BackupEDGE 03.05

MICROLITE CORPORATION

*User Guide - Release **03.05.04***

BackupEDGE 3.x User Guide - Revision 03.05.04 Build 1 - updated Dec 14, 2024

Microlite Corporation

2315 Mill Street
Aliquippa, PA 15001-2228 USA
(724) 375-6711 - Technical Support

https://www.microlite.com - Web
ftp://ftp.microlite.com - FTP
support@microlite.com - Support
sales@microlite.com - Sales

Table of Contents

Contents

1 - Introduction

Thank you for taking the time to read the User's Guide for Microlite *BackupEDGE™ 3.X* (referred to in this manual simply as *BackupEDGE*). As one of the most comprehensive data storage, retrieval and recovery products available for *UNIX*® and *Linux*® systems, *BackupEDGE* has many features and options that can help you effectively protect and manage your data. This manual will describe how to use them to get the most from your investment.

NOTE: Understanding the core concepts of the *BackupEDGE* architecture is the key to the most effective use of the product. Chapter 2, Anatomy of a *BackupEDGE* Backup, starts on page 40 and explains these concepts in detail.

BackupEDGE combines the following features:

- a powerful internal backup formatter which can archive and restore all of the file types typically encountered on a UNIX or Linux system, at very high speeds.
- Transparent Media™ technology, which provides an identical, full set of capabilities for all devices and network attached storage.
- a hardware reporting and control layer capable of taking maximum advantage of the features of today's most powerful storage *Devices*, while disappearing when legacy *Devices* are used.
- network capabilities that make *Remote Devices* respond and function as if they were attached to the local system.
- *Bare Metal Disaster Recovery* capabilities allowing bare metal disaster recovery on supported platforms[1].
- a flexible scheduler allowing the user to easily craft and manage multiple backup strategies.
- a secure encryption algorithm, to protect archives from unauthorized use (requires a separate license).
- A user interface that functions identically in character, graphical and *Web Services* modes. It is sophisticated enough to define advanced backup strategies, while simple enough to be used by persons without years of *UNIX* or *Linux* training.

Media Support

BackupEDGE can create and manipulate archives on any of the following media types...

- Network Attached Storage (NAS) servers/appliances using FTP, FTPS, NFS or CIFS.
- S3-Compatible (S3CLOUD) cloud backups to worldwide sites such as Amazon S3, Google Cloud Storage, Wasabi, Digital Ocean Spaces, Backblaze B2 and more.
- S3-Compatible Private Cloud (S3CLOUUD) services such as **MIN**IO.
- Removable Hard Disk Drives and Cartridges.
- Flash Media Cards.
- Tape Drives
- Blu-ray Disc™ BD-RE
- DVD Media, (DVD-RAM, DVD-RW, DVD-R, DVD+RW, DVD+R, DVD+R DL)
- CD-Recordables and Re-Writable Media (CD-R, CD-RW)

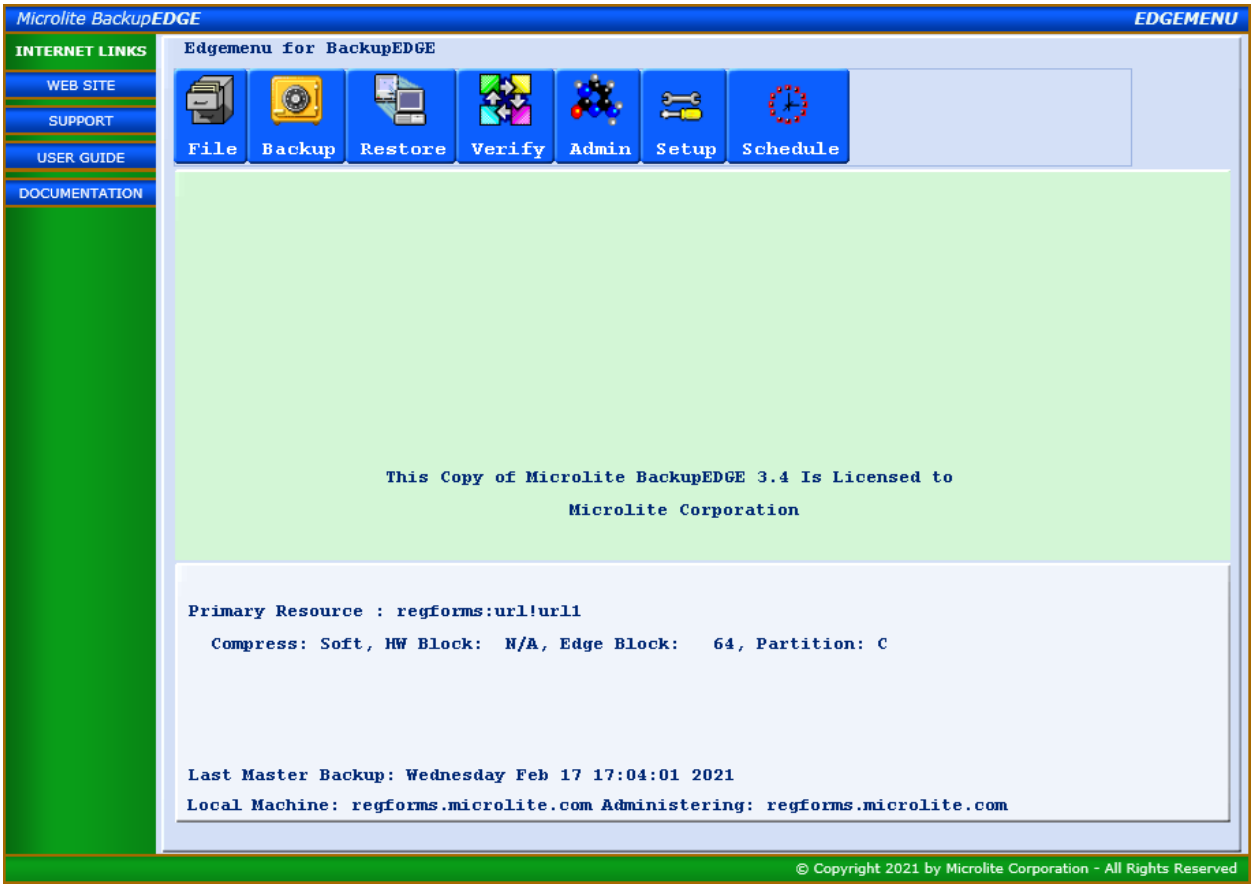
1. Linux (2.6.x - 6.x kernels), Xinuos SCO OpenServer 5.0.5-5.0.7/5.0.7V, 6.0.0/6.0.0V, UnixWare 7 (7.1.4,7.1.4+) and all Definitive.

