



Security & Privacy Brief

Introduction

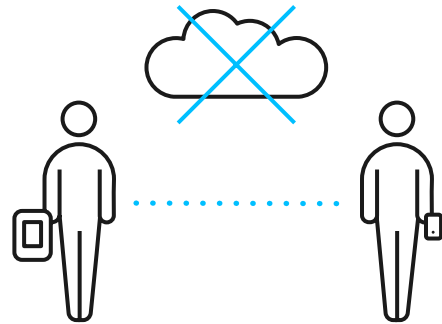
Security and privacy are two of the leading issues for users when transferring important files. Keeping data on-premises makes business and IT leaders feel more secure, but comes with technical challenges when there is a need to share data externally. If your employees can't easily use your secure tools, they'll resort to less secure options.

Sync offers the ability to sync files securely and privately, by replicating data only directly between trusted devices and keeping data encrypted in transit. This means that Sync neither hosts nor caches any content - there's no way for us (even if we wanted to) to view, modify, or remove data. All control rests within your devices (and those of others you choose to share with).

This brief explains the security and privacy attributes and features of Sync. Our product and engineering team is led by folks from Decru (NetApp), EMC, ZoneLabs and Check Point: security and managing data is in our DNA.

Files move directly between peers - no data lives in the cloud

Instead of uploading files to cloud storage so other devices can download them, Sync establishes a direct connection between your devices (peers), allowing data to exist at rest exclusively on private infrastructure.



By default, Sync will try to do this using multiple methods (defined later). One of them is the Tracker Server, which allows peers to find each other over the Internet or between subnets on the LAN that block multicast.

If peers cannot establish a direct connection between themselves (like when devices are behind a symmetric NAT), the Relay Server is used. Sync is very successful at establishing a direct connection, with more than 97% of all data transferred is directly from peer-to-peer. In the event that the Relay Server is used, only 128-bit AES encrypted pieces flow through it. These pieces are never stored at rest and the encryption keys are only possessed by the peers connected to the folder.

Sync is a fully distributed system – all data remains private

Sync keeps ALL your data (files, metadata, user information) private because it's a fully distributed system. Instead of the control functionality living in the cloud, it's handled by the peers themselves. No information about you, your devices, or where your files are going is stored on any server. Each peer learns information like what to send/receive by interacting with other peers and information like access control and licensing is synchronized between peers.

There are no passwords to be compromised – all security is cryptographic

Sync's security model is cryptographic instead of password-based. Cryptographic verification is required for peer introduction, and data access. All data is further encrypted in transit. Because of this there is no need to worry about insecure passwords, changing passwords or users writing passwords on post-it notes so they don't forget.

Sync offers two security models for folders: Standard and Advanced. The Standard one is appropriate for device-based permissions while the Advanced one is good for user-based permissions.

Device-based permissions - Standard folders

With these folders, each folder is associated with a few symmetric keys. When a folder is initially added to Sync a read/write (RW) key is created. Using a cryptographic hash function we derive a read-only (RO) key and a Folder ID. Having the RW key allows peers to modify the folder. Peers with RO key are cryptographically prevented from making any modifications to content on remote peers. The Folder ID is only used to locate peers that are connected to this folder and cannot be used to access the content.

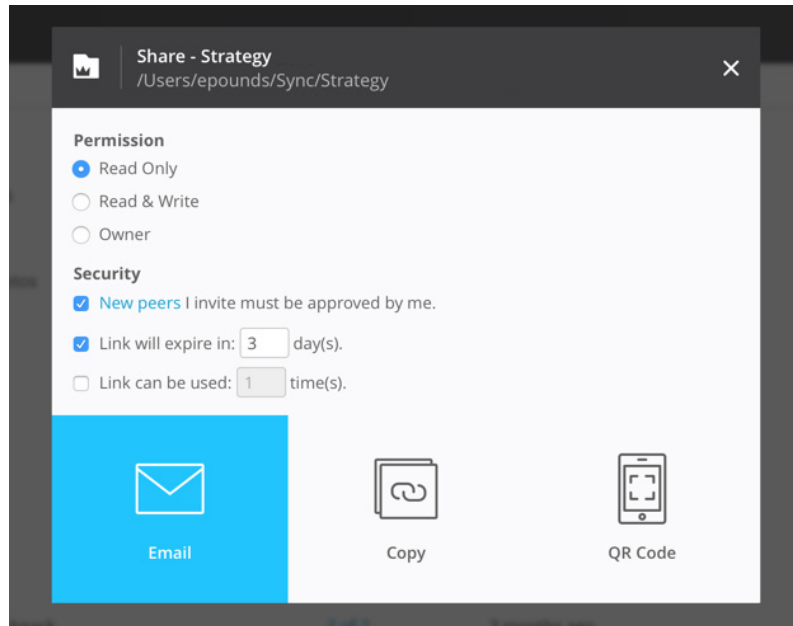
This model is ideal for syncing content between devices. It provides for fast initial connection and better overall transfer speed. It is also very easy to connect additional devices to such folders.

