Synology®

C2 Transfer Security White Paper

Last updated: Dec 28, 2022

Table of Contents

Introduction

Unauthorized document transfer access might have irrevocable consequences for businesses. The costs of probable legal liabilities and compensation may result in a critical business collapse. Therefore, you should have complete confidence that your encrypted data is safe and that only authorized recipients can access your data.

What is C2 Transfer?

A two-way file transfer service that brings down the possibility for the C2 Transfer server or an unauthorized person to access and decrypt **sensitive** information; only the **authorized sender** and **recipient** have access to the data.

What C2 Transfer provides

C2 Transfer is a user-controlled transfer platform, allowing users to monitor and regulate all transfer task functions. It optimizes the overall transfer security by protecting your transferred data with recipient authentication via the email address or phone number, shared link expiration, and end-to-end file encryption. For added convenience, C2 Transfer also includes an in-service watermark tool, and recipients are not required to create an account, saving users time and effort.

How C2 Transfer protects

To ensure strong encryption security, the **C2 Encryption Key (C2 Key)** is used as the primary key on the transfer portal, and data in transit is protected not only by encryption but also by the standard HTTPS protocol. C2 Transfer provides the file transfer service and the file request service based on the implemented security foundation. The C2 Transfer service facilitates two-way secure data transfer that has separate transmission encryption parameters but with the same level of security.

For file transfer, all sensitive information is encrypted on the sender's client until the data is decrypted by the recipient. When the recipient receives the transfer link, encryption and receiver verification methods are used to protect the data. C2 Transfer server has no way to access and decrypt the data. In addition, shared link verification option and access code authentication ensures the legitimacy of the recipient.

C2 Transfer doesn't just allow the sender to transmit data to recipients, but it also offers a way for the sender to receive documents from different recipients through the file request function.

Apart from the shared functionalities of the file transfer and file request, the coordination of RSA-(OAEP) and AES-GCM encryption for the file request is crucial for data protection. The implemented encryptions serve as the highest level of data security that a two-way file transfer service can provide to its users. C2 Transfer ensures that the file request function keeps the data unreadable until decrypted by the authorized file downloader.

Key security principles

C2 Transfer is Synology's solution for protecting and safeguarding your shared data. This white paper explains how this is done in a secure way. C2 Transfer utilizes a similar approach to security that has been implemented in other C2 services, namely, that we can best protect your secrets by not knowing them.

Privacy by design

It is impossible to lose, use, or abuse data that one doesn't possess, so our systems have been designed with an effort to reduce the amount of sensitive user data that we are able to access. This concept is utilized throughout the entire system, such as our inability to acquire or store your C2 Key during authentication. This means that there is no way that we could know your C2 Key, and if we don't know your C2 Key, we don't own your data.

You own your data

C2 Transfer is designed to make sure that only **you** and your chosen recipient have access to your data, which is encrypted and decrypted solely on the client-side. On top of that, our utilization of **end-to-end encryption** and recipient authentication keeps you and your data as safe as possible from anyone trying to gain access.

Designed for transparency and trust

When it comes to our service usage data collection methods, Synology strives to be as open and transparent as possible. Your permission will always be required when we collect any of your service usage data. On top of that, our team takes pride in their efficiency to react when investigating, verifying, resolving, or mitigating reports of any bugs or vulnerabilities with our products.

Protection on C2 services

To avoid users having to remember a number of encrypted passwords, C2 services have developed and implemented a single encryption key, known as the **C2 Encryption Key (C2 Key)**. This encryption key is used across all C2 services (except C2 Storage). Your C2 Key is not stored by any means on the Synology C2 server. Therefore, the only person who knows it is the individual who has access to your Synology C2 account. Since the C2 Key is being used to decrypt all of your stored encrypted data, we suggest that you use a key that is strong, easy to remember, and follows our C2 Key requirements. If you lose your C2 Key, Synology C2 will not be able to retrieve your encrypted data. Thus, it is critical that you keep your C2 Key as safe and secure as possible.

Synology C2 services provide the maximum possible security for your encrypted data by using the C2 Key to derive, encrypt, and decrypt all cryptographic and Derived Keys.

C2 infrastructure

Physical location

We currently operate data centers worldwide. All users are ensured that their data is hosted in the location of their own choice. For example, our EU-based data center allows business customers to comply with European data protection laws. New locations may be added in the future, however, this will not affect existing clients or their data. For more information about our data center locations, please visit our official website. Please see Synology C2 Services' Terms of Service and Privacy Statement for more details on legal guarantees.