In addition, *Backup**EDGE*** can manipulate SCSI/SAS Tape *Autochangers* and *Libraries*, providing for near-enterprise level backups.

User Interface

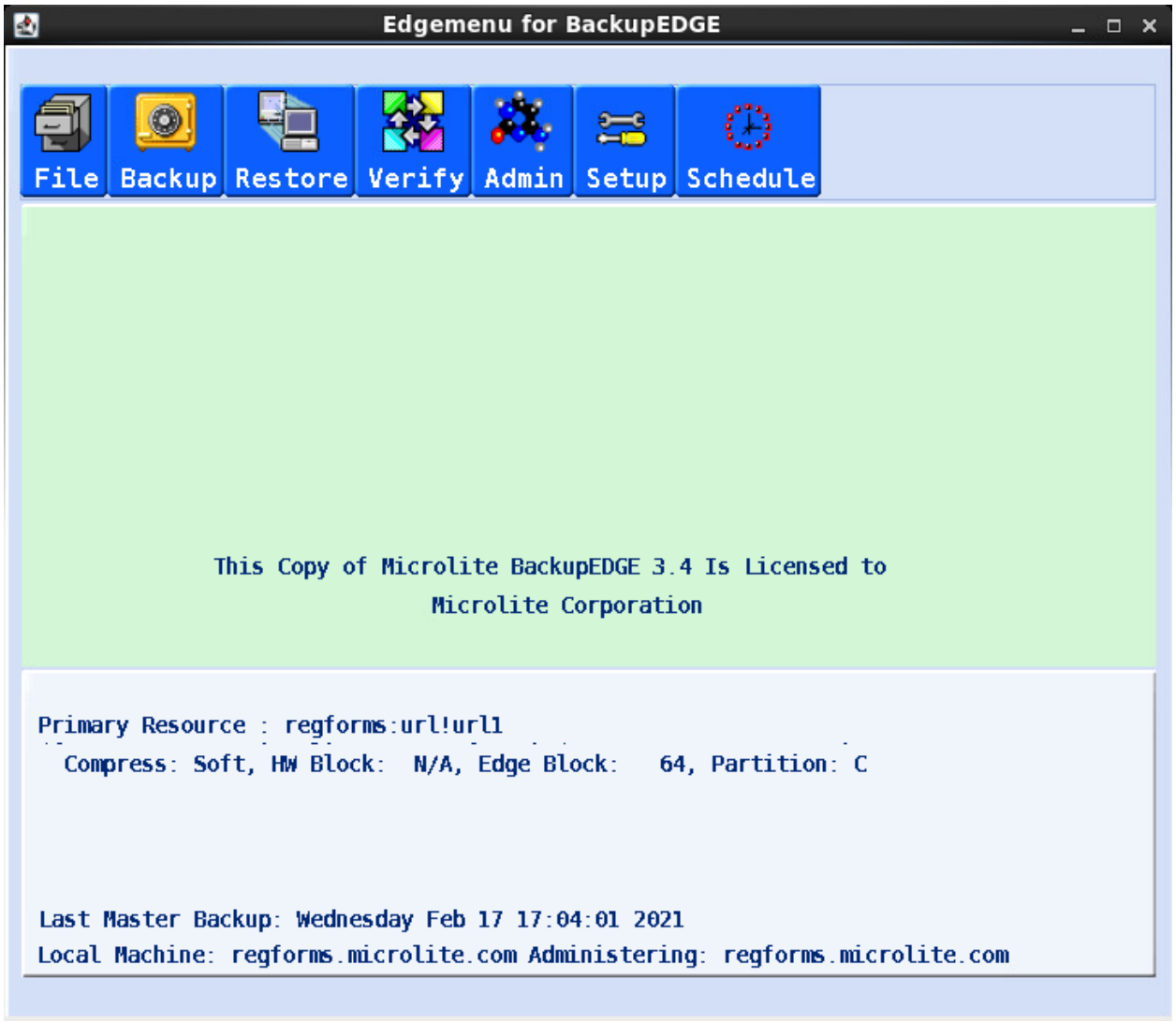
*Backup**EDGE*** is designed to be run via the *EDGEMENU* menu-driven user interface, which may be launched in one of three ways:

- in graphical mode as a *Web Service* from any web browser with a java plug-in, such as that on a Windows PC.



