Decryption Key Image Backups

Microlite BackupEDGE has an extremely powerful encryption option. During initial setup, 2048 bit Encryption and Decryption keys are generated. It is extremely important to make a backup of the Decryption Keys (called a **Key Backup**) so that they can be restored when necessary for:

- On-Demand Restore of Encrypted Files
- Bare Metal Disaster Recovery

When running physical hardware, we recommend **Key Backups** be made to removable media such as:

- CD-R/RW (Optical Media)
- SharpDrive (Removable Flash / Disk Media)
- Floppy Disk (Legacy, very rarely used)

These can be take and locked somewhere safe until actually needed.

It is not normally a good idea to perform **Key Backup** to network-based *Resource* such as URL (FTP/FTPS) or S3CLOUD (Amazon, Wasabi, etc.). Backing up the Decryption Keys to the same *Resource* being used for encrypted backups is kind of like placing the data in the vault, locking it, then writing the combination on the outside of the door above the dial. Decryption Keys should always be stored separately.

In physical and virtual situations where it is not possible to simply create a **Key Backup** on removable media, it is possible to create a **Key Backup** to an ISO file, then copy this ISO file off the server and into a safe place. The ISO file may be:

- copied to a PC or other system with an optical drive and burned to CD or DVD media.
- used as an ISO image by a virtual optical drive.

Creating an ISO File (Other) Resource

To create an ISO File Resource:

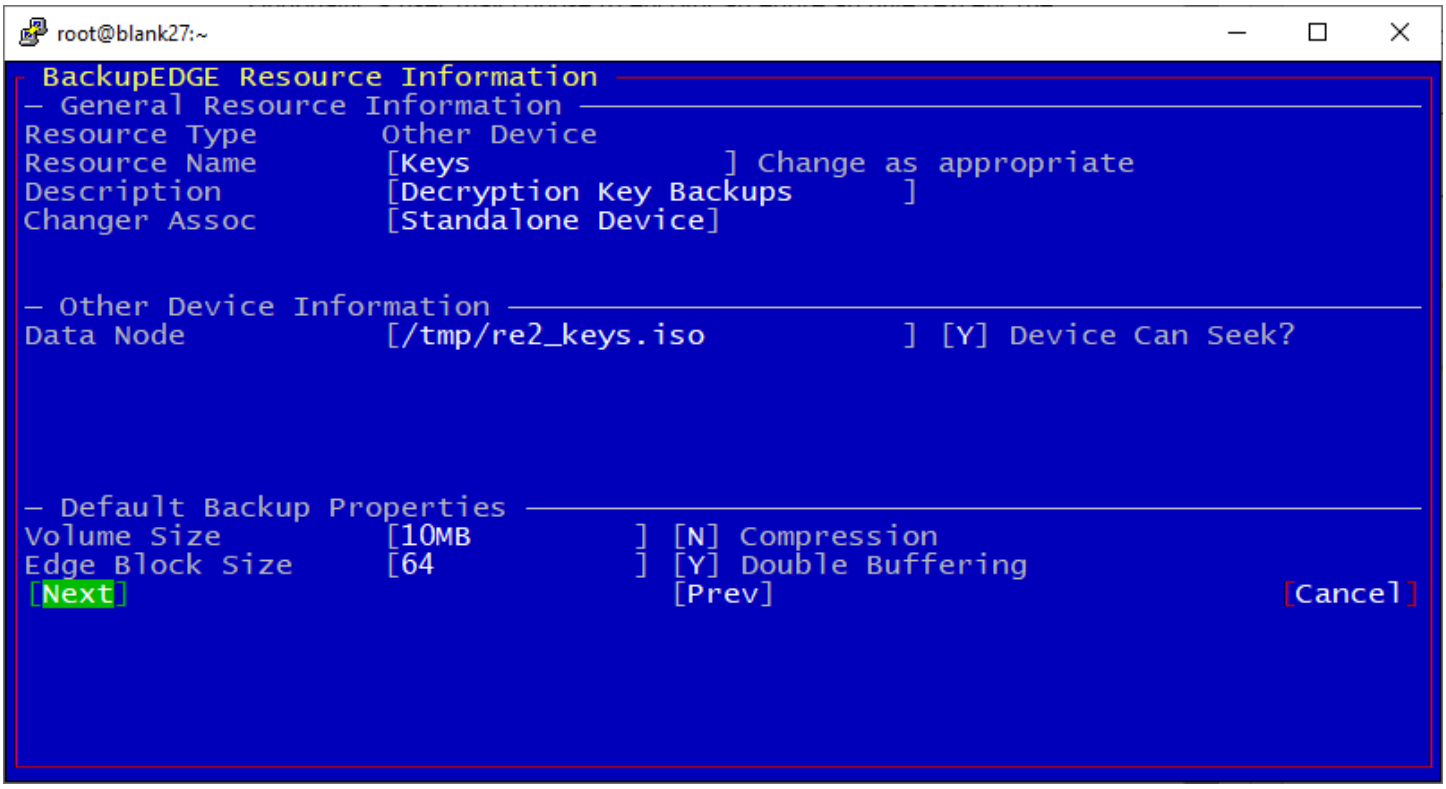
1. Launch ***EDGEMENU*** and select `[Admin]` -> `[Define Resources]`.
2. Scroll down and select `[New]`.
3. Select `Other Device (Other]`.
4. Change the Resource Name: to **`Keys`**.
5. `Tab` down to `[Next]` and hit `[Enter]`.

