VITRIUM ACTIVITY CODE GUIDE

Code	Description	Suggested Action
2fa	**Two Factor Authentication** Indicates that two factor authentication email with a verification code was sent to the end user.	**No action required.** This code simply notes that the end user should have received an email with a verification code to use in two factor authentication during login.
2ma	**Multiple Cached Users** Automatic login to a protected PDF failed due to multiple users cached in Adobe on this device.	**Access protected PDF content by manually logging in.** To re-enable automatic login (SSO lite), the user will need to clear Adobe cache. The user will then have to log in manually once, after which their username will be cached on the device and used automatically for subsequent logins.
2p3	**Inactive Document** The user is trying to unlock a file that has been deactivated in Vitrium. It will show an 'X' beside the content in the Content tab.	**No action required.** This means Vitrium's DRM is working as someone deactivated this content for a reason. If, however, that content should be reactivated, then go to the Content tab in Vitrium and click the 'X' beside the content in question to reactivate it.
3yq	**Account Not Found** The user does not exist in Vitrium, or an invalid username was entered. *Note: end users will see 3yq/bw5 error, but the Activity Log will show the specific code.*	Check to see if this user exists in Vitrium or in the system that Vitrium is integrated with (if you connect to a 3rd party system). If the user does exist, ensure they are using the correct username and that the user record is active. If they do not exist, you may need to add the user manually in Vitrium or in your other system.

Code	Description	Suggested Action
4k3	**Incorrect Permission** This occurs when there is no expiry date set or when a Group has not been assigned permission to the content.	**There are 2 ways to fix this issue:** 1. Make sure at least 1 of the 2 expiry fields in your DRM Policy has been set. If Vitrium is integrated with another system, ask your developer to review code. 2. Make sure the user has been correctly assigned to the Group if you've assigned permissions to the Group, or re-assign permissions for the user.
7ud	**Too Many Login Attempts** The user has failed to enter the correct password X number of times according to what is set in the Security Settings.	**No action required unless you do NOT suspect fraud or misuse.** This means Vitrium's password control feature is working. If you do NOT suspect fraud or malicious use, then you can reactivate the user. Go to the Users tab in Vitrium and click the 'X' beside the user in question to reactivate them.
ar1	**Access Revoked** The user no longer has access to the content.	**There are 2 situations where this error message might occur:** 1. Access was revoked while a user had web viewer content open on their screen or browser. 2. Another concurrent user opened a web viewer content which had exceeded the limit so the original user could no longer access the content.
bw5	**Incorrect Credentials** The user has mistyped their password or other login credentials. *Note: end users will see 3yq/bw5 error, but the Activity Log will show the specific code.*	**No action required unless the user calls or emails you.** Make sure the user is entering their correct password and there are no typos, extra spaces, or 'Caps Lock' key is on. If you have enabled the "Forgot Password" functionality, the user can always click on that to reset their password.
dovc3	**Exceeded Open Limit** The user has exceeded the number of times they are allowed to open a content as established in the DRM policy.	**No action required unless you do NOT suspect fraud or misuse.** This means Vitrium's DRM is working as the user has exceeded the number of times they are allowed to open a content. If you do NOT suspect fraud or misuse and the user needs to access the content again, you can reset their usage. ***How to Clear Use***

Code	Description	Suggested Action
dpvc3	**Exceeded Print Limit** The user has exceeded the number of times they are allowed to print according to the DRM policy.	**No action required unless you do NOT suspect fraud or misuse.** This means Vitrium's DRM is working as the user has exceeded the number of times they are allowed to print the content according to the DRM policy assigned. If you do NOT suspect fraud or misuse, you can clear their print use and reset their limits. ***How to Clear Use***
dpvc3	**Exceeded Print Limit** The user has exceeded the number of times they are allowed to print according to the DRM policy.	**No action required unless you do NOT suspect fraud or misuse.** This means Vitrium's DRM is working as the user has exceeded the number of times they are allowed to print the content according to the DRM policy assigned. If you do NOT suspect fraud or misuse, you can clear their print use and reset their limits. ***How to Clear Use***
dvc3	**Exceeded Content Limit** The user has exceeded the number of content files they can open according to the DRM policy.	**No action required unless you do NOT suspect fraud or misuse.** This means Vitrium's DRM is working as the user has exceeded the number of content they are allowed to open according to the DRM policy setting "Library or Account Limit". If you do NOT suspect fraud or misuse, you can reset their usage. ***How to Clear Use***
e2fa	**2FA Email Failed to Send** The two-factor authentication (2FA) email failed to send to user.	**Verify user's email address is valid.** This error occurs because the two-factor authentication (2FA) email with the verification code failed to send to the user. Check that the user has a valid email address and have them try logging in again. Remind them to check their junk or spam folder if they can't find the email.
f2fa	**2FA Verification Code Incorrect** The user entered an incorrect verification code for two-factor authentication (2FA).	**Ask user to check & re-enter the verification code.** This error occurs because the user entered the verification code incorrectly for the two-factor authentication (2FA) process. Ask them to check the code and re-enter it again.