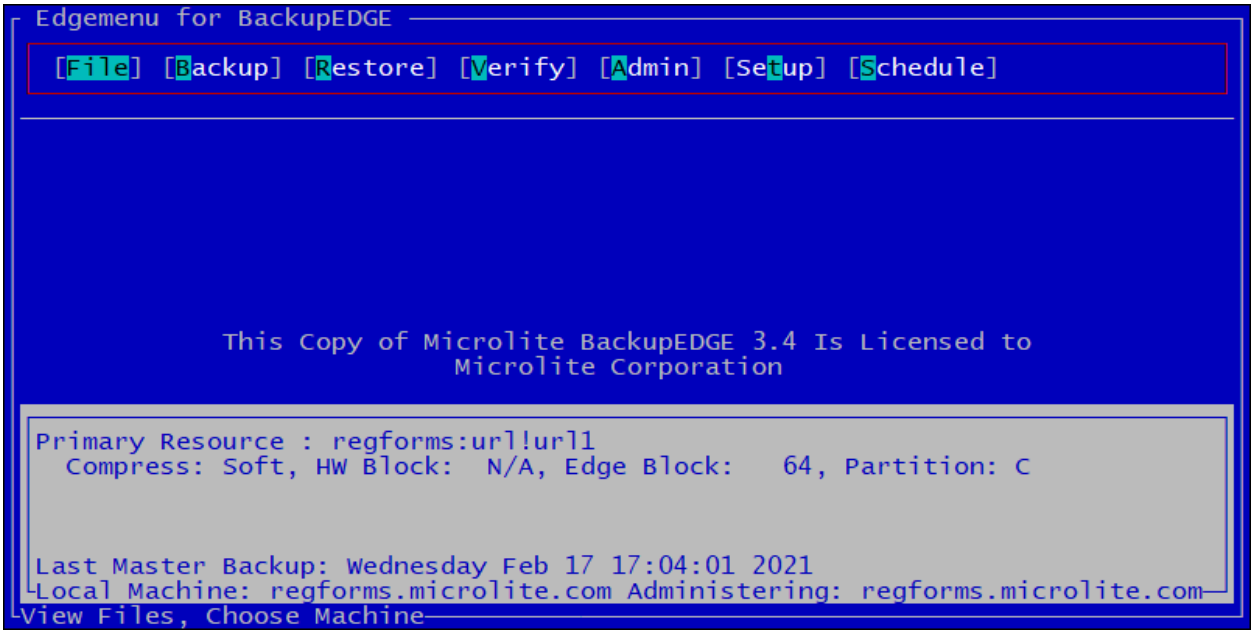
NOTE: Many web browsers have deprecated Java plug-in support. *Backup**EDGE*** is currently known to run as a *web service* only under the *Microsoft Internet Explorer* Java plug-in.

- in graphical mode on Linux X11 consoles or clients equipped with Sun Java 1.4.2 or later[1].



1. Linux Only.

- in character mode on system consoles, dumb terminals or xterm clients.



For reference purposes in this manual, and to save the space of including graphical screen shots everywhere, we're going to use a text representation of the character screen shots that looks like this:

```
+ Edgemenu for BackupEDGE ------------------------------------------------------+
|+-------------------------------------------------------------------------------+|
||  [File] [Backup] [Restore] [Verify] [Admin] [Setup] [Schedule]                ||
|+-------------------------------------------------------------------------------+|
|-------------------------------------------------------------------------------|
|                                                                               |
|                                                                               |
|                                                                               |
|                                                                               |
|                                                                               |
|                                                                               |
|                                                                               |
|                                                                               |
|             This Copy of Microlite BackupEDGE 3.4 Is Licensed to              |
|                               Microlite Corporation                           |
|                                                                               |
|+-------------------------------------------------------------------------------+|
||Primary Resource : regforms:url!url0                                           ||
||  Compress: Soft, HW Block:  N/A, Edge Block:   64, Partition: C              ||
||                                                                               ||
||                                                                               ||
||                                                                               ||
||Last Master Backup: Wednesday Feb 17 17:04:01 2021                            ||
|+Local Machine: regforms.microlite.com Administering: regforms.microlite.com-+|
+View Files, Choose Machine-----------------------------------------------------+
```

The current cursor position will be underlined. Hot Keys will be overlined. Blank lines in screen shots may be deleted to save space.

While it may also be administered and used from the command line, this manual focuses on using *Backup**EDGE*** with *EDGEMENU*, plus a few of the more useful command line tools. Advanced documentation can be found in machine readable format on the media the product is shipped on, as well as on the target system after installation and the Microlite Corporation FTP Site (`ftp://ftp.microlite.com`).

NOTE: Additional operating system support is added frequently in *Backup**EDGE*** builds. Please see the Microlite Web Site for the most current information.

2 - Major Changes / Improvements

2.1 - New Features In BackupEDGE 3.5 (03.05.04)

- OpenServer 6 D2M2 support on Proxmox (build 1).
- Added Red Hat Enterprise Linux 9.5 Support (build 1).
- Added Rocky Linux 9.5 Support (build 1).
- Added Oracle Linux Server 9.5 Support (build 1).
- Added Alma Linux 9.5 Support (build 1).

2.2 - New Features In BackupEDGE 3.5 (03.05.03)

- Added Support for Ubuntu Server 24.10 Oracular Oriole (build 3).
- Added Support for Ubuntu Desktop 24.10 Oracular Oriole (build 3).
- Added Support for OpenServer 6 D2M2 (build 3).
- Added Linux Mint 21.3 MATE support (build 2).
- Added Ubuntu 24.04 LTS Server Noble Numbat Support (build 2).
- Added Red Hat Enterprise Linux 8.10 Support (build 2).
- Added Rocky Linux 8.10 Support (build 2).
- Added Oracle Linux Server 8.10 Support (build 2).
- Added Alma Linux 8.10 Support (build 2).
- Added Red Hat Enterprise Linux 9.4 Support (build 1).
- Added Rocky Linux 9.4 Support (build 1).
- Added Oracle Linux Server 9.4 Support (build 1).
- Added Alma Linux 9.4 Support (build 1).
- Added Support for Virtual Clients on Promox 8.1.4
- Added Support for Virtual Clients on VirtualBox 7.0
- Added Support for Virtual Clients on QEMU-KVM 8.0
- Added Support for Virtual Clients on XCP-NG 8.2.1 with XEN Orchestra

2.3 - New Features In BackupEDGE 3.5 (03.05.02)

- Added New Product Release for Linux 6.X Kernels edelx60-64 (build 1).
- Added Red Hat Enterprise Linux 9.3 Support (build 3).
- Added Rocky Linux 9.3 Support (build 3.)
- Added Oracle Linux Server 9.3 Support (build 3).
- Added Alma Linux 9.3 Support (build 3).
- Added Red Hat Enterprise Linux 9.2 Support (build 1).
- Added Rocky Linux 9.2 Support (build 1.)
- Added Oracle Linux Server 9.2 Support (build 1).

