



KAPALYA Inc.

1200 Queen Emma Street  
Honolulu, HI 96813

Phone: 415 823 5440

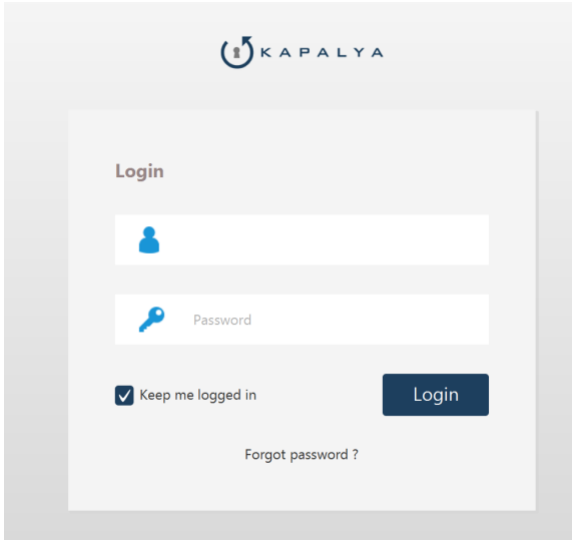
E-Mail: Sudesh@kapalya.com

# KAPALYA File System (KFS)

User Guide version 1.0

October 2017

## Login Process

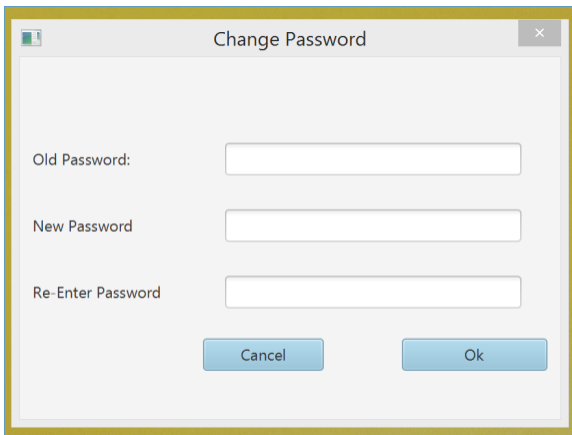


Users must login to the KFS application before they can start using the application.

To do so, simply enter your userid and password that was e-mailed to you by your administrator. Please note that userid and passwords are case sensitive.

You have the option of remembering your credentials by checking on the “Keep me logged in” box. If you donot check this box, then you will be prompted to enter your userid and password every time you use the application.

If you have forgotten your password, then you can recover your password by clicking on the “Forgot Password?” link You will be prompted to enter your e-mail address and instructions to recover your password will be e-mailed.



Upon successful login for the first time, you will be prompted to change your password.

You have to change your password before the application will launch. This is a security measure to ensure that no other persons or administrators know your password.

If you donot change your password, then the application will not launch.

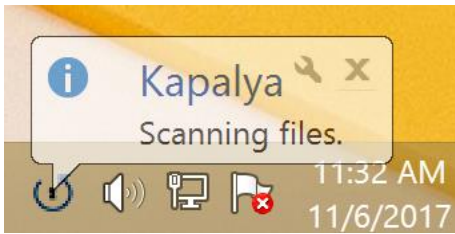
After successfully changing your password, you will be logged into the KFS application to ready to use it.



By clicking on the information icon at the to right hand corner will show you the version of KFS

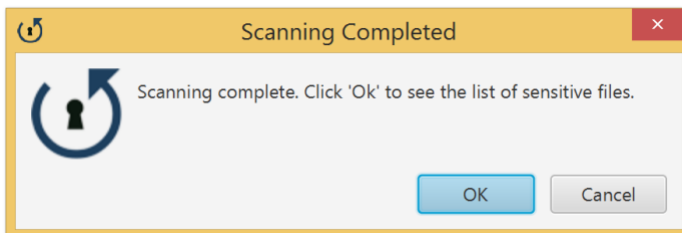
By clicking in the down arrow next to your userid name will allow you to “change your password; logout of KFS or exit the application. If you minimize the application or logout, the application will still be running and will appear in the system tray at the bottom right hand corner of your screen.