User-based permissions - Advanced folders

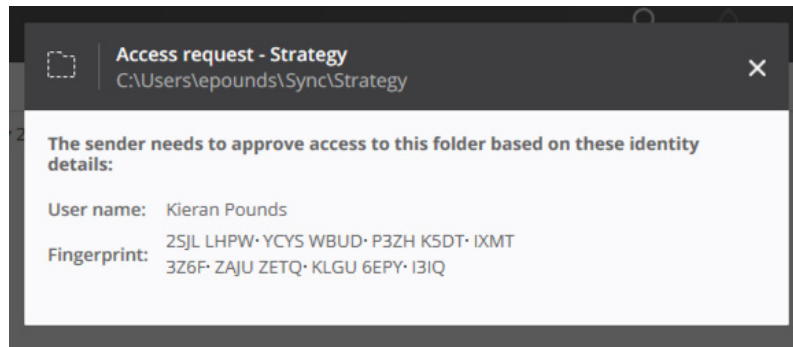
With these folders, each user has a unique identity and a private/public key pair is associated with this it. Each folder is associated with a unique X.509 certificate and a certificate authority (CA). This enables Sync to ensure that all operations such as transferring files, sharing folders, revoking access to folders, etc. are executed in a secure way. The Security model of Sync is designed in a way that

allows every peer to validate the permissions of another peer and all changes that were made. All this can be done in a fully distributed way with no need for a centralized authority.

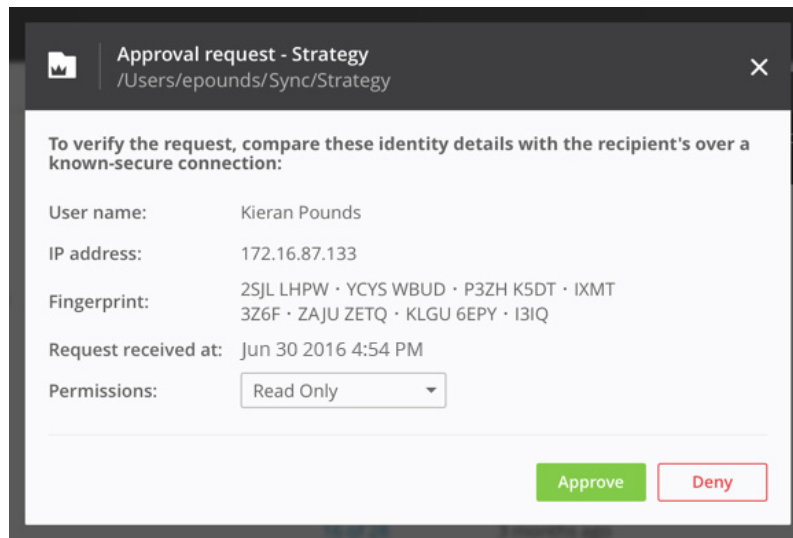
Owner shares folder



Details receiver sees



Details owner sees



This is the process by which certificates are created, signed, synced, and modified:

- When a folder is added to Sync, a primary root certificate (separate certificate authority) is created for the folder and is signed by the user who added the folder.
- When a user requests access to a folder, they send their public key to the owner. If approved, the owner generates a certificate for the requesting user and signs it with their private key. The user's permission level (read only, read and write, or owner) is specified inside the certificate.
- When access to the folder changes (new user, permissions change, disconnecting user), the owner creates a new certificate, signs it, and distributes it to all peers connected to the folder.
- If another user is granted owner permissions, a second root certificate is created and signed by the first root certificate, allowing them to create certificates for the folder.
- Each peer connected to the folder contains all certificates for the folder, allowing them to authenticate peers to send or receive files directly.

