tiCrypt
User Manual

Take Control Of Your Data

Tiffany Dixon, Thomas Samant

Tera Insights, LLC

Contents

1 Preface

tiCrypt is the secure solution to the storage, sharing and processing of data for enterprises. *tiCrypt* 's robust, secure and intuitive file sharing platform insures a secure environment for storage, organizing and tracking files within an enterprise, between users and throughout groups.

With *tiCrypt* , you can upload files and folders of any size, share files with other users and groups of users, and organize and search through all the files owned by you, shared to you, or shared from you to others. These, among the many other features, are naturally easy to use with drag-and-drop support and are 100% secure at every step through end-to-end encryption.

1.1 Why it is secure

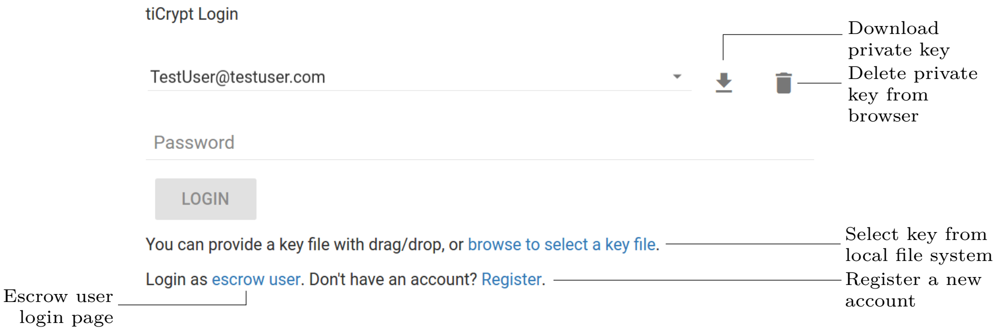
Public-private key pair *tiCrypt* 's foundation is in the mathematically-proven security of asymmetric (or public-private) key cryptography. This allows any user to encrypt data with the publicly accessible key, while only the private-key holder can decrypt that data. This also means that each user's private key file should be kept as safely and as closely as their password bound to it.

End-to-end encryption When uploading files, each file is first split into chunks, and each chunk is then encrypted with your public key in the web browser before being uploaded to the server. This implementation allows uploading files of any size, since they are all just arrays of chunks, and allows every piece of the file to be securely encrypted before being sent over the internet. Conversely, when downloading a file, each chunk is not and cannot be decrypted until received by you, the only holder of the private key. Thus, a file is completely secure from the moment it leaves your computer.

Sharing files In the setup described so far, to share a file with another user, you would have to redownload the entire file, decrypt it with your private key, then re-encrypt it with that user's public key, and finally reupload the entire new file, or to just share your private key and open a gaping security hole. But to avoid these disastrous scenarios, *tiCrypt* actually gives each file its own symmetric key and encrypts that key with your public key. Now sharing a file only requires you to re-encrypt that particular file's key with the new user's public key.

2 Registration

2.1 Creating an account



tiCrypt Login

TestUser@testuser.com

Password

LOGIN

You can provide a key file with drag/drop, or browse to select a key file.

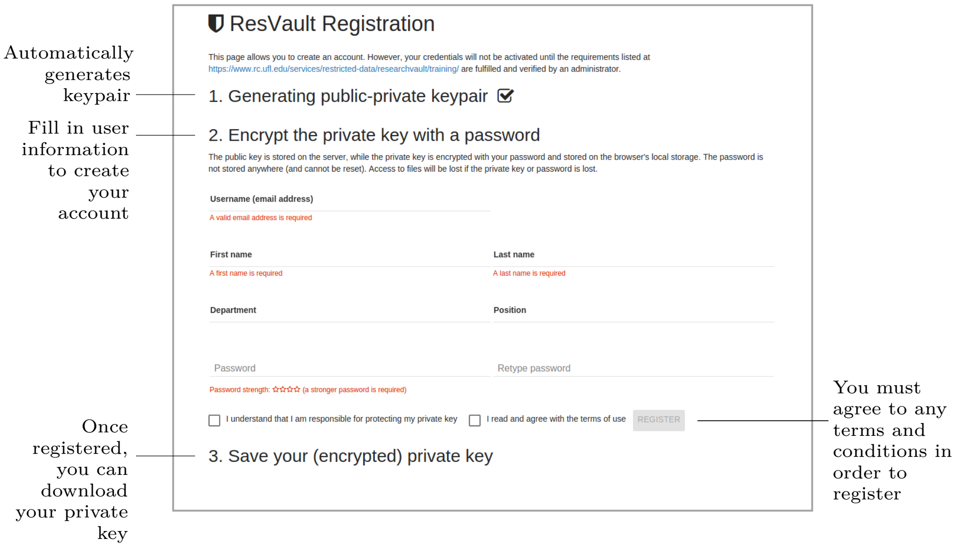
Login as escrow user. Don't have an account? Register.

Download private key
Delete private key from browser
Select key from local file system
Register a new account
Escrow user login page

Figure 1: tiCrypt Landing Page

The link to **Register** to use *tiCrypt* can be found on the login page of the application. Registration requires the following steps:

1. Generating a unique public-private key pair
2. Encrypting the private key with a password
3. Saving your encrypted private key



ResVault Registration

This page allows you to create an account. However, your credentials will not be activated until the requirements listed at https://www.rc.ufl.edu/services/restricted-data/researchvault/training/ are fulfilled and verified by an administrator.

1. Generating public-private keypair ☑

2. Encrypt the private key with a password

The public key is stored on the server, while the private key is encrypted with your password and stored on the browser's local storage. The password is not stored anywhere (and cannot be reset). Access to files will be lost if the private key or password is lost.

Username (email address)

A valid email address is required

First name

A first name is required

Last name

A last name is required

Department

Position

Password

Retype password

Password strength: ☆☆☆☆☆ (a stronger password is required)

□ I understand that I am responsible for protecting my private key □ I read and agree with the terms of use REGISTER

3. Save your (encrypted) private key

Automatically generates keypair
Fill in user information to create your account
Once registered, you can download your private key
You must agree to any terms and conditions in order to register

Figure 2: tiCrypt Registration Page

Generating a unique public-private key pair

This public-private key pair is generated in your browser and is essential for the secure use of *tiCrypt* . The public key is stored on the server you are using while the private key is stored on your browser's local storage. These keys are assigned to you, and only you.

Encrypting your private key with a password

The password you provide for your private key is the ONLY way to decrypt it. If you lose/forget your password, you will not be able to log onto *tiCrypt* or use the software in any way, including accessing any of your files.

Along with creating a secure password for your private key, the registration process will ask also for a username (the email you wish to use with *tiCrypt* and what you will use to login) ,full name, department, and position.

The last step is clicking the register button, which will allow you to move onto the next step of downloading and saving your private key.

Saving your encrypted private key

Again, your private key is not recoverable and should be stored accordingly. Some tips on storing your private key include storing it on:

- **Recommended** A USB Drive (prevents from data loss on a local computer and allows for use of *tiCrypt* on multiple computers and browsers)
- The local computer you will be accessing *tiCrypt* on, in an appropriately named folder and location

2.2 Uploading Your Key

To upload a private key at anytime on the login page, you may either drag and drop the file onto the web page or select **browse to select a key** which will allow searching for the key in your local file system. If you are dragging and dropping your key, you may need to wait a few seconds before dropping the file for this message to be visible.

