# Tresorit Best Practices User's Guide

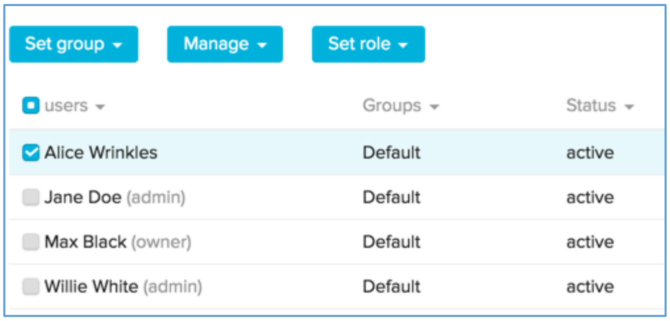
**INTRODUCTION** - Compared to most cloud sync and share services Tresorit is relatively easy to implement and use. However, important details can be missed that affect Tresorit's performance, and potentially your satisfaction with it. This guide is intended to highlight these details to assure that your implementation of Tresorit best meets your needs.

**GETTING ORGANIZED** – Many users of Tresorit are migrating from services like Dropbox, or from an internal server. In both instances, we recommend copying existing folders to a new location on your laptop or desktop, before syncing them to the Tresorit cloud.

Even though your Dropbox folders may already be synced to your computer, it is necessary to copy them into new or different folders on your computer. This is particularly important if you plan to close your Dropbox account. Do not attempt to sync Dropbox folders directly to Tresorit as performance is likely to be poor; this approach can also compromise the security of your data.

Syncing folders from a network drive or file server can also be problematic and is not recommended. However, if your file server runs a Tresorit supported operating system (Windows, OS X or Linux), you can install the Tresorit client app on it, and directly sync your folders from the files server to Tresorit.

**USERS and MEMBERS** - *Users* are individuals under your Business account who are managed from your Admin Center, under USERS and DEVICES. We recommend adding users to the Admin Center before sharing any tresors with them; this will assure they register as Business users first.

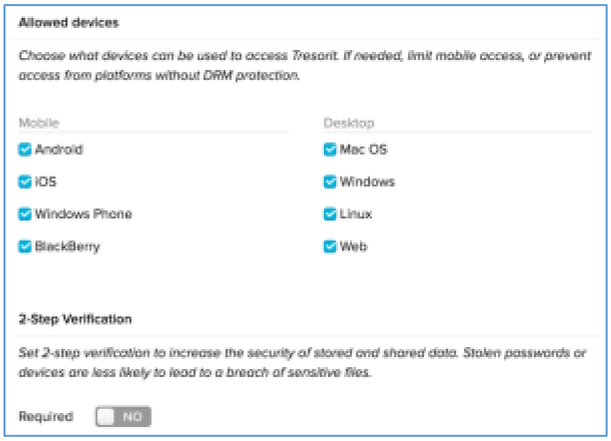


| ■ users ▾ | Groups ▾ | Status ▾ |
|---|---|---|
| ☑ Alice Wrinkles | Default | active |
| ☐ Jane Doe (admin) | Default | active |
| ☐ Max Black (owner) | Default | active |
| ☐ Willie White (admin) | Default | active |

*Members* are individuals with whom you share your tresors; they may be outside your account or under it.

Adding users to your Admin Center does not provide them access to any of your tresors, it only provides those users with access to a Tresorit for Business account. The sharing of your data is separate and managed exclusively from each tresor.

The key benefit to having users in your Admin Center is that you can monitor their activity, while controlling what they can, and can't, do. For example, under GROUPS and POLICIES, you can restrict devices used to access Tresorit, enforce 2-Step Verification, setup IP filters, turn off the ability to create Encrypted Links, deactivate "Remember me," turn-off Sharing, prevent tresor creation, deactivate synching, and enforce Timeout policies. New settings are regularly being added to GROUPS and POLICIES, so be sure to familiarize yourself with this aspect of Tresorit.



