VITRIUM.COM

Getting Started Guide

February 2020

Table of Contents

1.0 Introduction to Your Vitrium Security Account

1.1 About Vitrium Security

Vitrium Security is an enterprise content security and digital rights management (DRM) solution for organizations who wish to protect, control, and analyze their confidential, sensitive or revenue-generating content. It comes available in 3 different editions: Standard, Professional and Enterprise. The Enterprise Edition comes with REST APIs that allow an organization to integrate the user authentication or file processing components with their own internal or 3rd party systems.

1.2 Supported Formats

Vitrium Security protects over 20 file formats including:

Documents

Adobe PDF (.pdf)	Microsoft Word (.doc / .docx)	OpenOffice Processing (.odt)
Text Format (.txt)	Microsoft Excel (.xls / .xlsx)	OpenOffice Spreadsheets (.ods)
Rich Text Format (.rtf)	Microsoft PowerPoint (.ppt / .pptx)	OpenOffice Presentation (.odp)

Images

JPEG / JPG	GIF *(except animated GIFs)*
PNG	TIFF / TIF
BMP	

Videos

MP4	AVI
MOV	FLV
WMV	MK4

Audio

WAV
MP3

IMPORTANT NOTE: once protected, the formats are converted to a secured HTML5 web format or a protected PDF format (for documents & images only) and your users cannot edit them. Vitrium Security is designed to protect content with additional options and controls for blocking printing, copying, highlighting, setting expiry dates, open limits, browser limits, IP address limits and more.

1.3 Definition of Key Terms

Content Setting: For documents and images, this is the setting where you can allow printing or copying, and where you can choose the type of watermark to be applied. For video, it's where you can choose a specific watermark. Your trial account includes a default setting.

DRM Policy Setting: This is the setting where you can apply your digital rights management policies such as expiry date, offline access, content open limit, PDF or browser limit, IP address limit, account limit, print limit and more. Your trial account includes a default setting.

Users: These are the individuals who will be the recipients of your secured content, not to be confused with the staff users. You can add new users in the Users tab of Vitrium and grant them permission to view your secured content in the Content tab. For customers using Enterprise Edition, you can manage Users, Groups and Permissions in a separate system such as Active Directory, a SQL database, a CRM system, learning management system, or virtually any other type of system.

Staff Users: These are the administrative users of Vitrium who can log into the Vitrium application and perform various functions such as adding Content, applying permissions, viewing reports, and so on. If you want a staff user to be able to access content, you will also need to set them as an end user in the Users tab.

Groups: You can add Users into a Group if you wish to apply different DRM policy settings for different groups.

Permissions: This is where you assign Users or Groups to access your secured content. You can add them in the Permissions tab after you click Add Content, or you can click on the Permissions icon in the Content tab of Vitrium.

Web Link: This is the link to your secured content that you can send or share with your Users. They can open the link with any web browser on any device (desktop, tablet or smartphone).

Secured PDF: This is the other secured file output for documents that you can also share with your Users. The file can be downloaded and opened with Adobe Reader or Acrobat or FoxIt Reader on a desktop environment only. There are no plug-ins required to view the content but a user may need to disable their Adobe global object security policy.

IMPORTANT NOTE: the secured PDF file CANNOT be unlocked using Chrome or other browser's built-in PDF viewers. You must download the file and open it from your 'downloads' folder or from wherever you saved the file. And you must use Adobe Reader or Acrobat or FoxIt Reader to open the file. It won't open with Mac Preview, or any other PDF viewers.