Files are always encrypted in transit

Before any data is transferred from one peer to another, it is encrypted and signed. This ensures it cannot be read or modified by others while in transit over insecure networks.

Sync establishes an SSL connection between any two peers and then the data is AES 128-bit encrypted before it leaves the device. After the data is received by the other peer, it is decrypted. Only the peers connected to the folders have the keys. Encryption is turned on by default but we give users the option to turn it off for LAN transfers.

For Sync...AES-128 is better

- 40% faster than AES-256
- Differences between 128 and 256 bit are considered minimal by experts
- Estimated to take a supercomputer 1 billion years to decipher

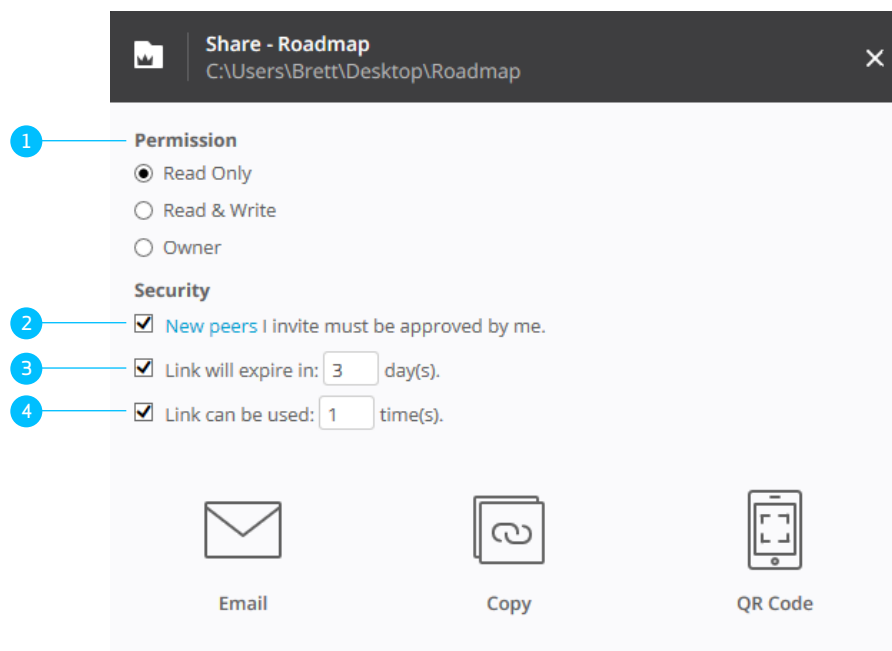
Forward secrecy is guaranteed by Sync communication layer

Forward secrecy means that if a session key is compromised it does not compromise past session keys. Forward secrecy protects past sessions against future compromises of secret keys. Encrypted communications recorded in the past cannot be retrieved and decrypted should session keys be compromised in the future.

Insecure, but easy-to-use, tools can be used to securely share files

When sharing a folder of files with another person, it's often easiest to just send them an email or copy a link into a text message. While these methods of communication are not always secure, Sync can use them to securely and privately share files.

When sharing a folder using a clickable link, the user has these options to control who has access to it and what type of access they have:



1. Permission level

- Read Only - can sync all contents of the folder to their devices; if they make changes to the folder, they will not be synced to any peers
- Read & Write - can sync all contents of the folder to their devices; if they make changes to the folder, they will be synced to all peers
- Owner - has read & write permissions; can also share the folder with others, change the permission level of users connected to the folder, and disconnect users from the folder; owners do have the ability to change



the permissions of other owners (the Owner property is only available for Advanced Folders) When you add a folder to Sync, you are given owner permissions.

When you add a folder to Sync, you are given owner permissions. When sharing with a link, you can create different links with a different permissions level. After the user clicks the link, you can also change their permission before approving their connection.