Site security

Synology data centers have passed rigorous inspections for strict security procedures and physical safety features, and meet Synology's high standards for incident response and access restrictions. Synology monitors employee access to its storage locations and implements different mechanisms to ensure data durability and fault-tolerant storage. With your data security in mind, the architecture of Synology C2 data centers aims to ensure that no valuable data will be lost. For more details, you can refer to the **Data Durability** section of this white paper.

C2 Transfer End-to-end Encryption

C2 Encryption Key provides security, privacy, and user data control which are fundamentals in an integrated and cost-effective cloud solutions for Synology account users. Data in transit and at rest are secured using rigorous encryption protocols which will bring your C2 Transfer experience to the greatest extent possible.

Encryption technology

Synology C2 services use two different types of encryption technology to protect the **data in transit** between the sender and the recipient, along with the **data-at-rest** that is stored on the cloud and the C2 server.

- **AES (Advanced Encryption System) Encryption**: A symmetric type of encryption that uses the same cryptographic keys for encryption and decryption, so the sender and recipient must both use the same key to keep a private information connection.
- **RSA (Rivest–Shamir–Adleman) Encryption**: An asymmetric type of encryption that uses a Key Pair that consists of the Public and Private Keys (Secret Key). Content that is encrypted by the Public Key can only be decrypted by the Private Key. As a result, keeping the Private Key confidential is necessary to ensure your data safety.

C2 Encryption Key data structure

The **C2 Encryption Key (C2 Key)** is provided by the user, and the AES-256-CBC encryption is derived from the encryption key through the PBKDF2 derivation function to reduce vulnerabilities of brute-force attacks.

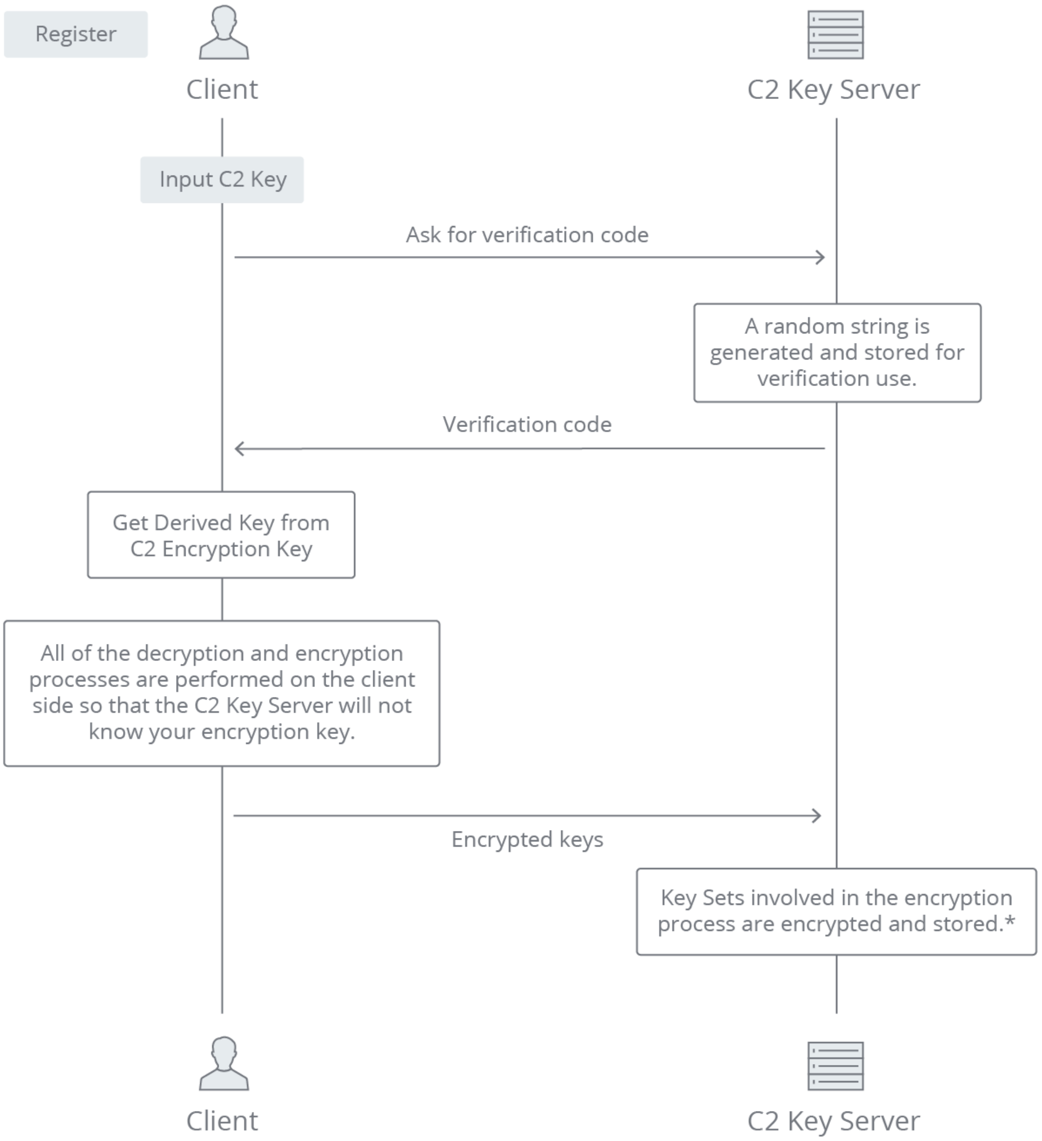
The Derived Key is used to encrypt and decrypt **verification codes** through **AES-256-CBC encryption**. Since the C2 Key server should not know about the encryption key, the verification for the encryption key is done by testing the ability to decrypt an encrypted verification code.

