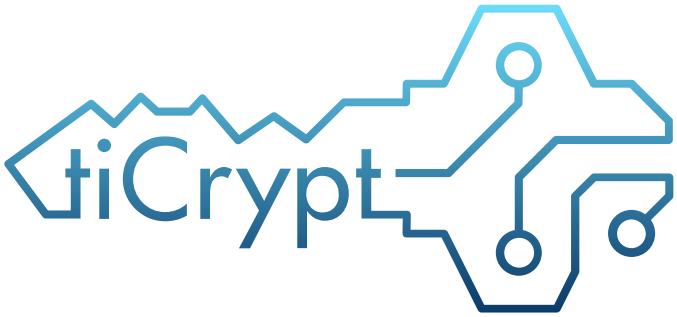


Admin Manual

Take Control Of Your Data

Tiffany Dixon

Tera Insights, LLC

Contents

1 Administrator Recommendations

Each and every part of tiCrypt is a carefully thought-out process, including the role of administrators and the boundaries that should exist for them within the system. One of the most important aspects of tiCrypt's administative system and its tools is the idea of isolation. If there should exist a possibility for unsafe collaboration between administrators, we have limited those interactions and highly advice against any actions that may pose a threat to the system. These actions and roles will be described in futher detail later on, so we highly suggest paying very close attention to our recommendations.

1.1 Basic Recommendations

1. The site key administrator should not be an escrow user.
2. There should be a limited amount of Super Admins

2 Admin Management Tools

All of the below tools can be found under the **Management** tab in tiCrypt.

2.1 User Management

The user management list gives a detailed list of user's

- First and Last Name
- Email
- Status (Active or Inactive)
- Role (User, Admin, or Super Admin)
- Permissions

All of the above may be modified in the **Actions** column by selecting the icon. From here you can also delete users, manage user groups, and view user info.

2.1.1 Roles Types

Every single individual who registers an account in tiCrypt has a specified role that is assigned to them by a supervising administator. These roles describe a type of "heirarchy" within the system by defining rank of power.

Super Admin This is the top ranking role, and these users essentially have very few limitations. Super Admins may:

- Modify permissions of other Super Admins, Admins, and Users
- Promote/Demote roles of other Super Admins, Admins, and Users
- Approve newly registered user accounts

There is no limitation to the number of users in each category, but it is highly recommended not to place too many users in the Admin and especially Super Admin categories. The Super Admin role is meant to be only a small number of trusted individuals.

Admins Admins have control over normal users and may modify different settings for them, but Admins may not modify other Admins.

- Modify permissions of Users

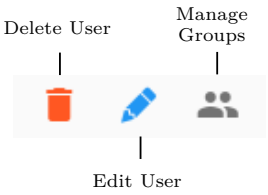
Users Users are essentially just normal users of tiCrypt and have no special privilages or authority in the system.

- Cannot modify any permissions

2.1.2 Modifying User Role

To modify a user role, select the icon and select the appropriate role from the dropdown in the upper right-hand corner.

