Table of Contents

Executive Summary 01

Introduction 02
Key security principles
Protection on C2 services
C2 infrastructure

C2 Password End-to-end Encryption 04
Encryption technology
C2 Encryption Key data structure
C2 Encryption Key registration and verification
Changing of encryption keys
Creation of a Recovery Code and C2 Key recovery

C2 Password User Data Protection 09
My Vault
Client protection
Creation of file transfers
Download of file transfers

Conclusion 11

Find your information

Synology publishes a wide range of supporting documentation.

In Knowledge Center, you will find useful Help and FAQ articles, as well as video tutorials breaking up processes into handy steps. You can also find User's Guides, Solution Guides, brochures, and White Papers. Experienced users and administrators will find answers and guidance in technical Administrator's Guides and Developer Guides.

Got a problem and unable to find the solution in our official documentation? Search hundreds of answers by users and support staff in Synology Community or reach Synology Support through the web form, email or telephone.
Executive Summary

In recent years, the necessity to create and maintain dozens or hundreds of online accounts with logins and passwords has become more and more prominent, especially with remote work on the rise and internet usage at an all-time high. Nothing is more secure than making sure that every one of your accounts that you create is using a unique or randomly-generated password, but where do you keep track of all of these passwords, and how can you ensure that your password security is up to par?

Deploying a password management solution is one of the simplest methods that you can use to implement and maintain proper password security.

**C2 Password** is the simplest and safest way to manage all of your accounts, passwords, and other sensitive data in one system while keeping your data synced across the devices you use the most. C2 Password allows you to create and store passwords while maintaining the highest level of protection for your data.

This white paper provides an overview of C2 Password, as well as detailed explanations of the processes for encryption, file transfers, and more.
C2 Password is a highly secure password management system that allows you to store, sync, and safeguard your passwords and personal information. With unlimited device syncing, you will be able to access your credentials from anywhere through a web portal or a browser extension.

Key security principles

C2 Password is Synology's solution for protecting and safeguarding your passwords and personal data. This white paper explains how this is done in a secure way. C2 Password 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 Password is designed to make sure that only you have access to your data, which is encrypted locally during storage. On top of that, our utilization of end-to-end encryption keeps you and your data as safe as possible from anyone looking 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.
Introduction

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 whoever has access to your Synology C2 account. Also, since this C2 Key will be 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 happen to 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.
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 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**

* The Public Key is not encrypted, since it will be used when performing file 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 Password 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, 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 Password.

**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 Password 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 Password User Data Protection

My Vault

All of the information associated with your stored data in C2 Password is protected using end-to-end encryption. Anything that you store in My Vault will first be stored via Cipher Data. Cipher Data are encrypted using the Advanced Encryption Standarded (AES) in Galois/Counter Mode (GCM) using a 256-bit key generated from your C2 Key. The AES 256-bit algorithm is well known as an impenetrable, military-grade encryption, and has even been approved by the U.S. National Security Agency for the encryption of top-secret information. The encryption and decryption processes are performed entirely on the client end of C2 Password in order to keep your C2 Key from being transmitted to the C2 Server.

Client protection

The C2 Password client is typically run as a browser extension and is supported on all major browsers for Windows and Mac devices. Any communication that takes place between your client and the C2 Server uses Transport Layer Security (TLS) protocol, and connections via the browser extension are protected with browser security controls. Furthermore, HTTP String Transport Security (HSTS) forces all connections to use TLS, helping mitigate the risk of downgrade attacks or misconfiguration, whereas Content Security Policy headers defend against injection attacks such as cross-site scripting.

The C2 Password client also makes use of an Auto-lock function that determines how My Vault behaves after being inactive for a specified amount of time. Timeout can be configured individually for each C2 Password client using standard time-based options, such as minutes or hours. When you lock My Vault, your data will remain encrypted on the device, and you will need to enter your C2 Key to unlock (decrypt) it. You do not need to be connected to the internet to do this.
Creation of file transfers

Aside from keeping your credentials all in one safe place, C2 Password also protects your files during transfer. Just imagine that you're sending some personal information, such as passport copies, financial statements, or insurance documents, to a bank or insurance firm; if the documents end up in the wrong hands or are leaked to an unanticipated recipient, it might lead to a slew of problems. We have taken this into consideration when designing C2 Password's file transfer function, so that your personal documents are always protected whenever you upload a file.

When you are performing a file transfer, your client will encrypt the transfer metadata and the Transfer Key via the User Key. Then, the encrypted transfer metadata and Transfer Key will be uploaded to the C2 Server. Once uploaded, the User ID and Transfer ID will be sent to the web client to generate the download URL, which will be used as a record of the transfer task. Your client browser will encrypt the file and the file metadata and send it to the C2 Server to complete the generating process of the download URL. This entire process prevents the C2 Server from learning of or decrypting the content of the uploaded data.

Notes:
• The C2 Server splits the file into multiple 64 MB chunks, and then splits it again into another 64 KB block within the 64 MB chunks to make the download response more efficient.
• Google Chrome cannot upload files larger than 128 MB.

Download of file transfers

Since our goal is to ensure that our users' data are safely sent to the intended recipient, restricting access to only the selected recipient is key. Here, we will use User A, the sender of the files, and User B, 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, 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.
Conclusion

Synology C2 Password makes staying on top of your password security simple and efficient by storing and synchronizing all of your accounts and passwords in one place. Along with the ability to generate, store, and manage passwords, you are also able to sync them and your other data across all of your devices, all while keeping your data safe and secure with state of the art encryption technology.

Synology C2 Password allows you to keep track of all of your company or personal internet accounts, conveniently keeping your password security up to date. Your business can maintain a suitable level of password security by adopting this password management solution.
Synology may make changes to specifications and product descriptions at any time, without notice. Copyright © 2021 Synology Inc. All rights reserved. ® Synology and other names of Synology Products are proprietary marks or registered trademarks of Synology Inc. Other products and company names mentioned herein are trademarks of their respective holders.