The Derived Key is also used to encrypt and decrypt the **Key Set (RSA Keypairs and AES Keys)** through **AES-GCM encryption**.

C2 Encryption Key registration and verification

C2 services have been designed with your security and data safety in mind, keeping your data protected when stored on our servers. To do this, we have implemented the use of an encryption key mechanism, the **C2 Encryption Key (C2 Key)**, to which only the user themselves has access. During first-time setup, you will need to set up your own C2 Key.

Registration


Register
Client
C2 Key Server
Input C2 Key
Ask for verification code
A random string is generated and stored for verification use.
Verification code
Get Derived Key from C2 Encryption Key
All of the decryption and encryption processes are performed on the client side so that the C2 Key Server will not know your encryption key.
Encrypted keys
Key Sets involved in the encryption process are encrypted and stored.*
Client
C2 Key Server

* The Public Key is not encrypted, since it will be used when performingfile transfers between users.

On the C2 Encryption Key setup page, you will be requested to register your C2 Key. Since this key will be used during encryption across all of your C2 services (except C2 Storage), please make sure to choose a key that is strong, memorable, and follows our C2 Key requirements.

After you have input your encryption key, your client will send a request to the C2 Key server to generate and store a random string in the form of a **verification code**. This will be used to test the ability of the client to decrypt the encrypted verification code later on. This makes it possible for the C2 server to verify your identity **without** needing to save your C2 Key. Once the verification code has been generated, it is sent to your client to generate the RSA Key, AES Key, and Derived Key, along with the encryption of said keys. All of the decryption and encryption processes are performed on the client end, so the C2 Key server remains unaware of the encryption key.

After the client has encrypted the corresponding keys and verification codes, they are then sent back to the server to store the user metadata, encrypted verification code, Private Key, Public Key, and AES Key. Once your registration has been successfully completed, the Recovery Code, Derived Key, and the Verification Key will be generated and encrypted on the client end.

Make sure to download or save your Recovery Code so that you can perform recoveries if needed in the future. The Recovery Code utilizes the same registration method as mentioned above when performing a recovery of your C2 Key.

Verification

If you have already registered your C2 Key and wish to access your encrypted data, you must input your C2 Key into the C2 Transfer portal to begin the decryption process. After entering your C2 Key, the Derived Key will be generated for decrypting the encrypted verification code on the client end. Then, the client will send a request to the C2 Key server to verify the verification code.

Once verified, the Public Key, encrypted Private Key, and encrypted AES Key will be sent to the client to be decrypted, and will then be used to decrypt the encrypted service keys obtained from the C2 server. By keeping the encryption and decryption processes on the client end, the C2 server is unable to retain any knowledge of your C2 Key or gain access to your encrypted data. Once the encryption and decryption processes are completed, you will be able to access your data in C2 Transfer.

Changing of encryption keys

If you use the same password for C2 Key as you do for other accounts, we recommend that you change your C2 Key to something else to limit the possibility of a data breach. You can change your C2 Key in your account settings in the C2 Transfer Portal. Once you input your old C2 Key, your client will submit a request to the C2 Key server to pre-verify the user metadata and the encrypted verification code. After the old C2 Key is verified, the old Key Sets will be decrypted via the old Derived Key and a confirmation code will be sent to your client.

