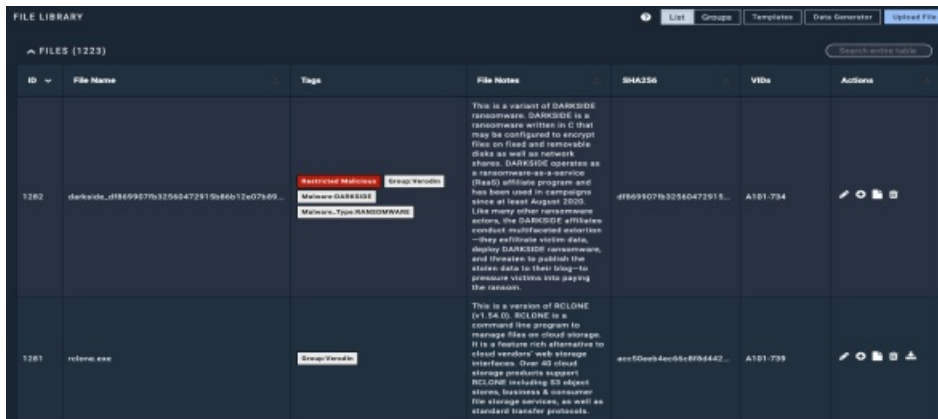


MANAGING FILES IN THE FILE LIBRARY

Viewing Files in the File Library

To view the files already in the file library, go to **Library > Files**. A list of the available files is displayed, as shown below. Note the following information about the file listing:

- If a file is approved and restricted as malicious, you see the **Restricted Malicious** tag.
- If you are an approver, you see a **Pending Approval** tag for files that have not yet been approved for use in Actions.
- User Tags are also shown in the Tags column of the file library listing, when configured. Notice that two different group tags are visible.



ID	File Name	Tags	File Notes	SHA256	VIDs	Actions
1262	darkside_d18699879b32565472819a86a12a079d9	Restricted Malicious Group: Vendor Malware: DARKSIDE Malware_Type: RANSOMWARE	This is a variant of DARKSIDE ransomware. DARKSIDE is a ransomware written in C that may be configured to encrypt files on fixed and removable disks as well as network shares. DARKSIDE operates as a ransomware-as-a-service (RaaS) software program and has been used in campaigns since at least August 2020. Like many other ransomware actors, the DARKSIDE affiliates conduct multifaceted operations—they exfiltrate victim data, deploy DARKSIDE ransomware, and threaten to publish the stolen data to their blog—to ensure victims are paying the ransom.	d18699879b32565472819a86a12a079d9	A101-734	[Actions]
1261	rdform.exe	Group: Vendor	This is a version of RCLONE (v1.54.0). RCLONE is a command line program to manage files on cloud storage. It is a feature rich alternative to cloud vendors' web storage interfaces. Over 40 cloud storage providers support RCLONE including S3 object storage, business & consumer file storage services, as well as standard transfer protocols.	acc10eb4ac06a8f854442...	A101-739	[Actions]

File Library listing

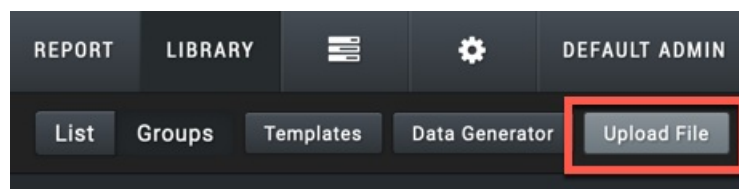
Adding Files to the File Library

You can easily add files to the file library.


 All files that are added must be approved before they can be used in an Action.

To upload a file to the file library

1. Go to **Library > Files**.
2. Click **Upload File**.



Upload File

 File size is limited to 300 MB by default. You can update it by going to **Settings > Director Settings**, and then clicking **Advanced**. See **Advanced Settings** (<https://docs.mandiant.com/home/msv-advanced-settings>) for more information.

3. Enter the following information for the new file:

- **File Restrictions:** Select an option:

Request None indicates to the approver that this file contains no malicious code and does not need to be restricted.

Restrict as Malicious indicates that this file is a known malicious file (for example, malware). This file should be restricted to Protected Theater, Email Theater, or Malicious File Transfer Actions.



You cannot download files marked as malicious, and Host CLI Actions created from these files can only run in Protected Theater. Files will appear with a **Pending Approval** tag in the list until they are approved.