Code	Description	Suggested Action
fa2fa	**2FA Attempts Exceeded** The user entered too many incorrect verification codes for two-factor authentication (2FA).	**Ask user to login again to generate a new 2FA verification code.** This error occurs because the user entered an incorrect verification code 3 times. The user will need to go through the login process again to generate a new verification code. Ask them to click on the verification code in their email and remind them to check their junk or spam folder if they can't find the email.
fdp	**No Permission to Download Content** The user no longer has permission to download protected PDF from web viewer.	**No action is required unless…**your DRM Policy Setting previously had "Allow Protected PDF Download" checked while the user had the web viewer content open, but then it was subsequently revoked. This left the download menu option visible in the browser, but the underlying permission no longer exists. If the user should have the ability to download the protected PDF from within the web viewer, then you'll need to ensure that there is a new DRM policy assigned to this user with the field "Allow Protected PDF Download" checked.
fe2fa	**2FA Verification Code Expired** The two-factor authentication (2FA) verification code has expired.	**Ask user to login again to generate a new 2FA verification code.** This error occurs because the two-factor authentication (2FA) verification code expired. The user will need to go through the login process again to generate a new verification code. Ask them to click on the verification code in their email and remind them to check their junk or spam folder if they can't find the email.
g45	**User Not Found** This occurs when the user does not exist or has been deleted.	**No action required unless**…if you wish to provide this user with access to your content, you will need to add them as a new user in the Users tab of Vitrium or in the other system that Vitrium is integrated with.
g55	**File Has Been Deleted** The file has been deleted and moved to the Recycle Bin.	**No action required unless…** the file has been deleted by accident. Restore the file to the relevant folder in the Content tab of your Admin to regain access.

Code	Description	Suggested Action
gf4	**DocCode Does Not Match in System** This occurs when the metadata in the Version\Unique Protected PDF does not match the data in your 3rd party system.	**Review info in your other system.** This error occurs when the unique document ID is found by ID, but the DocCode in the protected PDF does not match the one in the 3rd party system that's integrated with Vitrium. The PDF is permanently locked and cannot be repaired. Contact Vitrium Support if you require assistance.
gf5	**DocID Does Not Match in System** This occurs when the document ID in the Version\Unique protected PDF does not exist in the 3rd party system.	**Review info in your other system.** This error occurs when the document ID from the Version\Unique protected PDF does not exist in the 3rd party system that's integrated with Vitrium, likely because the DELETE function for the API was exercised. This locks the PDF unless you regenerate the original Version\Unique ID with another POST Version\Unique API call.
ipvc3	**IP Address Not Covered** The user has exceeded the IP address limit you have set in the DRM policy, or they are accessing the content outside of the allowed IP addresses.	**No action required unless you do NOT suspect fraud or misuse.** This means Vitrium's DRM is working as the user has exceeded the number of IP addresses that they are allowed to access the content from, or they are trying to access the content from an IP address that is not allowed. If you do NOT suspect fraud or misuse and you are authorized to do so, you may clear their IP address. ***How to Clear Use***
m47	**Inactive User Account** The user has been deactivated in Vitrium, either for a specific reason or by accident.	**No action required unless circumstances change.** This means Vitrium's DRM is working as someone deactivated this user for a reason. If circumstances have changed and you wish to reactivate that user, you can do this. Go to the Users tab in Vitrium and click the 'X' beside the user in question so a checkmark ✓appears.
m48	**Inactive Group Subscription** The group has been deactivated in Vitrium, either for a specific reason or by accident.	**No action required unless circumstances change.** This means Vitrium's DRM is working as someone deactivated this group subscription for a reason. If circumstances have changed and you wish to reactivate that group, you can do this. Go to the Group tab in Vitrium and click the subscription start or end date beside the group in question so the subscription start date is set to a time before the current time and the subscription end date is set to a future date.

Code	Description	Suggested Action
n4p	**No DRM Policy** This occurs when there has been no DRM policy assigned to this user or group if they are part of a Group.	**Update the permissions.** This means that a DRM policy has not been correctly applied to the user in question in the permissions, at any level (content, folder, user, or group). Check that there is a DRM policy assigned to this user where you assigned them permissions to the content. If you have Vitrium integrated with another system, you need to check with the developer who did the integration.
ps1	**Screen Print Attempt** The user has attempted to take a screen print of your content with a keyboard shortcut key such as Print Screen.	**No action required unless**...this occurs repeatedly for the same user. This event code is only tracked for the purpose of providing you insight about which users are attempting to take screen prints of your content. The event is triggered by a user pressing popular keyboard shortcut keys (Print Screen, ALT+Print Screen, etc.). It may be a sign of potential fraud or misuse, but it is completely up to you if you wish to take any action. *Note: the user may not be aware this is being logged.*
qe2	**Access Expired (Expiry Date)** The user's access to the content has expired according to the Expiry Date that was set in the DRM policy.	**No action required unless** … there was an error, or you wish to extend the date. This means Vitrium's DRM is working as the user's access has expired according to the "Expiry Date" setting in the DRM policy that has been assigned to that user. If this was an error (wrong date) or the user needs an extension to access their content, you can change the setting in your DRM policy but realize this will change it for everyone who has been assigned that policy. Alternatively, you could assign a different DRM policy to that user with an extended Expiry Date.
qw1	**User Subscription Expired** The user is trying to access their account outside of their subscription start and subscription end dates.	**No action required** … unless there was an error, or you wish to change the subscription dates for your user. This means that the Vitrium system is successfully blocking your user's access to content if their account is outside of their subscription start and end dates. You user may be in a group where their group subscription has ended or hasn't started yet. You can grant your user access by changing their subscription start and end dates, either at the user's level or at the group level that the user is in.

