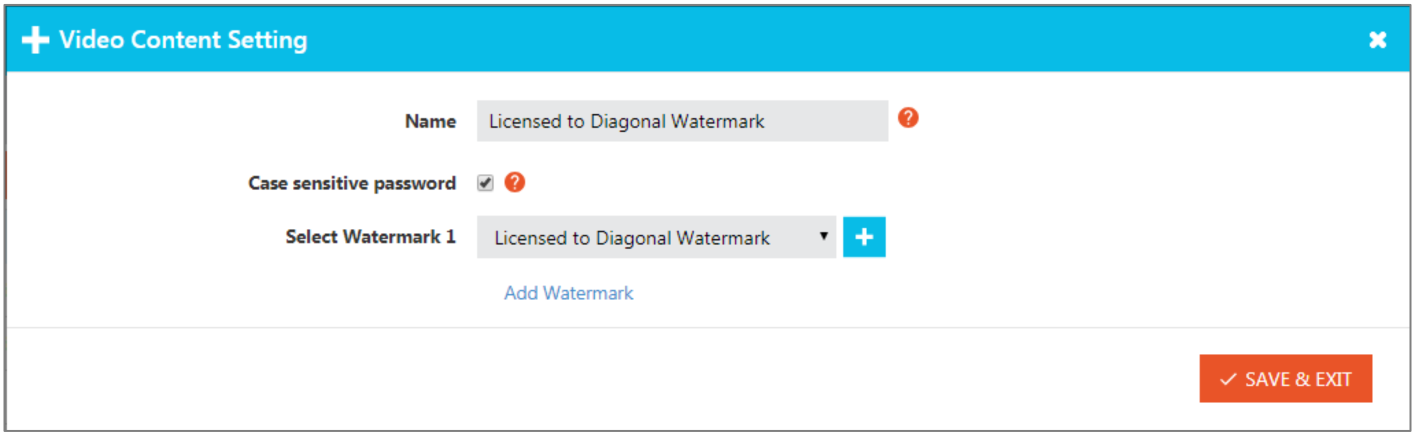
Package key: this option is a specific field for one of Vitrium's legacy customers and can be ignored

IMPORTANT NOTE: Content Settings can NOT be edited since these settings are contained within the protected PDF file and if a user already has the file, you cannot change that file, only send them a new file with the updated Content Settings. If you need to play around with different settings or watermarks, you will need to create multiple Content Settings, then delete those you no longer need.

FOR VIDEOS

To add a new Content Setting, click Add Settings, then select VIDEO SETTINGS from the drop-down menu.





Name: Licensed to Diagonal Watermark

Case sensitive password ☑

Select Watermark 1: Licensed to Diagonal Watermark

Name: enter a name for your Video Content Setting (we recommend one that includes details such as "Licensed to Diagonal Watermark")

Case sensitive password: this option allows you to force login credentials to be case-sensitive

Select Watermark 1: you can select an existing watermark from the drop-down list or create a new one by clicking the + symbol; to add a 2nd or 3rd watermark, click the 'Add Watermark' link and select from the list again

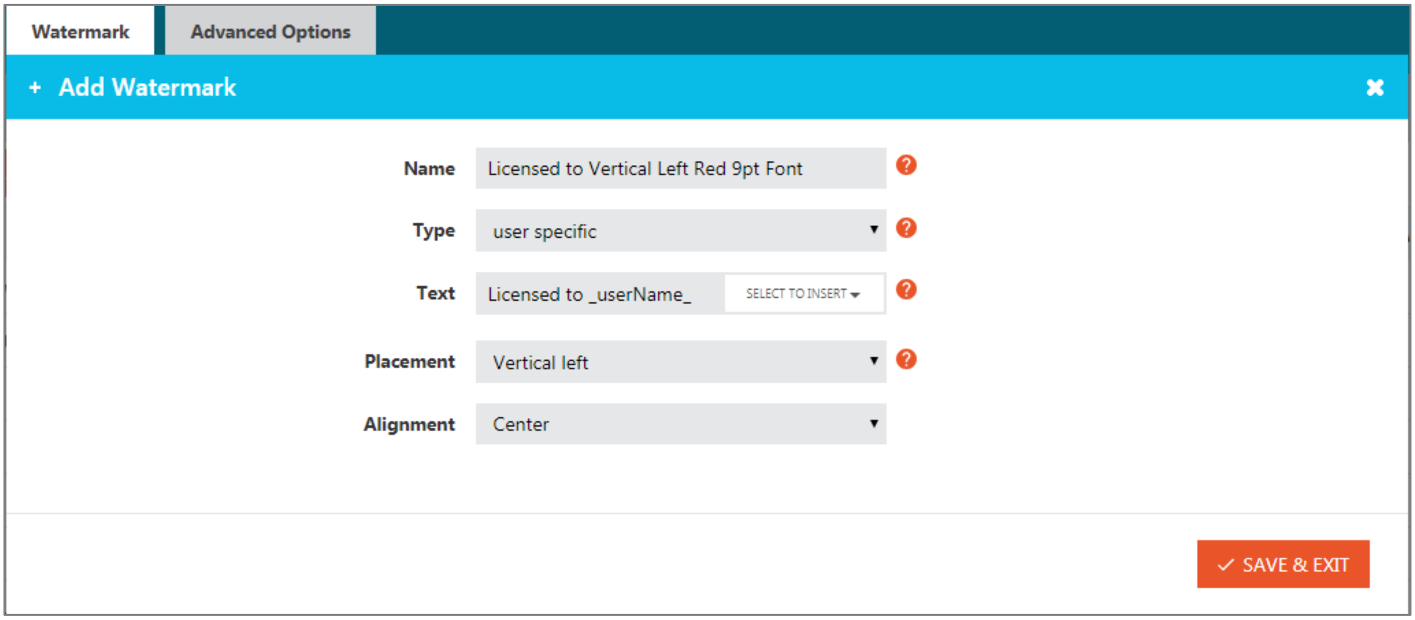
IMPORTANT NOTE: Currently, Video Content Settings can NOT be edited but we are looking to change that in a future release.

5.4 Watermark Settings

Watermark Settings are the protection & control settings for your watermark – whether you want to use a dynamic, user-identifying watermark or plain text watermark, what placement and alignment options you wish to choose, and what font, color, size, or opacity level you prefer.

To get started, click the **+ ADD WATERMARK** button and you will see this screen:

Watermark tab



Name: Licensed to Vertical Left Red 9pt Font

Type: user specific

Text: Licensed to _userName_

Placement: Vertical left

Alignment: Center

Name: enter a name for your watermark; we recommend one that includes details such as "Licensed to Vertical Left Red 9pt Font"

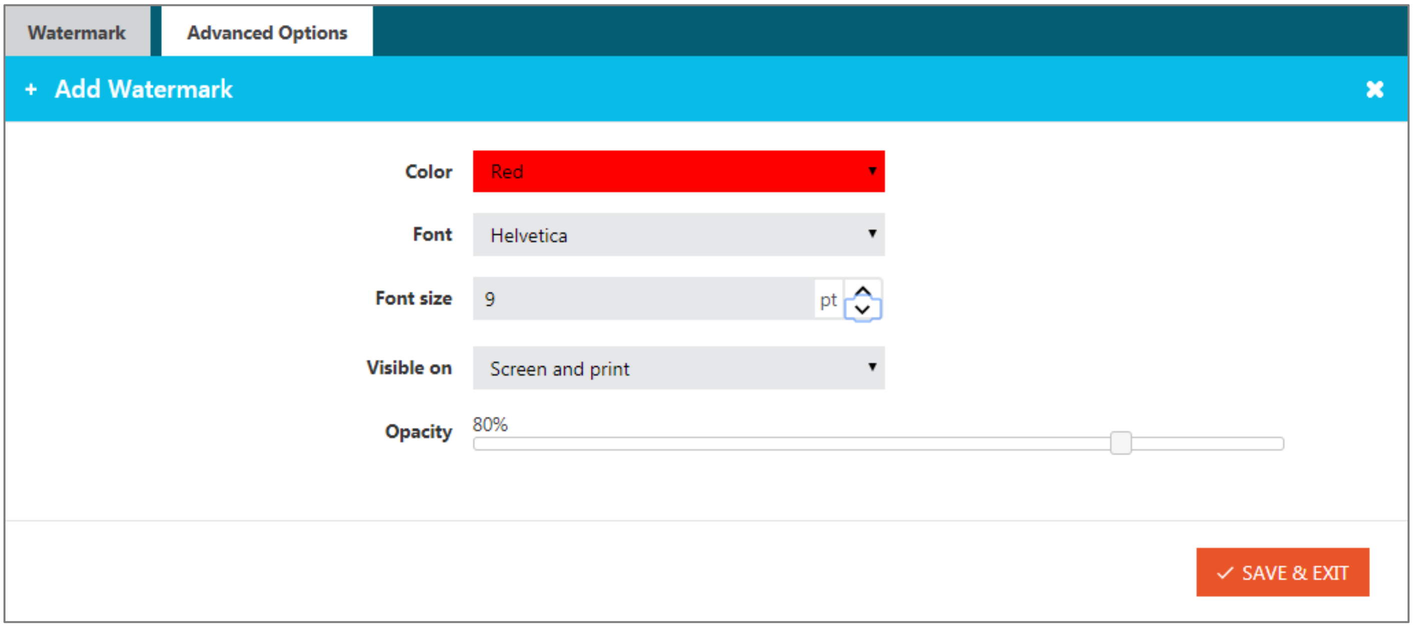
Type: you can select from two options:

> **User-specific:** this is a dynamic watermark where you can add user-identifying information in it
> **Text-only:** this is a generic watermark where you can enter plain text only (no dynamic data)

Placement: select the location where you would like to place the watermark (bottom, top, vertical left, vertical right, diagonal, or custom)

Alignment: select whether you want the watermark text to be left-, center-, or right-aligned

<u>Advanced Options tab</u>



Color: Red

Font: Helvetica

Font size: 9 pt

Visible on: Screen and print

Opacity: 80%

Color: select a color from the drop-down list

Font: select a font type from the drop-down list

Font size: enter a font size

Visible on: select either ‘screen and print’ or ‘print only’

Opacity: slide the scale up or down to select the opacity (or transparency level)

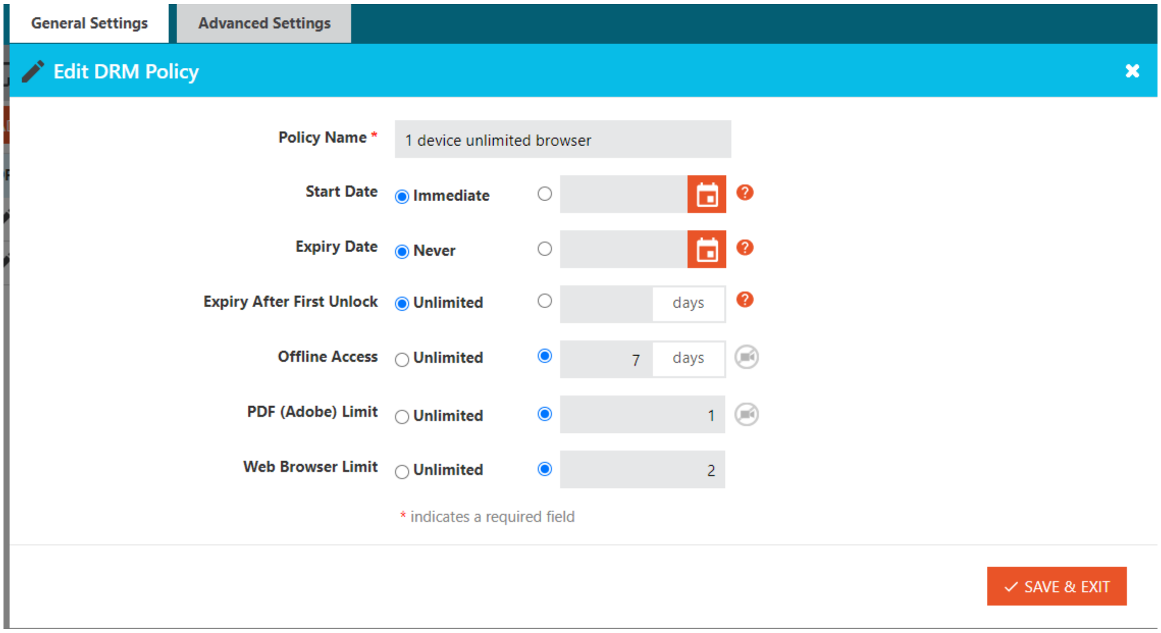
5.5 DRM Policy Settings

DRM Policy Settings are the protection & control settings that you can apply <u>at the user, group, file or folder level</u> – setting expiry date, offline access, device or browser limit, print limit, IP address limit, and so on.

SETTING UP A DRM POLICY

Go to Settings > DRM Policy Settings, then click the ‘Add DRM Policy button. Depending on which Vitrium edition you have will depend on which DRM policy fields you will see.