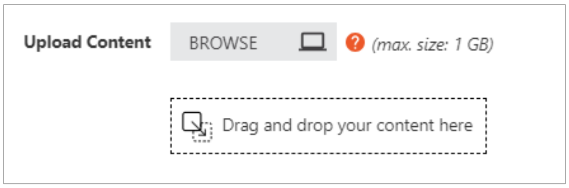
1.4 Overview of the Main Tabs

TAB	DESCRIPTION
DASHBOARD	The **Dashboard Tab** is where you will see different graphs showing you various analytical data about your content and their usage. Each graph shows up to 5 items (i.e. 5 files or 5 users). You can drill into each graph to show all the data where you can then export the information to a CSV file for further analysis.
CONTENT	The **Content Tab** is where you will upload and manage your files and folders. It's also where you can apply permissions to the content and access one of the two secured content outputs: the web link or secure PDF. You can also de-activate or revoke a file and view a report on the user activity.
USERS	The **Users Tab** is where you can add and manage the end users, not the staff users (staff users are managed in the Staff Users section in the Settings tab). In the Users tab, you can add a single user or multiple users, either manually or via a CSV file import. You can view the groups that a user is added to, clear the use of a particular user if they have exceeded their limits and you don't suspect any fraud. You can also de-activate a user or view a report of all that specific user's activity.
GROUPS	The **Groups Tab** is where you can add groups and assign individual users to that group, similar to the way you would add different files into a specific folder. You can de-activate a group and view a report on that group's activity.
REPORTS	The **Reports Tab** is where you can view an activity log of who is accessing your secured content, on what date and time, from which IP address, and more. Depending on which edition you have, there are up to 12 additional analytics reports with drill-down capability.
SETTINGS	The **Settings Tab** is where you can manage your Account Settings, Content Settings, Watermark Settings, DRM Policy Settings, Portal Settings, Staff Users and My Profile.
HELP	The **Help Tab** is where you can access various support links including this Getting Started Guide, How to Support Your End Users, Vitrium's API documentation (for Enterprise customers), and the Release Notes. It's also where you can submit a support ticket.

2.0 Adding Content & Applying Permissions

2.1 Adding Content

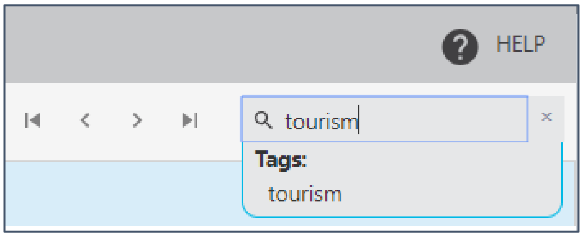
Go to the **Content Tab**, and click + ADD CONTENT



Upload Content: click Browse to select your file(s) from your computer or network drive, or drag and drop the file(s) to this location. You may upload a single file or multiple files at a time. Refer to section 1.2 above for a list of supported formats in Vitrium. If you upload multiple files, they must be of the same type – all documents or all images or all videos. This is because depending on what type of content you upload, the Content Settings will change.

Content Setting: select the default setting – if you wish to create a different Content Settings, refer to the full Administrator Manual for steps on how to set this up.

Tags: add any tags (or keywords) that are appropriate for the file – you can search for content by these tags in the search bar at the top right-hand section of the Content window. If you set up and enable the Portal, your users can also search for content based on these tags.



2.2 Applying Permissions

You can apply permissions to your content in one of two ways: (1) within the "ADD CONTENT" window or (2) by clicking the Permissions icon in the Content tab.

Option 1: Applying Permissions within ADD CONTENT window

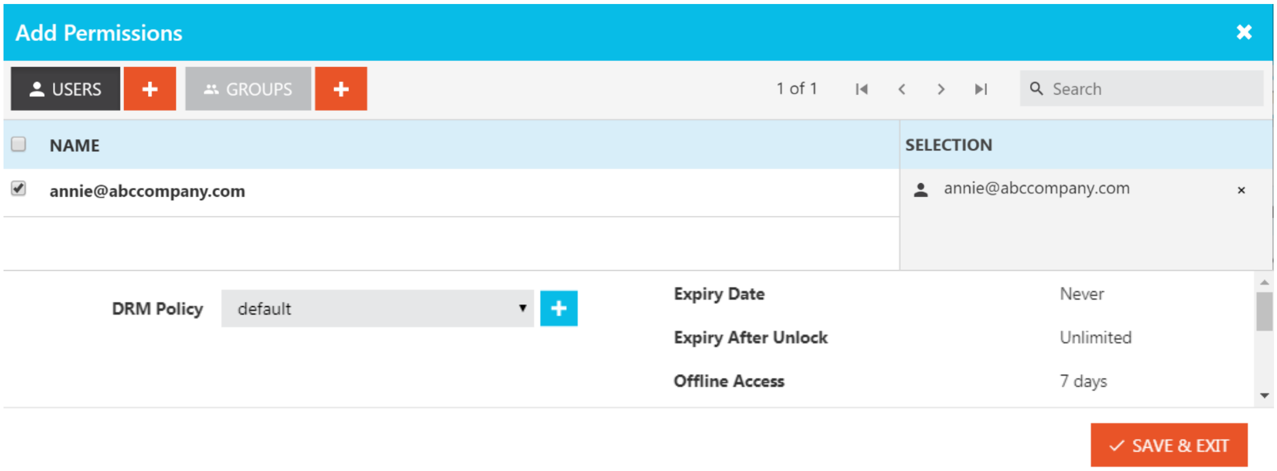
While you're still in the "ADD CONTENT" window and after selecting your file(s) and setting your Content Settings and Tags, click on the Permissions tab **Permissions**