The login page also gives options to download your private key(that you have already uploaded) by selecting the ⬇ icon and forgetting the key by selecting the 🗑 icon.

2.3 Logging In

Once you have registered, stored your private key, and your account has been activated by an administrator, you may login at the home page.

2.3.1 Steps to Login

1. Upload your private key (see Uploading Your Key)
2. Select your email from the drop-down selector. If your email is not listed, you may need to reupload your private key (see Uploading Your Key)
3. Type in your password
4. Press the Login button
5. If successful, you will see a Login successful notification as the page redirects.

2.3.2 Common Login Errors

Incorrect Password The password entered did not successfully decrypt the private key for use. Delete the current entry and carefully retype your password.

Account disabled pending approval Your account has not been marked as active by an administrator since registering. This error message may be altered by an admin to better describe the reason.

Error occurred while requesting challenge Your computer could not contact the server to authenticate a session. This could indicate a problem with your computer's internet connection, the server's connection, or any connection in between.

No key found at login screen The browser saves the encrypted private keys in local storage for easier logging in from the same computer. If you use a different computer or if you clear your web browser's cache, you will have to re-upload your key.

3 Interface and Account Management Tools

tiCrypt is functionally similar to other major file storage and sharing platforms, making the transition to using *tiCrypt* easy and intuative.

3.1 Your Key

One of the major tools that helps keep user information safe is the use of public/private keypairs. This is the only way for the system to verify a user's identity and allow/restrict actions within the system. When your key is no longer in the browser, such as when you select **Forget Key** or when the key is cleared after a period of time, certain actions are restricted until the key is successfully decrypted and available.

The Lock Icon If your key is no longer in memory, a 🔒 icon will appear in the top righthand corner of the screen. To decrypt and use your key again, select the 🔒 icon and an overlay will appear to enter in your password. If you attempt to perform an action that requires the use of your keypair when it is no longer available, this overlay will appear and you must enter your password to successfully load your key before performing the action.

3.2 System-Wide Tools

Tool-tips *tiCrypt* uses icons as a main tool for showing any possible actions. But in case you do not recognize the action described by the icon, hovering your mouse over any action icon will show a more informative tool-tip.

Drag and drop Essentially everything in *tiCrypt* can be performed with simple drag-and-drop including uploading and sharing files to any users or groups, downloading files, and transferring files in virtual machines.

3.3 Notifications

tiCrypt is equiped with numerous types of notifications to help users understand what is happening in the system, with their files, and between users. Notifications are a vital part of making certain that users are equipped to protect their data in ways that the system cannot. Every notification in *tiCrypt* is set for a reason, and it is important to understand what information each notification provides.

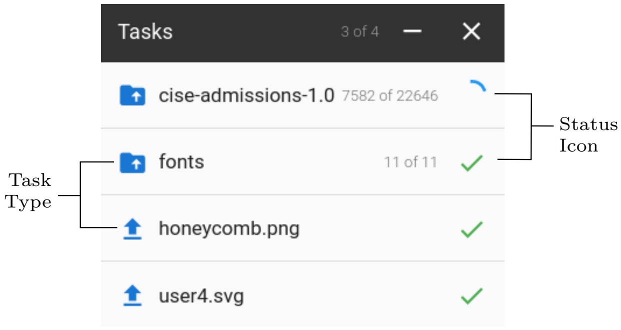
Notifications Extra information and progress on certain actions will be displayed in the bottom-left corner. Notifications will also be themed differently depending on the type and importance of the information being displayed. Different color notifications will signify differen things.

Color	Meaning
🟩	Success
🟦	Process Occurring
🟨	Validation
🟥	Error/Incorrect

Modals Many actions that require further action will bring up a modal to grab your attention. An important modal of this type delete, which requires an extra level of confirmation.

3.4 Task Manager

A great resource available to all users is the Task Manager that appears in the bottom right-hand corner of the screen. The task manager will show updates of different processes running in the system, how far along a process is, and which processes are being queued. Any process in the system that may take a longer period of time will show it's status through this manager.



Tasks 3 of 4

cise-admissions-1.0 7582 of 22646

fonts 11 of 11 ✓

honeycomb.png ✓

user4.svg ✓

Figure 5: tiCrypt Task Manager

Launching the Task Manager To launch the task manager, users can either start a process, which will automatically cause the manager appear, or click on the ≡✓ icon at the top of the screen. If there are no processes currently running, the manager will read ”none pending”.

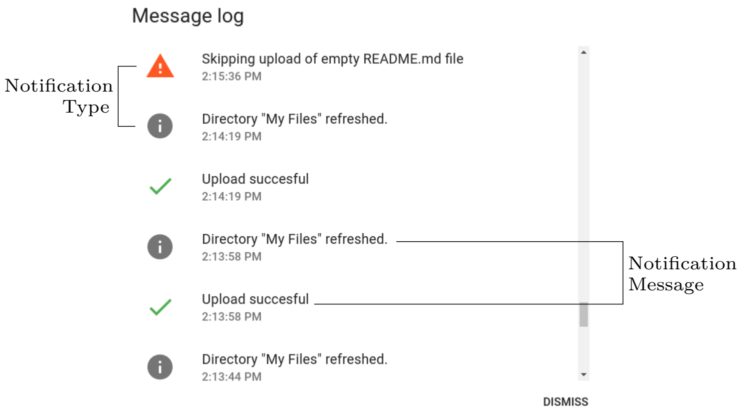
Status of a Process The status of a processes can be reviewed in more detail by hovering over the status icon. The task manager provides information about what percentage of a task is accomplished, if a process is pending, or time completed if successful.

Types of Tasks There are numerous types of tasks that can be quickly identified with the icon in front of it. Here is a comprehensive list of icons and the tasks associated with them.

Icon	Meaning

3.5 Message Log

Many task and processes in *tiCrypt* will generate notifications to give the user information on what's going on the system. The message log keeps track of all these notifications within a session. To review these notifications, select the ▤ icon.



⚠ Skipping upload of empty README.md file
2:15:36 PM

ⓘ Directory "My Files" refreshed.
2:14:19 PM

✓ Upload succesful
2:14:19 PM

ⓘ Directory "My Files" refreshed.
2:13:58 PM

✓ Upload succesful
2:13:58 PM

ⓘ Directory "My Files" refreshed.
2:13:44 PM

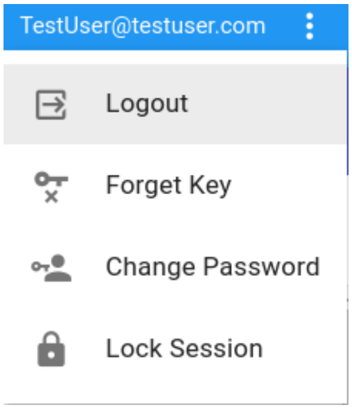
Figure 6: tiCrypt Message Log

Message Log Icons Each notification type is signified by an icon.

Icon	Meaning
ⓘ	Information
✓	Success
⚠	Warning
✗	Failure

3.6 Account Management Tools

To manage your *tiCrypt* account, simply click your on the ⋮ icon in the top right-hand corner. This will open up a menu which will let you logout, forget your key from the browser, change your password, or lock the session.