<u>Standard Edition accounts will see:</u>

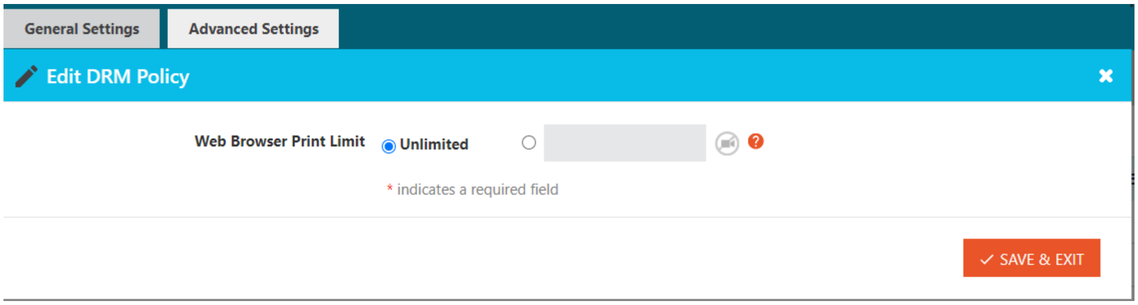


General Settings | Advanced Settings

Edit DRM Policy

Policy Name *	1 device unlimited browser		
Start Date	● Immediate	○	
Expiry Date	● Never	○	
Expiry After First Unlock	● Unlimited	○	days
Offline Access	○ Unlimited	●	7 days
PDF (Adobe) Limit	○ Unlimited	●	1
Web Browser Limit	○ Unlimited	●	2

* indicates a required field



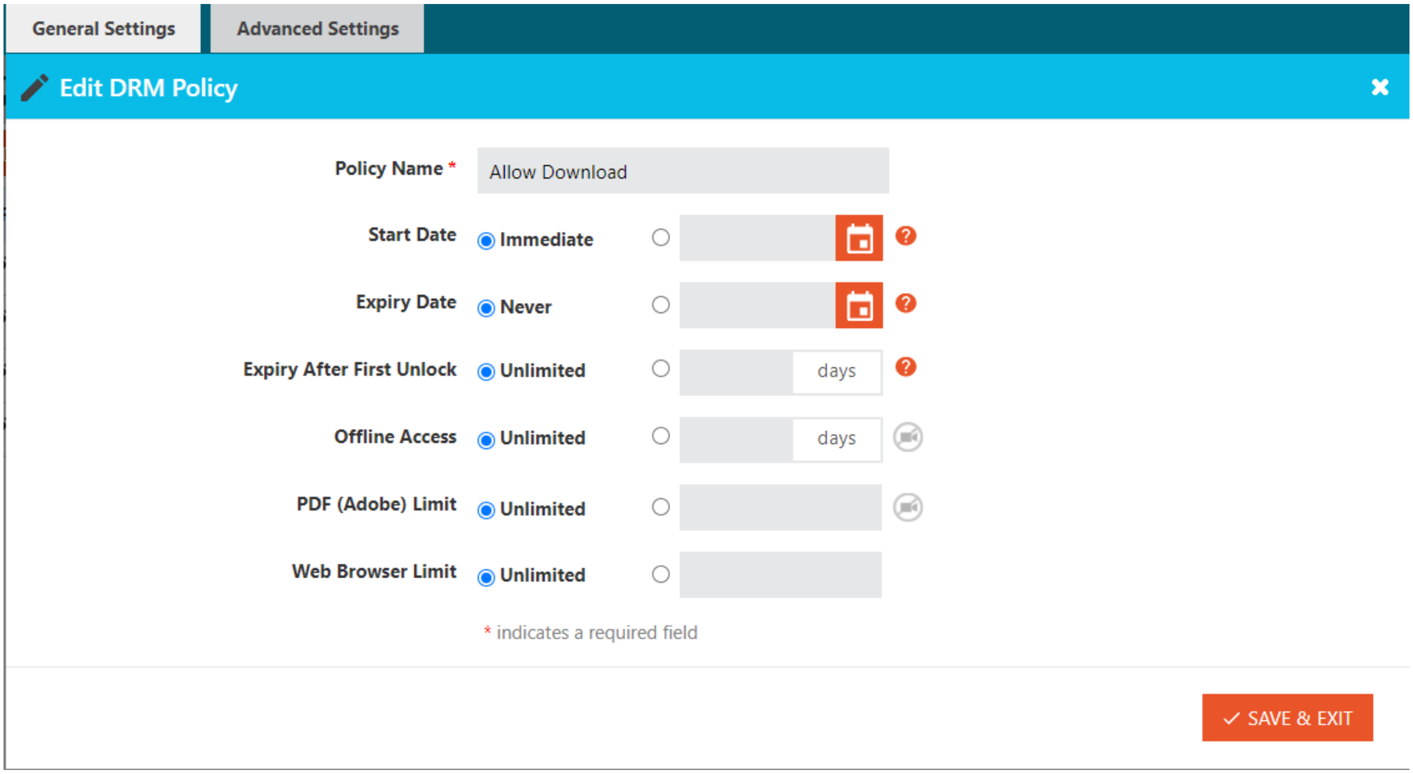
General Settings | Advanced Settings

Edit DRM Policy

Web Browser Print Limit	● Unlimited	○

* indicates a required field

Professional Edition accounts will see:



Edit DRM Policy

Policy Name * Allow Download

Start Date ● Immediate ○

Expiry Date ● Never ○

Expiry After First Unlock ● Unlimited ○ days

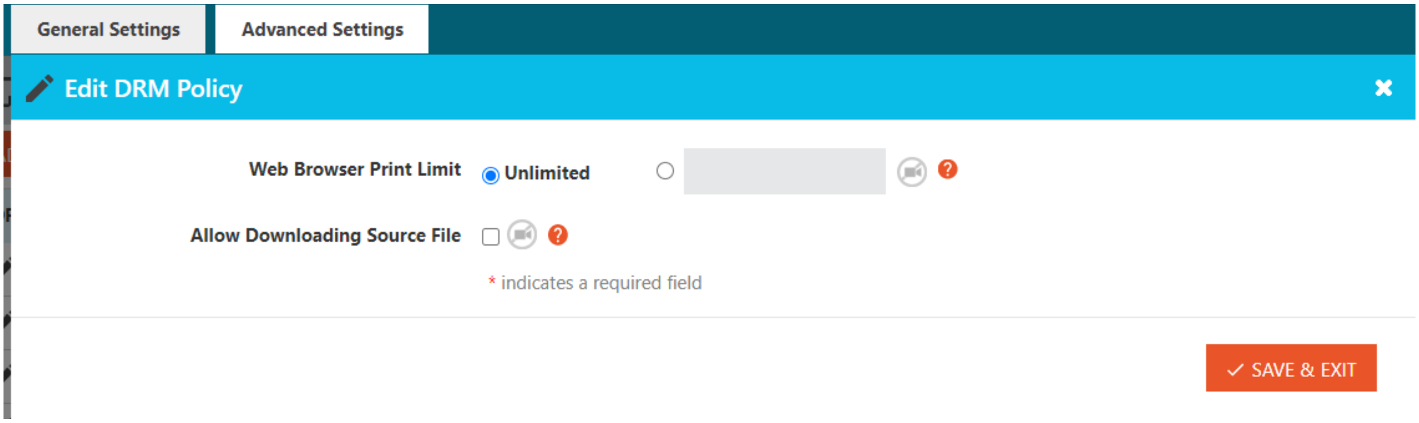
Offline Access ● Unlimited ○ days

PDF (Adobe) Limit ● Unlimited ○

Web Browser Limit ● Unlimited ○

* indicates a required field

✓ SAVE & EXIT



Edit DRM Policy

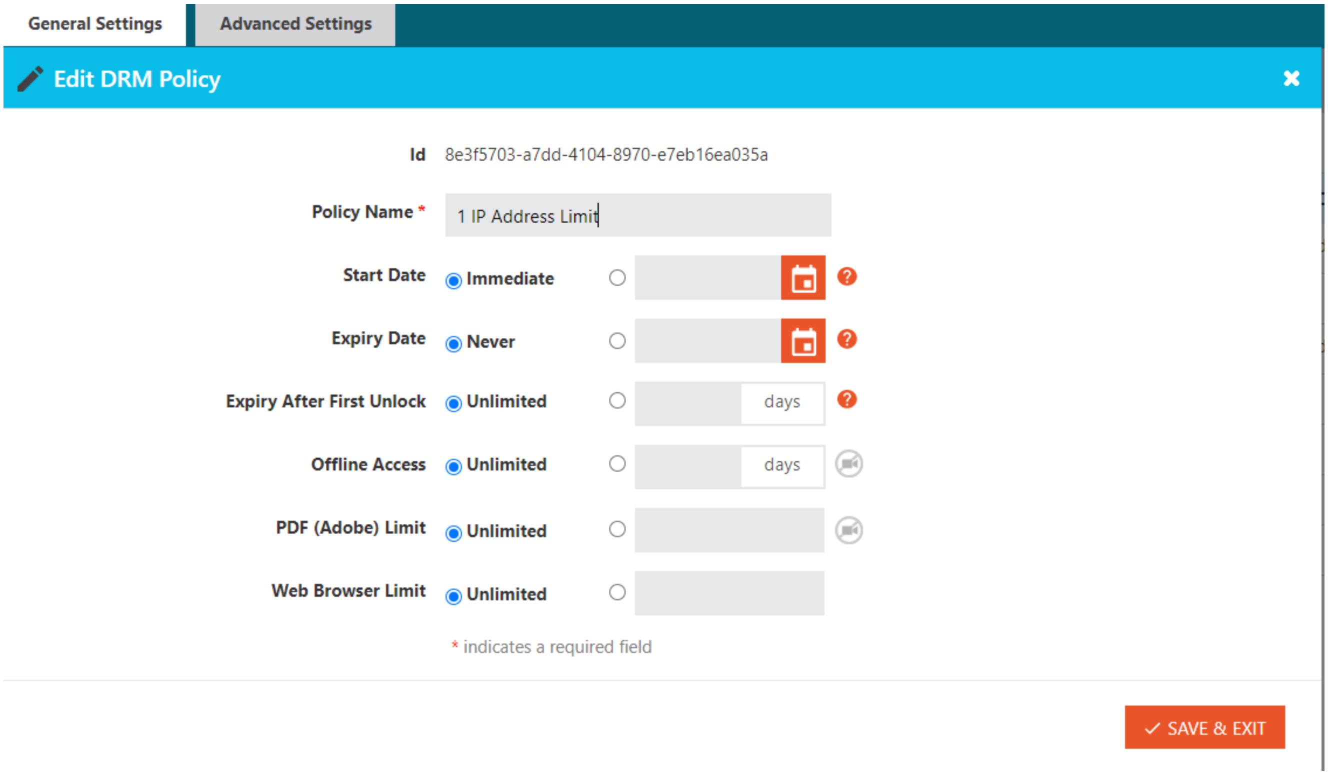
Web Browser Print Limit ● Unlimited ○

Allow Downloading Source File □

* indicates a required field

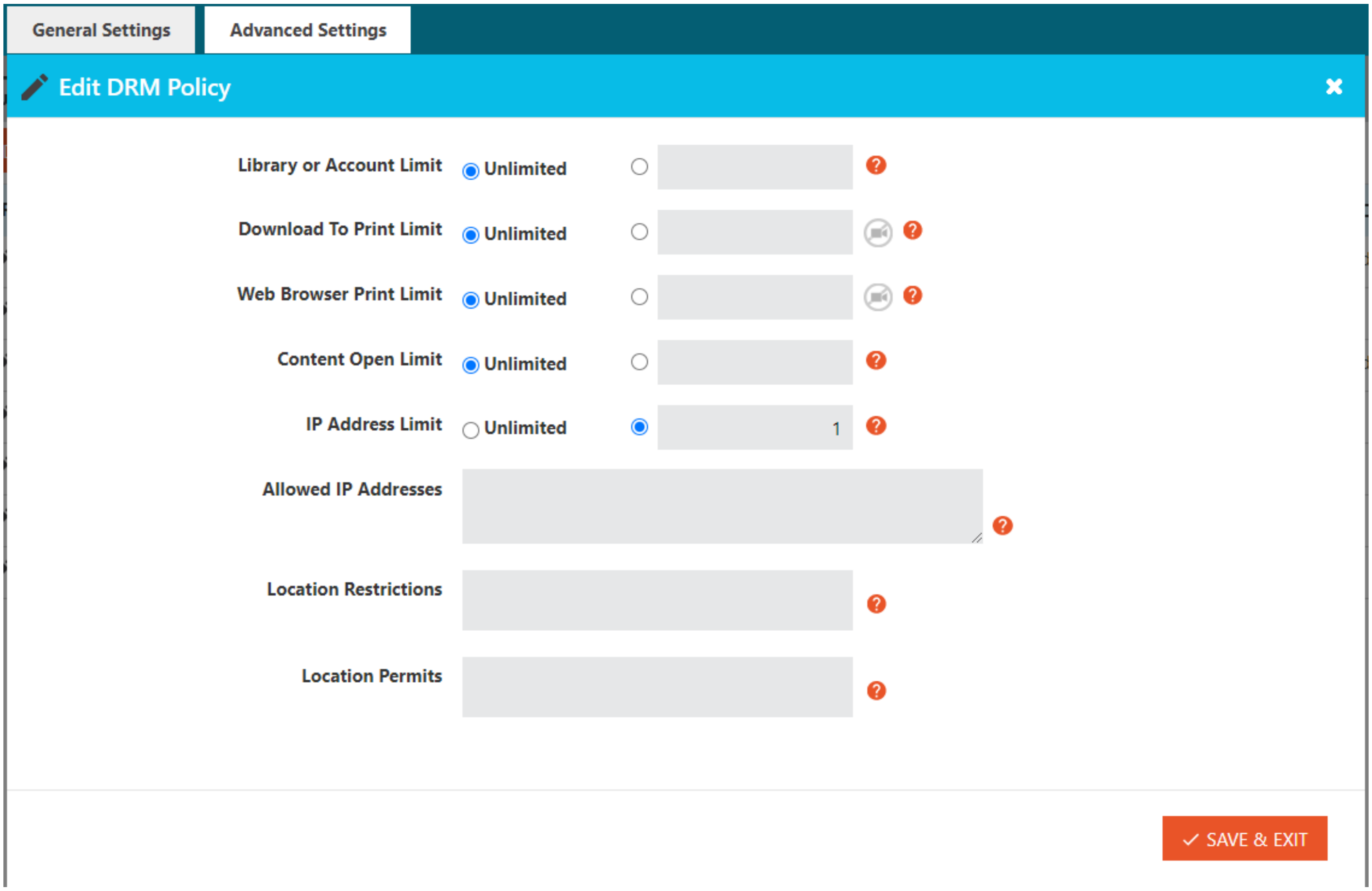
✓ SAVE & EXIT

Enterprise Edition accounts will see:



Id	8e3f5703-a7dd-4104-8970-e7eb16ea035a		
Policy Name *	1 IP Address Limit		
Start Date	● Immediate	○	
Expiry Date	● Never	○	
Expiry After First Unlock	● Unlimited	○	days
Offline Access	● Unlimited	○	days
PDF (Adobe) Limit	● Unlimited	○	
Web Browser Limit	● Unlimited	○	

* indicates a required field



Library or Account Limit	● Unlimited	○	
Download To Print Limit	● Unlimited	○	
Web Browser Print Limit	● Unlimited	○	
Content Open Limit	● Unlimited	○	
IP Address Limit	○ Unlimited	●	1
Allowed IP Addresses			
Location Restrictions			
Location Permits			

DRM POLICY RULES

There are two important rules you should know about before setting up your DRM policies:

RULE #1: The most lenient DRM policy setting will always apply. For this reason, Vitrium recommends ONLY setting a DRM policy at one level as the most lenient policy will take precedent if you have set it at multiple levels. It could also cause conflicts and be challenging to troubleshoot.

RULE #2: You must enter a value for EVERY field in a DRM policy. Do not leave anything 'not set' otherwise you will receive error messages when trying to unlock a file. So if you don't wish to set a value for any field, set it to NEVER or UNLIMITED.

DRM POLICY FIELDS DEFINED

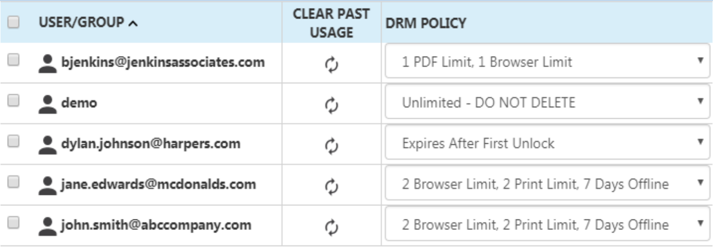
Policy Name	This is where you can enter a name for your DRM Policy (we recommend one that includes specific details about the policy such as "1 PDF Limit, 2 Browser Limit, 1 Day Offline Access")
Expiry Date	This is where you can define a specific date for when your content or file will expire for a particular User or Group. If you do not wish to set a date, then select *NEVER* as per Rule #2.
Expiry After First Unlock	This is where you can define a specific number of days that your content or file will expire after the first unlock by the User.

Offline Access	This is where you can set the maximum number of days that your User or Group can access your protected content or file when they are offline or not connected to the internet: – For the protected PDF file, the User doesn't need to do anything in order for the offline access feature to work. – For the secure web viewer, the User will need to click the 'Save to Browser' button to be able to save the content to the browser's cache.
PDF or Browser Limit	This is where you can set the maximum number of PDF applications like Adobe Reader or Acrobat or Foxit Reader(PDF) or browsers that a User can access your protected content or file on. – Total Limit: this is defined as the same as above. – Individual Limit: this allows you to separate the limits for PDF (the number of PDFapplications) versus the number of browsers.
Library or Account Limit	This is where you can set the total number of files that a User can access or unlock.
Web Browser Print Limit	This is where you can set the number of times a User can print the web version of a document or image. NOTE: a print session will be counted even if the person selects only 1 page.
Content Open Limit	This is where you can the maximum number of times a User can access or unlock a specific file.
IP Address Limit	This is where you can set the maximum number of IP addresses that a User will be able to access your protected content from. If you want to specify a particular IP address or range, enter 0 as the limit, then enter the IP address in the "Ignored IP Addresses" section.
Restricted Regions	If you want to block some regions from accessing your content, enter those region name here.
Permitted Regions	If you want to allow your content only in some regions and restrict from rest of the regions, enter those region (allowed ones) name here.

WHERE TO APPLY DRM POLICY SETTINGS

Before deciding where to apply DRM Policy, remember **RULE #1:** The most lenient DRM policy setting will always apply. For this reason, Vitrium recommends ONLY setting a DRM policy at one level as the most lenient policy will take precedent if you have it set at multiple levels, causing conflicts.

Where to Apply & Recommendations	Steps to Apply
File/Content Level It's recommended for Standard & Professional customers to set your DRM policy at the file/content level since you can see it visually every time you upload content and assign permissions. You can also easily change the permissions for a specific file, user or group from withing the Edit Content window.	1. In the Content tab, click Add Content 2. Select your File and click the Permissions tab 3. Select your Users or Groups 4. Select a DRM policy from the drop-down box 5. Click Save & Exit

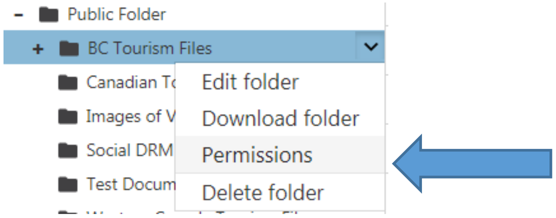


☐	USER/GROUP ^	CLEAR PAST USAGE	DRM POLICY
☐	bjenkins@jenkinsassociates.com	⟳	1 PDF Limit, 1 Browser Limit ▾
☐	demo	⟳	Unlimited - DO NOT DELETE ▾
☐	dylan.johnson@harpers.com	⟳	Expires After First Unlock ▾
☐	jane.edwards@mcdonalds.com	⟳	2 Browser Limit, 2 Print Limit, 7 Days Offline ▾
☐	john.smith@abccompany.com	⟳	2 Browser Limit, 2 Print Limit, 7 Days Offline ▾

Folder Level

Recommended if you have a lot of files that you sort into folders AND you require the same DRM policy for all files within a particular folder. If you set a DRM policy at this level, you need to be very cautious when setting a DRM policy at other levels to avoid potential conflicts.

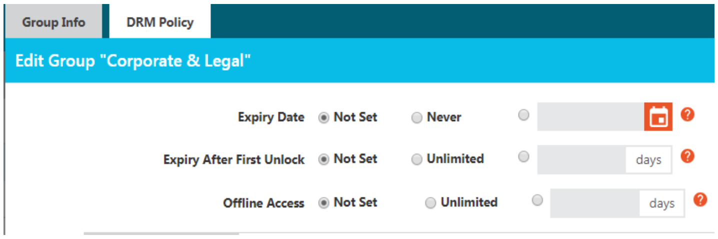
1. In the Content tab, in the folder section, click the arrow beside a folder and select Permissions
2. Click Add, then select your Users or Groups
3. Select a DRM policy from the drop-down box
4. Click Save & Exit



Group Level

Recommended if you have a specific policy required for a group of users. If you set a DRM policy at this level, you need to be very cautious when setting a DRM policy at other levels to avoid potential conflicts.

1. In the Groups tab, click on a Group
2. Select the DRM policy tab
3. Enter your policy values
4. Click Save & Exit

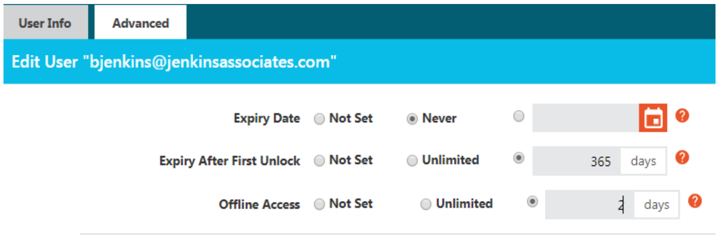
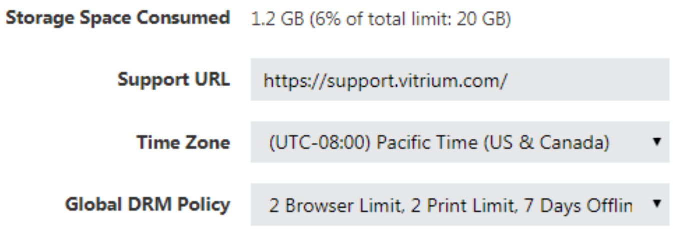


Edit Group "Corporate & Legal"

Expiry Date ● Not Set ○ Never ○

Expiry After First Unlock ● Not Set ○ Unlimited ○ days

Offline Access ● Not Set ○ Unlimited ○ days

<u>User Level</u> Only recommended for accounts with a small number of users where you will have different DRM policy for each user.If you set a DRM policy at this level, you need to be very cautious when setting a DRM policy at other levels to avoid potential conflicts.	1. In the Users tab, click on a User 2. Select the DRM policy tab 3. Enter your policy values 4. Click Save & Exit  User Info | Advanced Edit User "bjenkins@jenkinsassociates.com" Expiry Date ○ Not Set ● Never ○ Expiry After First Unlock ○ Not Set ○ Unlimited ● 365 days Offline Access ○ Not Set ○ Unlimited ● 2 days
<u>Global Level</u> Only recommended if you have 1 DRM policy that can be applied across your entire business or organization. If you set a DRM policy at this level, you need to be very cautious when setting a DRM policy at other levels to avoid potential conflicts.	1. Go to Settings > Account Settings 2. In the field "Global DRM Policy", select a policy from the drop-down list  Storage Space Consumed 1.2 GB (6% of total limit: 20 GB) Support URL https://support.vitrium.com/ Time Zone (UTC-08:00) Pacific Time (US & Canada) Global DRM Policy 2 Browser Limit, 2 Print Limit, 7 Days Offlin

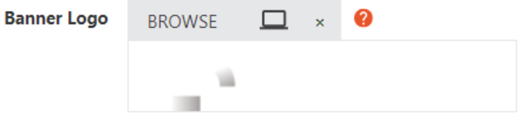
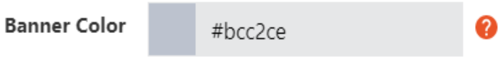
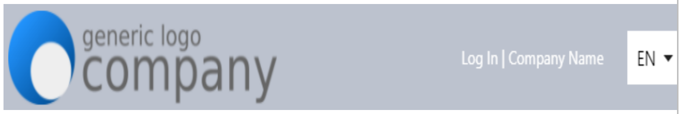
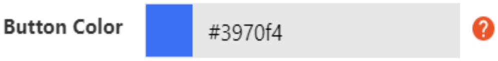
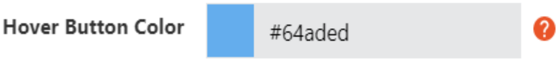
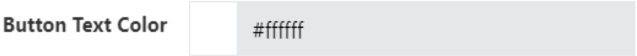
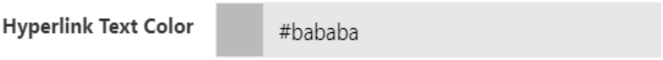
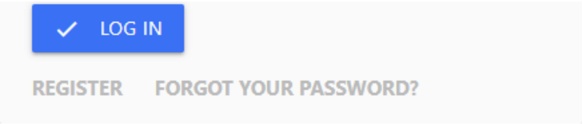
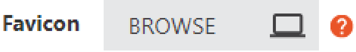
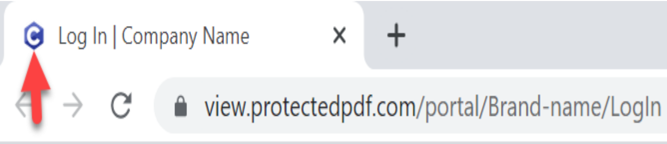
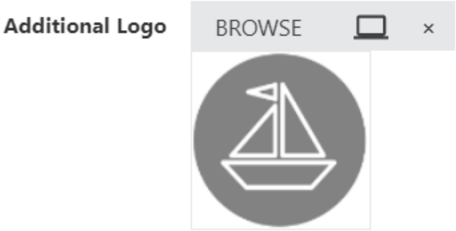
5.6 Web Viewer & Portal Settings