Once the confirmation code has been confirmed by the C2 Key server, you will be able to input your new C2 Key. When you do this, the new Derived Key, AES Key, and RSA Key Pair will be generated, and the old Key Sets will be re-encrypted via the new Derived Key to complete the encryption process. All previously stored data will be re-encrypted, and a new Recovery Code will be generated, meaning that the old recovery code will no longer be valid. This entire process may take some time to complete.

Creation of a Recovery Code and C2 Key recovery

Encryption key recovery allows you to restore access to C2 services by resetting your C2 Key and recovering your encrypted data stored on the C2 server. In order to use this function, however, you must have already downloaded or stored and have access to the **Recovery Code** that was automatically generated during the setup of your C2 Key. Make sure to keep your Recovery Code safe, since the C2 server does not keep your C2 Key and the only method to retrieve it is with your Recovery Code, which is encrypted and stored on the C2 server and can only be decrypted using the Recovery Code's Derived Key.

Creation

Your **Recovery Code** is automatically generated once you have completed the registration of your C2 Key. You can download and store this code somewhere safe in case you forget your C2 Key. After C2 Key setup is complete, your client pre-registers the Recovery Code by sending a request to the C2 Key server to generate a random string in the form of a verification code. Once the process is complete, the C2 Key server stores the user metadata and the verification code. The verification code is then transmitted to your client after the generation of the Recovery Code and derivation of the Recovery Code's Derived Key.

Your client will use the Recovery Code's Derived Key to encrypt the verification code and Key Set (Private Key and AES Key only). Your client will then use this Derived Key to encrypt the Recovery Code. After this encryption is complete, the client will send a request to accept the encrypted verification code, encrypted Private Key, Public Key, encrypted AES Key, and encrypted Recovery Code. Once accepted, the C2 Key server will store said keys along with the user metadata. Once the entire process is complete, the Recovery Code will be ready to save or download.

Recovery

When you need to recover your C2 Key, you will be asked to first enter your **Recovery Code** and then create a new C2 Key. Upon entering the Recovery Code, its Derived Key will be generated and the user metadata and verification code will be retrieved from the C2 Key server. The encrypted verification code will be sent to your client for decryption via the Derived Key that was generated by the Recovery Code. Your client will then send a request to verify the verification code and generate a random string in the form of a confirmation code, which is then stored along with the user metadata.

Once the verification process is complete, the C2 Key server will send the confirmation codes, the old Key Sets (derived via the old Derived Key), and the new Verification Key to your client. You will then be asked to set up your new C2 Key, which will be used to derive the Recovery Code's

Derived Key. When you do this, a new Recovery Code Derived Key, AES Key, and RSA Key Pair will be generated, and the old Key Sets will be re-encrypted via the new Recovery Code Derived Key to complete the encryption process. Similar to the registration process, after the C2 Key has been set up, all of your data will be re-encrypted and a new Recovery Code will be automatically generated, all of which may take some time. At this point, make sure that you download or save your Recovery Code for future recoveries.

Upon creation of the Recovery Code, your client will encrypt the RSA Key Pair and AES Key using the new Recovery Code Derived Key, which then also encrypts the new verification code and re-encrypts the old Key Sets. The client will then ask for the C2 Key server to allow and verify the user metadata along with the encrypted keys mentioned above. Once validated, your new C2 Key and Recovery Code will be ready to use, and your encrypted data will be accessible via the new C2 Key.

Notes:

- A new Key Set will be created each time you register, change, or recover your C2 Key. All old Key Sets will be re-encrypted after the C2 Key has been changed or recovered.

C2 Transfer User Data Protection

Creation of file transfers

C2 Transfer is designed to protect your files during transfers. Just imagine that you're sending confidential information, such as customer personal information, financial statements, or business secrets, to a business partner; if the documents end up in the wrong hands or are leaked to an unauthorized recipient, it might lead to a slew of problems. We have taken this into consideration when designing C2 Transfer's file transfer function, so that your business documents are always protected whenever you send or upload a file.