- **File Notes:** Enter notes about the file that can be helpful to the approver or to other potential users of the file.
- **User Tags:** Select or create new tags to indicate information about this file. Prepend *Group:* to the tag, to use the Groups view in the file library (see [Grouping Files in the File Library \(\)](#)).
- **File Info Type:** (Optional) Select a checkbox to indicate if this file is related to Personally Identifiable Information (PII) or Payment Card Industry (PCI), or if it's proprietary.
- **Applicable OS/Platform:** Select a specific platform to which this file applies, or select **General-OS/Platform**.
- **Select File:** Browse for and choose the file you want to upload.
- **Zip File:** (Optional) If you're uploading a file that has been compressed, choose the Zip file checkbox. The Validation Platform currently supports .zip, .zipx, and .gz formats. The compressed file cannot be in a folder.



If you need to compress a file from a Mac, we suggest using command-line tools to do so. When using the internal OS archiving tools from the GUI, many versions of macOS automatically adds a hidden directory. This directory prevents you from uploading the file.

- **Zip Password:** Enter a password for the zip archive, if applicable.
Supported Encryption levels are: 256-bit AES, 128-bit AES, and zip2.0 (legacy).

4. Click **Upload File**.

The file is uploaded and appears in the table in a **Pending Approval** state. If the file was compressed and you selected the **Zip File** checkbox, the file is decompressed.

Approving Files for Use in the File Library

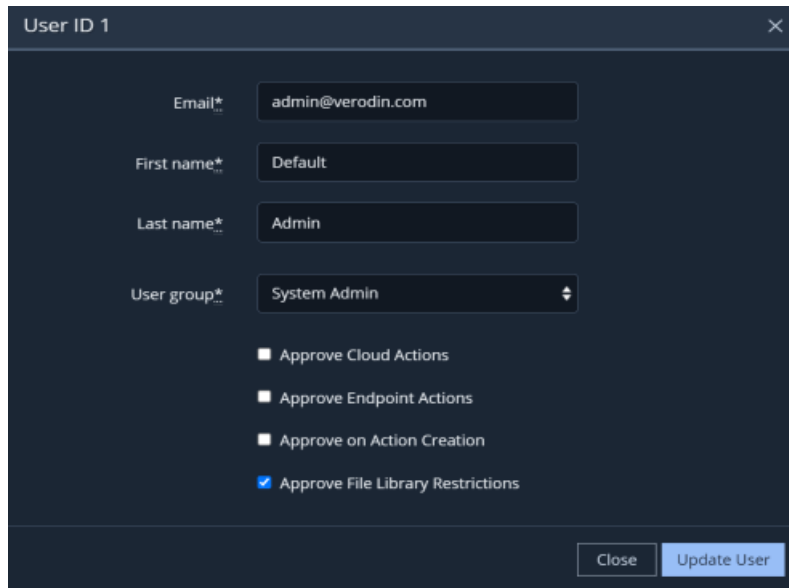
Once a file has been uploaded to the File Library, if it was set to **Restrict as Malicious**, it will appear in the file list with the red tag **Restricted Malicious**. If the file was set to **Request None**, the file appears with a purple tag **Pending Approval**.

File Approval Restrictions

Users who are permitted to approve files that have been uploaded to or edited in the File Library must have the **Approve File Library Restrictions** flag enabled on their user account, as shown in the screenshot below. Users who do not have this flag enabled can see the files they uploaded or edited but do not see the option to approve the file. If you do not have approval permissions and you should, contact your platform admin.



NOTE: You cannot use an uploaded file if the **Pending Approval** flag is set.



User ID 1

Email* admin@verodin.com

First name* Default

Last name* Admin

User group* System Admin

- Approve Cloud Actions
- Approve Endpoint Actions
- Approve on Action Creation
- Approve File Library Restrictions