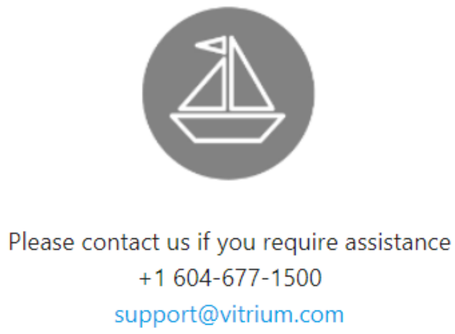
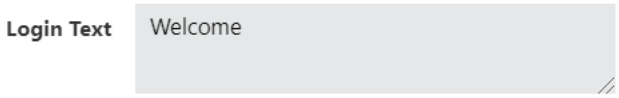
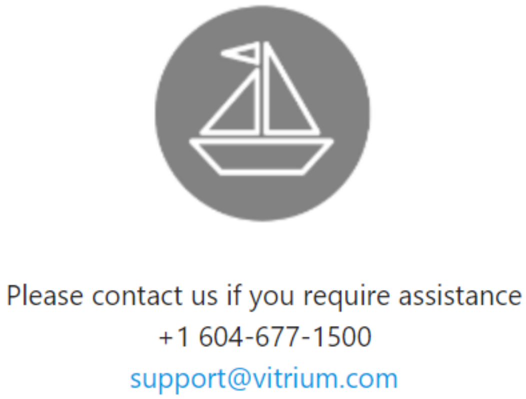
IMPORTANT NOTE: Only Vitrium Security Professional and Enterprise accounts will have access to the User Portal feature and will see Portal Settings in their account. Standard accounts will only see Web Viewer Settings.

Vitrium's Web Viewer login page and the User Portal login page can both be customized with your company's logo and brand colors. Some of the elements in Vitrium's Web Viewer Settings will apply to the Portal login page, which is why it is recommended to start updating the Web Viewer Settings.

UPDATING WEB VIEWER SETTINGS

Allow Password Recovery ☑	Check this if you wish for users to have the "Forgot password" link on your login page
Custom URL for Password Reset	<u>For Vitrium Security Enterprise customers only:</u> Enter a URL here this if you wish for users to have the "Forgot password" link on your login page
Custom URL for Error Page	<u>For Vitrium Security Enterprise customers only:</u> Enter a URL here if you wish to direct users to a different Error Page when they exceed DRM limits or encounter other errors
Change 'Forgot Password' To	Enter different words if you wish to change the "Forgot Password" link on your login page

 Banner Logo BROWSE	The logo that appears at the top left of the web viewer. We recommend using an image without a transparent background or one that matches the banner color.
 Banner Color #bcc2ce	The color that can be seen at the top of the Portal and Log in pages 
 Button Color #3970f4	The Color of the LOGIN button on the Log in page
 Hover Button Color #64aded	The Hover Button color can be seen when hovering over the LOG IN button.
 Button Text Color #ffffff	The color of the text on the LOGIN button
 Hyperlink Text Color #bababa	The color of the Hyperlink text below the LOGIN button for registering or password reset 
 Favicon BROWSE	A favicon is a small image that appears in the left-hand side of a website tab. The favicon image should be 16x16 pixels or 32x32 pixels, using either 8-bit or 24-bit colors.  Log In | Company Name view.protectedpdf.com/portal/Brand-name/LogIn
 Additional Logo BROWSE	The Additional Logo appears on the login page, just above the Login Text and the username input.

	 Please contact us if you require assistance +1 604-677-1500 support@vitrium.com
 Login Text Welcome	The login text is a block of HTML-capable text that appears just below the Additional Logo. this text can be used for support purposes, as can be seen below:  Please contact us if you require assistance +1 604-677-1500 support@vitrium.com

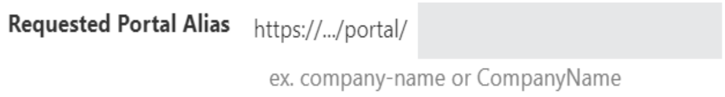
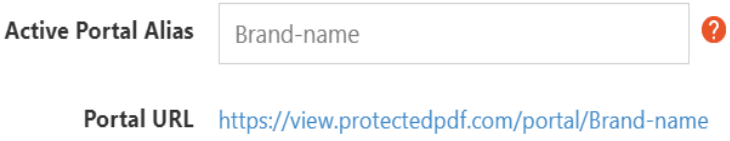
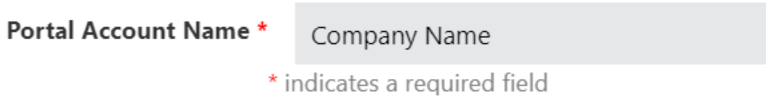
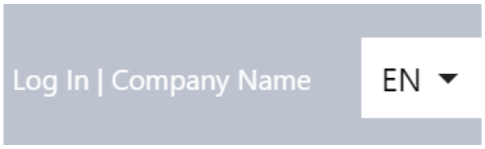
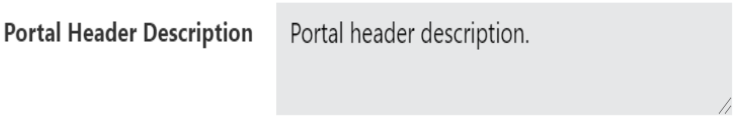
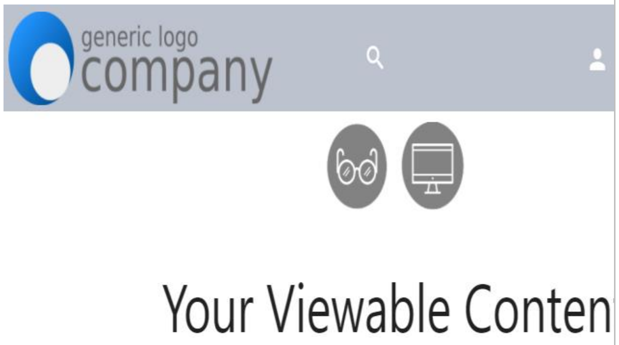
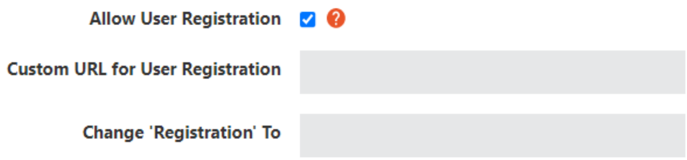
Once you have all the Web Viewer Settings created, these will also apply to the Portal once you enable it. Refer to further instructions for the Portal below.

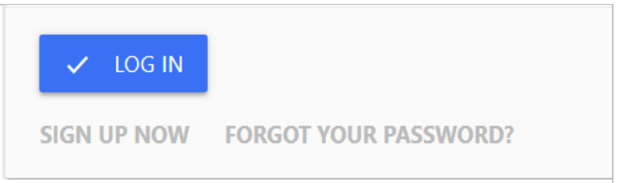
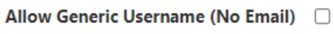
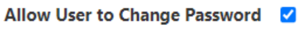
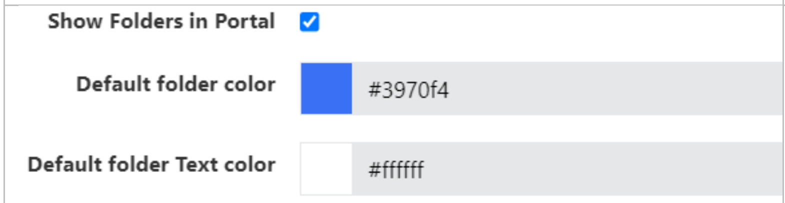
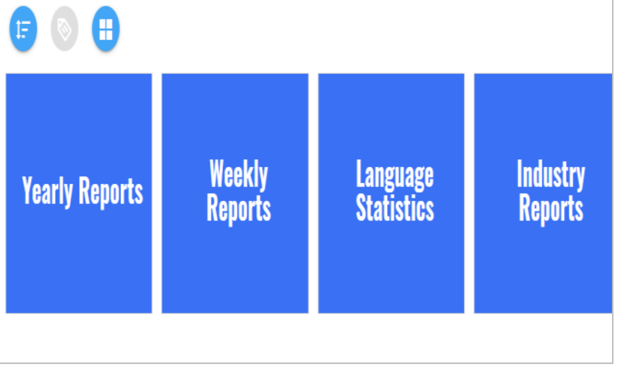
UPDATING PORTAL SETTINGS

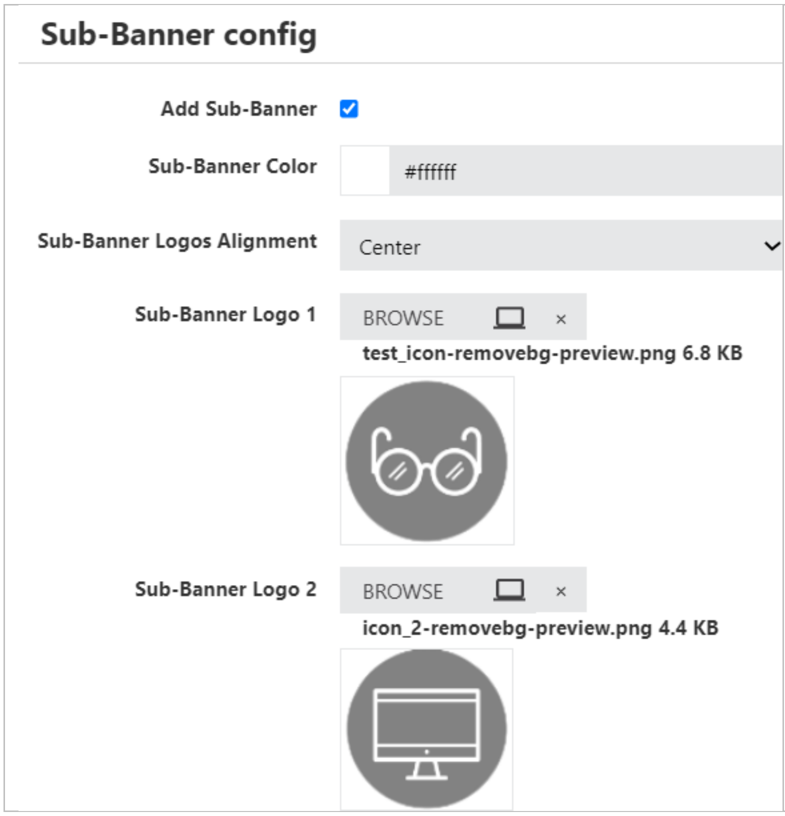
Vitrium's User Portal allows organizations to distribute protected content to end users in a central, secure web portal. The user can log into one place and access all their content, including any protected documents, images, videos or audio files that you have assigned to that particular user. The portal can be customized with your logo and branding.

1. From your Vitrium account, go to Settings > Portal Settings
2. Click the 'Enabled' checkbox and the following portal fields will appear below

 Enable Portal ☑	Check this box to enable the portal in your account. This may have already been done for you.