You'll see USERS and GROUPS showing in this tab. If you are using a trial account, you should see yourself set up as a USER here. Select yourself, then select the default DRM policy and click Save & Exit.

IMPORTANT NOTE: even if you have access to Vitrium as a Staff User, you will still need to assign yourself permission as a USER and set a DRM policy to access the protected content.

If you do not see any users listed here, click the + **symbol** beside Users to add a new one to test with. You can add more users later in the Users tab. Enter a **Username** and **Password** and leave the other fields blank until you become more familiar with the system. Click Save & Exit**.**

Don't forget to select the default **DRM Policy**, and then click **Save & Exit.**



Add Permissions

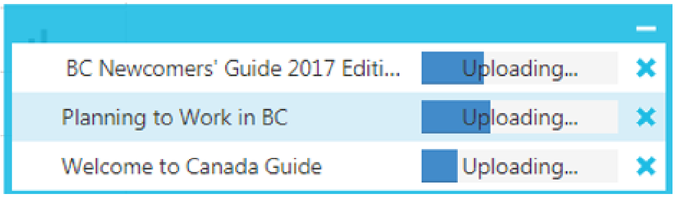
☐	NAME	SELECTION
☑	annie@abccompany.com	annie@abccompany.com

DRM Policy: default

Expiry Date	Never
Expiry After Unlock	Unlimited
Offline Access	7 days

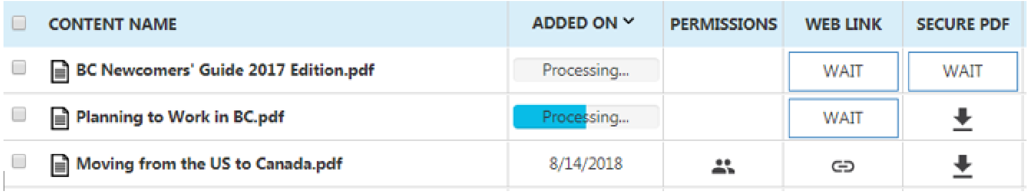
Your file will now go through 2 stages:

1. An **uploading stage** which is usually quite fast and you may even miss it.



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

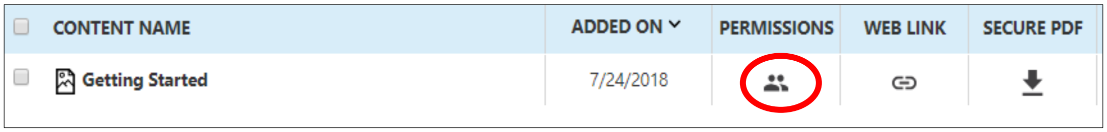
2. A **processing stage** which may take a bit longer depending on your file size or how many files you are processing. When the processing stage is complete, you will be able to test the unlock process of your newly secured content.



☐	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	👥	🔗	⬇

Option 2: Applying Permissions within the main Content tab

The second way you can apply Permissions is clicking on the Permissions icon 👥 in the CONTENT tab. You can also modify your permissions later this way as well.



