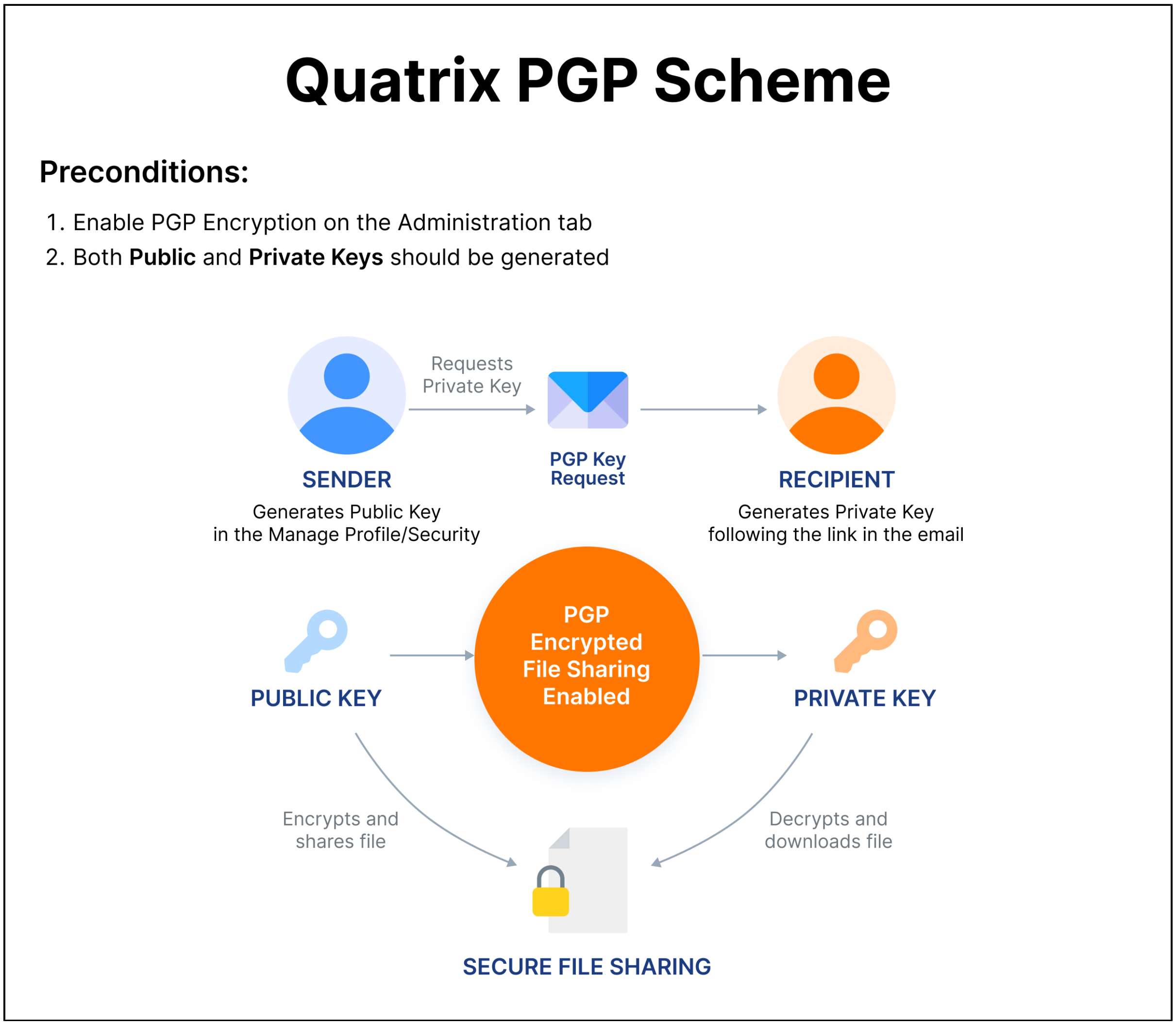
PGP encrypted file transfer

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.