Logging Out Logging out of *tiCrypt* will log you out of your current session and redirect you back to the login page. Always be sure to log out of *tiCrypt* after use.

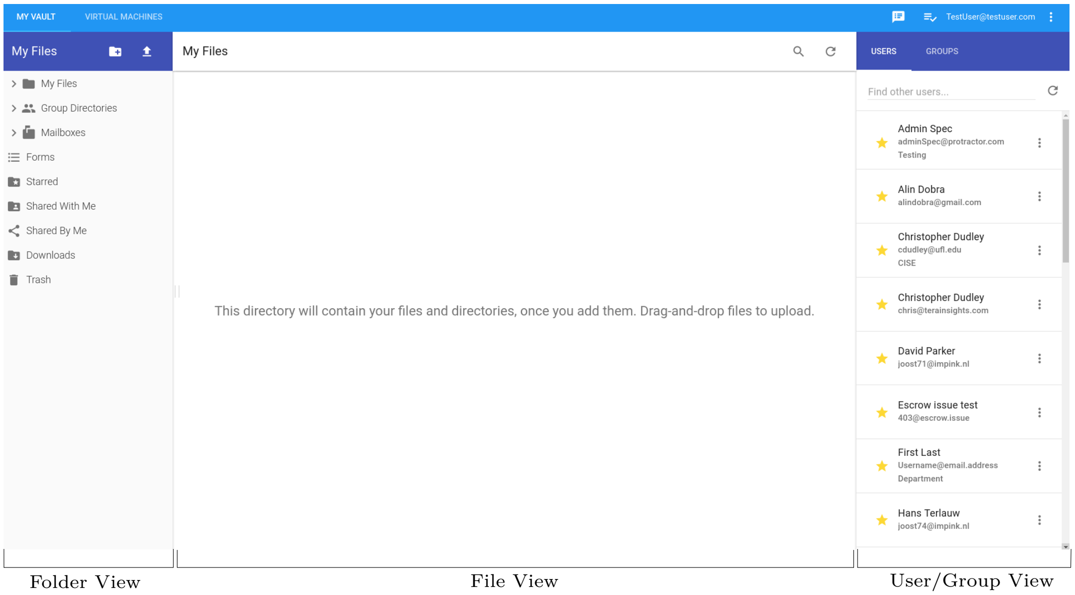
Forgetting the Key This option clears the key from browser memory. When the key is cleared from the browser memory, a 🔓 icon will appear to the left of the user email. This will happen after a set period of time specified by your administrator, even if this option is not selected.

Changing Your Password Changing your account password in *tiCrypt* is similar to other applications in which you must type in your current password, and then you will be allowed to create a new one. If the new password is strong enough, the password change will be accepted. When a new password is created, a new private key is also created and the old one will become obsolete. *Please* make sure to **download and safely store** your new key before exiting the modal!

Locking Your Session This is a great tool for not wanting to log out of *tiCrypt* , but instead locking it so others cannot use the logged in account. In order to unlock the session, the user must enter in their password.

4 File management

4.1 Vault Overview



This directory will contain your files and directories, once you add them. Drag-and-drop files to upload.

Admin Spec
adminSpec@protractor.com
Testing

Alin Dobra
alindobra@gmail.com

Christopher Dudley
cdudley@ufl.edu
CISE

Christopher Dudley
chris@terainsights.com

David Parker
joost71@impink.nl

Escrow issue test
403@escrow.issue

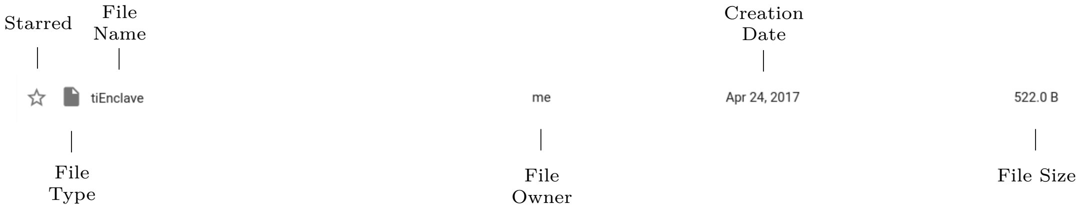
First Last
Username@email.address
Department

Hans Terlauw
joost74@impink.nl

In the *tiCrypt* Vault, there are three main panels which will be referred to many times throughout this section and the rest of the manual. These sections include the **Folder View** Panel, the **File View** Panel, and the **User/Group** Panel.

4.2 File Properties/Tools

4.2.1 Characteristics of a File



Starred Status Indicates if the file is *starred*, or marked as important. Any files with the starred icon filled in yellow will have a copy stored in the corresponding Starred folder.

Type of File The type of file can be noted by the icon that appears to the left of the file's name.

Name of a File The name of a file uploaded into *tiCrypt* will keep the same name from the local computer file, but may be renamed after being uploaded. If the name is too long for the current display width, hovering over the name will show a tool-tip with the full file name.

File Owner The owner of the file. File ownership is reflective on the original uploader and cannot be changed.

Creation Details Each file will have the date of its creation under the **Date Created** column.

Size of File The size of a file is given under the **Size** column.

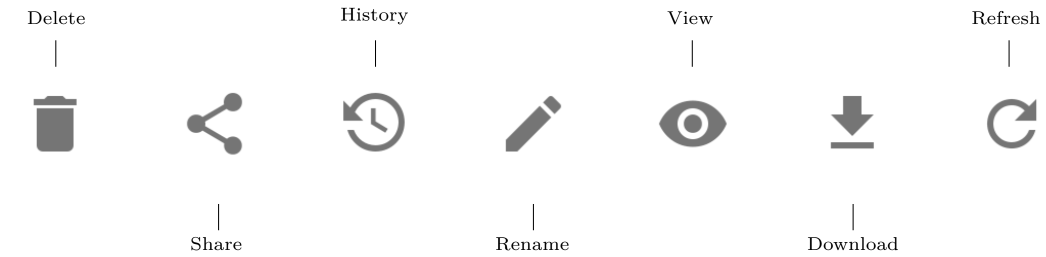
4.2.2 Uploading a File into a Directory

Upload Icon One option is to use the ⬆ icon. This appears in the top right of the folder view. This will allow you to upload files from files on your local computer. If a file is uploaded this way, the file will directly go into the folder that is open and the user can organize and move the file throughout the platform as needed with the drag and drop feature.

Drag and Drop Another way to upload a file is by using the drag and drop feature. By simply dragging the file from your local computer file into *tiCrypt* , it will upload into the folder you have open. You can also specify which folder you wish to upload the file in by dropping it over the correct folder in the tree view. The folder will be highlighted when you hover over it, as seen to the right.

The drag and drop feature can be utilized throughout *tiCrypt* to seamlessly move files throughout the platform to different locations to store or share your files.

4.2.3 File Actions Overview



4.2.4 Sharing a File

A file is very easily shared in *tiCrypt* with just the click of a button. To share a single file, right-click on the file and select **share** in the context menu or select the ⋖ icon from the list of file actions. Once either are selected, a sharing modal will appear on the screen. From this modal, you will be able to search for the users/groups you wish to share the file with. To confirm and share, select **Accept**.