☐	CONTENT NAME	ADDED ON	PERMISSIONS	WEB LINK	SECURE PDF
☐	Getting Started	7/24/2018	👥	🔗	⬇

3.0 Distributing Content

3.1 Secured Output File Types

As mentioned earlier in Section 1.2, Vitrium Security processes your file and creates 1 or 2 different types of secured formats depending on what type of content you uploaded.

For video files, the secured output will be a secure web link which you can locate in the Content tab, under the **WEB LINK** column.

For documents and images, the secured output will also be a secure **WEB LINK** but there is also a **SECURE PDF** option as well. This option is a protected PDF file that can be downloaded and saved to your local computer or network, and either emailed to your users or shared through your own website, an FTP site, a file sharing system, etc. The PDF file remains secure no matter where it goes as the security layers remain with the file at all times and it will always require authentication before anyone can view the content.

IMPORTANT NOTE: Vitrium strongly recommends TESTING your secure content before sending the web link or PDF file to your users. If you signed up for a free trial through the Vitrium website, you will be able to use the same username and password combo as long as you assigned yourself with Permissions to the file and applied a DRM policy.

3.2 Secure Web Link

Click on the **WEB LINK** 🔗 icon beside your newly uploaded file and enter your test user credentials. You can copy and paste this link in an email, post on your website, in a portal, or in any system that you share your content with users. In the Professional and Enterprise Editions, you can customize the URL links to use your own domain address.

Encryption Level:	256-bit AES encryption
Open With:	All supported web browsers (Chrome, Firefox, Safari, Edge, Internet Explorer, or Opera on any type of web-enabled device

3.3 Secure PDF File

Right-click on the SECURE PDF download ⭳ icon and save the file to your hard drive or network, then open it with Adobe Reader or Acrobat DC or FoxIt Reader. If you click on the file, it may download automatically to your ‘Downloads’ folder and you can open the file from that location. DO NOT try opening the file in Chrome’s built-in PDF viewer, Mac Preview or other PDF viewers as the file will not open that way. You must use Adobe Reader or Acrobat DC or FoxIt Reader.

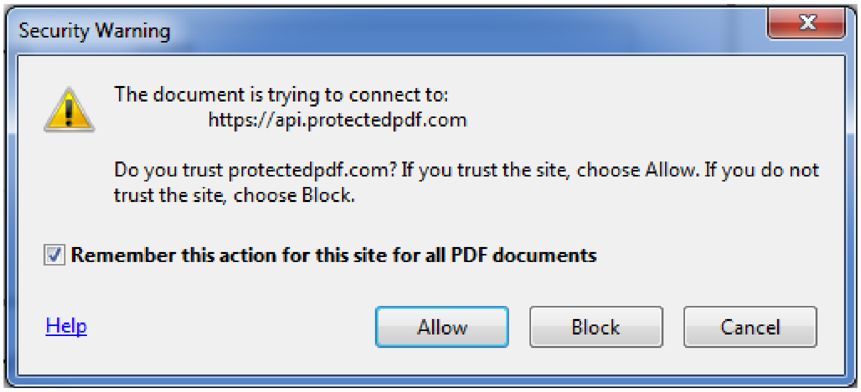
Encryption Level:	128-bit AES encryption
Open With:	Adobe Reader or Acrobat DC or FoxIt Reader (desktop only)

3.3 Additional Steps for Opening Secure PDF File

When opening a protected PDF file in Adobe/FoxIt Reader for the first time or second time, you may encounter a couple of different pop-up messages which require specific action:

1. Security Warning: this is a security message that will appear the first time you or your user unlocks a protected PDF file. It's asking you to confirm whether you trust the site that is trying to authenticate you. The default site is Vitrium's server. If you purchase the Enterprise Edition, the site may be your company's site depending on how you implement Vitrium in your environment.

   ACTION: check the box "Remember this action…", then click Allow.