**Allowed devices**

*Choose what devices can be used to access Tresorit. If needed, limit mobile access, or prevent access from platforms without DRM protection.*

| Mobile | Desktop |
|---|---|
| ☑ Android | ☑ Mac OS |
| ☑ iOS | ☑ Windows |
| ☑ Windows Phone | ☑ Linux |
| ☑ BlackBerry | ☑ Web |

**2-Step Verification**

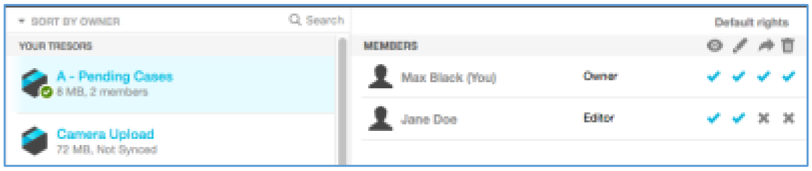
*Set 2-step verification to increase the security of stored and shared data. Stolen passwords or devices are less likely to lead to a breach of sensitive files.*

Required: NO

Once a policy is created under GROUPS and POLICIES you can assign it to individuals in your account under USERS and DEVICES. For every user there can be a unique policy. The rules set up under GROUPS and POLICIES can be changed at any time.

Additionally, from the Admin Center you can remove and add users as needed, and within seconds. If a user loses a device, you can remove their account by unlinking it; this immediately results in the account being logged out. For mobile devices removing a user also performs a remote wipe, deleting all locally stored files.

**SHARING** – Secure sharing is a central feature of Tresorit's service. As sharing is managed from tresors (the secure folders you create or drag into Tresorit), it is important to think about the people you will be sharing with before creating your tresors.



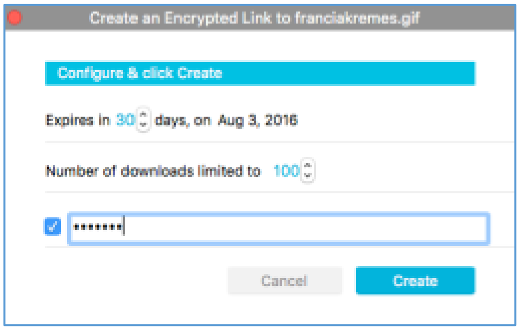
A - Pending Cases
8 MB, 2 members

Camera Upload
72 MB, Not Synced

| MEMBERS | | Default rights | | | |
|---|---|---|---|---|---|
| Max Black (You) | Owner | ✓ | ✓ | ✓ | ✓ |
| Jane Doe | Editor | ✓ | ✓ | ✗ | ✗ |

Sharing cannot be differentiated at a sub-folder level. In order words, all the folders and files you store in a tresor can be viewed by everyone with access to that tresor. Tresorit will be introducing functionality to address this limitation in a future release. If you think this limitation may present a problem, we recommend reorganizing your folder structure to accommodate your sharing requirements.

The good news is that Tresorit works dynamically by allowing you to select folders from any location on your computer to convert into tresors. In other words, unlike Dropbox, you do not need to place all folders into one central managed folder on your computer.



Create an Encrypted Link to franciakremes.gif

Configure & click Create

Expires in 30 days, on Aug 3, 2016

Number of downloads limited to 100

☑ •••••••

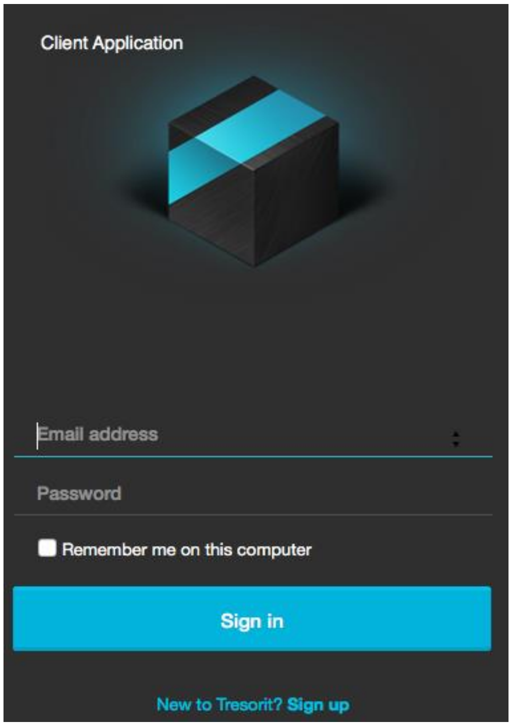
**ENCRYTED LINKS** – The simplest form of sharing with external, as well as internal, parties is by using Encrypted links. Once the Tresorit app is installed on your computer, any file (up to 1 GB) can be converted to an Encrypted Link. Encrypted Links can be password protected and limited in time and number of downloads. For added security, Encrypted Links can also be revoked at any time; this permanently cancels the Link and prevents it from working.