4.2.5 Checking History of a File

Every file has an audit feature which can be used to track its activity. However, only the owner of the file (the user who first created/uploaded it) can view this history. These audits keep track of who created the file, when it was first created, and who that file has been shared with since then.

4.2.6 Renaming/Deleting a File

A file can be renamed by right-clicking on it, and selecting **Rename** in the context-menu or by selecting the ✎ icon in the top righthand corner once a file selected.

Deleting a file can be done by selecting the **Trash** option from the context menu or selecting the 🗑 icon.

***Files are not permanently deleted until doing so from the trash folder. Therefore, if you accidentally delete a file, it can be easily restored from the trash folder.*

4.2.7 Starring a File

To the left of every file is a ☆ symbol which, when selected, will place that file into the **Starred** folder. Much like with conventional email, this feature allows the user to identify important documents and places them into the starred folder for future reference. A file can be un-starred as well simply by clicking on the star symbol once more, until it is no longer filled in.

4.2.8 Selecting Multiple Files

When a file is selected, it will be highlighted. To select multiple files, simply hold ctrl and select all the files you would like, much like a traditional file system on your computer. A user may select multiple files at a time for deleting and downloading. Any actions you can do with multiple files are located at the top right of the folder view.

4.2.9 Searching for a File

A file can be searched by name in the file view. This search is case-insensitive.

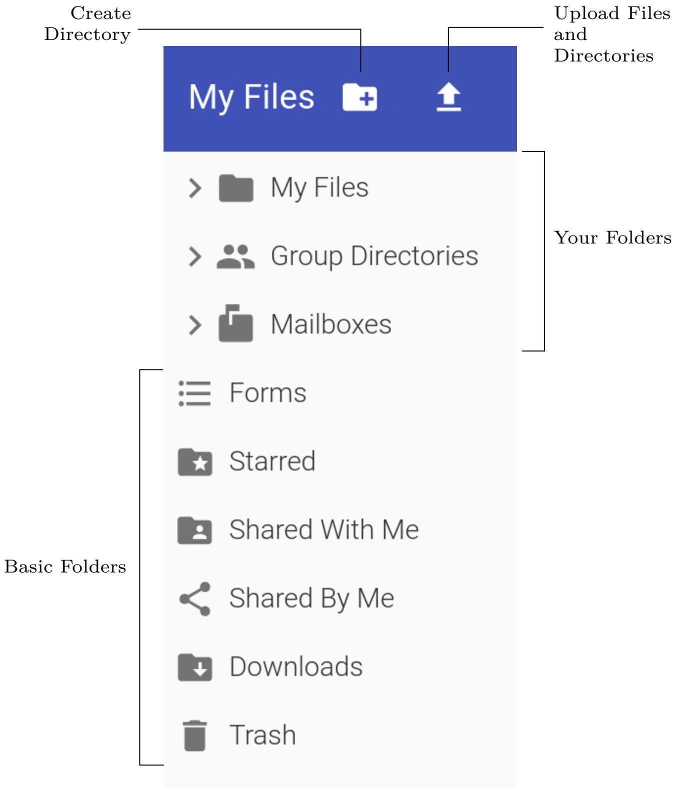
4.2.10 Downloading a File

Downloading from *tiCrypt* is done by just simply clicking on the ⬇ icon next to each file or by selecting **Download** from the context-menu.

⚠**Warning:** Downloading files onto your local computer removes the encryption and files are therefore no longer secure. Please be mindful of this when handling your files outside of *tiCrypt* .

4.3 Folders

4.3.1 Basic Folders



4.3.2 Folders that be Modified

My Files This folder is the included generic folder where all user files will be uploaded until a new folder is created.

Group Directories Contains directories for all the corresponding groups a user is in. These directories are shared will all members of the respective group.

Mailboxes This directory contains all the mailboxes a user owns.

4.3.3 Fixed Folders

Forms Contains all the forms a user owns.

Starred This folder contains all the files the user stars or marks as important.

Shared by me This folder contains all the files shared **by** you with other users/groups. These files are grouped by user, group, date, and an option to view all files.

Shared with me This folder contains all the files shared **with** you by other users/groups. These files are grouped by user, group, date, and an option to view all files.

Downloads This folder contains all the files that a user has downloaded onto their local machine.

Trash This folder contains all the files/folders a user has deleted.

Note: These basic folders cannot be deleted

4.3.4 Creating a folder

Click on the 📁 icon at the top right of the folder view. Folder names must be unique.

4.3.5 Renaming/Deleting a Directory

To rename or delete a directory, simply right click on the directory name in the folder view to bring up the context-menu and select **Rename**.

To delete a directory, right click on the folder to bring up on the context menu and select **Delete**.

4.3.6 Sorting files in folders

Within the folder view, selecting the name of a column will allow you to sort files in ascending or descending order by name, size, owner, or date.

5 Sharing features

tiCrypt users have the ability to share their uploaded files with other users using public/private key cryptography. The user who shares their file(s) encrypts them with their public key, and only the correct recipient(specified by the owner of the file) is able to decrypt the file with their private key.

5.1 User-to-user

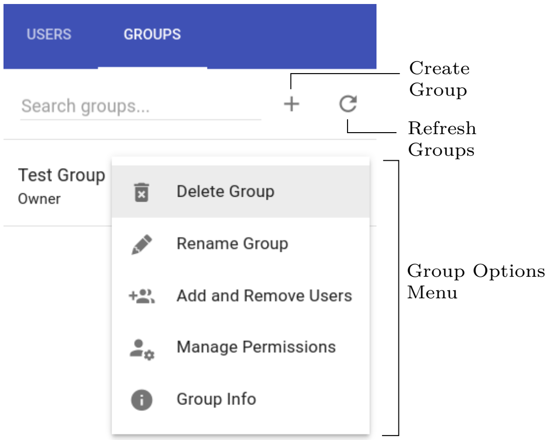
Sharing a file with another user can be done in one of two ways:

1. Drag the file(s) from your vault and drop it on the user's name in the **Users** tab in the User/Group panel. (The system will ask you to confirm some user information before sharing occurs.)
2. Select the < icon, which will bring up a modal that lets you share that file with one or many users/groups.

5.2 Groups

5.2.1 Creating Groups

One of the great features of *tiCrypt* is the ability to not only share files with individual users, but to share files with entire groups as well making it easy to share throughout teams. To create a group, follow these steps:

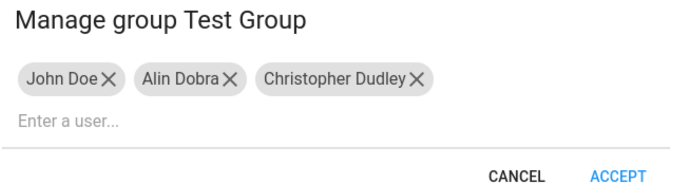


Complete Workflow for Creating Groups

1. In the User/Group panel, click on the **Groups** tab.
2. Click on the + button in the top right.
3. Name your new group

4. Add users to a group by selecting **Add and Remove Users**.

5. A modal will appear in which you can search for users and add them to the group. To confirm all changes, select **Accept**.