 Requested Portal Alias https://.../portal/ ex. company-name or CompanyName	The "Requested Portal Alias" is where you request to add a custom alias to the end of the portal domain. The URL will look like this: **https://view.protectedpdf.com/portal/your-alias-name** We recommend entering a simple alias with NO SPACES OR CAPITALIZED LETTERS. You will receive a temporary portal alias until your alias has been approved.
 Active Portal Alias Brand-name ? Portal URL https://view.protectedpdf.com/portal/Brand-name	Your Portal Alias will be activated once Vitrium approves the name and you receive the approval email. Until then, the system will issue you a temporary URL. The approval process normally takes less than 24 hours.
 Portal Account Name * Company Name * indicates a required field	The Portal Account Name will appear at the top right-hand side of the portal login page.  Log In | Company Name EN
 Portal Header Description Portal header description.	The Portal Header Description will appear in the center of the main portal screen after users log in. We recommend adding the <h1>, <h2>, <h3> or <h4> to change the heading size, with the respective </h> closing at the end.  Your Viewable Conten
 Allow User Registration ☑ ? Custom URL for User Registration Change 'Registration' To	Select this option if you wish to have new people self-register or sign up as a 'User' with access to your portal. IMPORTANT NOTE: Once a new user has been verified (via the email that's sent to them), someone from your organization may need to assign them permission to content unless you have already assigned "All Active Users" with permission. "Change 'Registration' To" changes the text of the registration button on the Portal login page. For example:

	
Allow Generic Username (No Email) □	Allow the user to use a Unique identifier other than an email address. e.g., “firstname.lastname”, “companyname”, “123456”.
Allow User to Change Password ☑	Select this option if you wish to allow users to reset or change their password.
Allow Protected PDF Downloads ☑	We only recommend allowing protected PDF downloads if you have more traditional users who like viewing PDFs in Adobe Reader, but they only work on the desktop version of Adobe Reader.
Show Folders in Portal ☑ Default folder color 🟦 #3970f4 Default folder Text color ⬜ #ffffff	This shows the default folder appearance without specific folder customization.  Yearly Reports Weekly Reports Language Statistics Industry Reports



Sub-Banner config

Add Sub-Banner ☑

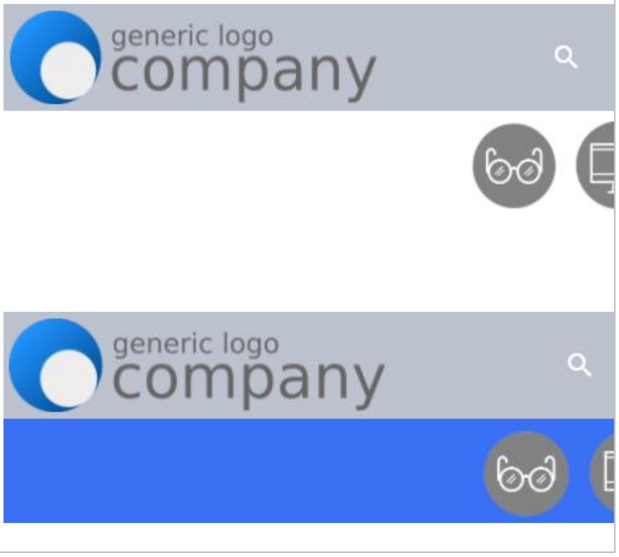
Sub-Banner Color: #ffffff

Sub-Banner Logos Alignment: Center

Sub-Banner Logo 1: BROWSE ×
test_icon-removebg-preview.png 6.8 KB

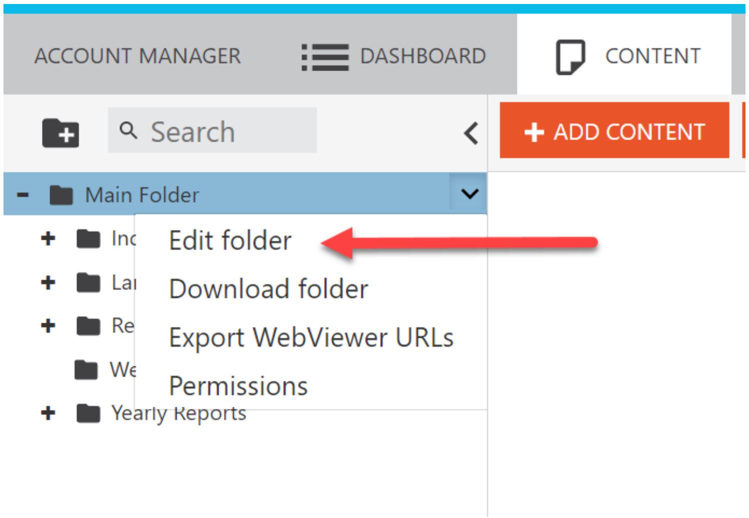
Sub-Banner Logo 2: BROWSE ×
icon_2-removebg-preview.png 4.4 KB

It is recommended to use a white Sub-Banner with pictures with a white background, or pictures without a background for colored Sub-Banners as can be seen below. Please Note Sub-Banner Logos are NOT clickable.

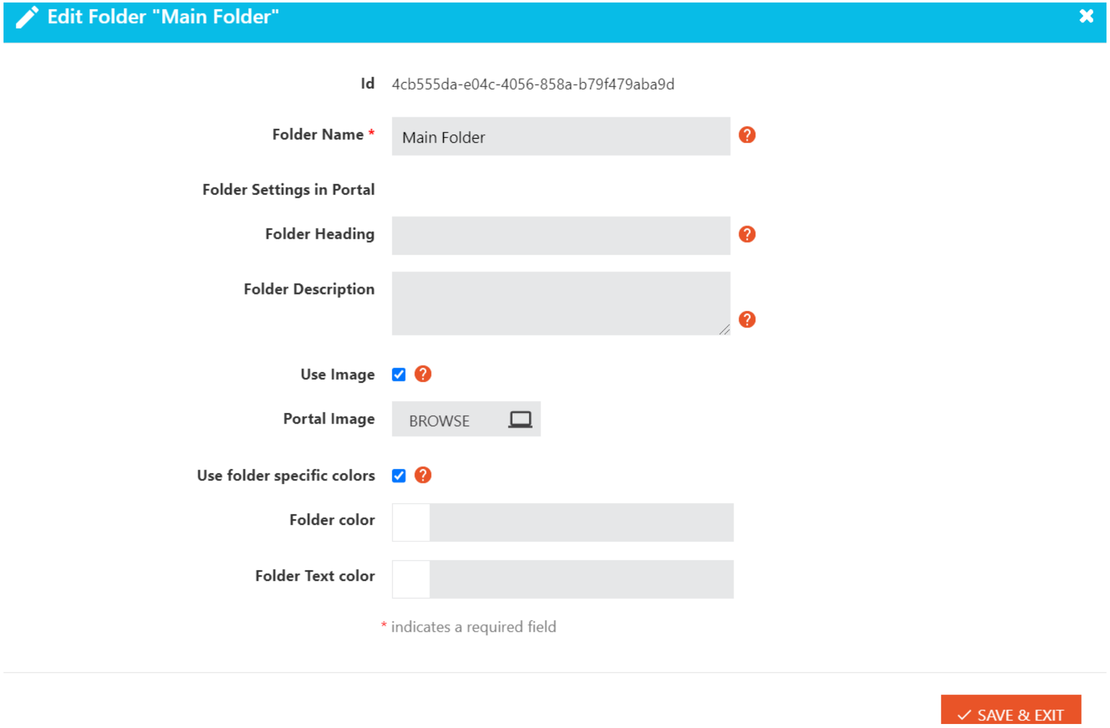


FOLDER CUSTOMIZATION

To enable folders in the portal, navigate to Portal Settings under the Settings tab and check the Show Folders in Portal checkbox. Make sure to save any changes.
To edit a folder, navigate to the Content tab. There you will see your list of folders (If you created folders). Click the arrow to the right of the folder name. In the drop-down menu, click edit folder.



The following menu will then appear:

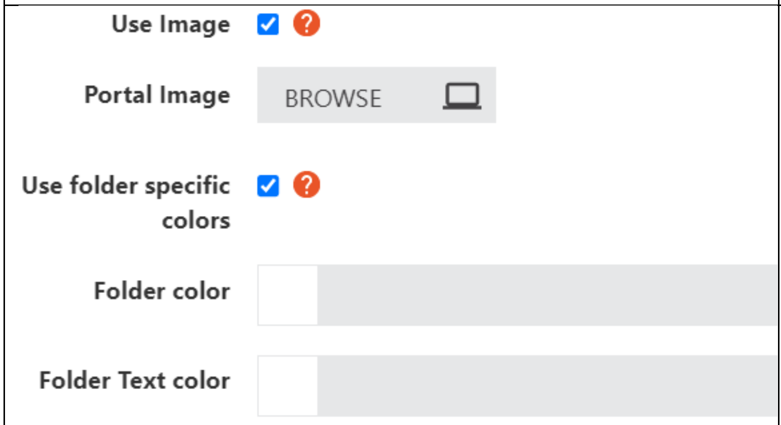
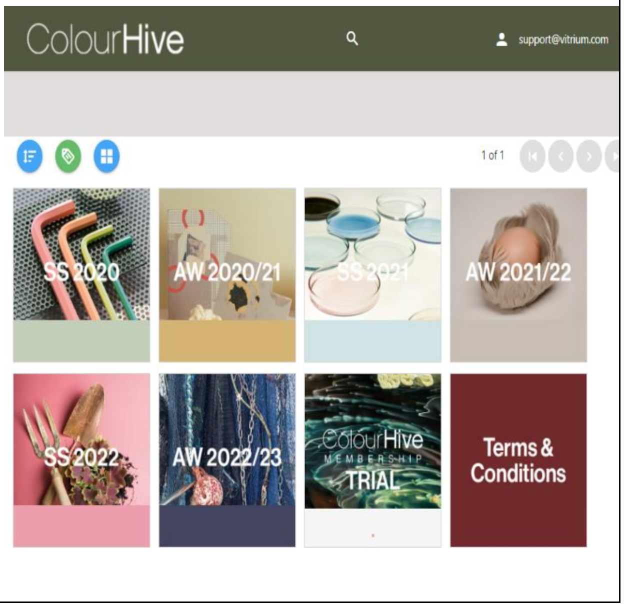


Edit Folder "Main Folder"

Id	4cb555da-e04c-4056-858a-b79f479aba9d
Folder Name *	Main Folder
Folder Settings in Portal	
Folder Heading	
Folder Description	
Use Image	☑
Portal Image	BROWSE
Use folder specific colors	☑
Folder color	
Folder Text color	

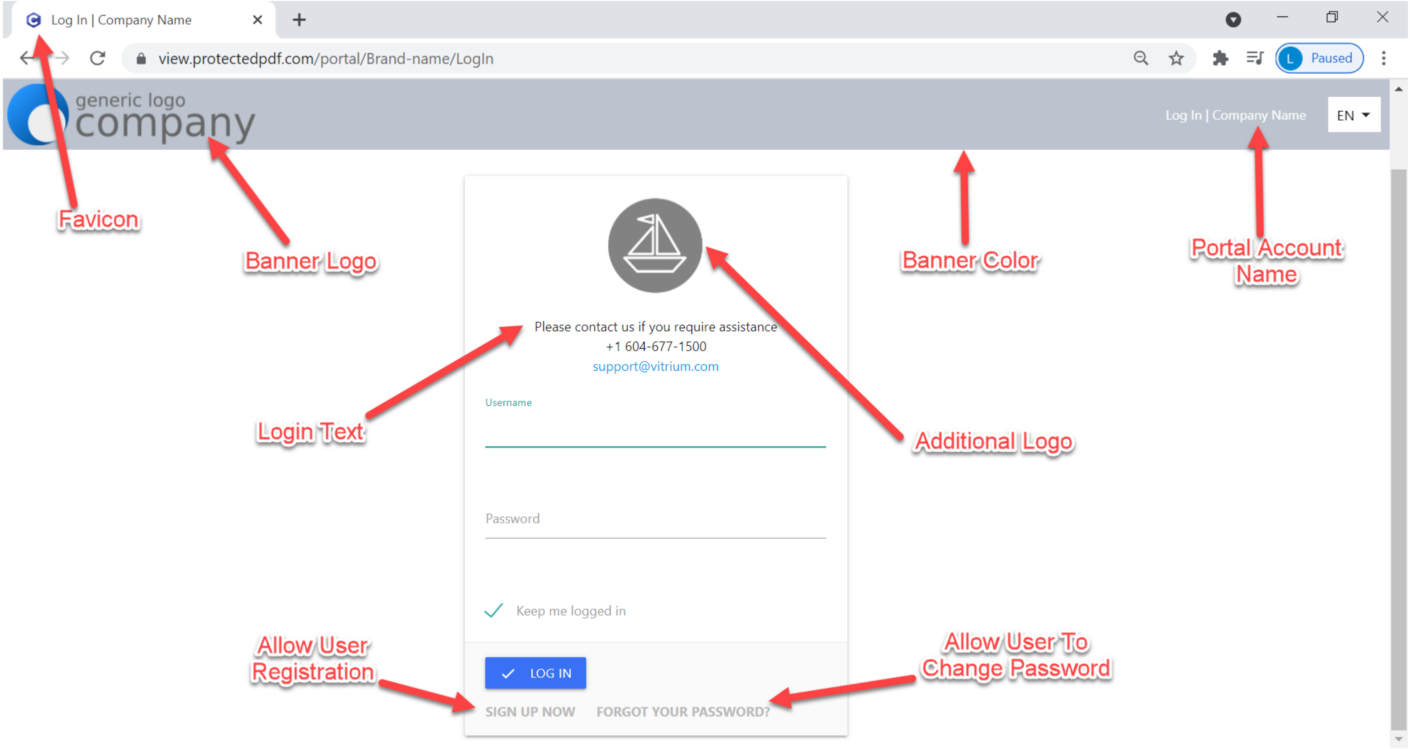
* indicates a required field

✓ SAVE & EXIT

Folder Name	The name of your folder should be as specific and concise as possible. For example: Board materials, Sales Department.
Folder Heading	This heading will be displayed to users as the folder name in Portal. If you leave it empty the Folder Name will be used for this purpose.
Folder Description	The content of this field should be a HTML code with styling. When a user opens this folder in the Portal, this description will appear at the top of the page.
 Use Image ☑ Portal Image BROWSE Use folder specific colors ☑ Folder color Folder Text color	A Portal with Portal Images and folder specific colors may look like this:  ColourHive support@vitrium.com 1 of 1 SS 2020 AW 2020/21 SS 2021 AW 2021/22 SS 2022 AW 2022/23 ColourHive MEMBERSHIP TRIAL Terms & Conditions

SAMPLE USER PORTAL

The portal login page will look similar to this:

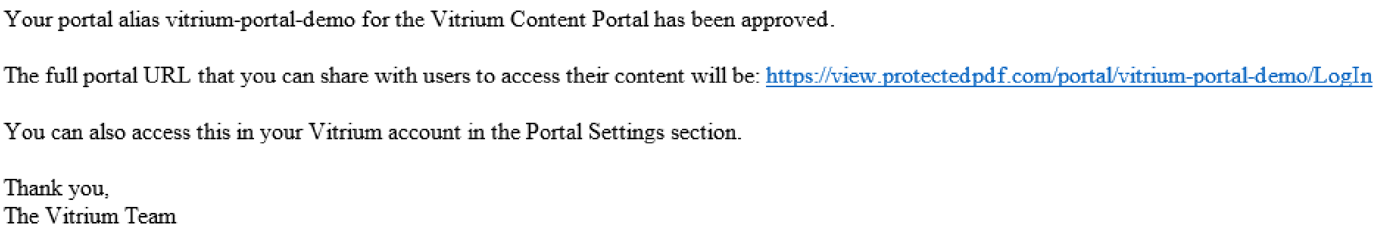


Please contact us if you require assistance
+1 604-677-1500
support@vitrium.com

PORTAL ALIAS EMAILS

After you've entered a name in the "**Portal Alias**" field and saved your Portal Settings, you will either receive an approval email with a link to the URL for your users, or you will receive a rejection email and you will need to go back into your Portal Settings and enter a different alias name and save your settings again.