On the **`General Resource Information`** screen,

1. For **Description**, use: `Decryption Key Backup`
2. For **Data Node**, use: `/tmp/re2_keys.iso`
3. For **Volume Size**, use: `10MB`
4. Change **Compression** from `[S]` to `[N]` for None

When complete, the screen should look like the one below:

General Resource Information Resource Screen – Ready for Saving



Select `[Next]` to save the *Resource*.

Creating Decryption Key ISO Image

To create an ISO File Image:

1. Launch ***EDGEMENU*** and select `[Setup]` -> `[Decryption Key Backup]`.
2. Select `[Keys]` from the *Resource List*.
3. Select `[Proceed]`. And follow the prompts. When complete, exit ***EDGEMENU***.

Copy the Decryption Key ISO Image

Copy the **Decryption Key ISO Image** file (`/tmp/re2_keys.iso`) off the server to a secure location. You may use it on a Linux desktop or PC burn a CD as an ISO image for safekeeping.

NOTE: Many PC burning programs may not be able to burn a CD from this file. This is a Windows issue. Linux programs like cdrecord, wodim, etc. have no problems.

Delete the Decryption Key ISO Image

The last step is to delete **Decryption Key ISO Image** file (`/tmp/re2_keys.iso`) from the server. This ensures that no one else will have access to it.

```
# rm /tmp/re2_keys.iso
```

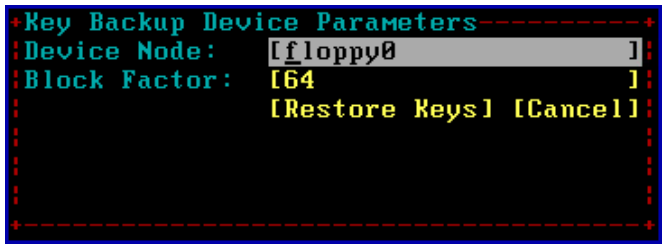
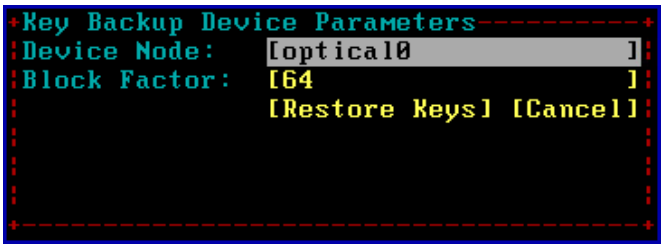
Note that you'll have to make sure that you delete the `/tmp/re2_keys.iso` before attempting to create the image for a second time.

Selecting The Decryption Key ISO Image in RecoverEDGE.

When performing bare metal disaster recovery, *Recover**EDGE*** will prompt for an archive to restore. If the header of the selected archive indicates that the archive has encrypted files, it will prompt for the Device Node (Resource Name) for the Decryption Key backup.

Load the CDROM or attach the **Decryption Key ISO Image** as appropriate.

Use the correct *Resource Name* (typically `optical0`) at the "**Device Node:**" prompt.

Default Resource	Type Resource Name
	

Then select `[Restore Keys]` to continue.

Microlite Corporation
Version 1.2 – June 23, 2021