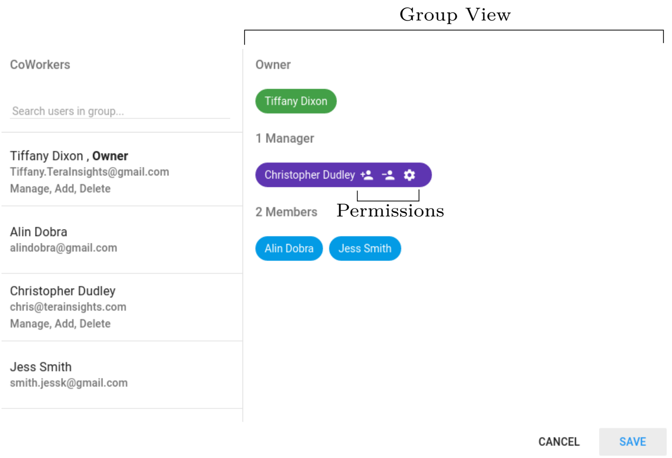


Manage group Test Group

John Doe ✕ Alin Dobra ✕ Christopher Dudley ✕

Enter a user...

6. The next step is to manage permissions within the group. To do this, select **Manage Permissions**, which will bring up a modal for which you can set permissions for each member of the group.



CoWorkers

Search users in group...

Tiffany Dixon , **Owner**
Tiffany.TeraInsights@gmail.com
Manage, Add, Delete

Alin Dobra
alindobra@gmail.com

Christopher Dudley
chris@terainsights.com
Manage, Add, Delete

Jess Smith
smith.jessk@gmail.com

Owner

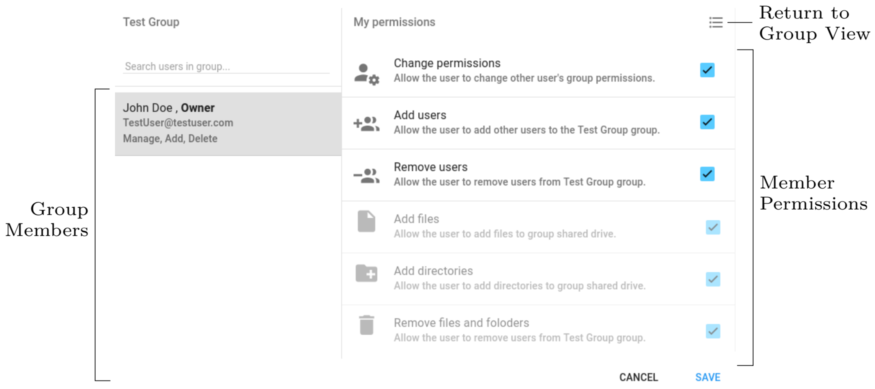
Tiffany Dixon

1 Manager

Christopher Dudley

2 Members

Alin Dobra Jess Smith



Test Group

Search users in group...

John Doe , **Owner**
TestUser@testuser.com
Manage, Add, Delete

My permissions

Change permissions
Allow the user to change other user's group permissions. ☑

Add users
Allow the user to add other users to the Test Group group. ☑

Remove users
Allow the user to remove users from Test Group group. ☑

Add files
Allow the user to add files to group shared drive. ☑

Add directories
Allow the user to add directories to group shared drive. ☑

Remove files and foloders
Allow the user to remove users from Test Group group. ☑

5.2.2 Modifying Groups

Viewing Group Details View group information by selecting **Group Info** from the dropdown menu.

Renaming a Group Users can modify the names of their groups by selecting **Rename Group** from the dropdown menu.

Deleting a Group To delete a group, select **Delete Group** from the dropdown menu.

5.2.3 Sharing Files with Groups

There are two ways to share files with groups.

1. Select the < on the file(s) and search for the group name in sharing modal.

2. Drap and drop the files you wish to share over the name of the group in the **Groups** panel.

6 Mailboxes

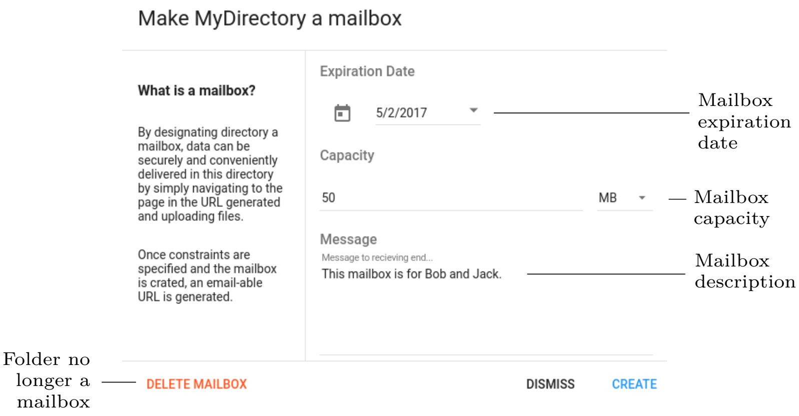
6.1 What is a mailbox?

Mailboxes are used to safely recieve files inside of *tiCrypt* from outside collaborators. A mailbox looks and acts just like a normal folder, and files placed inside them can be shared, downloaded, and viewed.

6.2 Mailbox Creation

A mailbox must be created from an existing directory. To turn an existing directory into a mailbox, select the option ”Make mailbox” from the context menu of the directory. This will bring up a mailbox creation modal in which you may create ”access points”, or secure url destinations where outside users users may drop files. Each end point requires

1. An expiration date, or a date where the end point will be destroyed
2. A maximum capacity
3. A description of the end point



Make MyDirectory a mailbox

What is a mailbox?

By designating directory a mailbox, data can be securely and conveniently delivered in this directory by simply navigating to the page in the URL generated and uploading files.

Once constraints are specified and the mailbox is crated, an email-able URL is generated.

Expiration Date: 5/2/2017

Capacity: 50 MB

Message: Message to recieving end... This mailbox is for Bob and Jack.

Mailbox expiration date

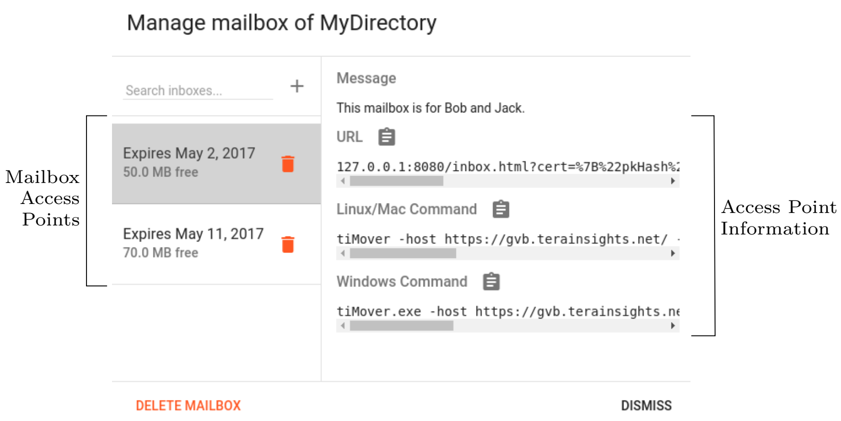
Mailbox capacity

Mailbox description

Folder no longer a mailbox

6.3 Mailbox Management

A single mailbox may have multiple access points that vary in expiration date and capacity. To manage access points for a mailbox, select **Manage Mailbox** from its context menu.



