

FAQ

- **Q: Why does the Fingerprint Software not register my fingerprints?**
 - *A: This can happen if your finger is too dry. Moisten your finger and try again.*
- **Q: How many users can the software register?**
 - *A: The Fingerprint software has been tested with up to 15 user accounts and may support more.*
- **Q: Is the password in the Fingerprint Software the same password as the Windows password?**
 - *A: Yes, the password must be the same as the windows password.*
- **Q: What is the Administrator account of the Fingerprint Software?**
 - *A: The account under which the Application was initially installed.*
- **Q: Can one user of the Fingerprint Software delete another user account?**
 - *A: No, although the administrator account can uninstall the software completely.*
- **Q: What will happen to the secured data if the Windows account is deleted?**
 - *A: If an administrator deletes the user from Windows User Accounts all that user's encrypted files, folders, and secure drive will inaccessible.*
- **Q: Can the administrator account access files or folders encrypted by other user accounts?**
 - *A: No, the only one who can access an encrypted file or folder is the encrypting user.*
- **Q: Can I still access the computer if I lost my Personal Security Mouse?**
 - *A: Yes, your account password will allow you to bypass any fingerprint prompts and access all Personal Security features.*
- **Q: What happens if the Personal Security Mouse is not connected to the computer when booting up the system?**
 - *A: The application will give you the choice of connecting the mouse or logging on with your password*

- **Q: Can I access my Secure Drive with a different fingerprint security device?**
 - *A: Only another IOGEAR Personal Security mouse will have access to the Secure Drive.*

- **Q: How big is the Secure Drive?**
 - *A: The default value is 128MB and the maximum size is 2GB.*

Notes:

If a user encrypts a shared folder the folder is not identified as encrypted, and none of the sub folders are marked as encrypted, they can be opened, and the names read, but all files in the folder are marked as locked and can only be opened by the user who encrypted it.

A non-encrypted file moved to an encrypted folder will be encrypted as the logged on user, and cannot be decrypted by anyone else.

An individual user cannot be removed from the application, the entire application must be uninstalled and reinstalled. Unless you have first decrypted all files and folders, the encrypted data will be lost.

Only the Administrator account can remove the fingerprint application

If you remove a user from “User Accounts” in Control Panel, that users Secure Virtual drive remains, and cannot be accessed even if you re-add the user.

If there is an existing P drive mapped, the secure virtual drive will default to the next available drive letter.

If an encrypted folder is moved to a different partition (as in a dual boot system, or across a network) the file remains encrypted and cannot be decrypted until it is returned to the partition and user who encrypted it

If you logon as user “A” you cannot encrypt or decrypt as user B, even if user B tries to use his/her fingerprint.

If the mouse is not connected or fails when the computer boots, you will be prompted to use the password log on. All other security features will also give you the password option.