DRM Policies Guide

Version 8.x
December, 2020

1.604.677.1500 (direct)
1.866.403.1500 (toll-free)

www.vitrium.com

Table of Contents

1.0 About Vitrium's DRM Policies

Vitrium's DRM policy settings are the digital rights management controls that you can apply at the user, group, file, or folder level. Depending on which edition of Vitrium you have, you can set an expiry date, a browser or PDF limit (similar to a device limit), limit the number of days of offline access, set a print limit, an IP address limit, and more.

1.1 Understand the 2 Important Rules

Before implementing Vitrium DRM policy settings, you should be aware of two important rules:

RULE #1: The most lenient DRM policy setting will always apply no matter where it's set.
If you set a DRM policy at multiple levels (user and group level for example), the most lenient policy will always override. Since this can get quite complicated and may cause policy conflicts, Vitrium recommends ONLY setting a DRM policy at one level, or reviewing the Section 4.0 to learn more about setting up DRM policies at multiple levels.

RULE #2: You must enter a value for EVERY field in a DRM policy.
If you only plan to set a DRM policy at one level (the group level for example), you need to ensure that no field is left to 'not set', otherwise the user will receive an error message when trying to login or access a protected content. You should set the field to Never, Unlimited or enter a specific date or numerical value depending on the policy field (see Section 2.1 for more details about these fields). If you are planning to set a DRM policy at multiple levels, you can leave a policy field to 'not set' as long as it's set at some level. Check out this video to learn more: *Vitrium DRM Policy Video #2: Setting DRM Policies at Multiple Levels.*

1.2 Different Levels You Can Apply a DRM Policy to

You can apply a DRM policy to different levels but we strongly recommend to most customers only applying a DRM policy to one level to limit the possible conflicts per rule #1 above.

DRM Policy Level	When to Set At This Level
Content level	A DRM policy is ideal to set at this level when you have a very specific DRM policy for different content and their respective users.
Group level	A DRM policy is ideal to set at this level when you can easily group your audience into different user groups and apply different DRM policies for each group.
Folder level	A DRM policy is ideal to set at this level when you have a lot of content that you prefer to group into folders and each folder requires a specific DRM policy.
User level	A DRM policy is only recommended to set at this level when you wish to apply different policies for each user.
Global level	We generally DO NOT recommended setting a DRM policy at this level, unless you ONLY have 1 DRM policy for all your users.

2.0 How to Create a DRM Policy

To set up a DRM policy in the Vitrium application:

1. Go to **Settings** > **DRM Policy Settings**
2. Click **Add DRM Policy**
3. **Name your policy** as you can then apply this policy at different levels
4. **Enter the field values** – depending on which edition you subscribe to will depend on what policy fields you will see – ensure you **set every field to some value** (unless you plan to set a DRM policy at multiple levels) – refer to Section 2.1 below for a description of each DRM policy field
5. Click **Save & Exit**

If you are an Enterprise customer or have an Enterprise trial, you should also review the Vitrium API Guide to learn more about how to apply a DRM policy via the APIs.

2.1 Description of the DRM Policy Fields

Below is a table describing each DRM policy field and which edition it's available in. We also recommend you watch the video: *Vitrium DRM Policy Video #1: An Introduction to the Policy Fields*.

Policy Field	Std	Pro	Ent	Description
Start date	X	X	X	Set a start date for when a user can access your content or set to Immediate.
Expiry date	X	X	X	Set an expiry date or select Never if this is not applicable to your DRM policy.
Expiry after first unlock		X	X	Set the number of days for content to expire after the first unlocks by a user, or select Unlimited if this is not applicable to your DRM policy. This can be useful for a trial-based or subscription-based model.
Offline access	X	X	X	Set the number of days your users may access content while in offline mode (or not connected to the Internet). If you do not wish to give Offline Access, set it to "0" per rule #2. IMPORTANT NOTE: If you set this field to Unlimited, this may disable the file replace or revoke functionality for the protected PDF file so we recommend setting a specific number.
Combined Limit	X	X	X	Set a total limit of browsers or devices that a user can access a secured content on. IMPORTANT NOTE: each browser (Chrome, IE, Mac, Firefox, etc.) is counted once, even if viewing the content on the same computer.
PDF limit	X	X	X	If you select this option, you can set the PDF limit individually i.e. how many PDF reader users can access secured PDF on. This is ideal in scenarios for those distributing both types of secured content for documents: protected PDF files and secure web links.
Browser Limit	X	X	X	If you select this option, you can set the Browser limit individually i.e. how many browsers, user can access secure web links on. This is ideal in scenarios