## Scanning Process



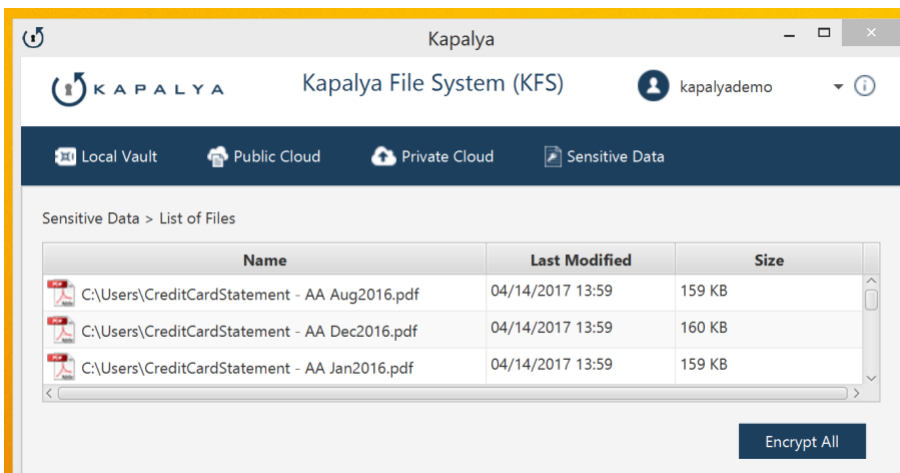
The first thing that happens automatically, will be a scan of your user directory on your computer. This automatic scan checks all your data files for sensitive information, specifically: Social Security #; Credit Card #; Drivers License # and State ID #.

A balloon at the bottom right corner of your screen will inform you that scanning is taking place.



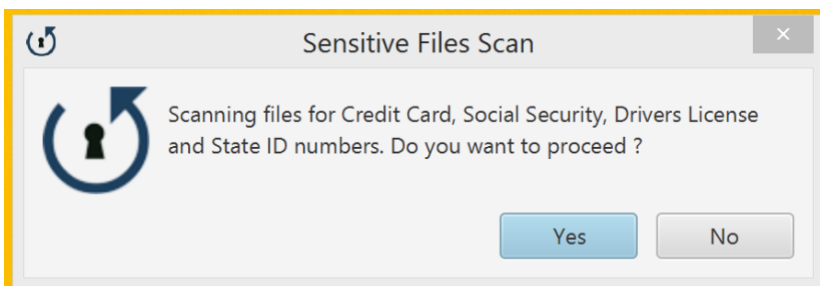
Once the scanning of sensitive information is completed, a dialog box will appear informing you that the scan is complete and ask you to view the list of files containing sensitive data.

Click “ok” to see a list of files containing sensitive data.



If your computer does not have any files containing sensitive data, then this list will not show any files. However, if any files containing sensitive data was discovered during the scan, then, all these files will be listed.

Please note, that some of these could potentially be false positives, meaning, they may contain a string of 9 digits looking like a SSN, but may be some other number.



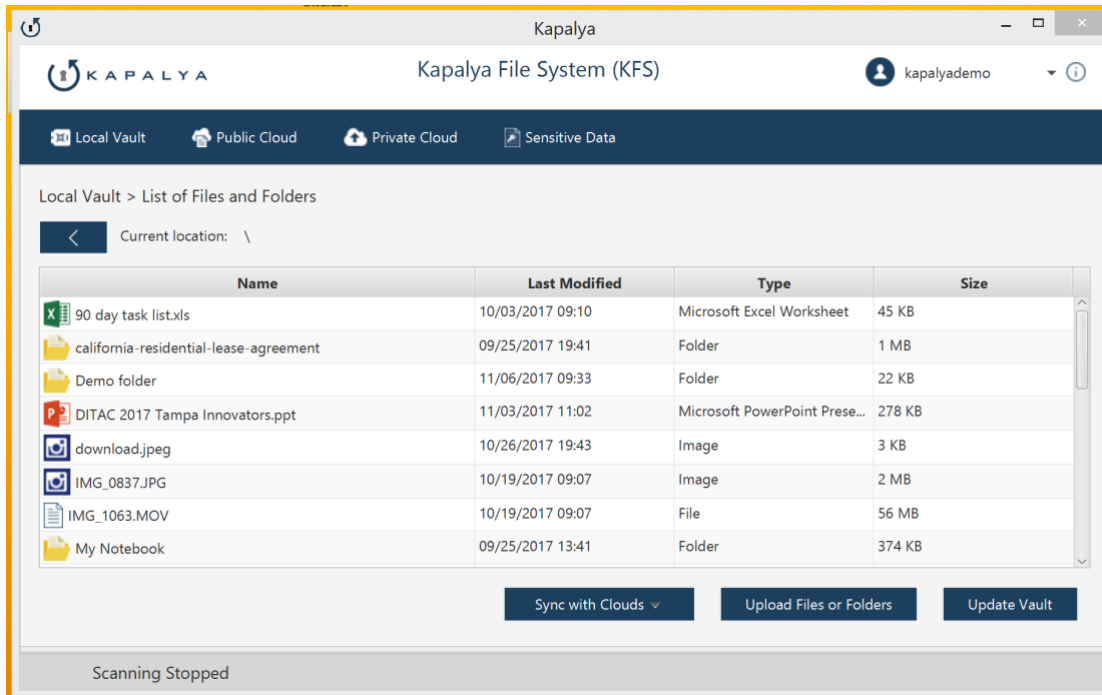
After you get a list of files, by right-clicking on the file to “open” the file you have the option to “open” the file, “encrypt” the file or “delete” the file. You can also select multiple files to encrypt or, you can encrypt all the files by clicking on the “encrypt all” button on the lower right hand corner.