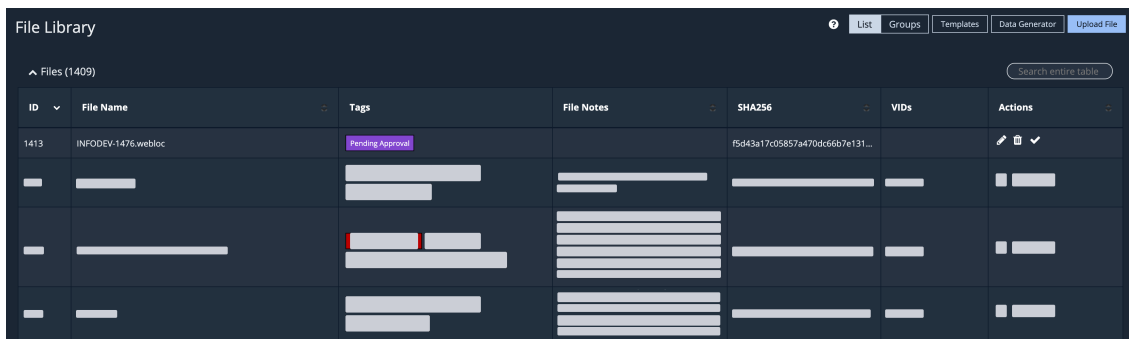
Close Update User

File Approval Permission

File Approval Process




TO APPROVE A FILE THAT IS PENDING APPROVAL

1. Go to **Library > File Library**.
2. Locate the file you want to approve. You can enter all or part of the string "pending_approval" in the search bar to narrow your results.



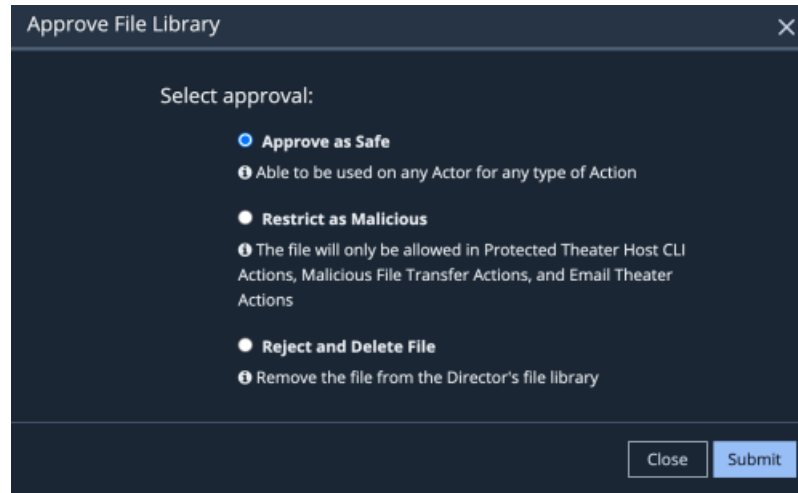
File Library

Files (1409)

ID	File Name	Tags	File Notes	SHA256	VIDs	Actions
1413	INFODEV-1476.webloc	Pending Approval		f5d43a17c05857a470dc66b7e131...		  