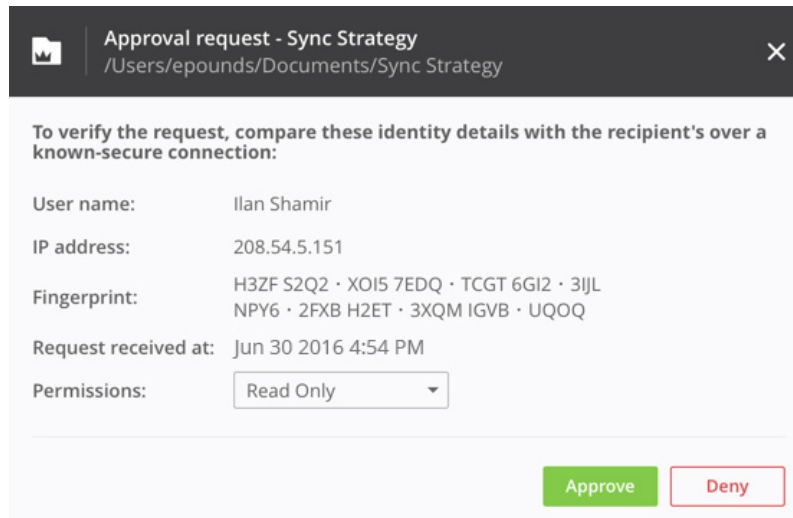
2. Connection approval options

- Approve new peers - users need to be approved if you have not approved them to connect to another folder (untrusted peer); this option speeds up the sharing process by auto-approving connection requests from known users (only available for Advanced Folders)
- Approve all peers - all users requesting to connect to the folder need to be approved
- No approval - all users are auto-approved to connect to the folder

If you are sharing something you intend to remain private, keep one of the approval options on to ensure only people you desire have access to the folder. When a user clicks the link, this is what the owner and requester will see:

Owner		Requestor	
Name	Status	Name	Status
 Sync Strategy	1 Approval request	 Sync Strategy	Pending approval

If approval is required to connect, the owner will be able to validate information about the user requesting connection:



Approval request - Sync Strategy
/Users/epounds/Documents/Sync Strategy

To verify the request, compare these identity details with the recipient's over a known-secure connection:

User name:	Ilan Shamir
IP address:	208.54.5.151
Fingerprint:	H3ZF S2Q2 · XOI5 7EDQ · TCGT 6GI2 · 3IJL NPY6 · 2FXB H2ET · 3XQM IGVB · UQOQ
Request received at:	Jun 30 2016 4:54 PM
Permissions:	<input type="text" value="Read Only"/>

The owner can communicate with the requester to validate the fingerprint of their certificate to guarantee they are who they are.

3. Link expiration by time

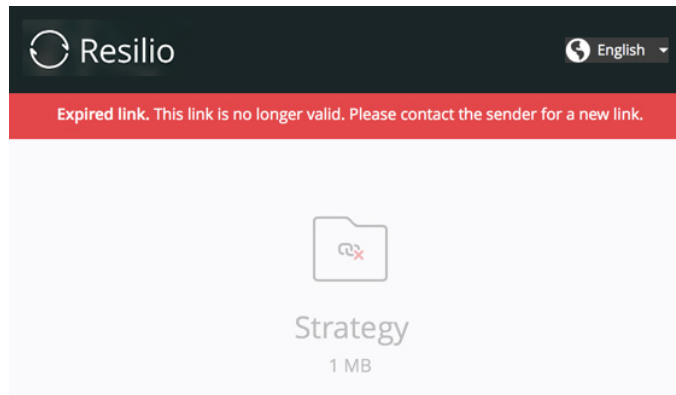
- Link expires in x days - after clicking the “Email” or “Copy” button, the link will be active for the number of days set
- Link does not expire by time - the link will never expire based on elapsed time

4. Link expiration by usage

- Link expires after x uses - the link can only be used to connect to the folder x number of times before it expires
- Link does not expire by usage - the link can be used any number of times

If you need to share a folder with 4 people, you could set the link expiration usage to 4, which would prevent a 5th person from connecting using that link.