When you are performing a file transfer, the Transfer Key is encrypted on the client side via the User Key, and the Transfer Key encrypts the transfer metadata. Then, the encrypted transfer metadata and Transfer Key will be uploaded to the C2 server. Once uploaded, the web client will generate the download URL, which includes the Transfer Key. Your client browser will encrypt the file and the file metadata and transmit them to the C2 server before completing the download URL generation process. When the URL is generated on the web client, the Transfer Key is not communicated to the C2 server. For this reason, C2 Transfer does not send a notification to the recipient. Instead, you must provide the link to your recipients using the available methods. This entire process prevents the C2 server from learning of or decrypting the content of the uploaded data.

Download of file transfers

Since our goal is to ensure that our users' data are only sent to trusted recipients, configuring access rules is key. Here, we will use User A, as the sender of the files, and User B, as the recipient of the files, for example. When User B receives the download link and enters it into their browser's address bar, they will be asked to enter their contact information, which will be used by the C2 server to authenticate and send the encrypted transfer metadata to User B's client for decryption. Upon completion, User B's client will send a request for a **One-Time Password (OTP)**, which will allow the C2 server to confirm that this user has the appropriate access.

Once confirmed, User B will receive the OTP via their email or mobile device, which can then be entered into the blank field that appears on their device. When the verification request has been completed, the C2 server will respond with the encrypted file to be decrypted by User B's client. User B should then be able to download the files.

In the case that the user's contact information is unconfirmed or blocked, it means that they were not granted access and do not have permission to download the files or access the transfer task. Using this approach, you can share sensitive documents while ensuring that only those with the appropriate permissions have access to them.

Creation of a file request

C2 Transfer has a file request feature that provides the same level of security as the file transfer function. We acknowledge that the file you expect to receive is as important as the file you send out. Through the file request link, C2 Transfer ensures that all data uploaded from third-party uploaders is encrypted and safe. File requesters must generate a secure file request link and share it manually with file uploaders.

When performing a file request, the file request key will be encrypted using the user public key on the client-side. Then, the C2 Transfer server will randomly generate and establish an upload URL, which includes the file request key. The URL is generated on the web client, and the key is not acquired by the C2 server. Therefore, the C2 server has no way to decrypt the transferred data. Since the URL holds the initial key used to encrypt and decrypt the task, the C2 server will not possess or transmit the URL to the user. The user is expected to provide the URL to the file uploaders.

File request upload

For a third-party individual to upload a file to a file request link, the individual is expected to go through the following process to ensure that the process is secure. Here, we will use User A, as the file requester and link sender, and User B, as the file uploader of the files, for example. When User B receives and opens a file request link from User A, the client will send a specific file request task ID and the user ID to the server and ask for the file request task's metadata to make the task appear on the user interface and be decrypted on the web client with the key contained in the URL.

After the task information is delivered to the client, User B will be prompted to input their contact details, and User B will input the OTP code they receive, and it will be sent to the C2 server for OTP code verification. Upon completion, an upload page will appear on the client of User B and will now be able to upload files.

The files uploaded will be labeled and encrypted in versions to better distinguish each upload. This design also ensures the uploaders will not be able to see what each other has uploaded on the file request task. Before User B uploads the selected files, the files and the keys used to encrypt the file content will be encrypted on User B's client with User A's public key. This ensures that the content is encrypted before it leaves the user's device and that only User A is allowed to decrypt the data since their private key will be required for the decryption process.

File request download

When all the uploaded files are encrypted and sent to the C2 Transfer portal, the recipient needs to click on the download button to download the file and save it on their device. Here, we will use User A, as the file downloader, and the recipient, for example. User A is required to enter their C2

Key to decrypt and access the transfer portal. When User A selects a specific file request task, the uploaded files will appear. The reason for this is that the moment when the C2 Key is entered, User A’s client sends the request from the server to provide all metadata and files needed at the same time. All decryption occurs on the client-side, allowing the client to obtain the private key used to decrypt the public key, which then decrypts the other keys necessary to decrypt the file. These files are organized first by the uploader’s contact detail, and then by versions. The order of the contact detail and versions only applies when the uploader has uploaded files more than once. Since the links are time-limited, User A can only view the sent data until the download deadline, after which the files are deleted from the server.

Conclusion

Synology C2 Transfer offers Synology account users a tool to secure data transmission of data at rest and in transit, to prevent data breaches due to vulnerability of technology and user behavior. Synology C2 Transfer prioritizes security while building its service to maintain business continuity at all times, allowing consumers complete control over their data.

C2 Transfer is a safe and convenient file transfer platform for C2 users who want to take data security to the next level by using the file transfer and file request functions that possess military-grade encryption for data transmission. With C2 Transfer, your business documents are kept within the business network, and the information transmitted is managed in a much simpler way.