File pending approval

3. Click **Approve File**  next to the file you want to approve and you'll see the following:




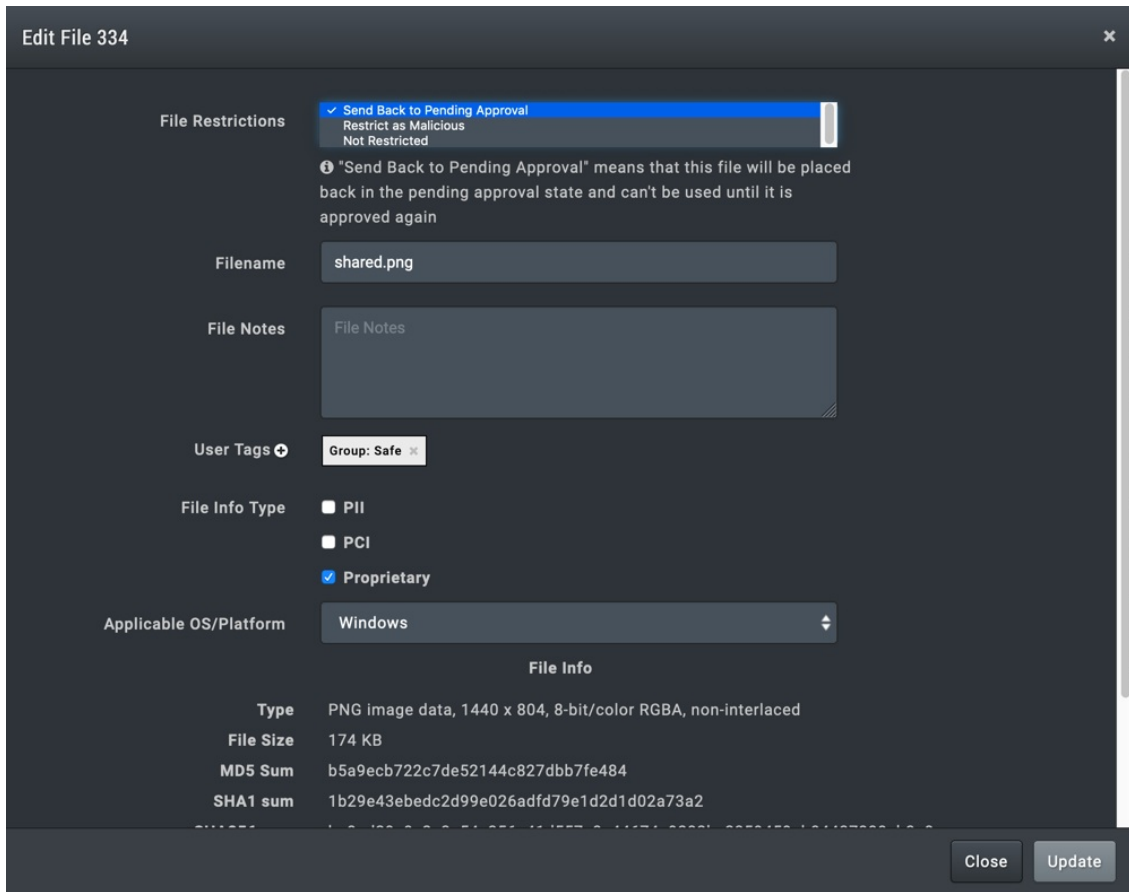
Approve a file

4. Select an approval status for the file.
5. Click **Submit**.

TO EDIT A FILE BEFORE APPROVING

In some cases, if you are the approver, you may want to make changes to a file before sending for approval or before approving its use. You can also use this procedure at any point in the lifecycle of a file in the File Library.

1. Go to **Library > File Library**.
2. Locate the file you want to approve.
3. Click **Edit File** () next to the file in the list and you'll see the Edit form as shown below:



File Restrictions

- Send Back to Pending Approval
- Restrict as Malicious
- Not Restricted

Info "Send Back to Pending Approval" means that this file will be placed back in the pending approval state and can't be used until it is approved again

Filename: shared.png

File Notes

User Tags: Group: Safe

File Info Type

- PII
- PCI
- Proprietary

Applicable OS/Platform: Windows

File Info

Type	PNG image data, 1440 x 804, 8-bit/color RGBA, non-interlaced
File Size	174 KB
MD5 Sum	b5a9ecb722c7de52144c827dbb7fe484
SHA1 sum	1b29e43ebcdc2d99e026adfd79e1d2d1d02a73a2

Close Update

Sending an edited file back for approval

4. Select the appropriate File Restrictions option, if necessary.











NOTE: When editing a file that was previously approved, you see an additional File Restriction choice of "Send Back to Pending Approval," which triggers another **Pending Approval** status on the file.

5. Click **Update**.

File Rejection Tracking

When you reject a file that is pending approval, or when you delete a file from the File Library, the platform logs information about the transaction in the rejection log. You can access the rejection logs by clicking **View Rejection Logs** at the bottom of the File Library page, as shown below.

1234	testService.service	Group:Verodin	Test service definition to simulate an attacker gaining persistence in a system	a2cd530daa8b644...	A104-723	   
1233	sshpas	Group:Verodin	sshpas is a simple and lightweight command line tool that enables a user to provide password (non-interactive password authentication) to the command prompt itself, so that automated shell scripts can be executed to take backups via cron scheduler	368ac24547c9c3d...	A104-728, A104-727	   

⏪ 1 to 50 of 1223 rows ⏩ Rows Per Page: 50

[View Rejection Logs](#)

Viewing Rejection Logs

The file rejection log tracks the following information:

- Timestamp of the file rejection (UTC)
- Username of the account that rejected the file
- The Message digest containing:
 - Filename
 - SHA256 hash
 - Username of the account that uploaded the file
 - Username of the account that rejected the file

Grouping Files in the File Library

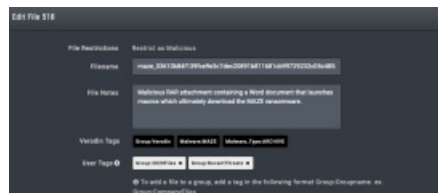
You can group files in the File Library based on file type, network segment, or any other category that is useful to you. Grouping is simply a way to catalog the files in your file library.

Adding a Group Tag to a File

A group tag is simply a User Tag with "Group:" prepended to the group name.

There are two methods for adding a group tag to a file:

- Add a file to the file library using the procedure found in [Adding Files to the File Library](https://docs.mandiant.com/home/managing-files-in-the-file-library#adding-files-anchor) (<https://docs.mandiant.com/home/managing-files-in-the-file-library#adding-files-anchor>). Set the User Tag with a group tag.
- Edit a file that is already in the file library and add a group tag.