If a user clicks on an expired link, they will see this error message:



When the receiver clicks the link, this is what happens:

- If Sync is not installed locally, it presents the user with a download page.
- If Sync is installed, the web page converts the link from “https://...” to “btsync://...” which calls on the local application.
- Sync uses the temporary key from the link to find the folder owner and sends a request for access. The requestor’s public key is sent to the owner.
- The folder owner receives the request and is asked to approve or deny it. This request shows the requestor’s user name, IP address of the device that clicked the link, and public key fingerprint.
- By comparing the public key fingerprint, the folder owner can make sure that the requester is who they are before giving them access to the folder.
- Once the approval is granted, the folder owner generates and signs an X.509 certificate for the requester and syncs it with all peers of the folder. This certificate allows the user to access the folder with the designated permissions level. There is no way for requester to get this certificate before all the steps above are successfully completed.
- The new certificate is synchronized to all peers connected to the folder, which allows the new user to securely connect to any folder peer.
- Once connections between peers are established, files transfers begin.

Note: The HTTPS link can also be pasted into the Manual Connection field, bypassing the link translation web page.

Our servers don't see the user-specific part of the sharing link

All the user-specific information is placed after the '#' sign, which means none of it is sent from the browser to the Sync server. The information after the '#' sign is only available locally.

Here is a sample link:

```
https://link.getsync.com/  
#f=output&sz=65E6&t=2&s=WEY6ZDG7UTZ7JW45LLJLZS76ZEILKJAUUV5UJNS  
HVNDKTRUF43PKQ&i=CVGHMUUX5SH3MZXZLFVIXCSUBIZSKBLGD&e=14723  
19615&v=2.4
```

This is converted this link by replacing everything before # to:

```
btsync://  
f=output&sz=65E6&t=2&s=WEY6ZDG7UTZ7JW45LLJLZS76ZEILKJAUUV5UJNS  
HVNDKTRUF43PKQ&i=CVGHMUUX5SH3MZXZLFVIXCSUBIZSKBLGD&e=1472  
319615&v=2.4
```

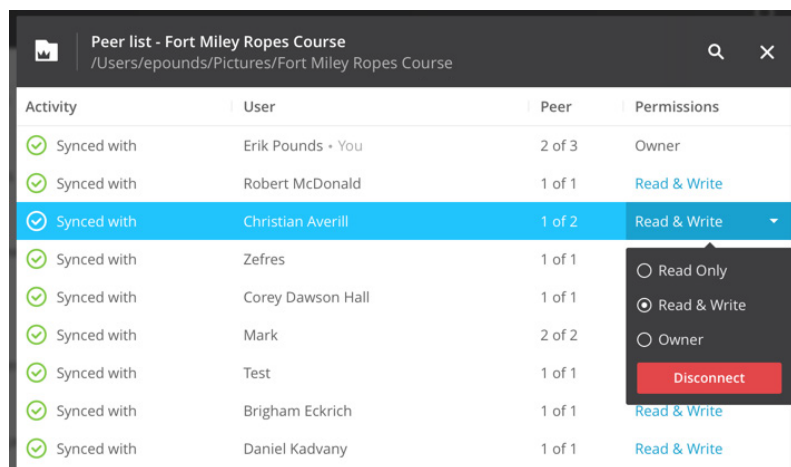
These are the components of a link to a folder, which is all that's required to start syncing data once access is granted:

```
btsync://f=<folder name><folder metadata><hashes><expiration time><product  
metadata>
```

- Folder name - (f=) name of the folder on the owner's device
- Folder metadata - (sz=) approximate size of the folder; (t=) type of folder link (Classic folder t=1, Sync 2.0 or later t=2)
- Hashes - (s=) folder ID in base32 encoding; (i=) temporary key used to connect with the folder owner
- Expiration time - (e=) link expiration time in Unix time format
- Product metadata - (v=) Version of Sync application which created the link

Folder permissions are controlled by owners and synchronized to all connected peers

When the owner granted initial access to the folder, the X.509 certificate was synchronized across all peers connected to the folder. Even after initially sharing the folder with another user, owners have authority to change the user's (and other owners) folder permissions.