				for those distributing both types of secured content for documents: protected PDF files and secure web links.
Web Browser Print Limit		X	X	Set the number of times a user can print the content. Select Unlimited if this is not applicable to your DRM policy per rule #2. This field is only applicable to those distributing the secure web links for documents or images. It is not applicable to the protected PDF file.
Content open limit			X	Set a limit on the number of times a user can unlock content. Select Unlimited if this is not applicable to your DRM policy per rule #2. This is useful when you only want your content opened a limited number of times, for a sneak peek or a trial purpose.
Library or account limit			X	Set a limit on the number of files (or links) that a user or group can open. Select Unlimited if this is not applicable to your DRM policy per rule #2. This is useful for a subscription or library model where the user can log into a library or a portal with numerous content but can only access files up to the library limit set here.
IP address limit			X	Set a limit on the number of IP addresses that a user can open content from. You can also enter "0" and then specific a specific IP address or range of IP addresses to limit the access even further. Select Unlimited if this is not applicable to your DRM policy per rule #2. This is useful for country-specific or corporate/academic site licenses.
Location Restriction			X	If you want to block some regions from accessing your content, enter those region name here.
Location Permits			X	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

2.2 Understanding the PDF and Browser Limit

For documents and images, Vitrium Security has two different types of secured outputs:

1. **Protected PDF File** – this type of protected content can only be opened with Adobe Reader or Acrobat or FoxIt Reader on a desktop environment only
2. **Secure Web Link** – this type of protected content can be opened with all types of browsers on all types of devices

For video content, Vitrium Security only has one type of secured output:

1. **Secure Web Link** – this type of protected content can be opened with all types of browsers on all types of devices

To understand how the 'limits' work in Vitrium's DRM policy, the colored matrix below represents how the PDF and browser limit works:

1. **ORANGE = PDF LIMIT – applicable to the Protected PDF File**

2. **GREEN = BROWSER LIMIT – applicable to the Secure Web Link**

		Work Computer	Home Laptop	Tablet	Smartphone
PDF Viewer	Acrobat				
	Adobe Reader				
Web Viewer	Chrome				
	Safari				
	Firefox				
	Opera				
	IE				
	IE Edge				

If you select TOTAL LIMIT (known as 'PDF and Browser Limit' for Standard Edition customers) and set it to 3, your user can access:

- 1 orange box + 2 green boxes
- 2 orange boxes + 1 green box
- 3 green boxes
- 3 orange boxes

If you select INDIVIDUAL LIMIT and set it to 1 PDF and 3 Browsers, your user can access:

- 1 orange box + 3 green boxes

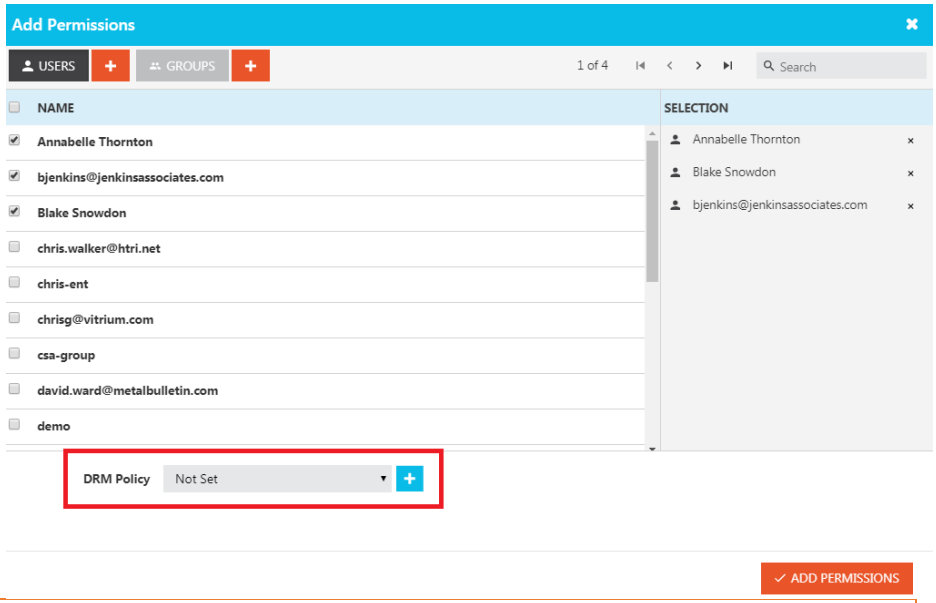
You can see how more restrictive the Individual limit can be which is ideal if you are looking to have more tighter DRM control over your content.

3.0 How to Set a DRM Policy at Different Levels

3.1 At the Content Level

A DRM policy is ideal to set at this level when you have a very specific DRM policy for different content and their respective users.

1. In **CONTENT** tab, click **ADD CONTENT** and add your file
2. Click the **PERMISSIONS** tab
3. Select your **USERS** or **GROUPS**
4. Select the **DRM POLICY** from the drop-down menu
5. Click **ADD PERMISSIONS**, then **SAVE & EXIT**

