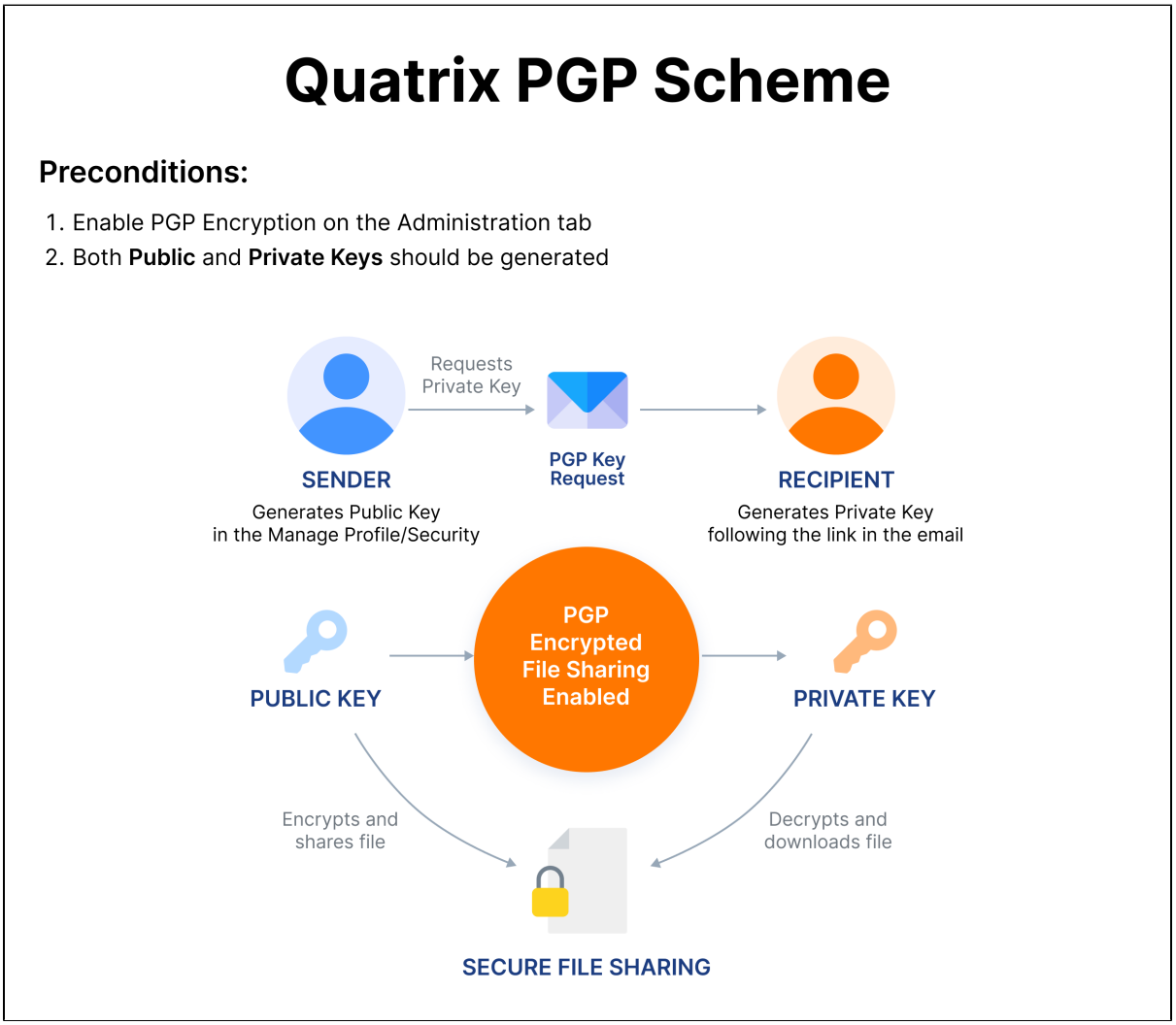
PGP encrypted file transfer

- PGP Key Generation
  - Public Key Generation
  - Private Key Generation
- Encrypting and Decrypting Files