Activity	User	Peer	Permissions
✓ Synced with	Erik Pounds - You	2 of 3	Owner
✓ Synced with	Robert McDonald	1 of 1	Read & Write
✓ Synced with	Christian Averill	1 of 2	Read & Write ▼
✓ Synced with	Zefres	1 of 1	<input type="radio"/> Read Only
✓ Synced with	Corey Dawson Hall	1 of 1	<input checked="" type="radio"/> Read & Write
✓ Synced with	Mark	2 of 2	<input type="radio"/> Owner
✓ Synced with	Test	1 of 1	<input type="radio"/> Disconnect
✓ Synced with	Brigham Eckrich	1 of 1	Read & Write
✓ Synced with	Daniel Kadvary	1 of 1	Read & Write

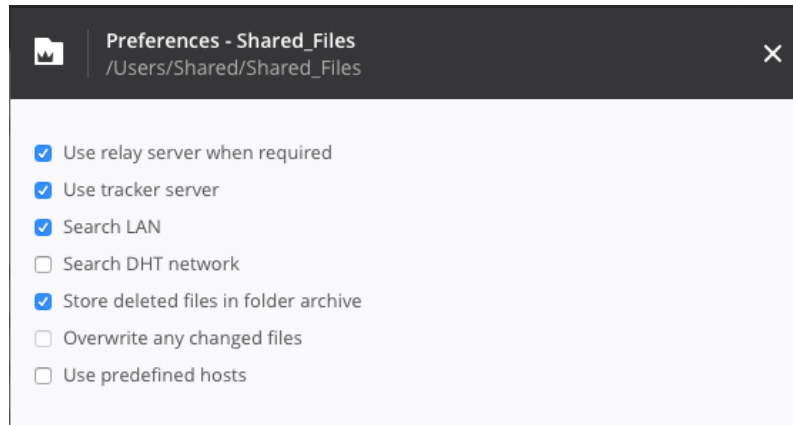
When permissions change (read only, read and write, or disconnected), a new certificate is generated and synced to all the peers. This ensures that the user cannot get the files from any other peer connected to the folder.

Certificates are not deleted, so there is a history of how access to the folder has changed over time. This also allows owners to be able to reconnect users that have been disconnected.

Note: this only applies to Advanced Folders

Each device has control over how it communicates and services can be limited to increase privacy

Sync uses various methods to establish connections between peers and transfer data. On a folder-by-folder basis, options can be enabled/disabled to control how Sync communicates.



These options are:

“Use relay server when required”

By default, Sync does its best to establish a direct a connection between peers to achieve maximum speed. However, if a direct connection is not possible, for whatever reason (sophisticated NATs, firewalls, proxy servers, etc.), this option will allow Sync to establish a connection via a relay server hosted by Resilio, Inc. and transfer data without a direct connection. This option is on by default.

If your device is connected to another device via the relay server, an icon noting this will appear in the peers list.

The relay server maintains full user privacy because:

- No user data lives at rest on, or is cached by, the relay server.
- Only encrypted data flows through the relay server.

“Use tracker server”

Resilio, Inc. hosts tracker servers for Sync to help peers to find out each other's IP address in order to establish a direct connection. Each peers sends this data to the tracker server:

- Folder ID (large random-generated number)
- Peer ID (large random-generated number)
- IP address (private address used by device)

Each peer of each folder learns the IP addresses of the other peers and attempts to contact them to establish a connection. This option is on by default.

“Search LAN”

Allows Sync to search your local network for other instances of Sync connected to the folder. Using multicast, this information is sent on the local network:

- Folder ID (large random-generated number)
- Peer ID (large random-generated number)
- LAN listening port

This option is on by default. If you choose to disable this option, either make sure that the use of tracker server is allowed or predefined hosts are configured.

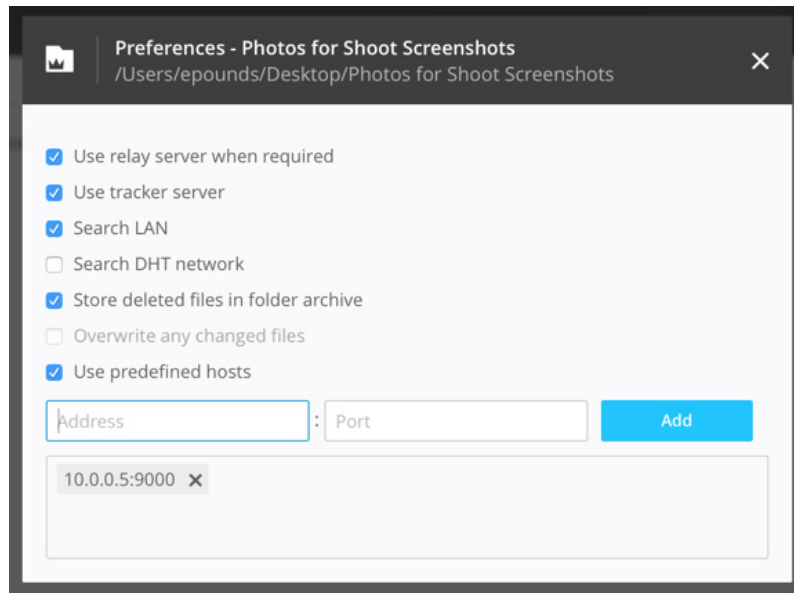
“Search DHT network”