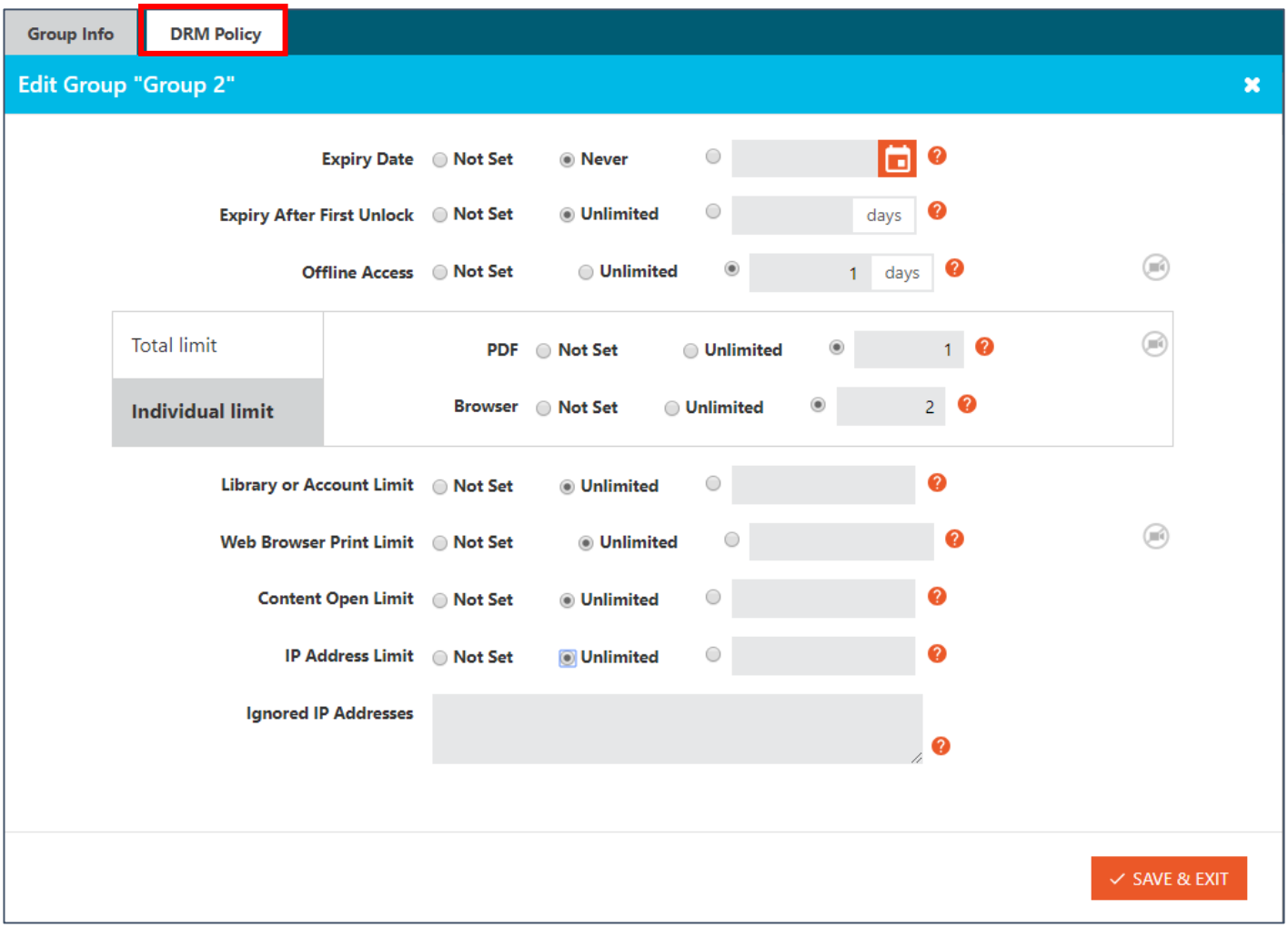


REMEMBER RULE #1: the most lenient DRM policy setting applies so if you have a DRM policy applied at the User or Group level already, be aware of the conflicts.

3.2 At the Group Level

A DRM policy is ideal to set at this level when you can easily group your audience into different user groups and apply different DRM policies for each group.

1. In **GROUPS** tab, click **ADD GROUP**
2. Set all the **DRM POLICY** fields
3. Click **SAVE & EXIT**

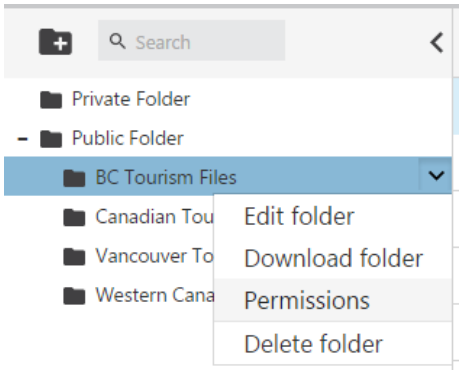


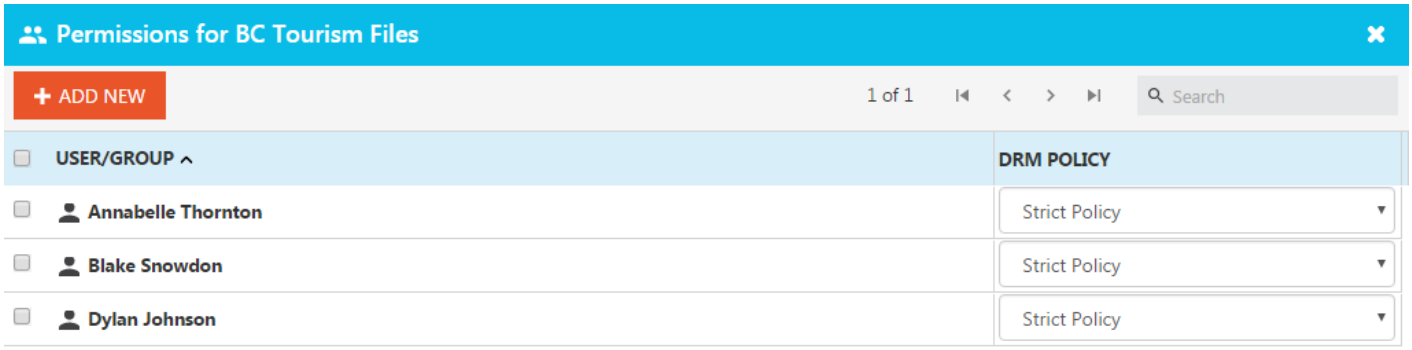
REMEMBER RULE #2: In order for a DRM policy to be effective, every policy field must be set at some level.