Approval Email



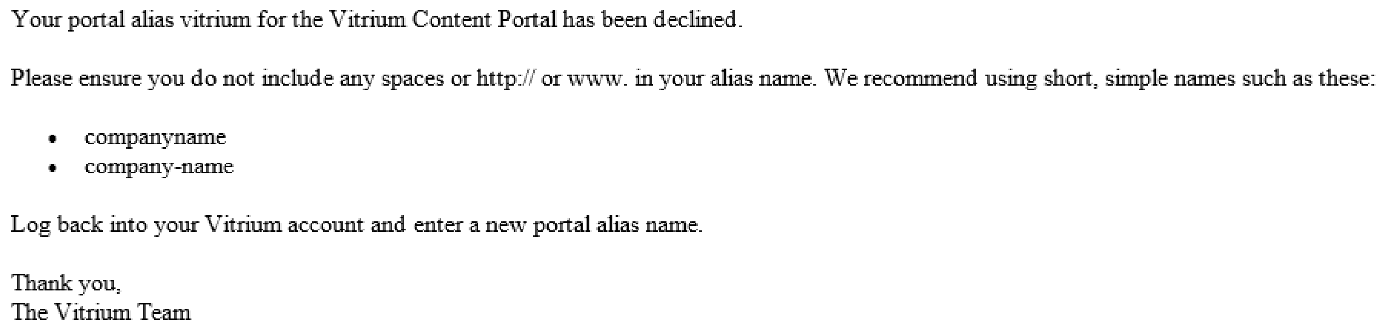
Your portal alias vitrium-portal-demo for the Vitrium Content Portal has been approved.

The full portal URL that you can share with users to access their content will be: https://view.protectedpdf.com/portal/vitrium-portal-demo/LogIn

You can also access this in your Vitrium account in the Portal Settings section.

Thank you,
The Vitrium Team

Rejection Email



Your portal alias vitrium for the Vitrium Content Portal has been declined.

Please ensure you do not include any spaces or http:// or www. in your alias name. We recommend using short, simple names such as these:

- companyname
- company-name

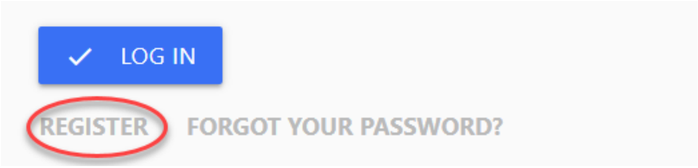
Log back into your Vitrium account and enter a new portal alias name.

Thank you,
The Vitrium Team

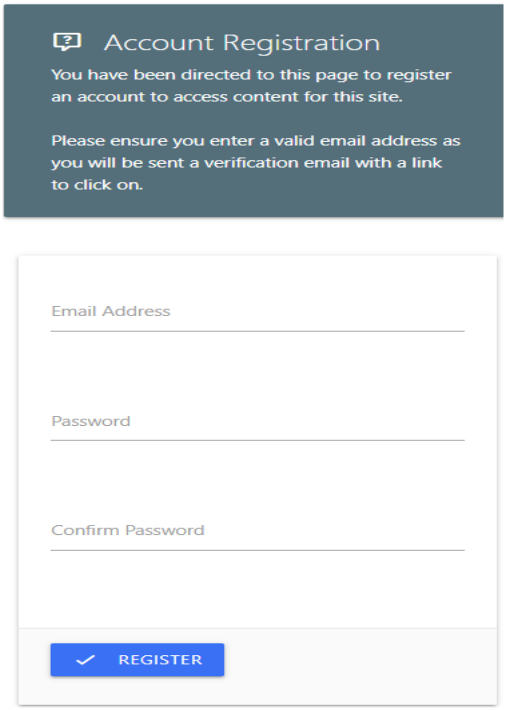
STEPS FOR USER SELF-REGISTRATION

If you selected "**Allow User Registration**" in your Portal Settings, then people will be able to self-register for your portal. The User account will remain inactive until the person has verified their email address. Please note that you will still need to apply content permissions to the new accounts. As stated earlier, the text of the button can be changed if desired. Here are the steps that will occur:

1. Person clicks the REGISTER link on your user portal login page



2. The user will then need to enter their email address, a password, confirm their password, then click REGISTER

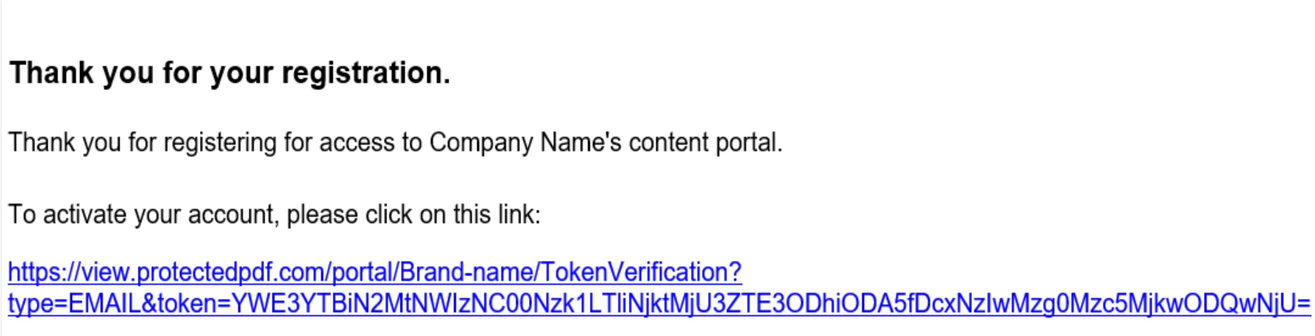


Account Registration

You have been directed to this page to register an account to access content for this site.

Please ensure you enter a valid email address as you will be sent a verification email with a link to click on.

3. A verification email will be sent to the user, and they will need to click to activate their account for the portal



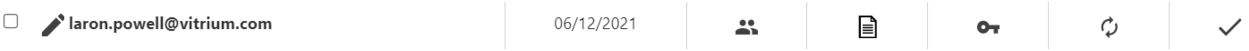
Thank you for your registration.

Thank you for registering for access to Company Name's content portal.

To activate your account, please click on this link:

https://view.protectedpdf.com/portal/Brand-name/TokenVerification?type=EMAIL&token=YWE3YTBiN2MtNWIzNC00Nzk1LTliNjktMjU3ZTE3ODhiODA5fDcxNzIwMzg0Mzc5MjkwODQwNjU=

4. The user clicks on the link to activate their account and you will then see them added as a User in Vitrium

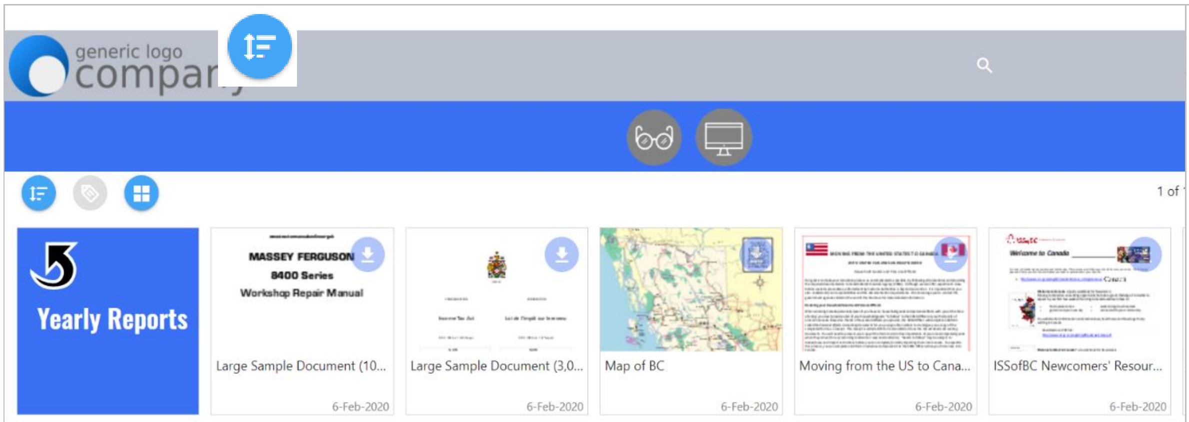


□	laron.powell@vitrium.com	06/12/2021					✓

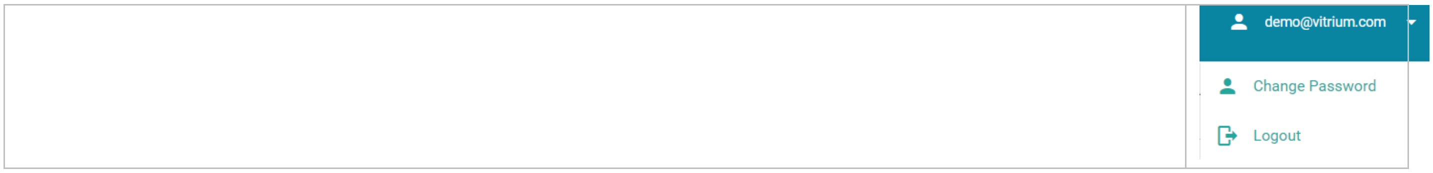
5. You will then need to assign that user with permissions to access your content before they can see anything in the portal

VIEWING CONTENT THROUGH THE USER PORTAL

Using the portal link, login to the portal with a test user and, once logged in, you will be able to access any files or content that the user has been assigned permissions to:

 generic logo company 1 of Yearly Reports MASSEY FERGUSON 8400 Series Workshop Repair Manual Large Sample Document (10... 6-Feb-2020 Large Sample Document (3,0... 6-Feb-2020 Map of BC 6-Feb-2020 Moving from the US to Cana... 6-Feb-2020 ISSofBC Newcomers' Resour... 6-Feb-2020 **Sort Options**	This button allows the user to sort the content by Title (File Name) or the Created Date, and in Ascending or Descending order
Tags Filter	This button allows the user to filter the content by tags that were added to the file upon upload
View Options	This button allows the user to change from a thumbnail (tiles) view to a list view; the thumbnail (tiles) view is the default and is what you see in the

	screenshot above
Web Version	If the user clicks anywhere on the thumbnail, it will open the web version of the content
Secure PDF	If the user clicks on the faded download icon, it will download the protected PDF format of the content which will need to be opened in Adobe Reader or Acrobat or Foxit Reader.
Tags nature, mountains	The user can also see the associated tags on each content by the grayed-out text just below the file name
Search	The user can search for the content file name
Change Password / Logout	The user can click on their username at the top right-hand side of the screen to select "Change Password" or "Logout"



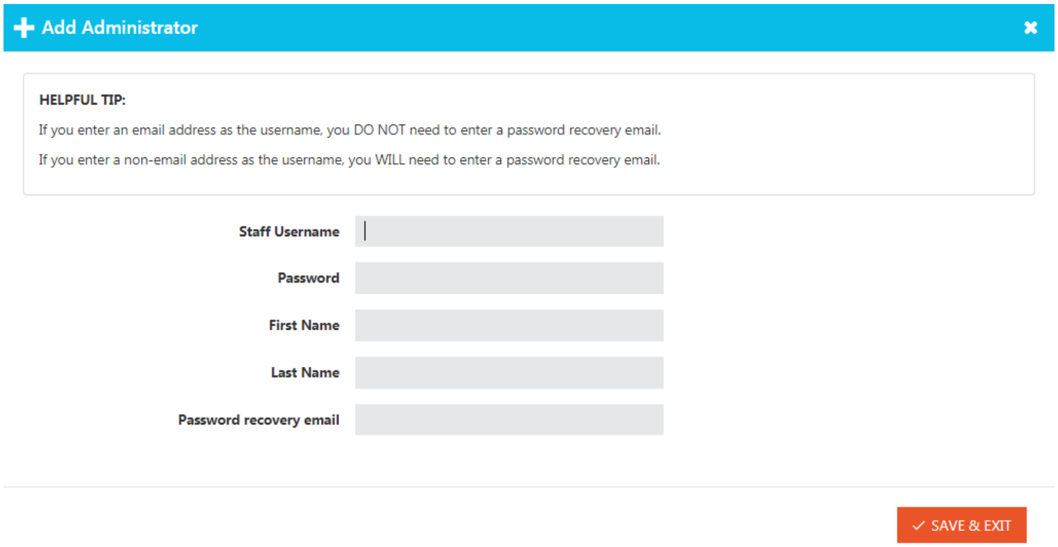
5.7 Staff Users

As defined in Section 3.0, Staff Users are those who can log into Vitrium and perform administrative functions such as adding content, adding users, assigning permissions, viewing reports, and so on. A Staff User can also be an End User, or person who can access your protected content, but you need to add them separately in the Users tab.