Code	Description	Suggested Action
rc7	**Country Restricted** The user is trying to access content from a country that is being blocked by the DRM setting "Location Restrictions".	**No action required unless there was an error.** This means Vitrium's DRM is working as the user is located in a country that has been restricted access to that content, according to the "Location Restrictions" setting in the DRM policy. The country location is set by the user's IP address. If the country was set incorrectly in Vitrium or you wish to allow that country access, you can go to that DRM policy in the Settings tab of Vitrium to update this setting.
rc8	**Country Not Permitted** The user is trying to access content from a country that is not permitted by the DRM setting "Location Permits".	**No action required unless there was an error.** This means Vitrium's DRM is working as the user is located outside of a country that has been permitted to access this content, according to the "Location Permits" setting in the DRM policy. The 'permitted' country location is set by the user's IP address. If the permitted country was set incorrectly in Vitrium or you wish to allow that country access, you can go to that DRM policy in the Settings tab of Vitrium to update this setting.
rc9	**Unexpected Error** This appears when a server time-out occurs.	**Hosted customers: contact the Vitrium support team right away.** The Vitrium team will likely know about this already as we have a 24-hour monitoring and alerting system in place, but it's still a good idea to contact us. **Installed customers: contact your IT department right away.** Your team may already know about this issue if they have 24-hour monitoring on their servers but it's always good to contact them anyway.
rqe2	**Access Expired** **(Expiry After First Unlock)** The number of days has passed after the user's first unlock session	**No action required unless there was an error or you wish to extend the time.** This means Vitrium's DRM is working as the user's access has expired according to the "Expiry After First Unlock" setting in the DRM policy that has been assigned to that user. If this was an error or the user needs an extension or the timeframe, you can update the "Expiry After First Unlock" field in the associated DRM policy.

Code	Description	Suggested Action
vc3	**Exceeded Device Limit** The user has exceeded the device limit that is set in the associated DRM policy.	**No action required unless you do NOT suspect fraud or misuse.** This means Vitrium's DRM is working as the user has exceeded the number of devices according to the "Device Limit" setting in the DRM policy that has been assigned to them. If you do NOT suspect fraud or misuse and you are authorized to do so, you may clear their usage (***How to Clear Use***) or increase the device limit in your DRM Policy Settings. *Note: changing this limit will also change it for all other users who have been assigned this DRM policy.*
ve2	**User Must Complete Email Verification** Self-registered user tries to log into portal *before* clicking on the verification link	**No action required, as the user is prompted to check their email.** However, if the user reaches out, you can redirect them to check their spam/junk folders, or toggle their account to active manually by finding them in the USERS section of your admin, and clicking the icon in the **Active** column so that it shows a check mark.
vf3	**Exceeded Concurrent Users Limit** The user has exceeded the concurrent users limit that is set in the associated DRM policy.	**No action required unless you do NOT suspect fraud or misuse.** This means Vitrium's DRM is working as the user has exceeded the number of concurrent users' they have logged in for that content according to the "Concurrent Users Limit" setting in the DRM policy that has been assigned to them. The user can log out of the content from their other device or wait for the other user to log out. In special circumstances when you don't suspect fraud or password sharing, you could also clear the user's usage to reset the limit. ***How to Clear Use***
vp3	**Exceeded Print Limit** The user has exceeded the print limit that is set in the "Download to Print" field in the associated DRM policy.	**No action required unless you do NOT suspect fraud or misuse.** This means Vitrium's DRM is working as the user has exceeded the number of times they are allowed to print the content according to the "Download to Print" setting in the DRM policy that has been assigned to them. If you do NOT suspect fraud or misuse and you are authorized to do so, you may clear their usage. ***How to Clear Use***

Code	Description	Suggested Action
w29	**No Permission** The user does not have permission to the content or has not been set up correctly in Vitrium or the system it is integrated with.	**Review info in Vitrium or your other system.** Check to make sure the user has been assigned permission (with a DRM policy) to access the content in question. Whether you manage users in Vitrium or another system that is integrated with Vitrium, check that permissions are set up and there is a DRM policy assigned. In some cases, you may need to ask the developer to check the integration code.