3.3 At the Folder Level

A DRM policy is ideal to set at this level when you have a lot of content that you prefer to group into folders and each folder requires a specific DRM policy. You can set the DRM Policy for Groups or Users at this level.

1. In **CONTENT** tab, click the arrow beside a **FOLDER**
2. Select **PERMISSIONS**
3. Add your **USERS** or **GROUPS**, then select a **DRM policy**
4. Click **SAVE & EXIT**



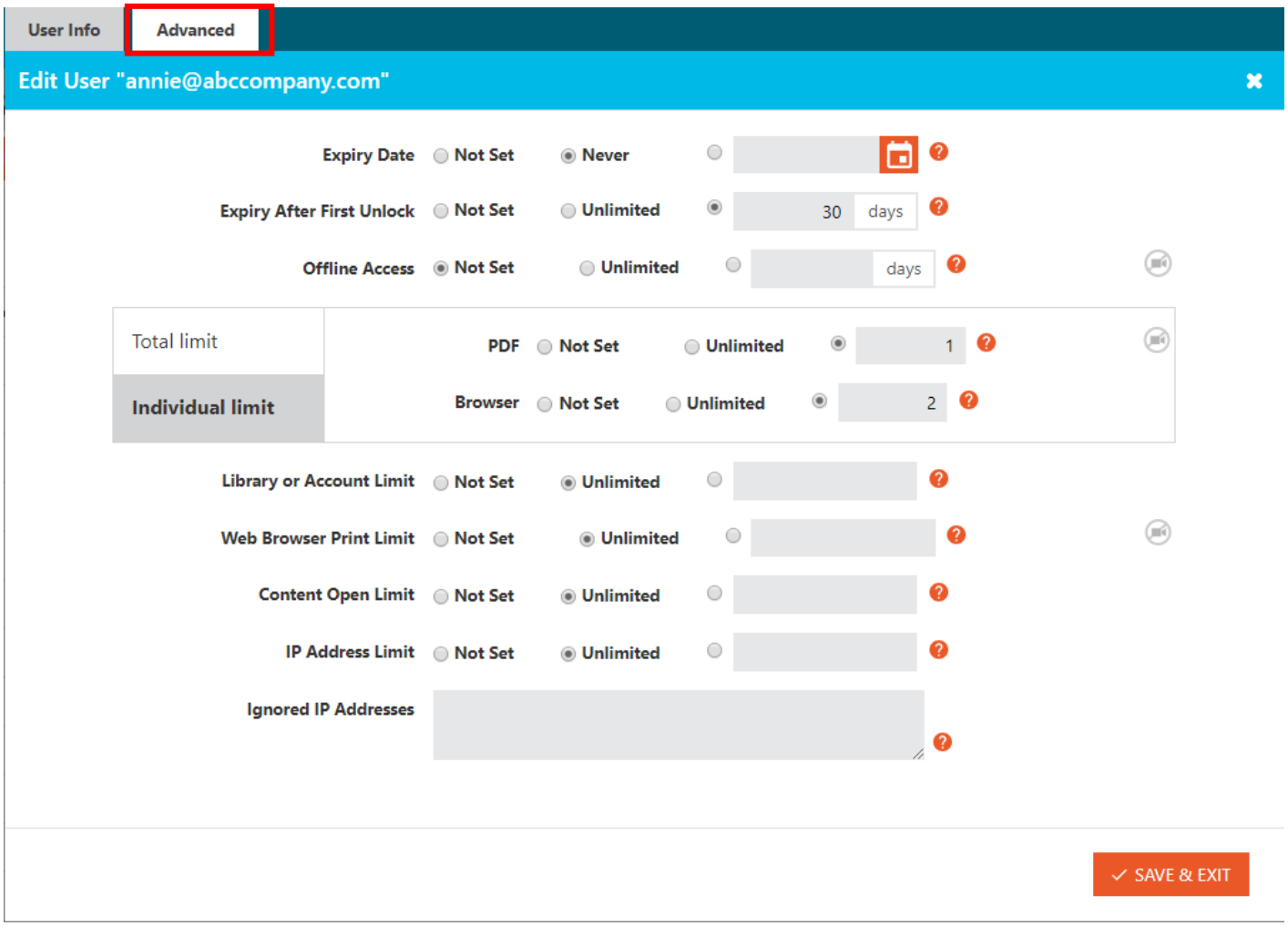


REMEMBER RULE #1: the most lenient DRM policy setting applies so if you already have a DRM policy applied at the User or Group level already, be aware of the conflicts.

