FAQs

Viivo accounts are always created on your device, and not in your web browser. As a company, our number one priority is keeping your data secure. When you create your Viivo account, public and private keys are generated to secure your private data and files. Because your account is created on your device, the chances of your data being prone to attack and exploitation are next to none. We have designed our system so that any account information that is stored in our servers is nearly impossible to retrieve by anyone other than you.

Simply put, a Locker is a folder that you want to protect: all files placed in this folder will be automatically encrypted. By default, you can have up to 5 Lockers enabled. If you are a Viivo Pro user, there is no limit to the number of Viivo Lockers you can set up.

Learn more about Viivo Lockers.

In short, Viivo offers secure support for Microsoft Windows 7 and 8, Mac OS X 10.7 and 10.8, iOS 6.0 and later, and Android 4.0 and later.

See a full list of supported operating systems and platforms.

The next step is to choose your cloud provider so you can begin securing your data. To secure your files, you need to move your data in the cloud to a Viivo-encrypted folder. The second you move them to the folder, your files will be encrypted. In some cases, you will see your files in the Viivo secure files, as well as the regular cloud files. (Not to worry, most providers will erase any copies after 30-to-90 days.)

Make sure to remember your password. It is impossible for anyone on the Viivo team to "reset" a password, if forgotten. If you do forget your password, you are at risk of unrecoverable data loss. It is only possible to reset a password through a desktop client that has previously logged into your account.

Recovery requires two keys. One key lives on our server and the other lives on your device. Having access to only one is not enough to recover. You need both.

Passwords are only recoverable from a previously authenticated device. These devices store a recovery code on our server that can be retrieved at a later time. If requested, the code is emailed and can be used by the client to decrypt your password that has been stored locally in CAPI (Windows) or the Keychain (Mac). Once a new password has been set, all devices must generate new recovery codes and be re-authenticated

Yes. Viivo 3.0 on desktop and 3.0 on mobile support Google Authenticator.

Learn more about MFA with Viivo.

Viivo uses FIPS (Federal Information Processing Standards) 140-2 validated cryptographic algorithms for encryption and decryption operations on Windows, Mac and iOS. On Android, while we still use 256-bit AES encryption, though we plan to cover FIPS compliance on that operating system soon. Viivo uses NIST Validation Certificate #1330 which was validated in 2010 with Microsoft Windows Enhanced Cryptographic Provider. For Mac and iOS we use NIST Validation Certificates #1964 and #1963 respectively.

As long as you have a valid subscription, you are entitled to upgrade to the latest version on all of your devices. Your client will automatically check for new versions periodically.

Get the latest version of our software.

Your Viivo account is "Entitled" for features based off which account level you have purchased. Instead of license keys or activation codes, we use the entitlement system to differentiate between the different versions of Viivo (Free/Pro). Some editions are entitled to features above and beyond what you get for Free (Like Customer Support for example)

Infrequently, new features are released through entitlement updates instead of client software upgrades

Yes, but you can only have one account per Viivo user profile.

Install Viivo on that computer and log in. Viivo will automatically initiate a key transfer to the new device once you have authenticated it.

Install Viivo onto the computer and log in. Viivo will automatically entitle the new device for the features you have purchased.

We're all about security. Because of this, we take the client-side encryption and signing approach. Any attempt to attack our servers would not impact you or your data.

No. Viivo does not need or ask for your account information for any cloud storage provider. Actually, we want you to use a different password for your Viivo account than you use for your cloud account. (Just a security suggestion – it's a good habit to do this for all accounts and passwords.)

We are currently running on iOS and Android phones across the country. Currently, we only offer decryption on mobile. Additional mobile and security features are planned for upcoming Viivo updates.

Viivo capabilities like encryption and compression work for all the major public clouds, including Google Drive. See a quick demo on how to secure and share your files in Google Drive.

One of the great things about Dropbox is the ability to easily share folders. You can share your Viivo encrypted files just as easily. Here are the steps you need to take:

1. Go to Dropbox.com and navigate to the Viivo-encrypted folder.
2. Right click on the sub-folder you wish to share and choose "Invite to Folder."
3. Once your invitee accepts, their copy of Dropbox will download the secured files.
4. Your invitee will need to install Viivo on their device in order to begin decrypting the files.
5. A request will be sent to you that must be approved before the files can be decrypted.

Yes. This way, your data is both secured with encryption and received by another person (or people) whom you've authorized.

If a Viivo user encrypts a file for an email address that is not yet associated with a Viivo account, Viivo will create temporary keys for that user and then will hand them off to that user once the account is created and email-verified. During this time, the server can technically decrypt the keys (Although of course it does not have the data itself).

Once the user creates his/her account, then the server re-encrypts those keys for the new user, using his/her new public key.

If you want to resume a zero-knowledge posture in our servers, you can still achieve that even at this point. You can deny the user, and then allow him /her again, which will generate entirely new keys which the server will never have seen before. In this case, the server will have no knowledge of keys being used on future encryptions. Then force a re-encryption of all data with the new keys. The easiest way to do this is in a “Synced” locker: move the data out of the decrypted folder to a temporary folder. Let the Viivo app remove the encrypted files from the Encrypted folder (usually in the cloud). Then move the files back into the decrypted folder. This will then cause re-encryption.

After issuing new keys and new encryptions, the server no longer has access (even theoretically) to any keys you’re using. This feature (pre-allow with forwarded keys) is only offered as a convenience. The preferred workflow is that the participants ask for access after they’ve created the account. The Viivo software automatically requests access if the new participant tries to read a document he/she has no access to. The owner gets an email telling him the participant has an account and wants copies of the keys for a particular document or folder. This is the preferred method and the best way to ensure our servers have zero-knowledge of your active keys

> Viivo secures your documents before they are synchronized to your Dropbox, Box, Drive and OneDrive. Our servers never see copies of your data or your passphrase. You have the keys to securing the data, not the cloud provider. Viivo security uses industry standards such as RSA 2048 and AES-256 to lock down data regardless of hackers, data snoopers or mistakes.
>
> Learn more about how our security works.

For security reasons, we do not currently expose a facility to delete your account. To stop using your account you can simply remove it from your devices (once you’ve verified all of your data has been decrypted).

Cancel your support subscription.

The path is quick and easy, but depends on your operating system.

Read our support forum's migration guide to use the latest edition of Viivo.

Viivo comes from PKWARE, the security and performance provider with a track record in innovation going back to the creation of the ZIP file standard in 1986. Viivo and other PKWARE software is in use by more than 30,000 businesses for billions of critical documents every day.