Allows Sync to use the Resilio DHT network to locate peers and their IPs. If you join the DHT network, your computer will store and share part of the DHT table. This option is for advanced users only. For most scenarios, it should be left off.

“Use predefined hosts”

Addresses of devices can be specified for this peer to communicate with to sync this folder. IP address and port number pairs can be specified.

This feature is useful in high-security networks where LAN search over multicast and contacting Tracker server is impossible or prohibited.



Ports

To understand which network ports Sync uses to communicate, please refer to this article:

<https://help.getsync.com/hc/en-us/articles/204754759>

Statistical information from Sync is sent in the clear so you know what BitTorrent's gathering

Sync does collect statistics from the Sync application. These statistics help us improve the product. Here is a list of the statistics we collect:

- Amount of data directly transferred with peers
- Amount of data transferred with peers by relay server
- Tracker packets, pings, and files received by client
- Add folder errors
- IP addresses seen by the tracker server
- Client operating system type and version
- Sync version
- Number of folders & files being tracked by Sync
- Current total size of folders added in Sync
- Language preference set
- Application install event
- Campaign code (installed from website, promotion page, etc.)
- Number of share links generated
- Number of share links accepted
- Number of share links failed
- Number of peers the engine is connected to

In Conclusion

Ultimately, the security of any file storage, syncing, and sharing solution is in the hands of the user or administrator. With most solutions, unauthorized access to files must be prevented using encryption, secure passwords, a robust firewall configuration, etc. The architecture of Sync provides an unprecedented level of security and privacy with almost no user setup required. Data can not be hacked, as there is no password to find, no person to exploit, and no server to attack. Sync is the most secure and easy to setup file syncing solution that you can use to share data quickly and efficiently to any person or device.

Glossary

Peer

A unique, logical device that is connected to a folder. Your laptop, phone, or virtual machine are all “peers”. Peers are often referred to as devices.

User

Unique identity of a person. A user can have multiple devices (or peers) linked to it. When linked, these devices will have the same user identity.

AES-128

Advanced Encryption Standard (AES), a Federal Information Processing Standard (FIPS), is an approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a block cipher that can encrypt and decrypt digital information. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits.

Cryptographic

Cryptographic protocols are widely used for secure application-level data transport. A cryptographic protocol usually incorporates at least some of these aspects:

- Key agreement or establishment
- Entity authentication
- Symmetric encryption and message authentication material construction
- Secured application-level data transport
- Non-repudiation methods
- Secret sharing methods
- Secure multi-party computation

DHT (distributed hash table)

Is a class of a decentralized distributed system that provides a lookup service similar to a hash table. DHTs form an infrastructure that can be used to build more complex services, such as anycast, cooperative Web caching, distributed file systems, domain name services, instant messaging, multicast, and also peer-to-peer file sharing and content distribution systems.

Multicast

Multicast is a one-to-many or many-to-many distribution, and is a group communication where information is addressed to a group of destination computers over a network simultaneously.

PKI (Public Key Infrastructure)

A PKI is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates, and manage public-key encryption.

SSL (Secure Sockets Layer)

SSL is a security protocol and is a standard security technology for establishing an encrypted link between a server and a client—typically a web server (website) and a browser; or a mail server and a mail client. It allows sensitive information such as credit card numbers, social security numbers, and login credentials to be transmitted securely. Normally, data sent between browsers and web servers is sent in plain text—leaving you vulnerable to eavesdropping. If an attacker is able to intercept all data being sent between a browser and a web server they can see and use that information.

X.509 certificate

An X.509 certificate is a digital certificate that uses the widely accepted international X.509 public key infrastructure standard to verify that a public key belongs to the user, computer or service identity contained within the certificate.