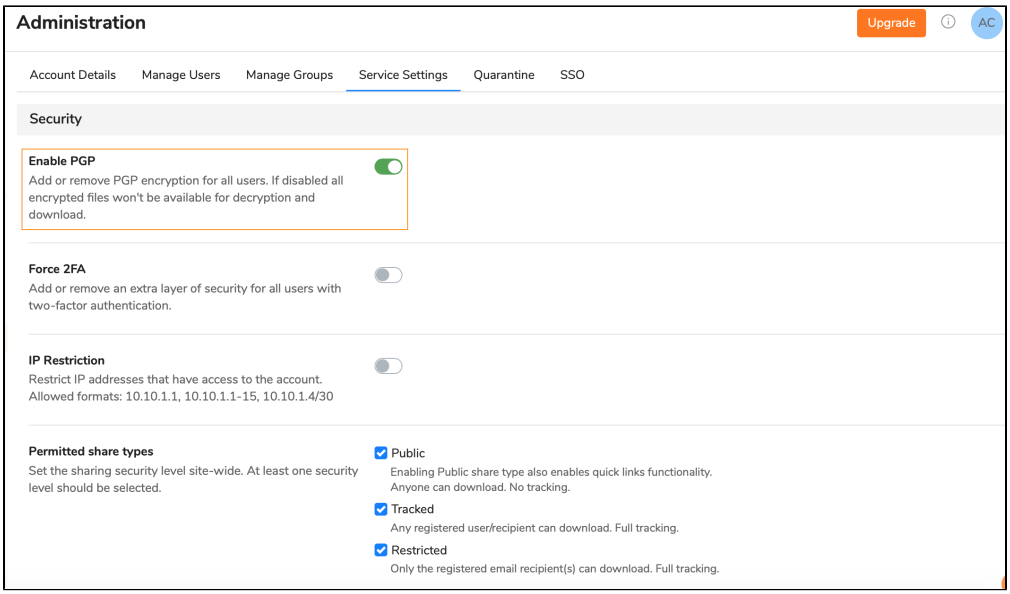
PGP (Pretty Good Privacy) is a protocol that is used for encrypting and decrypting files using a key pair. If you need to be certain that no one (really, no one) except the intended recipient can decrypt your confidential files, you may use PGP encrypted file transfer.

The diagram below displays how PGP works in Quatrix. It uses one key to encrypt the file (the public key) and another to decrypt (the private key) which traditionally makes it much more cumbersome to use than standard levels of encryption. But despite being cumbersome PGP is still a universally-accepted standard for file encryption.



Enable PGP encryption

The account owner or administrator can enable or disable PGP for the account on the Administration tab.



As soon as PGP is activated, all users can share PGP encrypted files, besides contacts that can only decrypt, download and return encrypted files.

> If you disable PGP, all encrypted files won't be available for decryption and download.

PGP Key Generation

To proceed with encrypted file sharing you need to check if private and public keys are generated.

As illustrated in the diagram above PGP uses a pair of keys - the public key locks; the private key unlocks. So when sharing files with your users or contacts you'll be encrypting with their public key and when you are acquiring files from your users the files get encrypted with your public key.

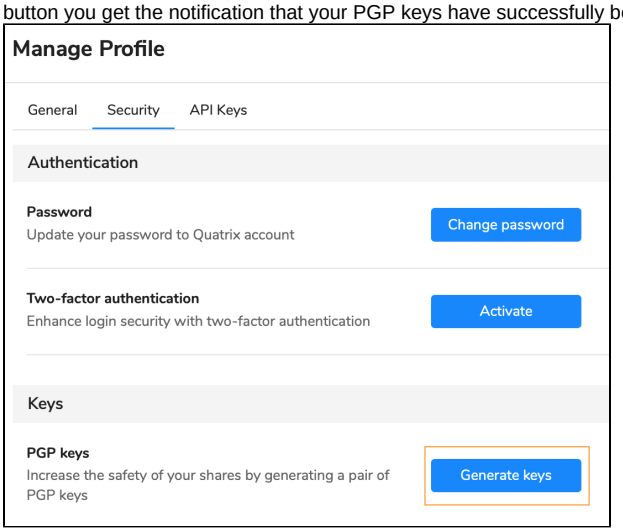
> Key Security
>
> Your keys are securely stored on the Quatrix platform, additionally all private keys are encrypted using your passphrase. The passphrase is not stored or remembered by Quatrix which gives you peace of mind that no one (and that includes Quatrix staff), can ever decrypt files in transit or at rest.