Security Warning

The document is trying to connect to:
https://api.protectedpdf.com

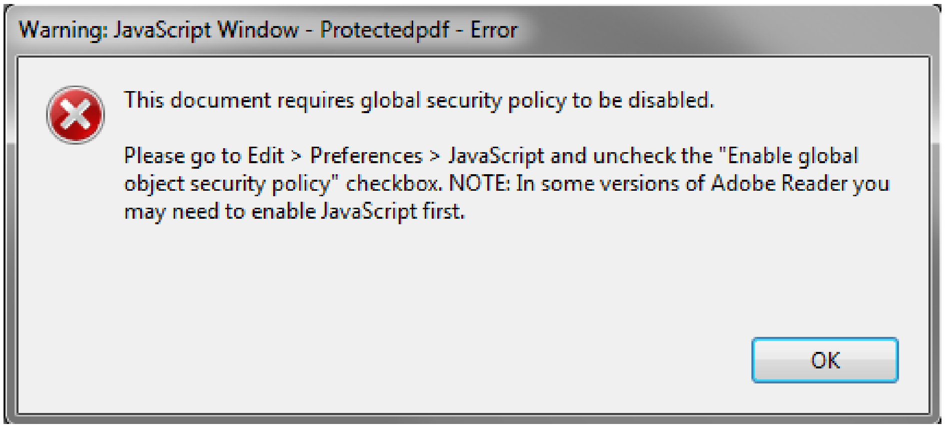
Do you trust protectedpdf.com? If you trust the site, choose Allow. If you do not trust the site, choose Block.

☑ Remember this action for this site for all PDF documents

2. JavaScript Warning: this is a message asking the user to disable Adobe's global object security policy. By disabling that feature, it will allow the protected PDF file to place a cookie in the user's Adobe settings so you can count their computer as part of the PDF/browser (device) limit. If tracking device limits is not important to you, there is a way to remove this message in the Content Settings – see Section 5.2 of the Administrator Manual (Set Acrobat cookie policy).

   ACTION for PC users: in Adobe, click Edit > Preferences > JavaScript and uncheck the 'Enable global object security policy' field

   ACTION for Mac users: in Adobe, click Adobe Reader > Preferences > JavaScript and uncheck the 'Enable global object security policy' field



Warning: JavaScript Window - Protectedpdf - Error

This document requires global security policy to be disabled.

Please go to Edit > Preferences > JavaScript and uncheck the "Enable global object security policy" checkbox. NOTE: In some versions of Adobe Reader you may need to enable JavaScript first.

4.0 Assisting Your End Users

Below are some of the common errors you may encounter with your users but you can also review the full manual on How to Support Your End Users.

4.1 Common Error Codes & Steps to Resolve Them

Vitrium has different error codes that appear for different end user issues. Below are some of the more common ones but we recommend keeping this **Error Code Reference Guide** handy as well: http://www.vitrium.com/support/pdfs/error_code_reference_guide.pdf

No access (w29): This error is received when user permissions have not been applied to the file in question. To correct this, click on the Permissions icon beside the file in question. If the user does not appear here, then click Add New, click on the user, then click Add Permissions, then Save & Exit and ask the user to try unlocking the file again.

Exceeded limit (vc3): This error is received when the User has reached their browser or application limit per the setting in the DRM Policy. If you do not suspect fraud with this User and wish to clear this person's usage so they can access the protected file, go to the Users tab, click on the Clear Use icon beside the User in question ⟳ and clear their usage. Once done, ask the User to log in again.

Credentials incorrect (bw5): This error is received when the User has entered the wrong credentials, often related to a typo. You can look up the correct credentials for the User or ask them to try again and be mindful of any uppercase or lowercase, and watch for any unnecessary spaces at the end.

Account not found (3yq): This error is received when the User does not exist in the Vitrium account. If you believe the User is added in the account, you can check to make sure they are using the correct username and password combo. If they are not in the system, you can add them as a new User. All of this can be done in the Users tab.

Account inactive (m47): This error is received when the User has been deactivated or their access to this file revoked. If you wish to re-activate the User, you can go to the Users tab and click on the X under the Active column which will change this to a ✓ and the User will be active again.

Access expired (qe2): This error is received if the expiration date for access to the file has passed, OR when a DRM Policy has not been set at any level. You can either change the expiration date, change the DRM Policy completely, or set a new DRM Policy to the file or User.

