Keep Your Private Key Safe

https://campus.barracuda.com/doc/86545866/

The encryption key is the key to restoring your data. When using the Backup Agent, data is encrypted with AES 256 bit military-level encryption before being sent to Barracuda servers for storage. Your encryption key allows you to decrypt the data when performing restores and makes your data readable on your computer. The key is 48 characters in length and can be chosen as a private key or managed key.

A **private key** is completely user defined, meaning you decide exactly what 48 characters comprise your encryption. Since you define what the key is, you are responsible for keeping that key in a safe location that can be accessed in the event of a computer crash. Unfortunately, if you do not have your private key when you need to restore files, you are unable to restore them.

Using private keys are not supported for remotely installing via RMMs.

A **managed key** is an encryption key tied to your username and password and is generated by the ECHOplatform agent. You do not need to keep a copy of your managed key. The ECHOplatform agent system remembers the key for you.

If you have one type of encryption and would like to switch to another, the ECHOplatform agent needs to perform a full account reset from the ECHOplatform agent side. This reset, purges the data for an account from the ECHOplatform agent side, and makes the account as if you had never backed up with us, allowing you to pick the type of encryption key you would like when you re-install the software.

The encryption key is needed in case you need to restore your data. If you do not choose a managed key or have upgraded from an earlier version of the Backup Agent, you need to export and save your encryption key in a safe place.

Creating an Encryption Key

To create an encryption key, perform the following g steps.

1. Open the Backup Agent Monitor by selecting Start->All Programs->Barracuda MSP->ESureIT Monitor. You can also double-click the status icon in the System Tray.
2. Select Preferences.
3. In the General Settings, expand the Encryption Key section.
4. Click Save and select the desired location, such as a USB Thumb Drive.
5. Select Print to print the key.

Notes: Preserve the encryption key in a safe place that you can access in the event of any damage to your computer backing up with the ECHOplatform agent or any environmental disaster that may

happen to your home or office.

If you lose your private encryption key, Barracuda is unable to recover your data because the key is encrypted on Barracuda servers.

When you choose the private key option, each account gets a unique private key. Do not assume the same key applies to all accounts.