You can run a scan on-demand anytime by clicking on the “sensitive data” from the top menu and clicking on “scan for sensitive data”. The application will prompt you that it will scan your computer for SSN, CC, DL and StateID numbers and you will be prompted to select the folder that you wish to scan.

## Encryption Process

Using KFS, data files and folders are encrypted at three locations: - local computer, public cloud (Amazon S3) and private cloud. The process of encrypting data files and folders at any of these locations is identical - you simply drag and drop the files or folders that you wish to encrypt to any of these locations and they will be encrypted and stored.

### LOCAL VAULT:



To protect files and folders on local computers, KFS creates a secure vault on each computer.

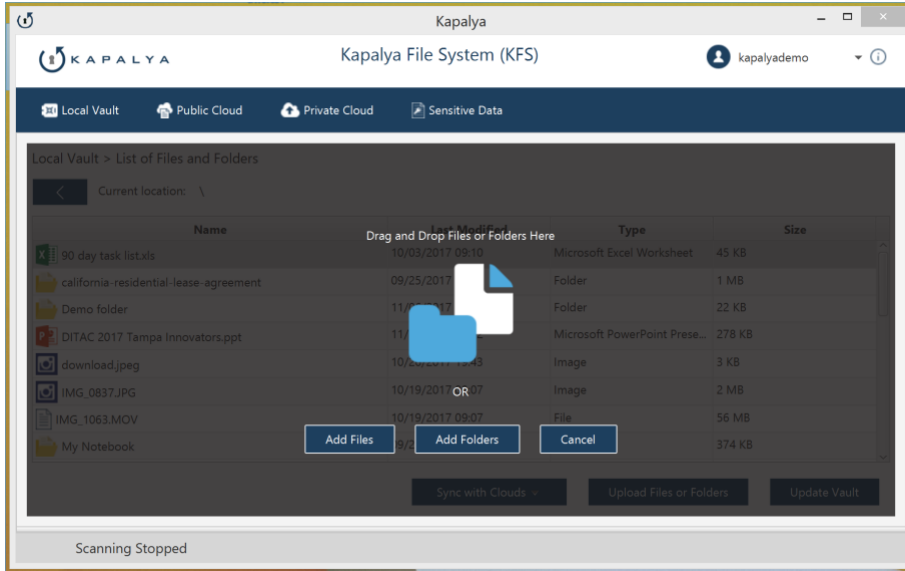
Whenever any file or folder needs to be encrypted, then, KFS moves these files and/or folders inside the local vault, and encrypts them. Files and folders appear under the “local vault” screen by clicking on the local vault tab from the top menu.

If you wish to see inside folders, then simply click on the folders and you will see all files and any sub-folders inside the folder. The top menu will also show the folder location that you are navigating.

Double-clicking on any file from within the local vault screen will open the file and you can start editing or reading that file. Once you save the file and exit the application, the file will automatically be encrypted and saved inside the local vault. However, since some programs like Microsoft Word, Excel, Access, Powerpoint open temporary files, which must be deleted when you close the program. To delete all temporary files, click on the “update vault” button at the bottom menu which will delete all temporary files and ensure that all files are encrypted inside the vault.

By right-clicking on any file inside the local vault, you can send that encrypted file to the public or private cloud, you can open the file and start using it, you can delete the file, you can copy the encrypted file to other media such as a USB drive or you can decrypt and move the file outside the local vault and save it somewhere else on your computer.

