Dell EMC MozyEnterprise®: Mozy Encryption Technology

The Mozy advantage

Simple

Seamlessly manage backup, sync, and mobile access for multi-user and server environments from a single web-based console.

Secure

Your data is safe with enterprise-grade encryption, world-class data centers, and Dell EMC.

Affordable

Keep costs low with no hardware to purchase and minimal overhead required.

Contact Mozy

mozyemeacorporatesales@dell.com
www.mozy.ie/enterprise

Types of encryption

Mozy secures your data using either 448-bit Blowfish or 256-bit AES encryption. If you elect to use the Mozy default encryption, the Blowfish algorithm is used; if you create your own key from a pass phrase, the encryption key is created using AES. You can find more information about how keys are created later in this document. Mozy supports three types of encryption keys, with specific benefits for each type.

- **Mozy default encryption key:** Mozy assigns an encryption key to your users. This key is stored and managed by Mozy for the most seamless experience.
- **Personal encryption key:** The user enters a pass phrase that is used to create the encryption key. Each user creates a unique personal encryption key.
- **Corporate encryption key:** The administrator enters a pass phrase that is used to create the encryption key. You can create a key for all users in the company or a unique one for each user group. The corporate key is also referred to as the c-key.

You determine the type of encryption key to use during the installation of the Mozy software, and that encryption is permanently associated with the files stored in the Mozy cloud. Dell EMC MozyEnterprise® customers can configure the encryption type using a client configuration to assign the encryption key type for users. You can also use the client configuration to automate the installation with a corporate encryption key. You can change the encryption type after you install the software. If you do change it, the software will re-upload all of your files to ensure that the stored files match your current encryption key.

Regardless of the type of encryption key used, files are encrypted in the first step of processing before they are sent to the Mozy cloud. This ensures that the files are secure before ever leaving your computer and remain so during transit and at rest in the Mozy cloud. If you are using personal encryption keys or a corporate encryption key, Mozy cannot read and will not escrow your encryption key; therefore, the files are never decrypted until you restore them to your computer.

Mozy default encryption

The Mozy default encryption keys are 448-bit keys created using the Blowfish algorithm. Mozy stores the key separately. This lets Mozy automatically decrypt your files when you download or restore them. Mozy® Sync always uses default encryption keys to ensure that your files can be updated among your computers, regardless of what type of encryption each of the endpoints use for backups.

Personal encryption keys

Personal encryption keys are 256-bit AES keys created using a pass phrase entered

by the user. When you download and restore files, you must supply this key to decrypt those files. Mozy does not have access to your personal encryption key and cannot decrypt files for you. When you reinstall the Mozy software or install it on a replacement computer, you must supply this same key to ensure continued access to files you have previously backed up.

Corporate encryption keys

Corporate encryption keys are created using the same process as personal encryption keys. To protect against unauthorized access to the encryption key, Mozy assigns a shared secret that is used to encrypt the corporate encryption key file using the Blowfish algorithm. This two-step process ensures that your encryption key is secure. Similar to personal encryption keys, Mozy cannot assist you in decrypting files you have backed up, as we do not have access to your key. Corporate encryption keys are shared among all users in your organization or within a user group and can be distributed to the local computers or stored on a network server for users to access.

Key Management Interoperability Protocol

MozyEnterprise supports backup encryption key management via the Key Management Interoperability Protocol. This enables automatic generation of keys that can be managed with an on-premises key management server (KMS), which increases at-rest data security via finer encryption granularity

Encryption key derivation for custom keys

When customizing an encryption key, whether personal or corporate, Mozy runs the passphrase you enter through multiple passes of the SHA-512 algorithm to create a hash of the passphrase. The 256-bit AES encryption key is created from the resulting hash. Mozy never has access to your encryption key and is not able to assist you in decrypting your files should you misplace the key.

Personal encryption keys

Once created, the encryption key is hashed through multiple passes of the SHA-512 hashing algorithm and then stored on the local system:

- On Windows, the hashed encryption key is stored in the registry. The key is additionally protected with the Microsoft Data Protection API and cannot be read by users or administrators of the machine.
- On Mac OSX, the hashed encryption key is stored in state.db.

Hashing the result ensures that the encryption key remains secure on the local system. You can also save the key to a .dat file for safekeeping should you need to reinstall the software in the future.

Corporate encryption keys

When creating corporate encryption keys, Mozy adds the encryption key to a .ckey file and encrypts the file using a shared secret. The shared secret ensures that even if your .ckey file is compromised, your encryption key cannot be read and used to decrypt your files. Keep in mind, the shared secret is not used to encrypt or decrypt your data. The shared secret is used to encrypt your encryption key adding another level of security to your data.

When you install the Mozy software on your endpoints, Mozy decrypts the corporate encryption key file so the encrypted passphrase can be stored on the local system. The encryption key is hashed through multiple passes of the SHA-512 hashing algorithm, encrypted with a Blowfish algorithm in CBC mode using a symmetric key obfuscated and hidden in the client binary, and then stored on the local system.

- On Windows, the hashed encryption key is stored in the registry. The registry entry is limited by access controls to SYSTEM. The key is additionally protected using the Microsoft Data Protection API, with a per-user encryption key, and cannot be read by users or administrators of
  the machine.
- On Mac OSX, the hashed encryption key is stored in state.db.

Which key is right for me?

The following table explains how the different types of encryption keys affect the capabilities available to users of the Mozy service.

Capabilities	Default Key	Personal Key	Corporate Key
Restore files using the backup software itself without providing an encryption key or taking extra, manual steps to decrypt.	Yes	Yes	Yes
Use the Mozy mobile app to obtain backed up files.	Yes	Yes	Yes; the .ckey file must be stored on a web server and accessible to mobile devices.
Use file preview in Mozy mobile app.	Yes	Yes	Yes
Use Mozy on the web to download and restore.	Yes	Yes; must manually decrypt with a decrypt utility.	Yes; administrator only; must manually decrypt with a decrypt utility.
Use the Mozy Restore Manager to restore files.	Yes	Yes	Yes, if the Restore Manager has access to the .ckey file from the location specified in the client configuration.
Use file preview, photo thumbnail, and file name search in Mozy on the web.	Yes	No; file name search is supported, but there is not file preview or thumbnail support.	No; the file name search is supported, but there is no file preview or thumbnail support.
Use Mozy Sync to update files on linked computers and to preview files and photo thumbnails.	Yes	Yes	Yes; however, Sync on mobile is not supported.

05/17, Data Sheet, H16342-IE