- Added Alma Linux 9.2 Support (build 1).
- Added Ubuntu 23.04 Lunar Lobster Support (build 1).
- Added Ubuntu 22.04.3 Jammy Jellyfish Support (build 2).
- Added Ubuntu 22.04.2 Jammy Jellyfish Support (build 1).
- Added Ubuntu 20.04.6 Focal Fossa Support (build 1).
- Added extra disk handling for asynchronous disk discovery *Recover***EGDE** (build 2).
- Improved Network driver handling in *Recover***EGDE** (build 2).
- Improved Unixware module management RecoverEDGE (Build 2).

2.4 - New Features In BackupEDGE 3.5 (03.05.01)

- Added Ubuntu 22.10 Kinetic Kudu Server Support (build 2).
- Added Ubuntu Server 22.04.1 LTS Support (build 2).
- Added Ubuntu Server 20.04.05 LTS Support (build 2).
- Added SUSE Leap 15.4 Support (build 2).
- Added SUSE Linux Enterprise Server 15 Service Pack 4 Support (build 2).
- Improved UEFI entries during disaster recovery (build 2).
- Improved installer for stricter security system profiles (build 2).
- Added zstd compression kernel module support
- Added Red Hat Enterprise Linux 9 Support (build1).
- Added Red Hat Enterprise Linux 9.1 Support (build1).
- Added Rocky Linux 9 Support (build 1).
- Added Rocky Linux 9.1 Support (build 1).
- Added Oracle Linux Server 9 Support (build 1).
- Added Oracle Linux Server 9.1 Support (build 1).
- Added AlmaLinux 9 Support (build 1).
- Added AlmaLinux 9.1 Support (build 1).
- Added Oracle Linux Server 8.7 Support (build 1).
- Added Red Hat Enterprise Linux 8.7 Support (build 1).
- Added Rocky Linux 8.7 Support (build 1).
- Added AlmaLinux 8.7 Support (build 1).
- Improve GPT Library use.

2.5 - New Features In BackupEDGE 3.5 (03.05.00)

- Added Ubuntu Server 2022.04 LTS Support (build 2).
- Added Rocky Linux 8.6 Support (build 2).
- Added Oracle Linux Server 8.6 Support (build 2).
- Added AlmaLinux 8.6 Support (build 2)
- Added Red Hat Enterprise Linux 8.6 Support (build 2)

- Updated Linux SharpDrives to use EXT4 filesystems.(build 1).

2.6 - New Features In BackupEDGE 3.4 (03.04.02)

- Added Ubuntu Server 2021.10 Support (build 2).
- Added support for zstd-compressed kernels (build 2).
- Added Backblaze B2 Support.
- Added more S3 Signature 4 sites.
- Added port support for *S3CLOUD Resources*.
- Updated network libraries.

2.7 - New Features In BackupEDGE 3.4 (03.04.01)

- Improved UEFI table cleanup after recovery (build 3).
- Improved SharpDrive debugging (build 3).
- Fixed a partition sizing error with GPT (build 3).
- Added Rocky Linux 8.4 Support (build 2).
- Added AlmaLinux 8.4 Support (build 2).
- Added SUSE Linux Enterprise Server 15.3 Support (build 2).
- Added openSUSE Leap 15.3 Support (build 2).
- Added UEFI MD Support for:
  - SUSE Linux Enterprise Server 15.3 (build 2).
  - openSUSE Leap 15.3 (build 2).
- Fixed bug in *Resource Manager* under *Recover**EDGE*** (build 2).
- Improved Error Reporting in Summaries.
- Improved Log File Messages.
- Improved MD Support for grub2 on BIOS systems.
- Added UEFI MD Support for:
  - Red Hat Enterprise Linux 8.x
  - CentOS 8.x
  - Oracle Linux Server 8.x
  - Red Hat Enterprise Linux 7.x
  - CentOS 7.x
  - Oracle Linux Server 7.x

2.8 - New Features In BackupEDGE 3.4 (03.04.00)

- Added Ubuntu 21.04 Server and Desktop Support (build 2).
- Updated network libraries (build 2).
- Dynamic loop device discovery added (build 2).
- Fixed disaster recovery with GPT onto devices originally DOS-formatted (build 2).
- Added support for Intel I210-series NICs (build 2).
- Added Ubuntu 20.04.2 LTS Server and Desktop Support.

- Added NVMe Support for:
  - Red Hat Enterprise Linux 8.x
  - CentOS 8.x
  - Oracle Linux Server 8.x
  - SUSE Linux Enterprise Server 15 SP2
  - Ubuntu Server 19.04, 19.10, 20.04 LTS, 20.10
- Added /dev/vdX hard drive node Support.
- Added ability or Grub2 to be installed without a /boot partition.
- Improved remote installation and EDGEMENU update issue.

2.9 - New Features In BackupEDGE 3.3 (03.03.01)

- Added Red Hat Enterprise Linux 8.3 Server Support (build 2).
- Added Oracle Linux Server 8.3 Support (build 2).
- Added CentOS 8.3-2011 Support (build 2).
- Added Ubuntu 20.10 Server and Desktop Support (Build 2).
- Added Ubuntu 20.04.1 LTS Server and Desktop Support (Build 2).
- Added Ubuntu 20.04 LTS Server and Desktop Support (Build 2).
- Added Linux Mint 20 Support (Build 2).
- Added Red Hat Enterprise Linux 8.2 Server Support.
- Added Oracle Linux Server 8.2 Support.
- Added CentOS 8.2-2004 Support.
- Improved S3CLOUD [Test URL] Support for Wasabi.
- Updated and Optimized EDGE.REMOVE.
- Fixed Legacy OSR6 psm_apm module handling.
- Fixed 32-Bit Linux SharpDrive Booting.