3.4 At the User Level

A DRM policy is only recommended to set at this level when you wish to apply different policies for each user. Doing it this way may be a more time-consuming process so it's only recommended when you have a small number of users.

1. In **USERS** tab, click **ADD USER**
2. Set all the **DRM POLICY** fields
3. Click **SAVE & EXIT**

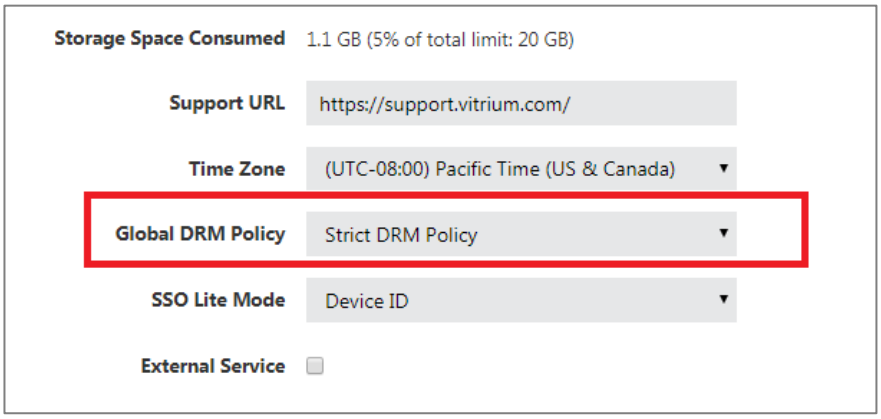


REMEMBER RULE #2: In order for a DRM policy to be effective, every policy field must be set at some level. Do not leave anything to 'Not Set' unless you have a DRM policy applied at other levels.

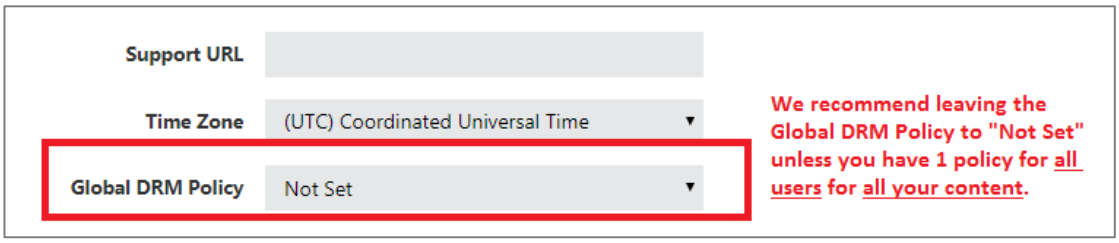
3.4 At the Global Level

We generally DO NOT recommended setting a DRM policy at this level, unless you know you'll only require 1 DRM policy for ALL your users.

1. In **SETTINGS** tab, click **ADD USER**
2. Set all the **DRM POLICY** fields
3. Click **SAVE & EXIT**



If you DO NOT wish to set a Global DRM Policy, select 'Not Set'