SETTING UP A STAFF USER

To create a new Staff User, click the + ADD STAFF button. Depending on which edition of Vitrium you subscribe to will determine what you see next.

Standard & Professional accounts will see:



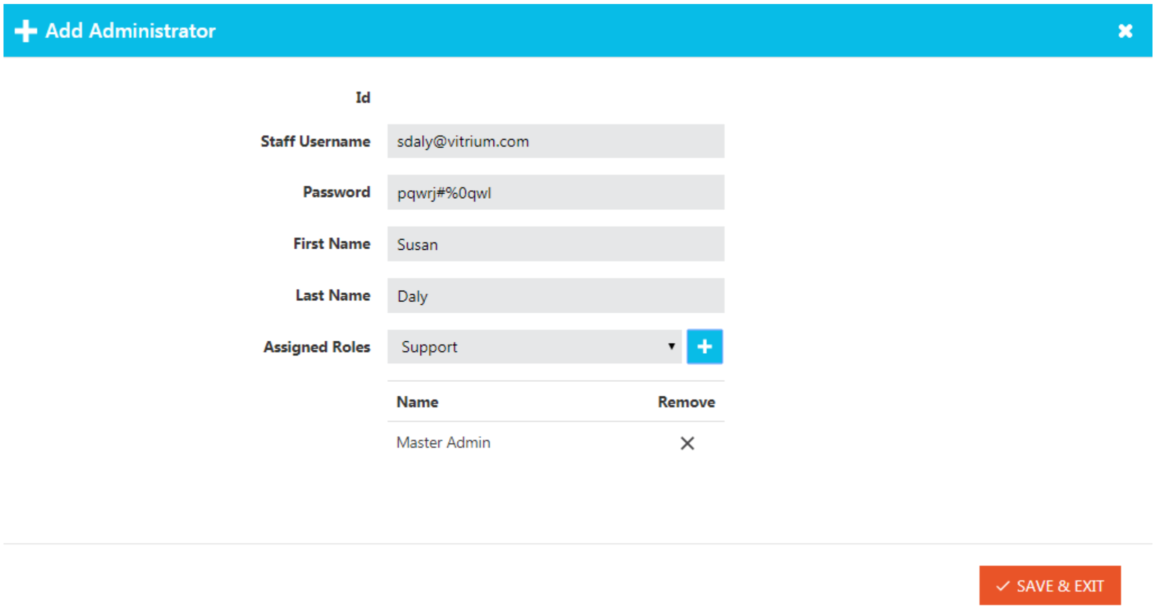
HELPFUL TIP:

If you enter an email address as the username, you DO NOT need to enter a password recovery email.

If you enter a non-email address as the username, you WILL need to enter a password recovery email.

Staff Username	
Password	
First Name	
Last Name	
Password recovery email	

Enterprise Edition accounts will see (with the addition of 'Assigned Roles'):



Id	
Staff Username	sdaly@vitrium.com
Password	pqwrj#%0qwl
First Name	Susan
Last Name	Daly
Assigned Roles	Support ▾ +

Name	Remove
Master Admin	✕

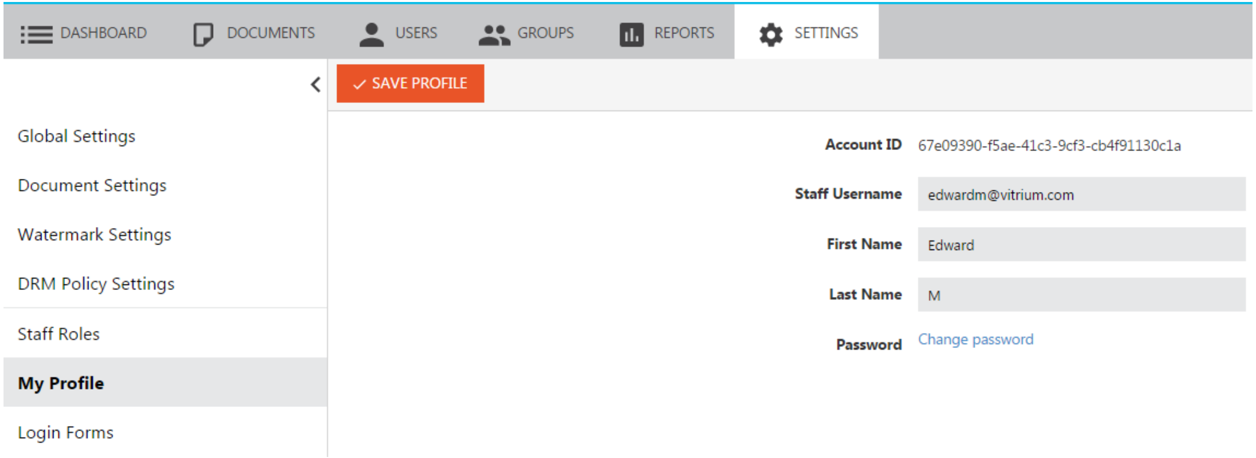
OVERVIEW OF STAFF ROLES

	Master Admin	Support	Permission Manager	Content Manager	System Viewer
Content / Folders					
View & Search Content	x	x	x	x	x
Edit Content	x			x	
Activate / Deactivate / Delete	x			x	
Download Protected PDF	x	x	x	x	
Access Secure Web Link	x	x	x	x	
View Report	x	x	x	x	x
Users					
View & Search Users	x	x	x		x
Edit Users	x		x		
Activate / Deactivate / Delete	x		x		
Edit Group Membership	x		x		
Clear Use & Provide Offline Unlock	x	x	x		
View Report	x	x	x		x
Import & Export Users	x		x		
Groups					
View & Search Groups	x	x	x		x
Edit Groups & Add / Remove Users	x		x		
Activate / Deactivate / Delete	x		x		
View Report	x	x	x		x

	Master Admin	Support	Permission Manager	Content Manager	System Viewer
Settings					
View All Settings	x	x	x	x	x
Edit Global DRM Policy	x		x		
Edit Support URL & Time zone	x	x	x	x	
Edit SSO Lite Mode & Enable External Services	x				
Edit Content Settings	x			x	
Edit Watermark Settings	x		x	x	
Edit DRM Policy Settings	x		x		
Edit Portal Settings	x		x	x	
Add & Edit Staff Users	x				
Edit My Profile	x	x	x	x	x
Manage Login Forms	x			x	
Dashboard / Reports					
View Dashboard & Reports	x	x	x	x	x
Export Reports	x	x	x	x	
MISCELLANEOUS					
API/Integration	x				

5.8 My Profile

Vitrium Security also allows you now to change your overall profile information. You can now customize your Username, First and Last name, as well as access the 'change password' functionality while logged in.



Account ID 67e09390-f5ae-41c3-9cf3-cb4f91130c1a

Staff Username edwardm@vitrium.com

First Name Edward

Last Name M

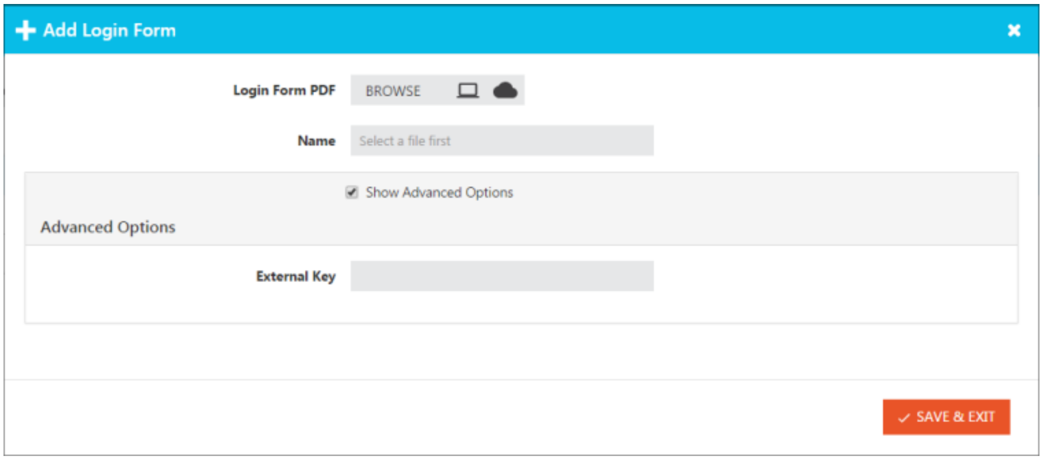
Password Change password

5.9 Login Forms

Available to Enterprise accounts only, if you are a Master Admin, you can upload different PDF login forms into your account. These are the login forms that appear on the protected PDF files only, not the web viewer versions.

To add a new Login Form, follow these steps:

1. Click the + ADD FORM icon.
2. Click Browse and select the desired login form.
3. Once done, enter the name you wish to use to label your login form.
4. Click 'Save & Exit' to activate the settings



Login Form PDF: BROWSE

Name: Select a file first

☑ Show Advanced Options

Advanced Options

External Key:

6.0 OVERVIEW OF VITRIUM'S WEB VIEWER

One of the two secured outputs for protecting documents and images within Vitrium is the WEB LINK (the other is the protected PDF file). When a document or image is uploaded into Vitrium, it gets converted to a secure, HTML5 file that can be shared via the web link you'll see in your Content tab. When clicked on and unlocked, what your users see is Vitrium's proprietary web viewer. Below is a description of all the various features in the web viewer.

6.1 Offline Access / Save to Browser

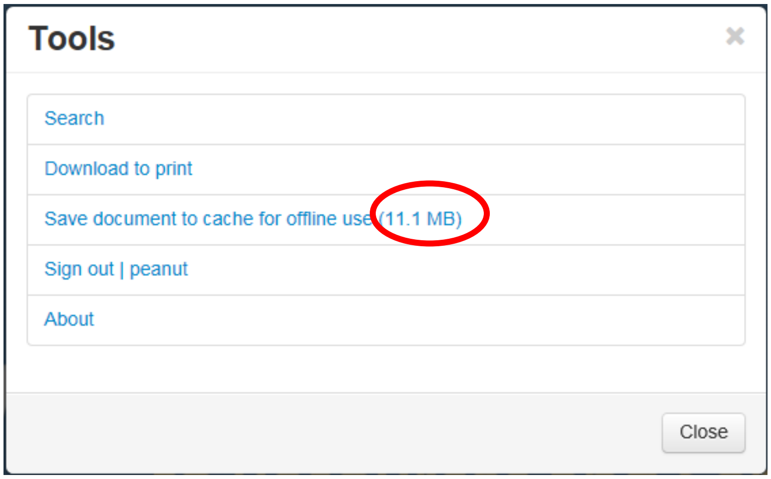
With Vitrium's web viewer, you do have the ability to access the content offline.

IMPORTANT NOTE: In order to provide offline access for users, you need to ensure the DRM policy has a number of days set for 'Offline Access'. If you set it to 0, the user will not be able to access the content offline and the 'save to browser' button will not appear in the web viewer.

1. In the web viewer, click the **'Save to Browser'** button ⤓ at the top right-hand side of the page and you will see the content 'saving'.
2. **Bookmark or save the web link** in your browser so you can retrieve it again when you're in offline mode or airplane mode.
3. Once you're offline, you should be able to view and access your content.
4. Later, when you no longer require viewing that content in offline mode, we recommend 'deleting' the content cache. You can do this by clicking on the delete button at the top right-hand side of the web viewer. This will effectively delete or remove the content taking up space in your browser's cache or memory.

Where is the content being saved? The content is actually being saved to your browser's cache or memory.

How many files can I save to the browser? This will largely depend on what browser you're using, what type of device you're using, and how much space you have remaining in your browser's cache or memory. We recommend checking your browser's memory to see how much space you have left. Then, you can check to see how large your content size is by clicking the Tools button ≡ in the web viewer and review the (MB) beside the "Save document to cache..." line



Why does it take so long for large files to save? This is based on a number of different factors including the performance of the browser itself, the type of device you're using, and how large (in MB) the content is.

6.2 Highlighting & Notes

Vitrium's web viewer allows users to **HIGHLIGHT** any part of the content including specific lines of text or freeform highlighting. It also provides the ability to add comments or notes to specific places in the content with the **NOTES** feature.