2.10 - New Features In BackupEDGE 3.3 (03.03.00)

- Updated Linux GPT Libraries (build 3).
- Updated all communications and security libraries where appropriate (build 3).
- Excluded new modules in *Recover**EDGE*** for Linux (build 3).
- Added Ubuntu 19.10 Server Support (build 2).
- Fixed an xterm-256 / ncurses emulation issue in Linux 5.x Kernels (build 2).
- Improved Test URL menu option to work better with Wasabi (build 2).
- Added New Product Release for Linux 5.x Kernels - edgelx50_64.
- Added Ubuntu 19.04 Server Support
- Updated Compression Libraries

2.11 - New Features In BackupEDGE 3.2 (03.02.03)

- Added SUSE Linux Enterprise Server (SLES) 15 Service Pack (SP) 1 Support (build 2).

- Added LVM support in *Recover**EDGE*** for multiple SLES and openSUSE releases (build 2).
- Added additional fields to *Dealer Information* section of *Backup Reports* (build 2).
- Modernized HTML version of the *Backup Reports* (build 2).
- Updated the Java detector to work better with SLES / openSUSE (build 2).
- Added support for *Recover**EDGE*** for Red Hat Enterprise Linux (RHEL) 8.
- Improved multiple archives per medium support for tape drives under Linux.

2.12 - New Features In BackupEDGE 3.2 (03.02.02)

- Added network bonding support in *Recover**EDGE*** for the Red Hat Enterprise Linux 7 family, including CentOS 7, Oracle Linux Server 7, and Scientific Linux 7.
- Added network bonding support in *Recover**EDGE*** for Ubuntu 18 / 17 / 16 servers.
- Added a *Resource Edit* tab to *Recover**EDGE***[1].
- Improved handling of network stack calls (Linux).
- Updated all communications and security libraries.

2.13 - New Features In BackupEDGE 3.2 (03.02.01)

- Resolved an LVM boot time issue after a recent Linux patch (build 8).
- Added SUSE Enterprise Linux Server 12 SP4 Support (build 7).
- Added SUSE Linux Enterprise Server 15 Support (build 6).
- Added Ubuntu 18.04 support (build 6).
- Added openSUSE Leap 15 Support (build 4).
- Updated all communications and security libraries (build 4).
- Improved S3CLOUD Performance (Build 3).
- Added CentOS 7-1804 (CentOS 7.5) support (Build 3).
- Added Scientific Linux 7.5 support (Build 3).
- Improved Ubuntu 18.04 LTS support (build 3).
- Added SharpDrive booting support to LEAP 42.x [FDISK / BIOS Only] (build 3).
- Updated all communications and security libraries (build 3).
- Added Red Hat Enterprise Linux 7.5 Support (build 2).
- Added Oracle Linux Server 7.5 Support (build 2).
- Added ClearOS support (beginning with ClearOS 7.4).
- Added Xinuos SCO OpenServer 6 Definitive 2018 (D2M1) support.
- Added Xinuos SCO UnixWare 7 Definitive 2018 (2DM1) support.

2.14 - New Features In BackupEDGE 3.2 (03.02.00)

- Improved UEFI .efi File Management (build 3).
- Updated all communications and security libraries (build 3).

1. Does not include OpenServer 5.

- Added Ubuntu 17.10 support (build 2).
- Updated all communications and security libraries (build 2).
- Added GPT debugging (build 2).
- Added UEFI Support for the following operating systems.
  - Red Hat Enterprise Linux 7 and later (build 1).
  - Oracle Linux Server 7 and later (build 1).
  - CentOS 7 and later (build 1).
  - Scientific Linux 7 and later (build 1).
  - SUSE Enterprise Linux Server 12 SP2 and later (build 1).
  - openSUSE LEAP 42.2 and later (build 1).
  - Ubuntu 16.04 LTS and later.
- Added Support for SUSE Enterprise Linux Server 12 SP3.
- Added Support for openSUSE LEAP 42.3.

2.15 - New Features In BackupEDGE 3.1 (03.01.05)

- Added Support for Oracle Linux Server 7.4 (build 3).
- Added Support for Red Hat Enterprise Linux 7.4 (build 3).
- Added Support for Ubuntu Server 16.04.3 LTS (build 3).
- Improved Tape Drive Error Message Reporting (build 3).
- Full support (including *RecoverEDGE*) for Ubuntu 17.04 and 16.10 server (build 2).
- Support for Amazon S3 Signature Version 4 and with it all worldwide Amazon S3 sites.
- Improved XFS filesystem handling.
- Compression level added to reports.
- Updated all communications and security libraries.

2.16 - New Features In BackupEDGE 3.1 (03.01.04)

- Support for Red Hat Enterprise Linux 7.3 and CentOS 7.3 (1611) (build 2).
- Support for GPT-configured disk drives in many Linux distributions (build 1).
- Updated all communications and security libraries (build 1 & 2).

2.17 - New Features In BackupEDGE 3.1 (03.01.03)

- Commercial Java Code Signing Certificate updated in Java web client (build 6).
- Updated all communications and security libraries (build 6).
- Added Hyper-V as a Linux P2V supported platform (build 5).
- Added Ubuntu 16.04 LTS support (build 5).
- Improved database management for Fast File Restore / Instant File Restore (build 5).
- Updated all communications and security libraries (build 4).
- EDGEMENU and Help File cosmetic improvements (build 4).
- Ubuntu 15.10 patch (build 4).

- Support for Xinuos *OpenServer 5 Definitive D1MO*, *OpenServer 6 Definitive D2MO*, and *UnixWare 7 Definitive D2MO* (Build 3).
- Support for CIFS Backup and Disaster Recovery - Linux (Build 2).
- Improved support for bootable SharpDrives - Linux (build 2).
- Updated all communications and security libraries (build 2).
- Support for Ubuntu 15.10 Server (build 1).
- Linux 4.x Kernel Support and distributables (build 1).
- Updated all communications and security libraries (build 1).