Public Key Generation

You should generate public keys at first - follow 3 simple steps below:

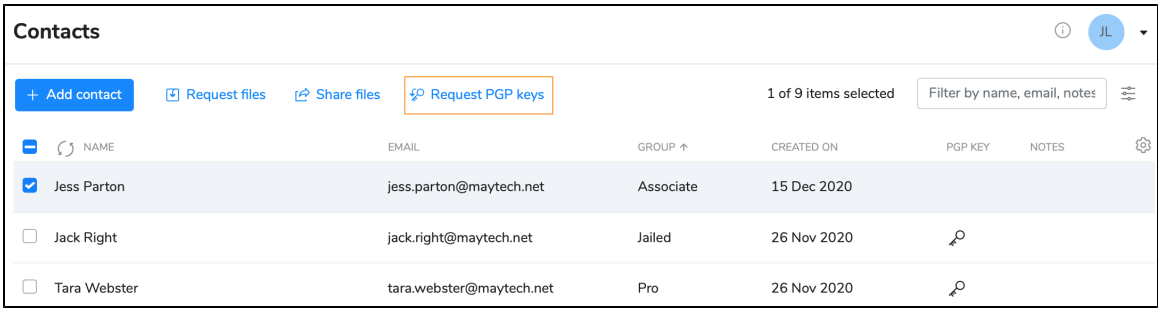
1. Click on the link with your name at the top right and follow the Manage Profile link.
2. Open the Security sub-tab.

3. Click on the Generate Keys button which opens the window for creating the passphrase for your keys. After clicking on the Generate keys button you get the notification that your PGP keys have successfully been generated.



and then request another pair of keys from the intended recipient - send PGP key generation request.

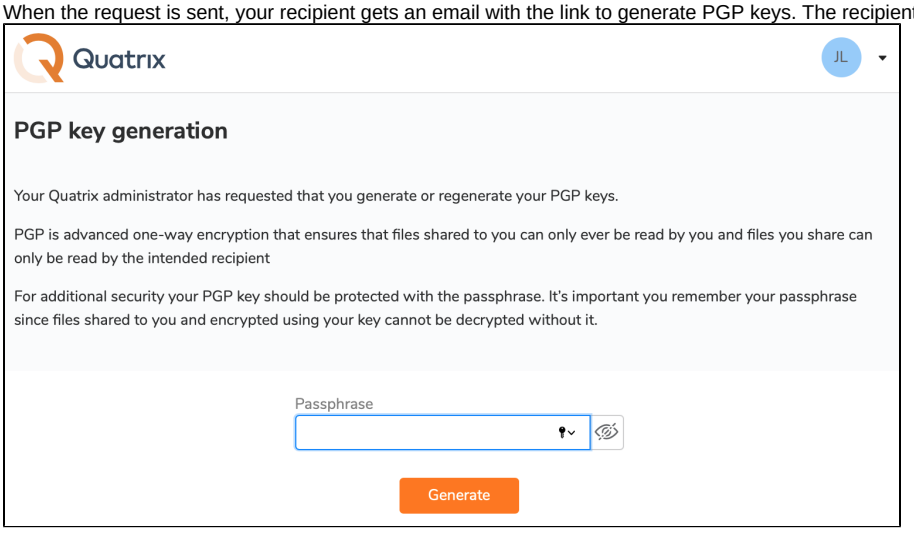
You should determine who you are going to share encrypted files with, tick the boxes next to them either on the Contacts**,** or on the Administration tab and select the Request PGP keys button from the top menu.



Besides you can send the request while adding your contacts by ticking the Request PGP keys check box.

Private Key Generation

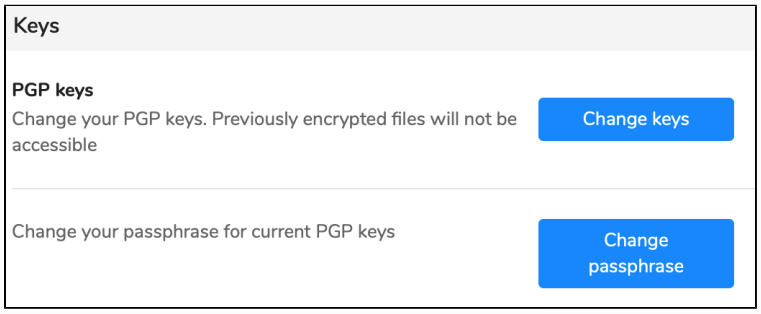
When the request is sent, your recipient gets an email with the link to generate PGP keys. The recipient follows the link and generates PGP keys.



Once PGP keys are generated, a confirmation email will be sent to the sender of the request.