Quatrix PGP Scheme

Preconditions:

1. Enable PGP Encryption on the Administration tab
2. Both **Public** and **Private Keys** should be generated

Requests Private Key

PGP Key Request

SENDER

Generates Public Key in the Manage Profile/Security

RECIPIENT

Generates Private Key following the link in the email

PUBLIC KEY

PGP Encrypted File Sharing Enabled

PRIVATE KEY

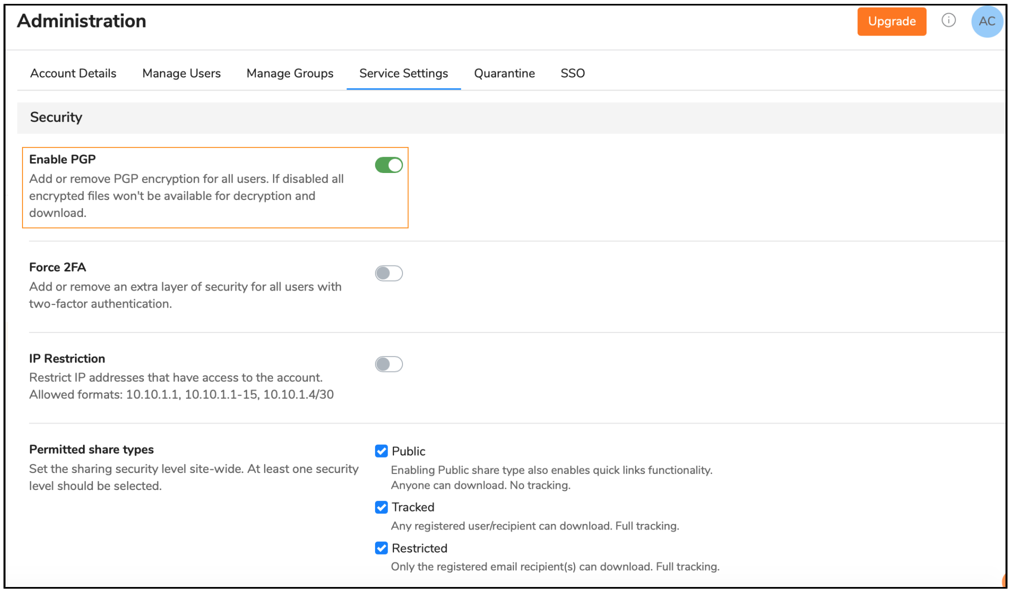
Encrypts and shares file

Decrypts and downloads file

SECURE FILE SHARING

Enable PGP encryption

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



Security

Enable PGP ●
Add or remove PGP encryption for all users. If disabled all encrypted files won't be available for decryption and download.

Force 2FA ○
Add or remove an extra layer of security for all users with two-factor authentication.

IP Restriction ○
Restrict IP addresses that have access to the account. Allowed formats: 10.10.1.1, 10.10.1.1-15, 10.10.1.4/30

Permitted share types
Set the sharing security level site-wide. At least one security level should be selected.

☑ Public
Enabling Public share type also enables quick links functionality. Anyone can download. No tracking.

☑ Tracked
Any registered user/recipient can download. Full tracking.

☑ Restricted
Only the registered email recipient(s) can download. Full tracking.

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.

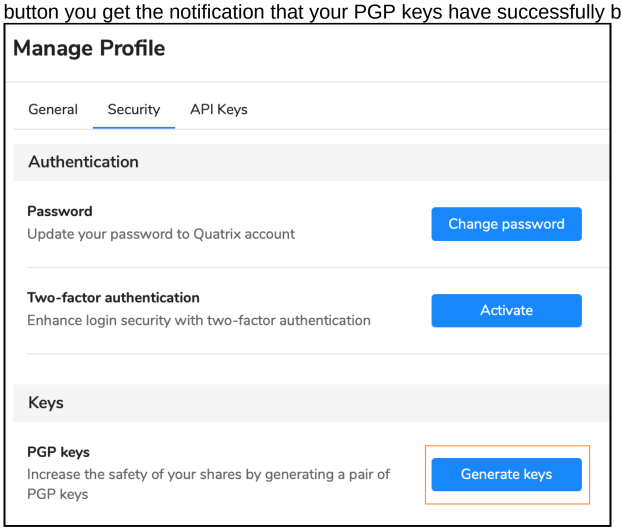
> Key Security
>
> Your keys are securely stored on the Quatrix platform, additionally all private keys are encrypted using your passphrase. The passphrase is not stored or remembered by Quatrix which gives you peace of mind that no one (and that includes Quatrix staff), can ever decrypt files in transit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