2.18 - New Features In BackupEDGE 3.1 (03.01.02)

- Support for Red Hat Enterprise Linux 6.7 (build 2).
- Improved MySQL/MariaDB detection for newer versions (build 2).
- Updated all communications and security libraries (build 2).
- SharpDrive now supports FDISK or GPT partitioning. (build 1).
- *NFS Backups* now supported for backup and disaster recovery (build 1).
- Updated all communications and security libraries (build 1).
- Ubuntu 15.04 is now supported (build 1).
- Internal double buffering setting now defaults to ON (build 1).

2.19 - New Features In BackupEDGE 3.1 (03.01.01)

- Red Hat Enterprise Linux 7.1 support (build 4).
- Updated all communications and security libraries (build 3).
- Added Google Cloud Storage support to *s3cloud* Resource type (build 3).
- Ubuntu 14.04.2 supported. (build 3).
- Fixed issues on *Recover**EDGE*** with OpenServer 6 and Dell servers with newer USB chipsets (build 3).
- Reclamation may be disabled on fsp, s3cloud, url Resources (build 2).
- Added Standard Amazon S3 Bucket Resource (s3cloud) and Worldwide Region Support.
- Updated all communications libraries for latest security patches and improvement.

2.20 - New Features In BackupEDGE 3.1 (03.01.00)

- Java Graphical and ncurses character interface updates (build 3).
- CentOS 7 support (build 2).
- CentOS 7 / Red Hat Enterprise Linux 7 support (build 2).
- Commercial Java Code Signing Certificate added to Java web client (build 2).
- Improvements in communications libraries and in Amazon S3 support (build 2).
- Red Hat Enterprise Linux 7 support, including MD device support.
- Ubuntu 14.04 LTS support.

- Communication libraries have all SSL/TLS vulnerability updates through (CVE-2014-0224) June 05, 2014.
- *Recover**EDGE*** bnx2 network driver support improved.

2.21 - New Features In BackupEDGE 3.0 (03.00.07)

- New **P2V** capability built into RecoverEDGE for Linux. See page 300.

2.22 - New Features In BackupEDGE 3.0 (03.00.06)

- Updated GUI to support newer JAVA releases (build 5).
- New user accessible info provided under edge.segadm -terse flag (build 4).
- Better FFR/IFR Index database management for deleted archives (build 4).
- Detection of VMware host for RecoverEDGE under osr6 and uw7) (build 4).
- Improved Desktop Icon Support (build 3).
- Linux internal detection and improvements (build 3).
- Updated communications libraries (build 2).
- Improved “Copy To” function with network / AWS backups (build 2).
- Improved USB keyboard support when used with (build 2).
- Switched default ISO boot loader to LILO for increased compatibility (build 2).
- SUSE Linux Enterprise Server (SLES) 11 SP2 support.
- Added Ubuntu 12.10 and 13.04 Server support.
- Improved SharpDrive™ autodetection.
- Added BNX2 firmware download support to *Recover**EDGE*** for Linux.
- Improved GRUB, devicemap, and udev recognition.

2.23 - New Features In BackupEDGE 3.0 (03.00.05)

- Added Xinuos SCO UnixWare 7.1.4+ support (build 6).
- Added *Recover**EDGE** Resource Manager* [does not include OpenServer 5] (build 6).
- Improved *Recover**EDGE*** swap initialization and extended partition detection in Linux (build 6).
- Support for Open SUSE 12.2 (build 5).
- Improved *Recover**EDGE*** performance for UnixWare 7.1.4 and OpenServer 6/6v (build 5).
- MD RAID support for Red Hat Enterprise Linux 6.x and CentOS 6.x.
- SUSE Linux Enterprise Server (SLES) 11 SP2 support.

2.24 - New Features In BackupEDGE 3.0 (03.00.04)

- First 3.0.x Linux kernel support.
- Ubuntu 10.10 / 11.04 / 11.10 / 12.04 support.
- OpenSUSE 11.4 support.
- Xinuos / SCO OpenServer 6.0V support (build 3).

2.25 - New Features In BackupEDGE 3.0 (03.00.03)

- Red Hat Enterprise Linux 6.2 support (03.00.03 build 7).
- CentOS 6.2 support (03.00.03 build 7).
- Red Hat Enterprise Linux 6.1 support (03.00.03 build 5).
- CentOS 6.0/6.1 support (03.00.03 build 5).
- Red Hat Enterprise Linux 6 support (03.00.03 build 3).
- *SharpDrive*™ USB / SATA removable flash / disk / cartridge support (Linux, OpenServer 6, UnixWare 7. See “Configuring SharpDrive Backups” on page 80.
- *Recover**EDGE** SharpDrive* boot support (Linux).
- LTO5 tape drive support.
- *Recover**EDGE*** support for bzipped / lzma-compressed kernels (Linux).
- *Scheduler Copy To* support for *Sequence Retention*. See page 218.
- New default for tape drives - Multiple Archives Per Medium Disabled.

2.26 - New Features In BackupEDGE 3.0 (03.00.02)

- Multiple retention times per-schedule are now permitted.

2.27 - New Features In BackupEDGE 3.0 (03.00.01)

- Added GRUB2 support for Ubuntu 9.10 and 10.04LTS.
- Improved MySQL and *Recover**EDGE*** Error Reporting.
- Updated License Manager.

2.28 - New Features In BackupEDGE 3.0 (03.00.00)

- MySQL Hot Backups.
- Blu-ray Disc (BD-RE) support.
- All Blu-ray, DVD and CD resources renamed “optical”.
- Multiple Archives per medium support on tape, BD-RE, DVD+RW, DVD-RAM and REV media.
- New more flexible Scheduler.
- Quotas on URL, FSP and AWS *Resources*.
- Archive Retention Times.
- Disk-to-Anything-to-Anything Backups.
- Updated Web Browser / Java version of *EDGEMENU*.

