mozypro Online Backup

MozyPro Security White Paper

Industry-leading Security for Unsurpassable Data Protection

Executive Summary

This white paper describes the security and privacy features of the MozyPro backup service as it relates to the handling of user data. To give the reader a basic understanding of security and privacy principles applied to the system, the scope of this document is confined to the architectural concept level.

The MozyPro backup service security and privacy model is built on the principle of strong encryption, which includes using both data and transport encryption to protect our customers' data.

Mozy uses two types of data encryption, and allows the user to select their data encryption method at the time of installation. The first method uses the OpenSSL implementation of the keyed, symmetric block cipher known as Blowfish. This method encrypts data with a 448-bit key that is automatically generated during installation.. The second method uses 256-bit AES encryption, which is the de-facto standard used by the United States government and the National Security Agency. This method enables customers to specify a personal key known only to them and only stored only at their location.

Note: For the strongest security, select 256-bit AES encryption and specify a personal key.

In addition to data encryption, all communications between customer computers and MozyPro Servers are encrypted using a certified 128-bit SSL connection with two-way certificate verification.
The fundamental security questions that need to be answered are:

- What security mechanisms are employed when trying to write (back up) my data to a remote server?
- What security mechanisms are employed when trying to read (restore) my remote data?

Write (Backup) Process

Step 1
After the installation has completed, the Configuration Wizard starts. One of the steps in the Configuration Wizard is selecting the type of encryption you want to use. Users choose between two options for encryption:

- Encrypt my data with MozyPro's own 448-bit key
- Encrypt my data using 256-bit AES encryption with my own personal key

If you select Mozy's own 448-bit key, your data is automatically encrypted with no user intervention required. However, if you select AES encryption, you are prompted to enter a personal key (passphrase).

The length of the passphrase is not restricted. The Mozy client software uses a cryptographic hash of the passphrase. For convenience, you are asked whether you want to save the personal key to a file. If you select to save the key to a file, the key is saved as a plain text file to your hard drive. If you lose or forget your personal key, then all associated encrypted files cannot be decrypted by Mozy or any other entity.

Step 2
The backup process begins by making two Secure Sockets Layer (SSL) TCP connections through port 443 to the policy servers and the data servers. Both connections use two-way SSL certificate verification. Trusted server certificates, as well as the personal key and client certificate, are embedded in the mozybackup.exe binary.

Step 3
Next, the Mozy backup process authenticates the client with the Mozy remote servers. The username and the password are stored in the registry in a doubly-encrypted format, as well as being protected by an access control list (ACL) that grants access only to the system account. The first encryption process uses a symmetric key embedded in the Mozy client, and the second process uses Windows Cryptographic Services, utilizing a system-specific key stored in the Local Security Authority (LSA).

Once the name and password are extracted from the registry and decrypted, they are hashed and sent over both SSL connections that were established in Step 2. If both authentications succeed, the backup process continues with Step 4.

Step 4
In the final process of backing up, the Mozy backup process encrypts each file and transfers it to the remote Mozy servers. The encryption process reads the personal key out of the secure registry location, decrypting it with the Windows Cryptographic Services, and then decrypting it again with the shared symmetric key embedded in the mozybackup.exe binary.
For each file to be backed up, it is first encoded with a proprietary algorithm, and then encrypted with the Blowfish cipher using a symmetric key, or AES using the user-specified personal key. The file is then transferred over the SSL connection to the data servers, which was established in Step 2. This process continues until the last file is prepared and sent. At the end of the process, the Mozy log file is transferred and the connection closed.

The encrypted files are stored in a temporary directory until either the backup has completed or been canceled. Once the backup is complete or canceled, the files are removed from the temporary directory.

Read (Restore) Process- Reading (restoring) from the client

Step 1
For security reasons, users should always have to log in to the local machine from which the data was backed up. The login process requires a reasonable level of authentication to prevent unauthorized users from accessing the file system with the Windows Explorer interface.

Step 2
There are three ways to restore the data from Windows:

- With the restore tab of the client
- With the virtual drive created when you install the Mozy client, which contains a copy of all the files and folders that have been backed up
- By right-clicking in Windows Explorer and selecting the files to restore

Using any of these three options, a user can select the files and directories to be restored. The restore process then follows Steps 2 and 3 as previously described in the Write (Backup) Process.

Step 3
The restore process continues by requesting the files to be restored from the Mozy servers. The files are then copied to the local machine where they are decrypted. The decryption process begins with the decryption of the personal key using Windows Cryptographic Services and the shared symmetric key embedded in the mozybackup.exe binary. Each file to be restored is decrypted with the Blowfish cipher with a symmetric key, or AES using a personal key, and then written to the local machine in the location designated by the user. This process continues until the last file is written to disk and decrypted.

Read (Restore) Process- Reading (restoring) from the Web site

Step 1
First, an administrator must log in to the MozyPro Admin Console or a user logs in to the web console. Each must use a valid username and password. This website is secured by HTTPS and a signed SSL certificate.

Step 2
Administrators can access the backed up snapshots of any user’s machine that the administrator has administrative control over. Once the files are selected through the web application, the application creates a zip file that contains the files to be restored.

For end users, the user can click on a list of machines that are assigned to the user. The user can click on the name of the machine to be restored, then click Restore Files. Once the files are selected through the web application, the application creates a zip file that contains the files to be restored.

In both cases, the zip file is available to download from an unalterable, expiring URL. This URL must be considered sensitive data because no authentication is required to access it. The 41-character string shown in bold is an example of a secure hash of the URL which the MozyPro server checks to verify that the URL has not been altered.

http://downloads.mozy.com/r/1167/16249/18870/1160667383/334a67ceca1f4f5f3809061722da0cd7812603ac/mozy_2006_10_12_08_36_18870.zip

Step 3
After the zip file has been downloaded and extracted to a temporary directory, the files are ready to restore if you selected Blowfish encryption. If you selected AES encryption, the zip file needs to be decrypted using the Mozy Crypto Utility. The Mozy Crypto Utility is a stand-alone application that decrypts local file trees. You must enter your personal key into the Mozy Crypto Utility at the beginning of the decryption process. Once the files have been decrypted, they are ready to restore. The Mozy Crypto Utility can be downloaded at the link below.

http://www.mozy.com/downloads/mozycryptoutil.exe

Conclusion

In conclusion, MozyPro allows you to choose either 448-bit Blowfish encryption with a symmetric key, or 256-bit AES encryption with a personal key, to encrypt your data before it is sent over the Internet. An SSL connection is then used for maximum security when transporting your data to and from the Mozy data centers. The ability to use Blowfish or AES with a personal key prevents others from being able to access your data.