Manage Profile

Authentication

Password
Update your password to Quatrix account

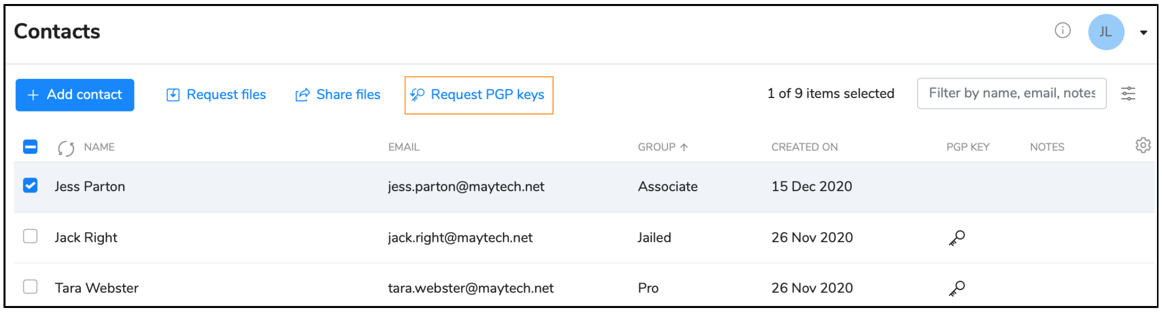
Two-factor authentication
Enhance login security with two-factor authentication

Keys

PGP keys
Increase the safety of your shares by generating a pair of PGP keys

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.



Contacts

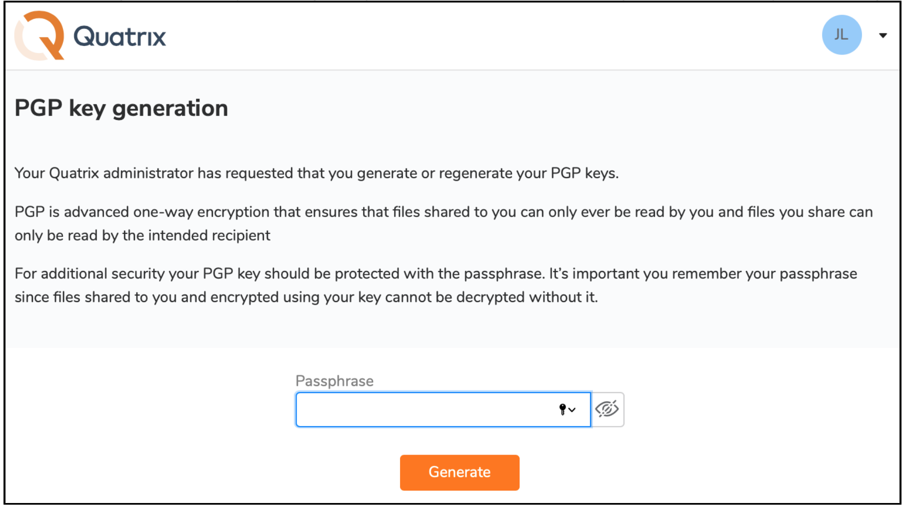
1 of 9 items selected

▬	NAME	EMAIL	GROUP ↑	CREATED ON	PGP KEY	NOTES
☑	Jess Parton	jess.parton@maytech.net	Associate	15 Dec 2020		
□	Jack Right	jack.right@maytech.net	Jailed	26 Nov 2020	🔑	
□	Tara Webster	tara.webster@maytech.net	Pro	26 Nov 2020	🔑	

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.



PGP key generation

Your Quatrix administrator has requested that you generate or regenerate your PGP keys.

PGP is advanced one-way encryption that ensures that files shared to you can only ever be read by you and files you share can only be read by the intended recipient

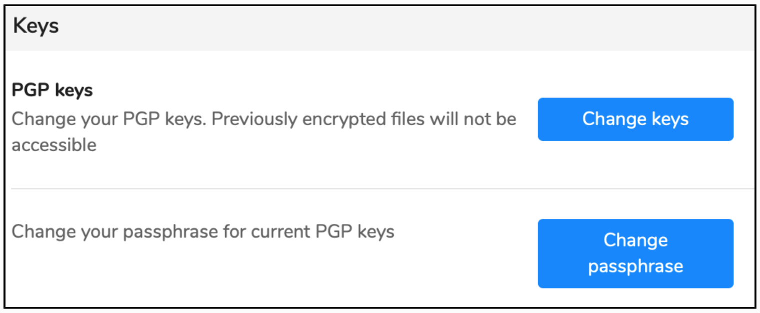
For additional security your PGP key should be protected with the passphrase. It’s important you remember your passphrase since files shared to you and encrypted using your key cannot be decrypted without it.

Passphrase

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.