Expires May 2, 2017
50.0 MB free

Expires May 11, 2017
70.0 MB free

Message
This mailbox is for Bob and Jack.

URL
```
127.0.0.1:8080/inbox.html?cert=%7B%22pkHash%2
```

Linux/Mac Command
```
tiMover -host https://gvb.terainsights.net/ -
```

Windows Command
```
tiMover.exe -host https://gvb.terainsights.ne
```

6.3.1 Creating Multiple Access Points

To add an access point to a mailbox, select the + icon. This will then ask for access point information such as expiration date, capacity, and description.

Tip: Use the mailbox descriptions wisely to manage who has access to each access point and for what purpose.

6.3.2 Access Point Types

There are 2 ways for an outside user to reach these access points including

1. URL : These can be accessed right through the web-browser of the outside user's computer

2. Command : These are meant to be entered into the command prompt of the outside user's computer

6.3.3 Delete an Access Point

If an access point is no longer needed, it can be deleting by selecting the 🗑 icon.

6.3.4 Deleting a Mailbox

Deleting a mailbox means turning the mailbox back into a normal folder. To do so, select Delete Mailbox within the manage mailbox modal. When a mailbox is deleted, all of the files that were transferred to it remain inside.

7 Virtual Machines

Virtual Machines are a special tool to aid users in manipulating their files/data in an OS-specific environment. Essentially, this tool provides the user to run very unique operating systems and corresponding applications based on their individual needs. Administrators will be able to build virtual machine templates based on individal user/department need, and users in turn will be able to run these virtual machines using their own encrypted drives.

7.1 Outside Software Requirements

In order to run a virtual machine using *tiCrypt* , you must have a functioning Remote Desktop Client installed. The following are suggested RDCs based on your local computer's operating system.

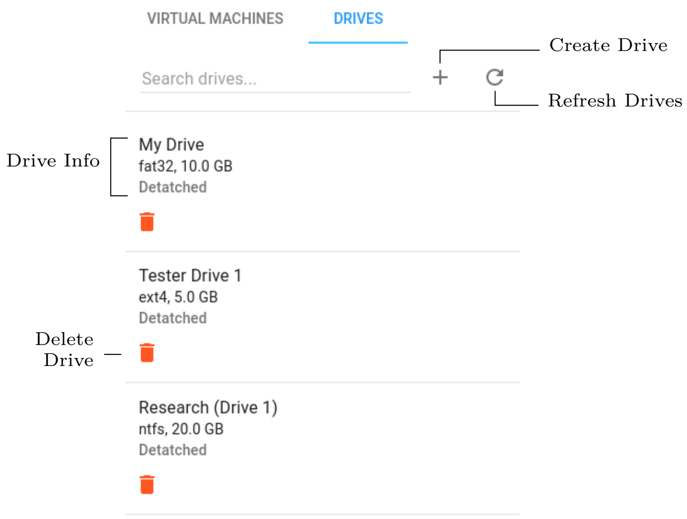
Operating System	Suggested RDC
Windows	Microsoft RDS
Linux	Vinagre
Mac OS X	Microsoft Remote Desktop

7.2 Creating a Virtual Machine

There are two steps required to create a virtual machine in *tiCrypt* including

1. Creating an encrypted drive for virtual machine local storage
2. Choosing a virtual machine template

7.2.1 Creating an Encrypted Drive



My Drive
fat32, 10.0 GB
Detatched

Tester Drive 1
ext4, 5.0 GB
Detatched

Research (Drive 1)
ntfs, 20.0 GB
Detatched

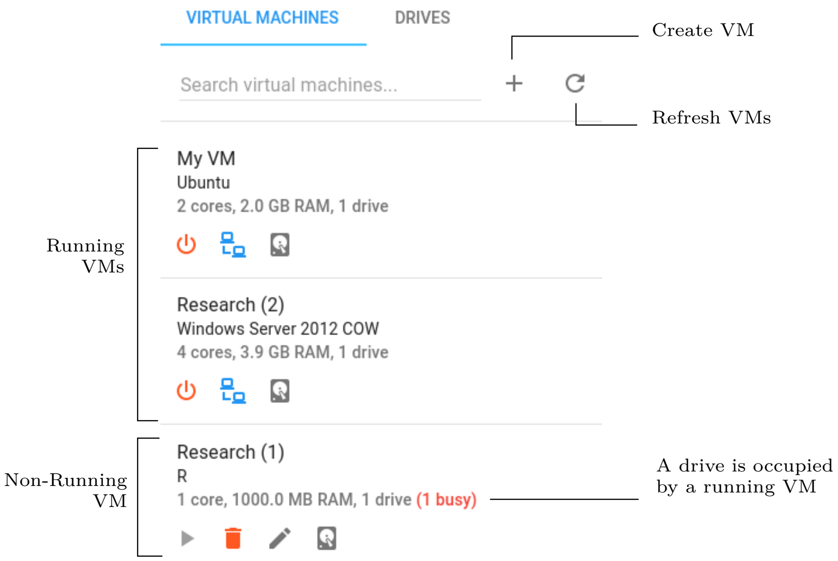
To create an encrypted drive, select the **Drives** tab and select the + icon. This will bring up a modal in which you can give the encrypted drive a name, a drive type, and a drive capacity. The drive types are as listed:

Drive Type	Description
Linux/ext4	Can be only attached to Linux VMs
FAT32	Can be attached to both Linux and Windows VMs
Windows/NTFS	Can only be attached to Windows VMs

Once everything is specified, click **Accept** to create the drive. Keep in mind, these drives cannot be edited.

7.3 Creating a VM Template

The next step is creating a virtual machine template. This can be done by selecting the + icon in the **Virtual Machines** tab.



My VM
Ubuntu
2 cores, 2.0 GB RAM, 1 drive

Research (2)
Windows Server 2012 COW
4 cores, 3.9 GB RAM, 1 drive

Research (1)
R
1 core, 1000.0 MB RAM, 1 drive (1 busy)

7.3.1 Selecting a Virtual Machine Template

Virtual machine templates are provided by your administrator. You should ask for a detailed description of each template, which operating system it uses, and which applications it has pre-installed to determine which template best suits your needs. When creating a new virtual machine, a dropdown list of all available templates will be available.

7.3.2 Attaching Drives

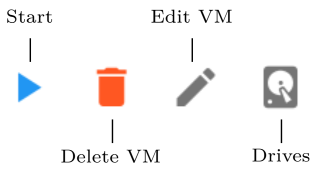
When creating a virtual machine template, you will be asked to select its ”Home Drive” or the main storage for the virtual machine. This drive is selected from existing drives. An extra drive can be added for additional storage. Be mindful of which operating system your virtual machine is running, because this will determine which drives you should attach.

7.4 Running a Virtual Machine

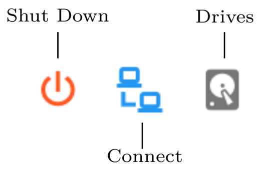
7.4.1 Virtual Machine Menus based on Status

Virtual machines will display different menus based on their status of connection. A virtual can be powered-off, on and not connected, or on and connected.