Highlighting Options

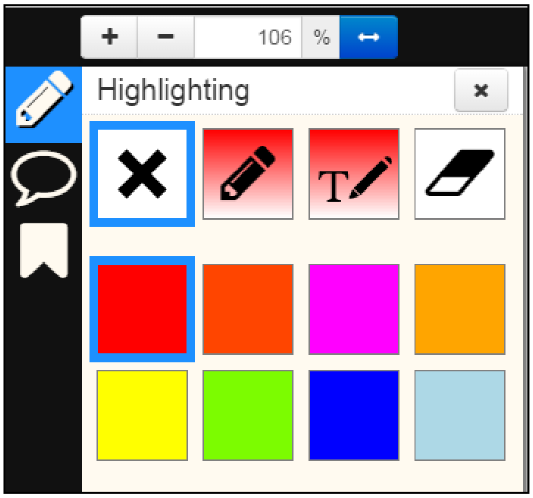
Marking up your content with Vitrium's highlighting tool is very simple. Click on the **Pencil icon** in the left-hand side of the web viewer toolbar and 4 options will appear:

Read Mode – this is the default when you do not require highlighting anything

Draw Free Shape – this allows for free-form highlighting of your content and you can select any color from the pallet shown

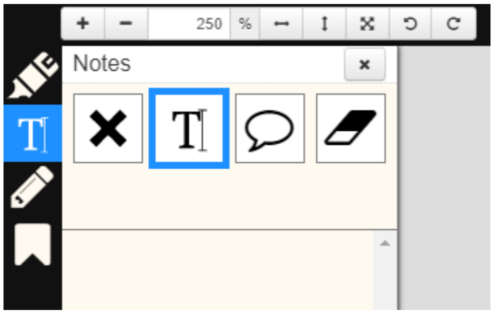
Highlight Selected Text – this allows you highlight text in your content: a word, sentence or entire paragraph and you can select any color from the pallet shown

Delete Annotation – this option allows you to delete/erase any of the highlighting that you have done on your content



Notes Option

Adding notes in your content with Vitrium's web viewer is very simple. Click on the **Notes icon** in the left hand side of the web viewer toolbar and 3 options will appear:



Read Mode – this is the default when you do not require adding notes

Text Field – this allows you to write plain text in the document, user can also use this to fill forms in web-viewer

Create Note – this allows you to add a note anywhere you want in the content: click this icon then click where you want to place your note on the page you're viewing, then type in your note and click Save

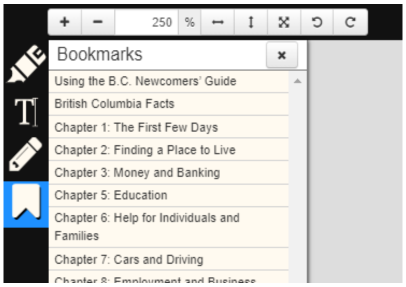
Delete Annotation - this option allows you to delete/erase any of the notes that you have added

Once all your notes are added, you can click on the Notes icon again and a list of all your notes will appear on the left-hand side and you can click on any one of them to quickly jump to the note on that page. You can also hover over any note you've added in your content to view what the note says.

6.3 Bookmarks

If your document has bookmarks in it, then these same bookmarks will also appear in the Vitrium secure web viewer. Bookmarks are a great feature that allows users to select what section of the document they want to review or read.

IMPORTANT NOTE: The original PDF document must already have bookmarks in it prior to being uploaded and protected with Vitrium Security.



Bookmarks

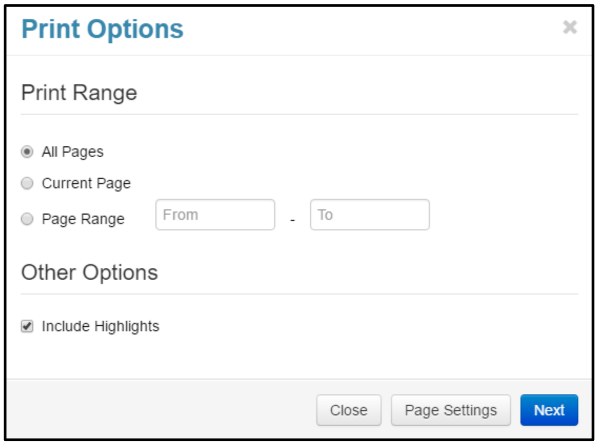
Using the B.C. Newcomers' Guide
British Columbia Facts
Chapter 1: The First Few Days
Chapter 2: Finding a Place to Live
Chapter 3: Money and Banking
Chapter 5: Education
Chapter 6: Help for Individuals and Families
Chapter 7: Cars and Driving
Chapter 8: Employment and Business

6.4 Printing

Printing in Vitrium's secure web viewer is usually quite straightforward but there are a few key points to be aware of. We recommend you review this entire section to understand how this print feature works and what situations you may encounter.

IMPORTANT NOTE: If you want your users to be able to print your content, you need to ensure you have Allow Printing checked in your Content Settings and those Content Settings are applied to the specific content.

1. In the web viewer, click the Print icon that appears in the top right of the toolbar.
2. A Print Options dialog box will appear. You can select All Pages, Current Page or a Page Range, and you also have the option to include Highlights. Click Next. This will then kick-start the 'processing of your printing'.



Print Options

Print Range

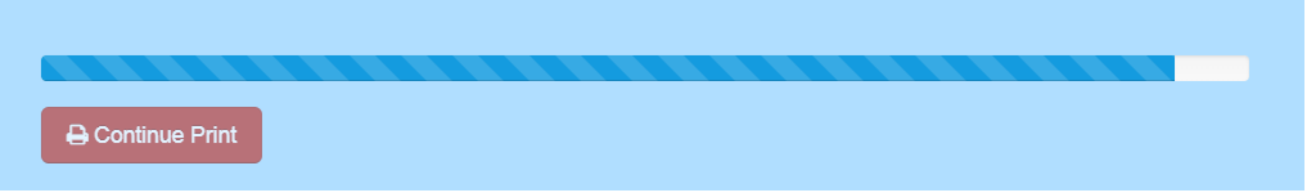
● All Pages
○ Current Page
○ Page Range From - To

Other Options

☑ Include Highlights

3. The content is then processed into a high-resolution format for printing purposes so that the images and text come out crystal clear. The web viewer format is low-resolution which is why this processing step is

necessary. Here’s what you will see when the file is processing for printing:



4. You will then see your web browser’s printing dialog box and you will need to click Print or Okay.

In 90% of cases, this will print your document just fine. In some cases, you may see the **‘Continue Print’** button which will appear for two different reasons:

- **If your document is over 100 pages,** you will see the ‘Continue Print’ button as the web browser’s memory cannot process the amount of data to convert the web viewer file into a high-resolution format. If you click the ‘Continue Print’ button, the document will continue processing and print the next set of 100 pages.
- **If your original document has different or page sizes** (i.e., portrait and landscape, or A4 and A5 pages), then each section of the document that has the same page layout or page size will print at a time and you will see a ‘Continue Print’ button that you will need to click to print the next set of pages. In some cases, if the file has been created in Adobe InDesign or Illustrator, these page sizes can sometimes differ by 1/10th of an inch or centimeter and even these slight variations can cause disruption in the web viewer print process. If you continually see the ‘Continue Print’ button and it's not obvious that your page sizes are different, check with your design team to see if there are different pages sizes in your content. You can also submit a ticket to our support team to look into this for you.

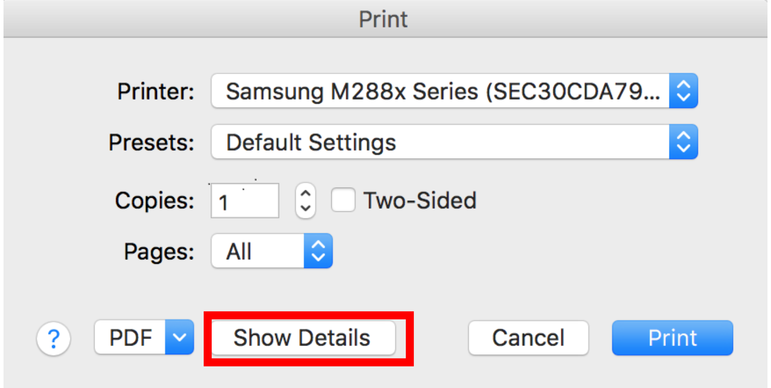
IMPORTANT NOTES:
For Mac (Safari) users: We recommend using Google Chrome to print your document.

For Windows (IE) users: You will need to check your Page Setup before printing documents (see steps below). This is only required once.

Why do blank pages print out? If this issue occurs, you will need to check your browser's print settings and ensure that Page Headers and Footers are set to --blank-- before printing. Refer to the steps below for how to check these.

For Mac Users:

1. When you get to step 4 in the printing steps (see above) and you see the Print dialog box, click **Show Details** and make sure that Page Headers and Page Footers are set to **--blank—**and then you can print your document or image.

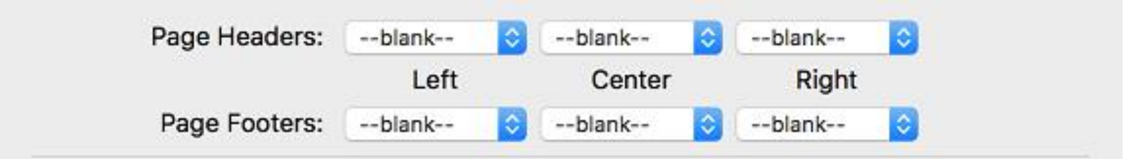


Printer: Samsung M288x Series (SEC30CDA79...

Presets: Default Settings

Copies: 1 □ Two-Sided

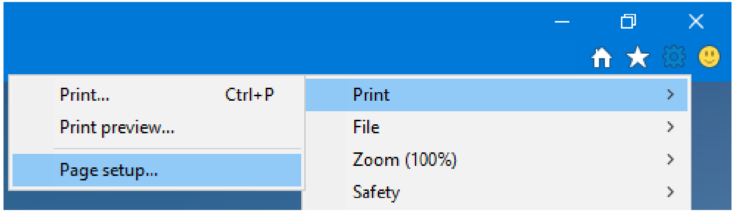
Pages: All



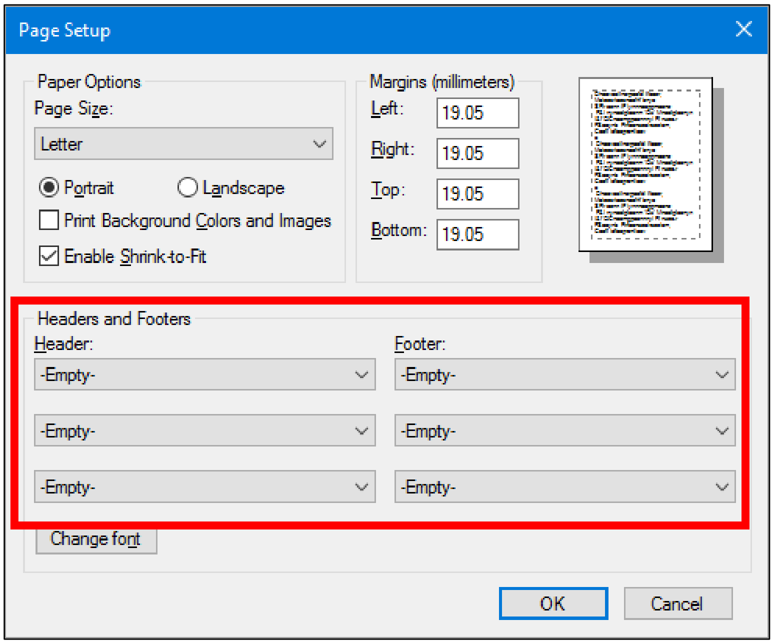
	Left	Center	Right
Page Headers:	--blank--	--blank--	--blank--
Page Footers:	--blank--	--blank--	--blank--

<u>For IE Users:</u>

1. Click on the Settings icon ⚙ at the top right-hand corner of your browser (or press Alt + x)
2. Select **Print**, then **Page setup...**



3. Ensure that the <u>Headers and Footers</u> are set to **-Empty-** and click **OK**



Paper Options
Page Size: Letter
● Portrait ○ Landscape
□ Print Background Colors and Images
☑ Enable Shrink-to-Fit

Margins (millimeters)
Left: 19.05
Right: 19.05
Top: 19.05
Bottom: 19.05

Headers and Footers

Header:	Footer:
-Empty-	-Empty-
-Empty-	-Empty-
-Empty-	-Empty-

4. Now you can go back and follow the 4 steps above to print your document or image.

7.0 HELP TAB

The Help Tab is where you'll find helpful information about Vitrium and your account. You'll see links to this Administrator Manual, as well as other manuals and guides, links to the Introductory Video, Vitrium's Knowledge Base, and a link to the Release Notes page. Enterprise customers will also find links to the inline API code (Swagger) that they can review and test out including an External Service Test page if you have that service enabled.