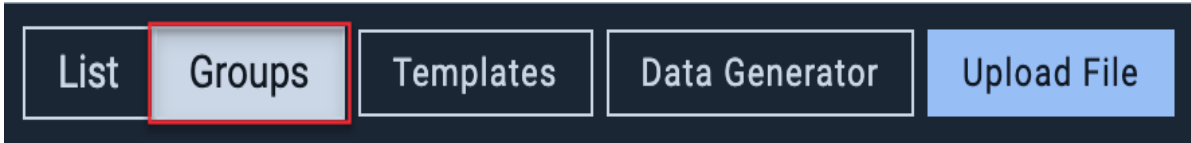


(<https://dyzz9obi78pm5.cloudfront.net/app/image/id/629cec32e07dc756be50aa02/n/file-add-group-tags.png>)

Adding group tags to an existing file in the file library

Viewing File Groups

To view file groups in the file library, click **Groups**.

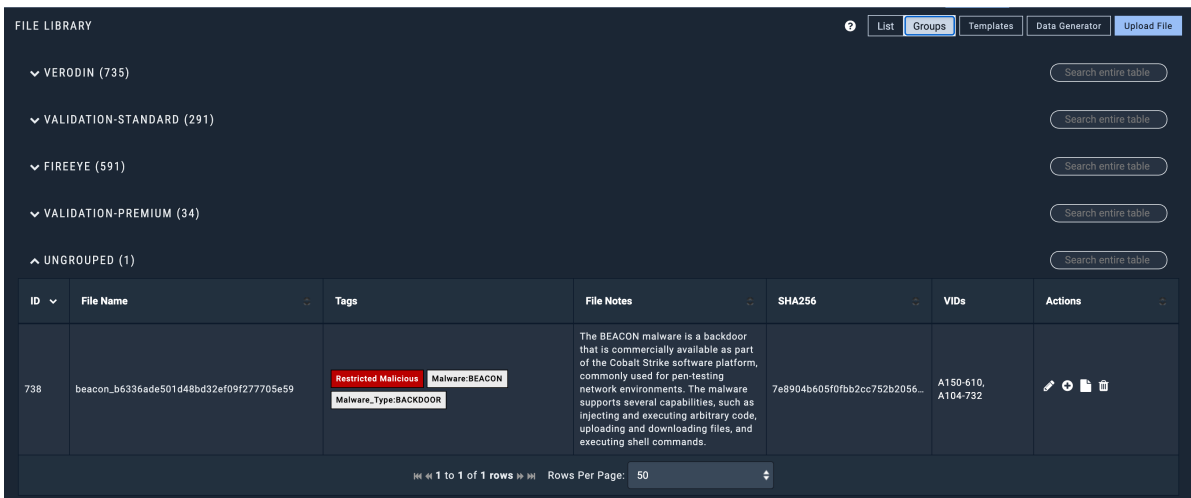


(<https://dyzz9obi78pm5.cloudfront.net/app/image/id/629cec32e07dc756be50a9f9/n/view-groups.png>)

Viewing File Groups

The file groups are shown as in the example screenshot below. Files that do not have a group tag are in the "Ungrouped" category.

Each file group has its own search bar, so you can search for a given file within the group, narrowing the results.






FILE LIBRARY

Navigation: List Groups Templates Data Generator Upload File

Groups:

- VERODIN (735) Search entire table
- VALIDATION-STANDARD (291) Search entire table
- FIREEYE (591) Search entire table
- VALIDATION-PREMIUM (34) Search entire table
- UNGROUPED (1) Search entire table

ID	File Name	Tags	File Notes	SHA256	VIDs	Actions
738	beacon_b6336ade501d48bd32ef09f277705e59	Restricted Malicious Malware-BEACON Malware_Type:BACKDOOR	The BEACON malware is a backdoor that is commercially available as part of the Cobalt Strike software platform, commonly used for pen-testing network environments. The malware supports several capabilities, such as injecting and executing arbitrary code, uploading and downloading files, and executing shell commands.	7e8904b605f0bb2cc752b2056...	A150-610, A104-732	  

1 to 1 rows Rows Per Page: 50

Group view of File Library



NOTE: A file can appear in more than one group. For example, if you have a file `xyz.zip`, and you label that file as Group: A and Group: B, the file will appear in both the Group A and Group B groups.