Archive encryption key security: Advice for users

Who is this article for?

√ Ø Code42 for Enterprise

√ Ø CrashPlan for Small Business

This article applies to versions 6 and 7.

Other available versions:

Version 5 | Version 4

Overview

Code42 app encrypts all user data before it leaves endpoint devices for storage in Code42 backup archives. No one can decrypt a user's data without that user's archive encryption key. To protect the keys, Code42 offers three levels of security. For users of Code42 apps, this article describes whether and how to implement the two advanced levels. However, Code42 strongly recommends keeping to the default, standard level of security.

Administrators of Code42 environments are encouraged to see another article about administrative decisions and controls regarding archive encryption keys.
Before you begin

Your administrator may have already configured your Code42 app to use advanced key security. In that case, the next time you open your Code42 app on your desktop, it prompts you to define your credentials. For instructions, see either:

- Create a new archive key password
- Upgrade Code42 app security to custom key

Step 1: Consult your administrator

Do not change the security settings in your Code42 app without first consulting the administrator of your Code42 environment. The advanced security settings may not be suitable for your Code42 environment.

In addition, your administrator may lock the security settings so that you cannot change them. To learn if that is the case:

1. Open the Code42 app on your desktop.
2. Navigate to Device Preferences:
   - **Code42 app version 6.8.3 and later:** Select Settings.
   - **Code42 app version 6.8.2 and earlier:**
     i. Click Details.
     ii. Select the arrow next to your device name.
     iii. Choose Device preferences.
4. Look for a button labeled Upgrade.
   
   If you do not see the Upgrade button, you are not allowed to change the security for your archive encryption key. Consult your Code42 environment administrator.
Step 2: Choose a security option

To protect the encryption keys for your backup archives, Code42 offers three levels of security, summarized below. For more detailed comparison of the options, and for further warnings about their risks, see the information for administrators (https://support.code42.com/Administrator/6/Planning_and_installing/Security_hardening_best_practices/Archive_encryption_key_security#Step_1:_Choose_a_security_option).

**Option 1: Account password security (default configuration)**

User data cannot be decrypted and read without the archive encryption key. The data owner gets the key by supplying the account name and password. Administrators of the Code42 environment also have access to the key, and so to your backed-up data.

**Code42 strongly recommends the default**

The standard, default security option allows administrators to help users recover data. The other two options lock administrators out of user data. Code42 not only recommends that users stick with that default option, Code42 also recommends that administrators lock that security setting (https://support.code42.com/Administrator/6/Administration_console_reference/Device_Backup_-_Security_settings_reference) so that users cannot change it.

**Option 2: Archive key password security**

You create a private password, known only to you, that protects your encryption key. The key is encrypted before it is stored on the Code42 server. Administrators cannot read your key or your backed-up data. You also define a recovery question and answer to help you when you forget your password.

**Option 3: Custom key security**

https://support.code42.com/CrashPlan/6/Configuring/Archive_encryption_key_security (https://support.code42.com/CrashPlan/6/Configuring/Archive_encryption_key_security)
You define your encryption key. That key never leaves the device where it is created. If you lose that key, your backed up data is also lost. There is no way to recover it.

Step 3: Implement a security option

Follow the links below for instructions about implementing advanced security.

Considerations

- **You cannot revert to standard password security**: Once you set any one of your Code42 apps to use advanced key security (options 2 or 3 below), there is no reversing the process. The only way to resume the standard account password security is to discard all of your backup data and start over.

- **The settings affect all your devices**: When you change the security setting at one Code42 app, you change it for all of the devices that back up data to your Code42 account.

Option 1: Account password security

The recommended, standard option is configured by default.

Option 2: Archive key password security

Follow the instructions at [Upgrade Code42 app security to archive key password](https://support.code42.com/CrashPlan/6/Configuring/Upgrade_Code42_app_security_to_archive_key_password).

Option 3: Custom key security

Follow the instructions at [Upgrade Code42 app security to custom key](https://support.code42.com/CrashPlan/6/Configuring/Upgrade_Code42_app_security_to_custom_key).

Related topics

- [Archive encryption key security](https://support.code42.com/Administrator/6/Planning_and_installing/Security_hardening_best_practices/Archive_encryption_key_security)
- [Upgrade Code42 app security to archive key password](https://support.code42.com/CrashPlan/6/Configuring/Upgrade_Code42_app_security_to_archive_key_password)
- [Create a new archive key password](https://support.code42.com/CrashPlan/6/Configuring/Create_a_new_archive_key_password)
- [Change your archive key password](https://support.code42.com/CrashPlan/6/Configuring/Change_your_archive_key_password)
- [Set and answer a recovery question](https://support.code42.com/CrashPlan/6/Configuring/Set_and_answer_a_recovery_question)
- [Upgrade Code42 app security to custom key](https://support.code42.com/CrashPlan/6/Configuring/Upgrade_Code42_app_security_to_custom_key)
Upgrade Code42 app security to custom key

https://support.code42.com/CrashPlan/6/Configuring/Archive_encryption_key_security (https://support.code42.com/CrashPla...