Changing PGP Keys vs Passphrase

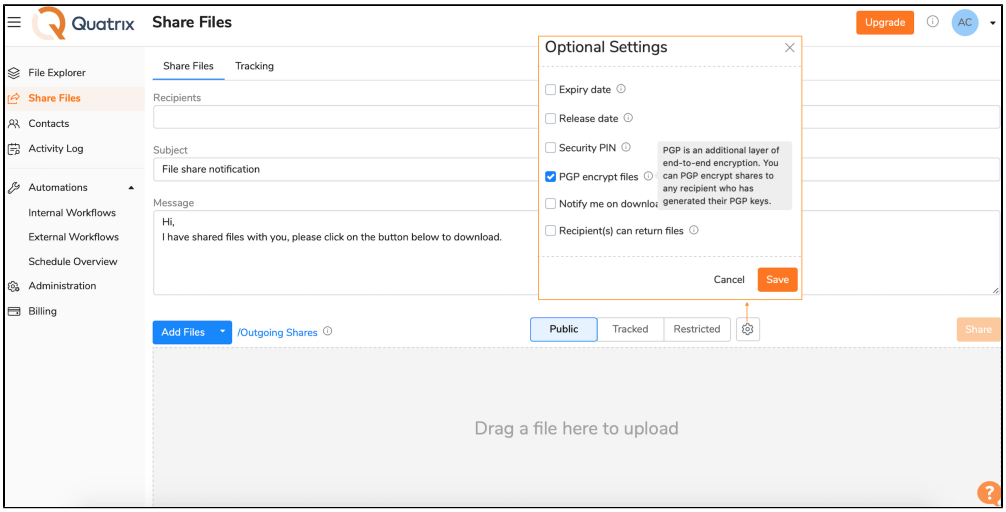
Your PGP keys can be changed at any time on the Security sub-tab, but all previously encrypted files won't be accessible as they were encrypted with the different PGP keys. If you noticed that your passphrase was compromised, you can simply change the passphrase to your keys by clicking on the Change Passphrase button. This preserves you the right to decrypt all previously encrypted files.



Encrypting and Decrypting Files

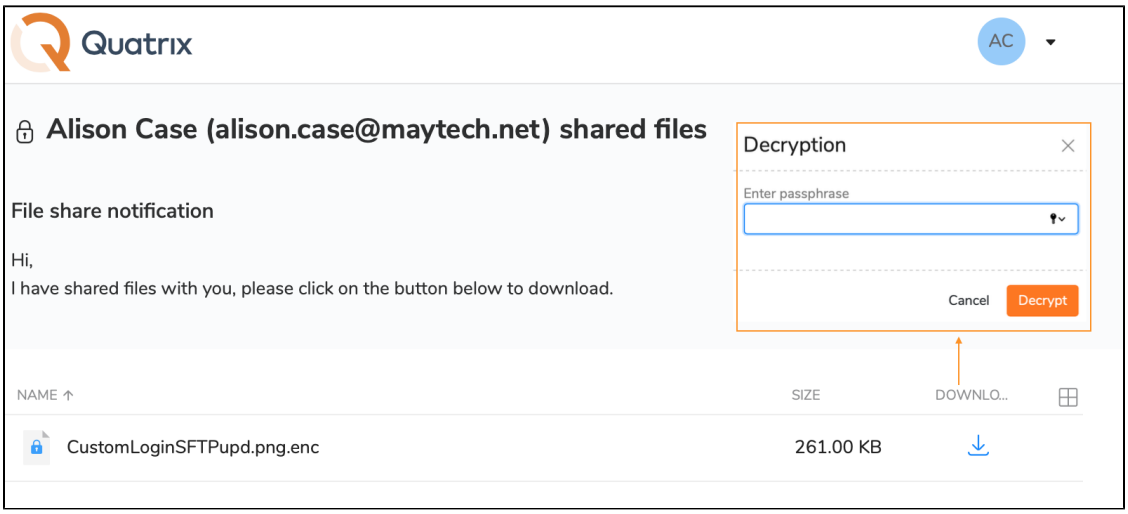
Encrypting files is a way to protect them from unwanted access. There are a few simple steps to share and acquire files with advanced PGP security in Quatrix.

To share encrypted files you should select the PGP encrypt files check box on the Optional Settings section while sharing files.



If your recipient hasn't generated PGP keys, the email will be highlighted in red and you will be notified of missing keys. You should request keys from your recipient on the Administration or Contacts tab to proceed with encrypted file sharing.

You can easily decrypt files by following the Download link from the email and entering the passphrase while downloading files. You can store your files locally or on Quatrix cloud.



If you forgot your passphrase, you won't be able to decrypt shared files! To proceed with encrypted file sharing you need to change your PGP keys on the Security sub-tab.