To sync all your files and folders inside the local vault with a public or private cloud, click on the “sync with clouds” button at the bottom menu and all files from your local vault will be synced with either the private cloud or public cloud.

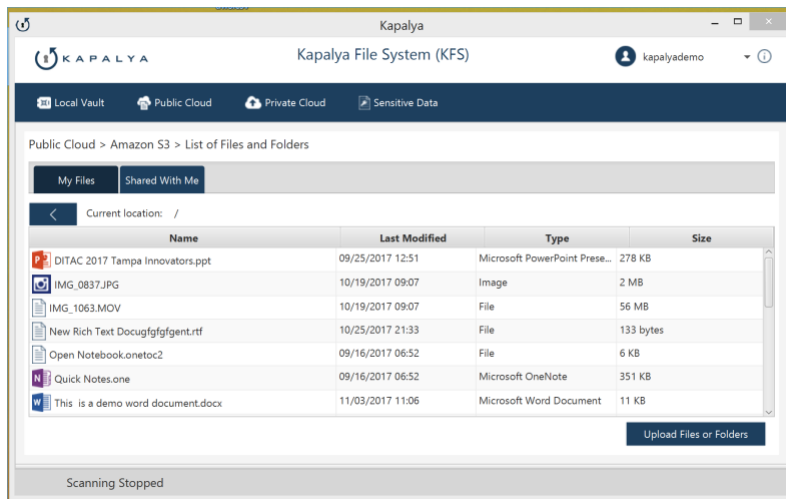


To upload files or folders inside the local vault, click the “upload Files or Folders” button from the bottom menu. You will be prompted to either drag and drop the files and/or folders or you can click on “add files” or “add folders” button from the menu and select the files and/or folders to upload inside the vault.

Once you have finished uploading the files and/or folders, then click “cancel” from the upload menu and all files/folders uploaded will now appear inside the vault.

The same procedure applies whenever any file or folder is uploaded to the public or private cloud.

## PUBLIC CLOUD



To protect files and folders on public cloud (currently only integrated with Amazon S3), KFS encrypts all files and folders inside the local vault, then uploads them to Amazon S3, ensuring that all data is transferred encrypted and land on the public cloud encrypted preventing any public cloud admins access to this data.

Files and folders appear under the “Public Cloud” screen by clicking on the Public Cloud tab from the top menu.

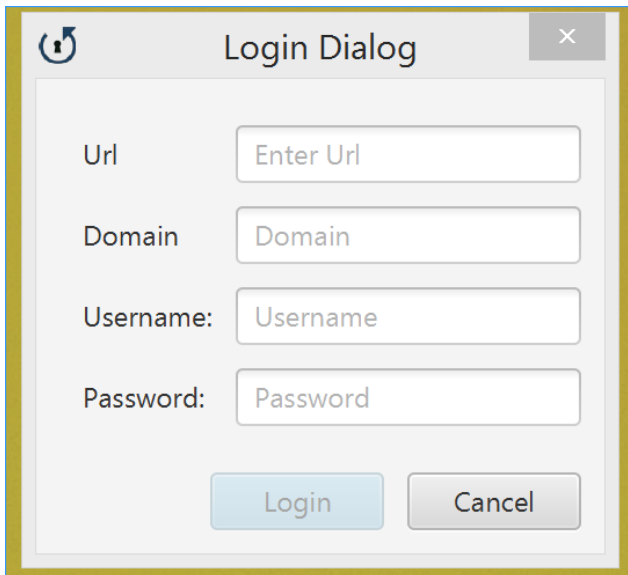
If you wish to see inside folders, then simply click on the folders and you will see

all files and any sub-folders inside the folder. The top menu will also show the folder location that you are navigating.

By right-clicking on any file inside the public cloud, you can open the file and start using it, you can delete the file, you can download the file or you can share the encrypted file with another user. This is a very powerful feature because it allows you to share encrypted files with other users WITHOUT having to e-mail them any attachments. Once you click on the share icon, you will be prompted to enter the e-mail of that user. Once you enter their e-mail, they will receive an e-mail notification that a file has been shared with the. They login to KFS from their computer and will be able to see the file shared with the and also be able to decrypt and read the file.

If any user has shared a file with you, then click on the “Shared with me” tab and you will see a listing of all files shared with you and by whom.