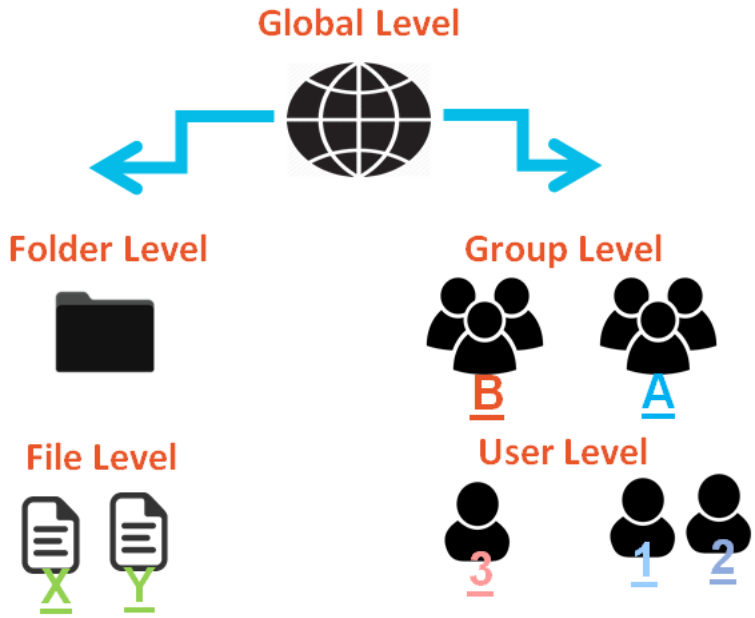


4.0 Setting DRM Policies at Multiple Levels

You may have situations in your business where setting DRM policies at multiple levels makes sense. However, we recommend you map out the policies in a grid as we've suggested below AND you have a clear understanding of the two key rules:

RULE #1: The most lenient DRM policy setting will always apply.
RULE #2: You must enter a value for EVERY field in a DRM policy.

We also encourage you to check out this video to learn more: *Vitrium DRM Policy Video #2: Setting DRM Policies at Multiple Levels.*



		DRM Policy Set	Expiry Date	Expiry After First Unlock	Offline Access	PDF Limit	Browser Limit	Print Limit
Global level		YES	NEVER	30 days	30 day	2	2	1
Folder level		NO						
Group A	Group A	YES	NEVER	15 days	15 days	3	2	2
	User 1	YES	NEVER	UNLIMITED	60 days	4	4	UNLIMTED
	User 2	NO						
Group B	Group B	NO						
	User 3	NO						
User1	Content X	NO						
	Content Y	YES	NEVER	1 day	1 day	1	1	0
User2	Content X	NO						
	Content Y	NO						
User3	Content X	NO						
	Content Y	YES	10/4/2018	20 days	20	2	2	1

SCENARIO 1: The DRM Policy that applies to **User1 for Content X** and **User1 Content Y**:

DRM Policy Applied	Expiry Date	Expiry After First Unlock	Offline Access	PDF Limit	Browser Limit	Print Limit
YES	NEVER	UNLIMITED	60 days	4	4	UNLIMITED

For User 1 content Y, because you've applied a DRM Policy at the User, Group and Global levels already, there's no need to apply the DRM Policy at the content level. Per rule #1 the most lenient DRM Policy will be applied.

SCENARIO 2: The DRM Policy that applies to **User2 for Content X** and **Content Y**:

DRM Policy Applied	Expiry Date	Expiry After First Unlock	Offline Access	PDF Limit	Browser Limit	Print Limit
YES	NEVER	30 days	30 days	3	2	2

For User2 Content X and Y, the 'Expiry after First Unlock' and 'Offline Access' fields at the Group level will never apply since the Global level values are higher and more lenient, per rule #1.

SCENARIO 3: The DRM Policy that applies to **User3 for Content X:**

DRM Policy Applied	Expiry Date	Expiry After First Unlock	Offline Access	PDF Limit	Browser Limit	Print Limit
YES	NEVER	30 days	30 days	2	2	1

The DRM Policy at the Global level will apply since there are no DRM Policy settings set at other levels for this user.

SCENARIO 4: The DRM Policy that applies to **User3 for Content Y:**

DRM Policy Applied	Expiry Date	Expiry After First Unlock	Offline Access	PDF Limit	Browser Limit	Print Limit
YES	NEVER	30 days	30 days	2	2	1

In this case, the Global DRM Policy will apply since it has the most lenient or similar values and there is no need to apply another DRM Policy at the content level for this user.

This is a more complex example but it reinforces the need for customers to really plan out how you will set your DRM policies in Vitrium. If you need further guidance from the Vitrium team, please contact the support team today: support@vitrium.com.