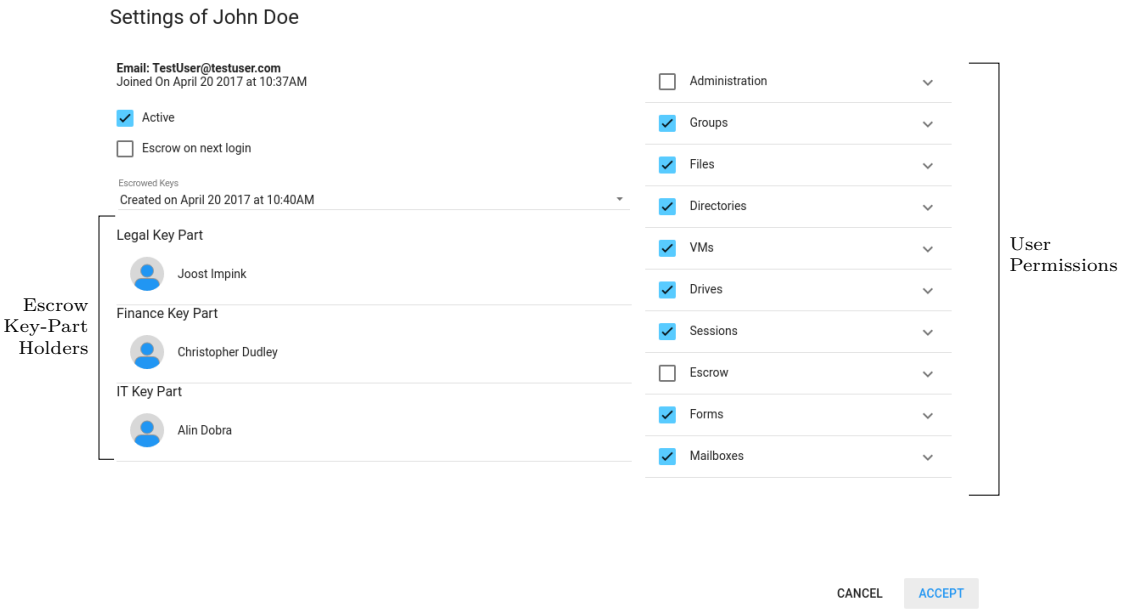
2.1.3 User Actions



- **Delete User** Deletes the selected user from *tiCrypt*
- **Edit User Profile** Edits a user's status (active vs inactive), role, permissions, and escrow
- **Manage Groups** Manage groups of a user

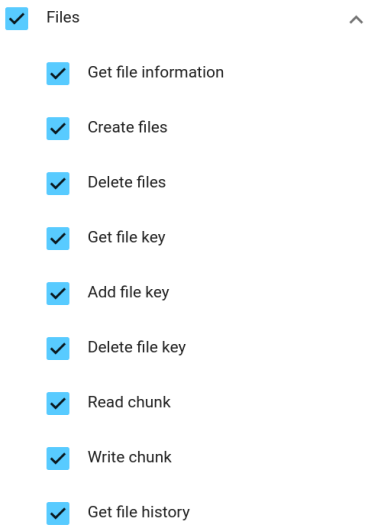
2.1.4 Editing a User

Selecting the icon will make the editing modal appear as shown below.



Basic User Information This edit modal offers a basic overview of the user including the email, the date/time the account was created, and whether or not the user is active.

User Permissions User permissions are broken up into different sections as shown below.

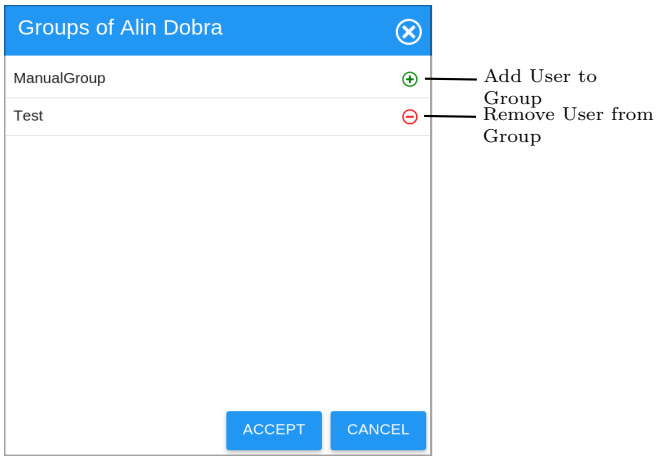


To add a permission, check the box next to permission name. To remove a permission, click the box again to make the check disappear.

Each permission type is broken down into specific actions to help customize permissions as much as possible per user. If the main permission box is checked, all the of the corresponding permissions inside will also be selected.

Escrow Key Parts If a user key has been escrowed, a list of all the escrow parts will be listed as well as the users that have access to them.

2.1.5 Managing User Groups



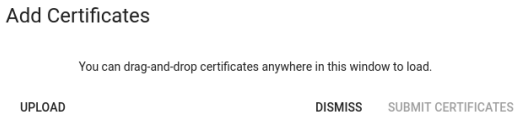
To modify user groups, select the icon. This menu will allow admins to add and remove users to groups they are apart of.

To add a user to a group, select the icon to the right of the group name.

To remove a user from a group, select the icon to the right of the group name.

To save all changes, select **Accept**.