## PRIVATE CLOUD



The Login Dialog window contains the following fields and buttons:

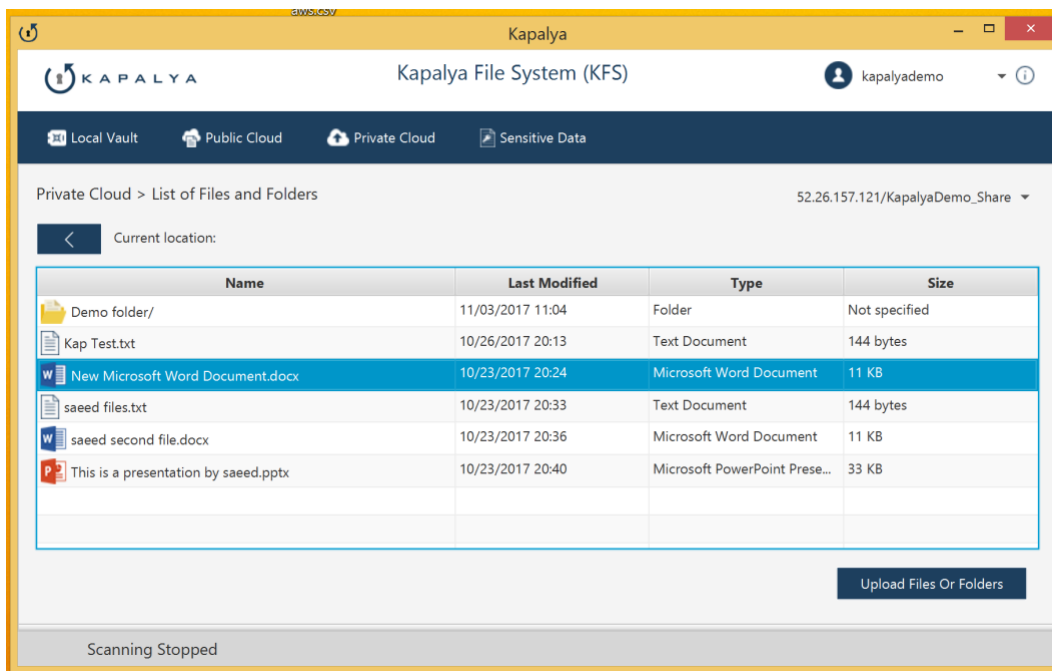
- Url:
- Domain:
- Username:
- Password:
- Login button
- Cancel button

To protect files and folders on private cloud KFS encrypts all files and folders inside the local vault, then uploads them to private cloud, ensuring that all data is transferred encrypted and land on the private cloud encrypted preventing any private cloud admins access to this data.

Files and folders appear under the “Private Cloud” screen by clicking on the Private Cloud tab from the top menu.

However, you will have to login to your private cloud BEFORE you will be able to upload any encrypted files or folders.

Please consult your local administrator for your private cloud file shares and credentials.



The interface shows the Kapalya File System (KFS) with a top menu containing: Local Vault, Public Cloud, Private Cloud, and Sensitive Data. The current view is 'Private Cloud > List of Files and Folders' with the address bar showing '52.26.157.121/KapalyaDemo\_Share'. The current location is shown as '< Current location:'. Below is a table of files and folders:

Name	Last Modified	Type	Size
Demo folder/	11/03/2017 11:04	Folder	Not specified
Kap Test.txt	10/26/2017 20:13	Text Document	144 bytes
New Microsoft Word Document.docx	10/23/2017 20:24	Microsoft Word Document	11 KB
saeed files.txt	10/23/2017 20:33	Text Document	144 bytes
saeed second file.docx	10/23/2017 20:36	Microsoft Word Document	11 KB
This is a presentation by saeed.pptx	10/23/2017 20:40	Microsoft PowerPoint Prese...	33 KB

At the bottom right, there is an 'Upload Files Or Folders' button. At the bottom left, it says 'Scanning Stopped'.

If you wish to see inside folders, then simply click on the folders and you will see all files and any sub-folders inside the folder. The top menu will also show the folder location that you are navigating and the file share that your are connected to.

By right-clicking on any file inside the public cloud, you can open the file and start using it, you can delete the file, or you can download the file.

If you wish to connect to a different file share, then click the down arrow next to the file share and you will be prompted to disconnect. Once you click “ok” to disconnect, then KFS will disconnect you from the current private cloud. Then, to login to another private cloud file share, click on “private loud” from the top menu and you will be prompted to login to another private cloud file share.