2.29 - Operating System Abbreviations

Throughout this manual we will refer to specific operating systems using the following abbreviations:

- *Linux* - Linux operating systems (EM64T / AMD64 / IA32) with a 2.6.x through 5.x kernels.
- *OSR6* - Xinuos SCO OpenServer 6.0.0, 6V and 6 Definitive D2M0 and D2M1.
- *OSR5* - Xinuos SCO OpenServer 5 (5.0.5 - 5.0.7, 5.0.7V and 5 Definitive D1M0 and D2M1).

- *UW7* - Xinuos SCO UnixWare 7.1.4, 7.1.4+ and 7 Definitive D2M0 and D2M1.

2.30 - Specific Operating System Release Support

Operating systems add releases, patches and updates too rapidly to be included in tables in this User Guide. The Microlite Web Site (`http://www.microlite.com`) has two sections to keep users apprised of currently supported operating systems and releases. From the home page, see the links for **Linux Support Tables** and **UNIX Support Tables**.

2.31 - Specific Device Support

This user guide cannot hope to keep up with the capabilities of various devices on each operating system. The Microlite Web Site (`http://www.microlite.com`) has a full support section, plus a Device Compatibility section under `Device Support Tables`. Please see the web site for technical details on device issues.

3 - Terminology

3.1 - Terms Used In This Manual

An understanding of the basic terms used in this manual will help the reader to understand the concepts used by *Backup**EDGE***.

As *Backup**EDGE*** runs equally well on *UNIX* or *Linux* systems, and both are similar, the term *UNIX* when used throughout this manual may be taken to mean either *UNIX* or *Linux*, unless a specific reference must be made.

Absolute Pathname: A filename beginning with a slash (`/`). A file saved with an absolute pathname (such as `/etc/termcap`) may only be restored to the `/etc` *Directory*.

Access Control List: An additional security permission level above the User/Group/Other permissions normally associated with UNIX files.

Advanced Schedule: A *Scheduled Job* created by the user to perform archiving tasks which differ in capability from the default *Basic Schedule*.

Archive: a collection of files of a particular *Domain* at a particular time, such as "*Master Backup of the domain* `system` *at midnight on October 1st, 2014*".

Archive Device: The floppy disk drive, tape drive, DVD, CD-R, CD-RW drive, etc., used to backup and restore files. You may also backup and restore to a regular file. *Archive Devices* are described to *Backup**EDGE*** with a *Resource*.

Archive ID: an identifier that uniquely identifies an *Archive*. All *Instances* of the same *Archive* have the same *Archive ID*. It is stored in the *Label* for every *Segment* of every *Instance*.

Autochanger: A *Device* containing one or more tape drives and one or more tape cartridge storage slots (also called magazine elements). Tapes may be moved automatically between storage slots and tape drives by *Backup**EDGE***. Also known as a *Library* or *Autoloader*.

Autoloader: See *Autochanger*.

Background Task: Background and *Foreground* have special meaning to the *UNIX* Operating System. *Foreground* tasks are generally run in interactive mode, meaning that information from the program is displayed on the screen and input is typed on the keyboard. *Background* tasks run as "unattached" programs requiring no display output or keyboard input. They can be started automatically by the *UNIX* `cron` or `at` scheduling programs, or by a *Foreground* program.

Backup Domain: See *Domain*.

Basic Schedule: The default system backup *Scheduled Job* created during initial installation or the first time the *Basic Schedule* command is accessed from *EDGEMENU*. This is the most frequently run full system backup task. Generally, a *Basic Schedule* is used to perform daily *Master Backups*. More complicated arrangements usually use *Advanced Schedules*.

Binary File: A file containing characters other than those in the ASCII decimal range of 32 to 127 (hex 20 to 7f). A compiled C program is an example of a *Binary File*. *Backup**EDGE*** can backup and restore these files without special consideration.

Bit-Level Verify: See *Level 2 Verify*.

Block: Unit of measure. There are typically 512 characters, or bytes, in a *Block*.

Block Size, Edge: See *Edge Block Size*.

Block Size, Hardware: See *Hardware Block Size*.

Block Size, Tape: See *Hardware Block Size*.

Blu-ray Disc:. A Device which can record on all CD and DVD media, plus 25GB and 50GB BDR (write-once) and BD-RE (re-writable) media. *Backup**EDGE*** can be used with BD-RE, DVD and CD media on these devices.

Bootable Tape: Media created in a *Bootable Tape Drive* (see below).

Bootable Tape Drive: Tape drives that have a BIOS allowing them to be booted from as if they were a CD-ROM. Used for creating archives that can boot directly into disaster recovery mode. The Hewlett Packard (*OBDR*) standard is supported.

Button: A prompt for an action using the character interface. “Press the `[Next]` Button” means “use the arrows or `[Tab]` key until the `[Next]` prompt is highlighted, then press `[Enter]`”.

CD-Recordable: A *Device* which can record on write-once CD media. The term *CD-R/RW* is used in this manual to refer to both *CD-Recordable* (*CD-R*) and *CD-Rewritable* (*CD-RW*) *Devices* and media unless a specific reference must be made.

CD-ReWritable: A *Device* which can record on re-writable CD media. The term *CD-R/RW* is used in this manual to refer to both *CD-Recordable* (*CD-R*) and *CD-Rewritable* (*CD-RW*) *Devices* and media unless a specific reference must be made.

CD-R/RW: A reference to either *CD-R* or *CD-RW Devices* and media.

CIFS Backups. Backups using the Common Internet FileSystem network transport protocol. Also known as SMB or SAMBA backups.

cpio: A backup utility program included with the *UNIX* Operating System.