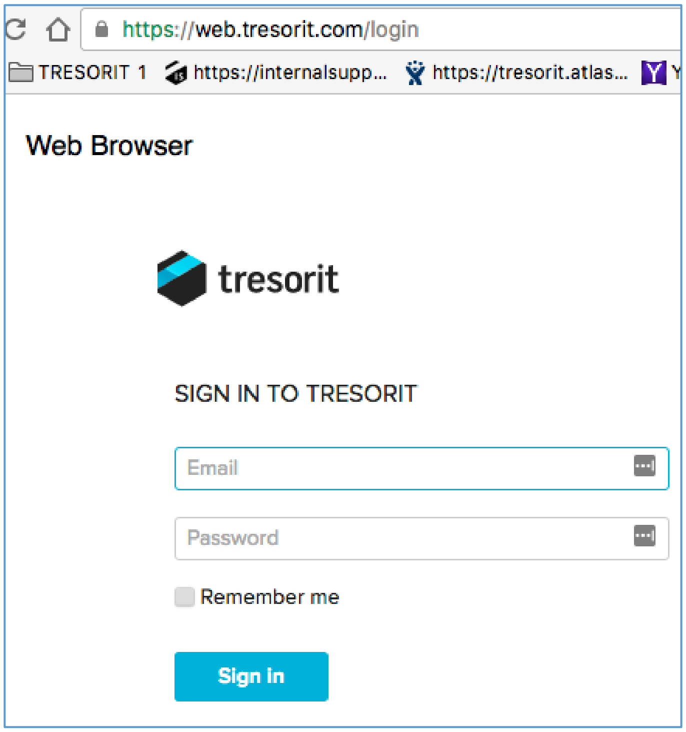
**ENCRYPTION, CONTROL and ZERO-KNOWLEDGE –** Prior to being compressed and synced to the cloud all tresored files are encrypted. This is an automatic function that is universally applied to all files in Tresorit. Unlike add-on solutions of other services, users of Tresorit do not have to activate encryption. Additionally, files *always* remain encrypted while transported and stored in the Tresorit cloud, until they are synced or downloaded to another device – either one of your own or with someone you are sharing – or to a supported browser. This is called client-side or end-to-end encryption. Legacy cloud storage and collaboration service, like Dropbox, work differently as they decrypt and then re-encrypt files at various times while managing them. This makes your data vulnerable and could result in it falling into the wrong hands.

Another key aspect of Tresorit's security and control policy is **Zero-knowledge**. Zero-knowledge means passwords are never stored in the cloud where they could be accessed by a hacker or wayward administrator.

Tresorit does not offer **local encryption** but highly recommends implementing it. Since the release of Windows 7, Microsoft has included BitLocker with its operating system. For Mac users, FileVault has been available since OS X 10.3 was released. Even if you are not syncing tresors, local encryption protects against the leakage of files that are cached temporarily when using Direct File Open.

**CLIENT APP** and **WEB ACCESS** – Tresorit runs as an application on your computer and mobile devices, and also in available via your browser (see supported versions here). For maximum performance and functionality, we recommend installing the Client App. After being added to your Admin Center, or as an external shared party to your tresor, users only need to go here to set up their account: web.tresorit.com/signup. Afterwards, they can download the Tresorit Client App from the Web Access page, once logged in or from here: https://tresorit.com/download.


Client Application
Email address
Password
Remember me on this computer
Sign in
New to Tresorit? Sign up


https://web.tresorit.com/login
TRESORIT 1
https://internalsupp...
https://tresorit.atlas...
Web Browser
tresorit
SIGN IN TO TRESORIT
Email
Password
Remember me
Sign in