Keys

PGP keys

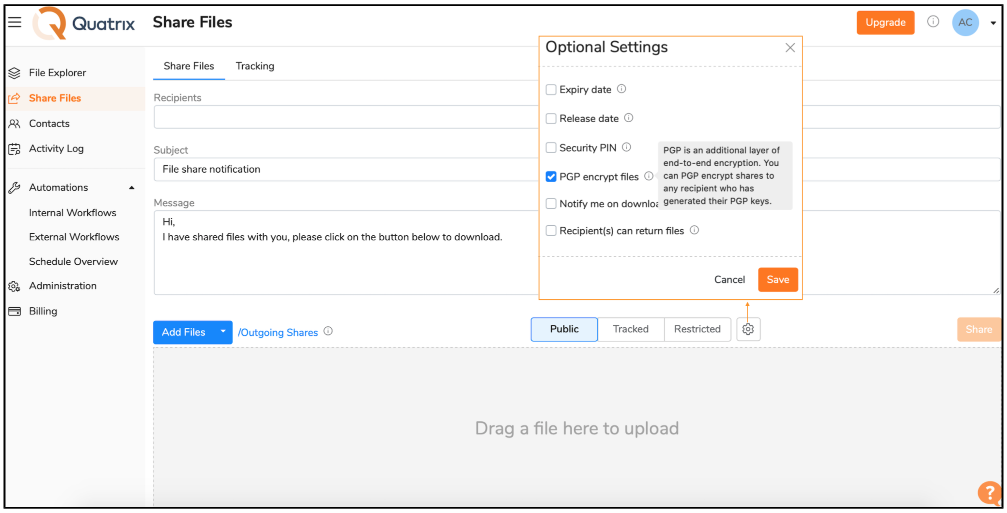
Change your PGP keys. Previously encrypted files will not be accessible

Change your passphrase for current PGP keys

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.



Share Files

Subject: File share notification

Message:
Hi,
I have shared files with you, please click on the button below to download.

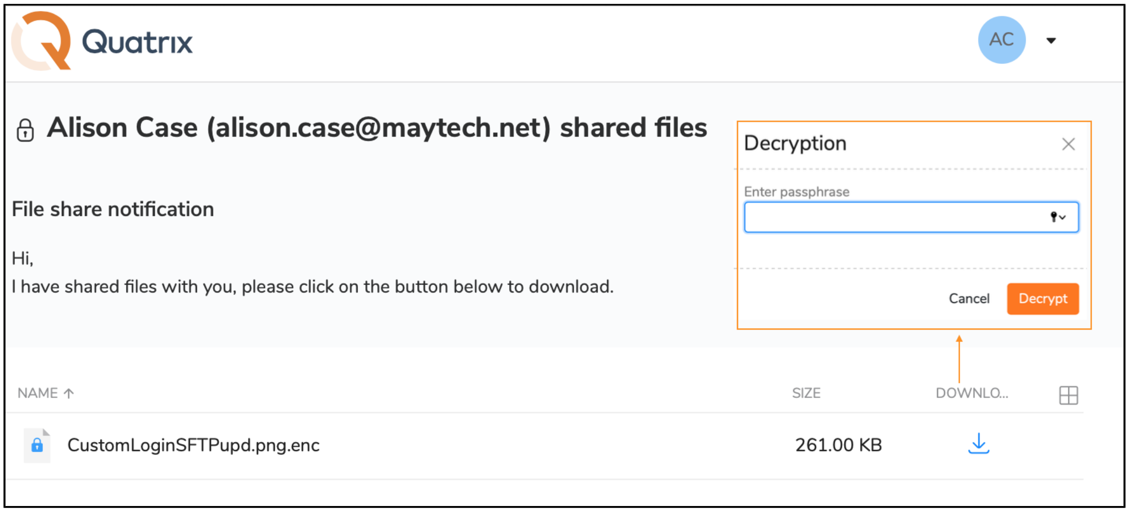
Optional Settings

□ Expiry date
□ Release date
□ Security PIN
☑ PGP encrypt files
□ Notify me on downloa
□ Recipient(s) can return files

PGP is an additional layer of end-to-end encryption. You can PGP encrypt shares to any recipient who has generated their PGP keys.

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.



🔒 Alison Case (alison.case@maytech.net) shared files

File share notification

Hi,
I have shared files with you, please click on the button below to download.

NAME ↑	SIZE	DOWNLO...
CustomLoginSFTPupd.png.enc	261.00 KB	

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.