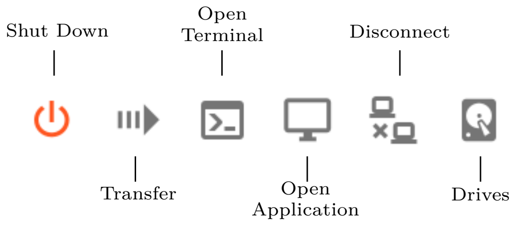
Powered-off When a virtual machine is powered-off, the only actions available are start, delete, edit, and view attached drives. The is the *only* time in which you may edit your virtual machine. This includes changing which encrypted drives are attached to it.



On but Not Connected When a virtual machine is on but not connected, the drives attached are considered to be "in use" or "busy". What this means is that you cannot launch another virtual machine that uses any of the same encrypted drives. The virtual machine is on, but in this stage, it is not connected. Being connected to a virtual machine requires a cryptographic interaction with the use of your private key that is decrypted in the browser. In this stage, the virtual machine is on, but the user can move about tiCrypt and complete other tasks.

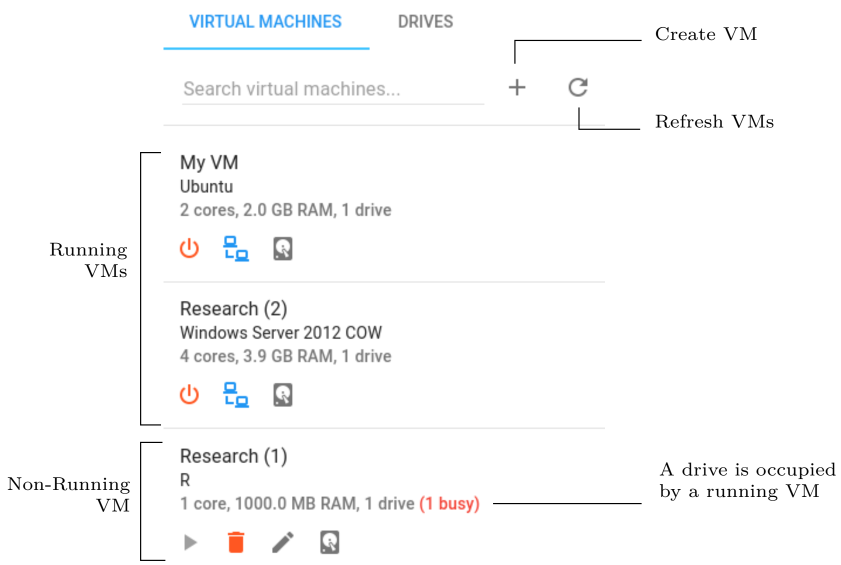


On and Connected When a virtual machine is both on and connected, cryptographic authentication has occurred using your private key and a private SSH connection is established. This is the point when you can do the most interation with the virtual machine including transferring files to the attached drive from your vault and connecting to the virtual machine via a terminal or RDC.



7.4.2 Viewing Existing Virtual Machines

A list of all existing virtual machines will be listed under the **Virtual Machines** tab. To start a virtual machine, select the ▶ icon to the right of the virtual machine name. Once the VM is successfully running, there will be an option to connect to the virtual machine by selecting the 🖧 icon, which will prompt you to enter in your password for verification.



VIRTUAL MACHINES DRIVES

Search virtual machines...

My VM
Ubuntu
2 cores, 2.0 GB RAM, 1 drive

Research (2)
Windows Server 2012 COW
4 cores, 3.9 GB RAM, 1 drive

Research (1)
R
1 core, 1000.0 MB RAM, 1 drive (1 busy)

Create VM

Refresh VMs

Running VMs

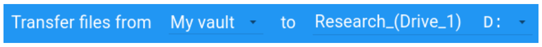
Non-Running VM

A drive is occupied by a running VM

7.5 Transferring Files Between Vault to Drive

tiCrypt makes it possible to simply transfer files from the vault onto an encrypted virtual machine drive. To do so, select the III▶ icon next to the on and connected virtual machine name.

Selecting Views To change which drives are being viewed, select the correct drives from the top left.

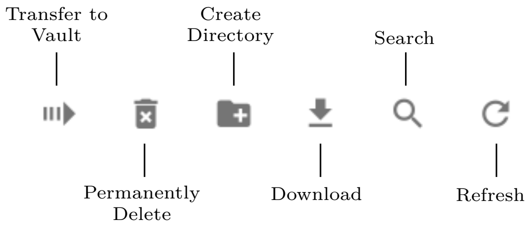


Transfer files from My vault ▾ to Research_(Drive_1) D: ▾

Transferring Files/Directories To and From the Vault To transfer files/directories between the drive and your vault, either drag and drop the file/directory from one side to the other, or select the III▶ icon once you have selected all the files/directories you wish to transfer. Files that are transferred but already exist in the drive will be replaced with the newer version.

Note: Transferring a file to a drive does not delete the original from the tiCrypt vault; it simply makes a copy on the encrypted drive.

7.6 Drive Actions

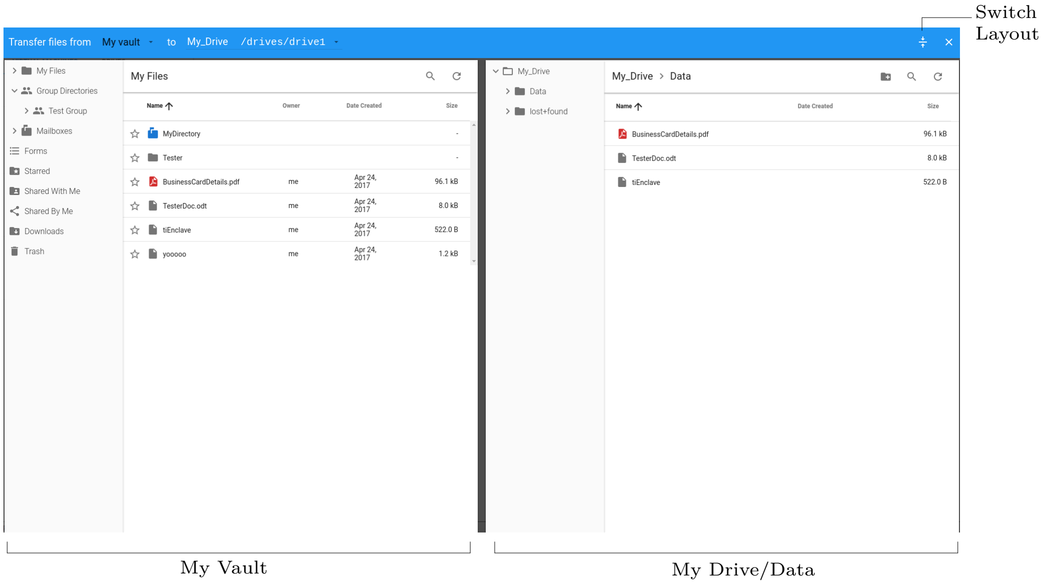


Transfer to Vault Any files/directories that are selected will transfer to the vault. Any files that already exist in the vault will be?

Permanently Delete Any files/directories that are selected will be deleted from the drive.

Create Directory Creates a new directory in the open directory on the drive. Directories are created just in the normal vault to make organization of files simple.

Download All files/directories that are selected will be downloaded from the drive onto your local computer.