4.2 Common Errors When Opening the Secure PDF File

These are the more common errors we see when end users are sent the secured PDF file:

The User must open the PDF file with Adobe Reader or Acrobat or FoxIt Reader on a desktop computer only. The common mistake is the User might be trying to open the file in a different PDF viewer such as the Mac PDF Viewer or a web browser's built-in PDF viewer. The User needs to download the PDF first to their hard drive or a network drive, then open the file with Adobe or FoxIt Reader. If they are using a tablet or a smartphone, you should send them the secured web link, not the PDF file.

The User may need to disable the Global Object Security Policy in their Adobe program. The steps were outlined in section 3.3 above. The User only needs to do this for the first unlock session. The setting will remain the same and future unlocks will be more seamless. The User needs to:

1. Open Adobe Reader, go to Edit > Preferences
2. Go to the JavaScript under the Categories section
3. Uncheck the "Enable global object security policy" – you need to disable this policy in order to unlock the protected file
4. Click OK once this setting is disabled (or unchecked)
5. Open the protected PDF file and click Allow on all the communication messages

The User requires the PDF file to communicate to the Internet in order to unlock the PDF file. In most environments, this is usually quite simple and the User must simply click "Ok" or "Allow" on all communication prompts that pop up in their Adobe program, but in more strict IT environments, they may run into a proxy server or firewall issue, in which case, they or their IT department needs to provide this access. More information about this can be found in this article: https://support.vitrium.com/hc/en-us/articles/201655944-Proxy-Firewall-Error

5.0 Overview of Reports

REPORT NAME	REPORT DESCRIPTION
User Activity Log	This report shows the user-level activities associated with your account including successful and unsuccessful unlocks for different files, the date and time, the method used, IP address, tracking ID, the application used, and more.
Successful Unlocks by Content	This report shows all the files that have been successfully unlocked within your Vitrium Security account (with the specified date range that you have selected). If you drill in to a file, you can see which Users unlocked the file. You can also filter by content type.
Failed Unlocks by User	This report shows the list of Users with the most 'failed' attempts in unlocking your secured documents. This is a good indicator to help you identify possible fraud or perhaps something simpler such as a User who continually forgets his or her password.
User Applications	This section shows all the types of applications used to unlock your secured content – which browsers or applications such Adobe Reader or Acrobat or FoxIt Reader and how

	many times. If you drill further into one type of application, you will see the various versions used.
User Locations by Country	This report shows the total unlocks by User Count for each country (within the specified date range). If you drill in further to a country, you will see all the users who accessed your content from that particular country including their IP address.
Read-Through-Rate (RTR) by Content	This report shows the read-through-rate for a particular file in your account (within a specified date range). You can drill in further on a file to see the list of users who have opened that file and what their specific RTR is.
Read-Through-Rate (RTR) by User	This report shows the read-through rate for a particular user in your account (within the specified date range). You can drill in further on a user to see the list of files that they have opened and what their specific RTR is.
Views by Content	This report shows you the most actively viewed files in your account by the number of users who opened them (within the specified date range). You can drill in further on a file to see which Users were the most active with that file.
Views by User	This report shows you the total number of files unlocked by users in your account (within the specified date range). You can drill in further on a user to see which files they were the most active with.
Time Spent by Content	This report shows the total time duration (in hours and minutes) that was spent collectively by all your users on each file (within a specified date range). If you drill in further, you can see which user spent the most time on a particular file.
Time Spent by User	This report shows the total time duration (in hours and minutes) that was spent by each of your users (within a specified date range). If you drill in further, you can see the time duration of each file for that particular user.
View-Rate by Content	This report shows the view rate of each particular video in your account (within the specified date range). You can drill in further on a video to see the list of users who have opened that video and what their specific View Rates are.
View-Rate by User	This report shows the view rate for a particular user in your account (within the specified date range). You can drill in further on a user to see the list of videos they have opened and what their specific View Rates are.

6.0 Getting Help

There are a number of ways you can get help from Vitrium including:

1. Watching Videos
2. Visiting the Vitrium Help Center
3. Click the Help tab in your Vitrium account
4. Submitting a support ticket to Vitrium:
    a. Submit a ticket: https://support.vitrium.com/hc/en-us/requests/new

b. Send an email to: support@vitrium.com