2.2 Certificate Management



When selected, this will bring up a modal where certificates can be viewed and new ones can be added by selecting **Add**. Existing certificates will appear in a list with its type, the date uploaded, whether its valid and processed. To confirm all changes to the certificates, select **Submit Certificates** to exit.

2.3 Virtual Machine Management

The Virtual Machine management tab lets admins view all the virtual machines in the system, and information associated with them including owner, template, name, ID, Host Server, IP Address, and MAC Address. Admins also have the ability to shutdown any virtual machine by selecting the icon.

2.4 Drive Management

The drives tab allows a view of all the different drives in *tiCrypt* as well the owner and size of each drive.

2.5 Searching and Sorting

There are 3 types of sorting options available there are easily built into the existing managament tables.

2.5.1 Searching by Contains

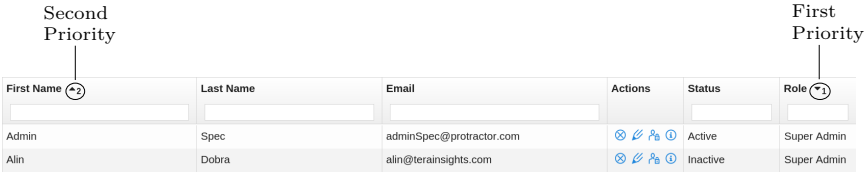
Any column that has a white input box below its name is able to be searched using letters and numbers. For example, by searching the letter ”a” in the name column, anyone whose name contains an ”a” will appear in the list. This search is not alphabetized or sorted.

2.5.2 Sorting Alphabetically/Numerically

To sort the columns by in this manner, simply select the bolded column name. Keep in mind, numbers in this search will come before letters when done in the ascending order (black arrow facing up). To switch the order to descending (black arrow facing down), simply select the bolded column name again. To unsort the list, select the bolded column name a third time, or until the arrow symbol disappears.

2.5.3 Sorting using Priority

tiCrypt also offers searching through its list using its own priority method. By holding shift and selecting a column name, this will number the column according to priority and sort the different columns with this numbers in mind. The priority number of the column will appear to the right of the column name. When selecting muliple columns and priorities, continue to hold down shift while clicking on each column name.



For example, you can sort users by role as first priority, and then name by second priority. This means that the users will be grouped by role, and then ordered alphabetically by name in each group.

To undo priority settings, click on the column name until the number has disappeared.

3 Admin Monitoring Tools

Super Admins and Admins have access to *tiCrypt* 's monitoring tools. This tools allows for visuals of different *tiCrypt* activities involving system:

- files
- directories
- groups
- sessions
- users

This monitoring tool is real-time and allows the information to be displayed in the forms of:

- gauges
- graphs
- tables

The interface also allows the graphs to be moved around and organized as desired using a grid system. The graphs will not move or close when navigating away from the Monitoring tab and will remain even after logging out.

3.1 Recommended Monitoring Tabs

Even with the correct tool, sometimes it can be difficult to understand the information needed to tell if a system is running correctly and safely. Here are some recommendations for useful groups of information, and what that information may mean.

1. File Transfers (Table Form)

   This graph will let the admin know how many Bytes/s of information is being transferred in the system at a given point in time. If this value is very large, this could indicate large amounts of data moving inside the system between users, which could amount to unwanted leaks of information or overaccess of information.

4 Key Escrow

Key Escrow is tiCrypt's way of protecting the recovery process of lost keys in the system. It works by essentially splitting up a user private key cryptographically into a specified number of parts and sending the peices to different escrow users. The default number of parts is 3, so this is the example value we will use to describe the system. Once the key is split up, the 3 pieces of the key are given to 3 different escrow groups, so each escrow group has a different part. Escrow users in tiCrypt are separated by groups, and groups may only receive 1 part of the escrowed key. This is done to avoid collaboration and malicious behavior between users of the same group.

4.1 Admin Role in Key Escrow

The admin plays a very crucial role in the Key Escrow process, including arguably the most important role, making sure the user's private key is escrowed.

The easiest way to streamline this process is to always escrow a user's private key when first activing their account in *tiCrypt* .

4.1.1 Escrowing User Keys

To escrow a user's private key, select the icon next to the user's name in the **Managament** tab. In the editing modal, check the **Escrow on next login** option.

To see this option, the user must be an active user.