Switch Layout

My Files

Name	Owner	Date Created	Size
☆ MyDirectory			-
☆ Tester			-
☆ BusinessCardDetails.pdf	me	Apr 24, 2017	96.1 kB
☆ TesterDoc.odt	me	Apr 24, 2017	8.0 kB
☆ tiEnclave	me	Apr 24, 2017	522.0 B
☆ yooooo	me	Apr 24, 2017	1.2 kB

My_Drive > Data

Name	Date Created	Size
BusinessCardDetails.pdf		96.1 kB
TesterDoc.odt		8.0 kB
tiEnclave		522.0 B

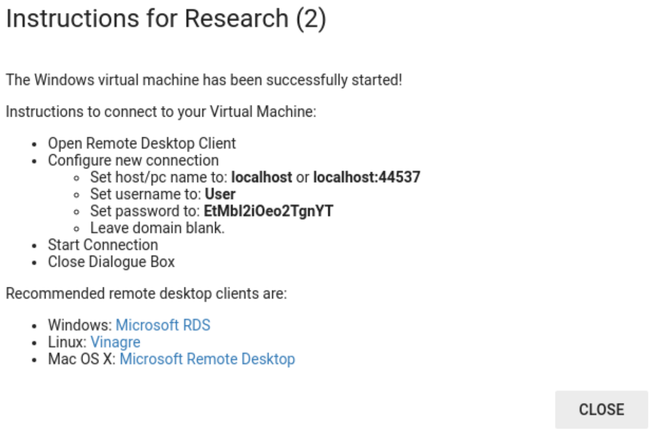
My Vault

My Drive/Data

7.7 Launching a Virtual Machine

Now that a virtual machine has been created, it is running, and files have been transferred to it, it can now be launched.

To launch a virtual machine using the Remote Desktop Client, select the 🖥 icon which will bring up an instruction menu much like the one below.



Instructions for Research (2)

The Windows virtual machine has been successfully started!

Instructions to connect to your Virtual Machine:

- Open Remote Desktop Client
- Configure new connection
    - Set host/pc name to: **localhost** or **localhost:44537**
    - Set username to: **User**
    - Set password to: **EtMbI2iOeo2TgnYT**
    - Leave domain blank.
- Start Connection
- Close Dialogue Box

Recommended remote desktop clients are:

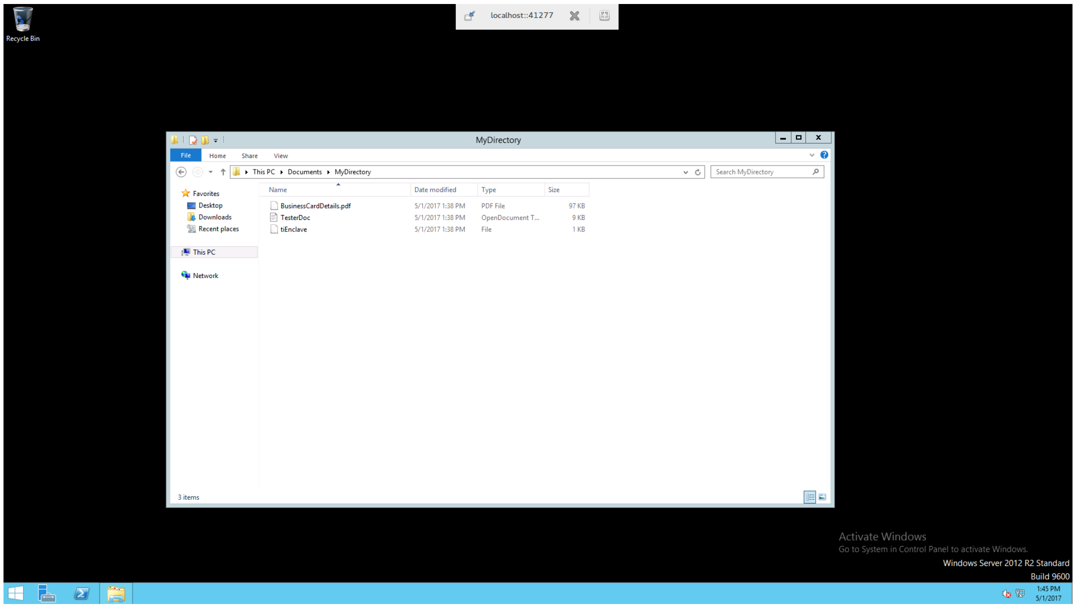
- Windows: Microsoft RDS
- Linux: Vinagre
- Mac OS X: Microsoft Remote Desktop

Make sure in your RDC that you are picking the correct protocol.

Operating System	**Protocol**
Unix/Linux	SSH
MS Windows	RDP

Recommendations for remote desktop clients are given at the bottom of the instructions if one is not already downloaded on your local computer.

Once you enter in all the correct information and click connect on your RDC, then the virtual machine will open and start. Below is an example of a Windows virtual machine and accessing the files that were just tranferred over to the encrypted drive.



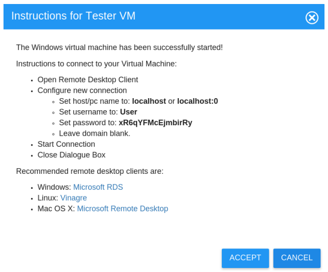
Name	Date modified	Type	Size
BusinessCardDetails.pdf	5/1/2017 1:38 PM	PDF File	97 KB
TesterDoc	5/1/2017 1:38 PM	OpenDocument T...	9 KB
tiEnclave	5/1/2017 1:38 PM	File	1 KB

Figure 14: Windows Virtual Machine Example

7.8 Complete Overview/Step-by-Step

To create and launch a Virtual Machine, follow these steps:

1. Create an Encypted Drive on the **Drives** tab.
2. Create a Virtual Machine OS template on the **Virtual Machines** tab and attach the encrypted drive.
3. Start your virtual machine by selecting the ⬆ icon to the right of the virtual machine name.
4. Connect to the virtual machine by selecting the 🖧 icon.
5. Transfer files to and from your virtual machine by selecting the ▶ icon.
6. Now, you may either
    a) Use the virtual machine by operating it through the terminal. To open the terminal, select the >_ icon.
    OR
    b) Open up the virtual machine on a remote desktop viewer by selecting the 🖥 icon and following the steps below.
7. Select the 🖥 icon, which will bring up an instruction menu much like the one below



Instructions for Tester VM

The Windows virtual machine has been successfully started!

Instructions to connect to your Virtual Machine:

- Open Remote Desktop Client
- Configure new connection
    - Set host/pc name to: **localhost** or **localhost:0**
    - Set username to: **User**
    - Set password to: **xR6qYFMcEjmbirRy**
    - Leave domain blank.
- Start Connection
- Close Dialogue Box

Recommended remote desktop clients are:

- Windows: Microsoft RDS
- Linux: Vinagre
- Mac OS X: Microsoft Remote Desktop

8. Follow the instructions and put the corresponding host name, user name, and password into the RDC on your local computer and then connect.

    Note: Make sure in your RDC that you are picking the correct protocol. The Remote Desktop Viewer should be downloaded on the host computer, this is NOT an application on the tiCrypt interface. A list of recommended RDC's appear in the instruction menu at the bottom.

Operating System	Protocol
Unix/Linux	SSH
MS Windows	RDP

9. To shutdown the VM, exit the Remote Desktop Client, disconnect the VM by selecting the 🖧 icon, and power off by selecting the ⏻ icon.