Cron: A *UNIX* Operating System program that always runs when the operating system is in multi-user mode. It constantly looks in a set of files called `crontab` files for programs to run and times to run them.

Device: A *Device* is a piece of hardware, such as a disk drive or a printer, that is attached to a computer. Almost every *Device* is assigned a *Device Node* to access it through software.

Device Node: The name which the operating system uses to access a physical *Device*. For example, `/dev/hd0` is one possible name for a primary hard disk, while `/dev/lp0` is a typical name used to access a line printer. *Devices* are found in the `/dev` *Directory*.

Differential Backup[1]*:* A backup of any files or *Directories* in a *Sequence* that have been created or modified since the last *Master Backup* of that *Sequence*.

Directory: A unit of organization in a *UNIX* filesystem. Files are organized into groups, called a *Directories*. *Directories* may contain files, other *Directories*, or both. Also called a *Folder*, usually by users of Microsoft Windows.

Disaster Recovery: The process of restoring all of your operating system and user data in the event of a hard drive change or failure, or other catastrophic loss of data. Also called *Crash Recovery*.

Domain: Also called a *Backup Domain*. This is the complete definition of a group of files or objects to be protected by *Backup**EDGE***. It describes a list of files to be protected (included) or not protected (excluded) by backups of this *Domain*, any preparation scripts to be run before and after the backup, lists of *Raw Filesystem Partitions* within the *Domain*, and more.

dump: A backup utility program included with the *UNIX* Operating System.

DVD-RAM: A next-generation storage *Device* capable of writing and reading up to 4.3GB (uncompressed) of data per platter, while also being able to read standard *CD-R/RW* media.

1. In previous versions of *Backup**EDGE*** this was known as an Incremental Backup.

DVD-R: A write-once storage *Device* capable of writing and reading up to 4.3GB (uncompressed) of data per platter, while also being able to read standard *CD-R/RW* media.

DVD-RW: A storage *Device* capable of writing and reading up to 4.3GB (uncompressed) of data per platter, while also being able to read standard *CD-R/RW* media. The media performance and longevity are different from DVD-RAM.

DVD+RW: A next-generation storage *Device* capable of writing and reading up to 4.3GB (uncompressed) of data per platter, while also being able to read standard *CD-R/RW* media. The media performance and longevity are different from DVD-RAM.

DVD+R: A write-once format supported by second generation DVD+RW *Devices*.

Edge Block Size: The number of 512 character segments of data that can be read or written at one time by *Backup**EDGE***.

Element: A tape *Autochanger* is composed of up to four types of *Elements*. **dt** *Elements* are **D**ata **T**ransfer units. That's the tape drive or drives. **st** *Elements* are called **St**orage units. Those are the slots or other places that media or cleaning cartridges are stored. **ie** *Elements* are **I**mport/**E**xport units. These are used to get a tape into and out of a larger *Library* without actually opening the case. Finally, **mt** *Elements* are **M**edium **T**ransport units. These are technically the robotic arms that move things around. Only the largest *Libraries* have **ie** *Elements* that can be addressed. Desktop *Autochangers* typically only move cartridges between **dt** and **st** *Elements*, although **mt** *Elements* may be referenced.

Encryption: The ability to hide information from unintended recipients by combining the data with an *Encryption Key*, such that only with the corresponding decryption key can the original information be recovered.

Encryption, RSA: An asymmetric cipher used by *Backup**EDGE*** for exchange of AES encryption keys.

Encryption, AES: A symmetric cipher used by *Backup**EDGE*** for encrypting data on an archive.

Expired Archives: See *Retention Time*.

Fast File Restore: The Microlite-defined term for *Quick File Access*, which means being able to position to any particular spot or spots on backup tape and restore files or *Directories* without having to wait while each individual file on the media is read and examined. Referred to as *FFR*. For non-tape media, see *Instant File Restore*.

FastSelect: A user-interface construction used within *EDGEMENU* whereby selections can be made using the arrow keys while the cursor is on a `[Next]` button or other prompt.

Filename: The human readable name for a *File* or *Directory*.

Filesystem: A filesystem is a hierarchy of files and *Directories*, typically mounted under the system *Root Directory*, and contained on a single hard drive or other direct access storage *Device*.

FTP Backups. The creation of backups across the network using any computer, device or appliance equipped with an FTP and / or FTPS server as a valid storage device.

Folder: See *Directory*.

Graphical User Interface (GUI): A picture-oriented navigation screen using mouse movement and clicks for navigation, as opposed to typical data terminals using keyboard input, typed and line draw characters. The typical GUI used by *UNIX* systems is called the *X Window System*. Terms such as *KDE* and *Gnome* also refer to GUIs built (generally) on top of the *X Window System* to provide a specific "look and feel".

Hardware Block Size: The number of bytes of data that the storage *Device* writes at one time as a "block" of data. As *Tape Devices* are the most likely *Devices* to have this capability set or changed, this manual usually refers to *Hardware Block Size* as *Tape Block Size*.

Icon: A picture or text image, usually displayed on the *Graphical User Interface* (*GUI*) of the *UNIX* system. Single clicking or double clicking the *Icon* usually executes the program described by the *Icon*.

Incremental Backup: A backup of any files or *Directories* in a *Sequence* that have been created or modified since the last *Differential* or *Incremental Backup* in that *Sequence*. It is possible to have multiple active *Incremental Backups* within a *Sequence*.

Instance: one particular copy of an *Archive* on a *Medium*. In general, when one refers to a *Backup*, one is talking about one *Instance*.

For example, when the *Scheduler* runs a *Scheduled Job*, it creates one instance of a new archive for each Domain that is supposed to be backed up as part of the *Scheduled Job*. If a *Scheduled Job* is supposed to back up the `System` and `mysql` *Domains*, then the *Scheduler* will create one *Instance* for each of two new *Archives*.

Instance ID: an identifier that uniquely identifies an *Instance*. All *Instances* have a unique *Instance ID*. Each segment of the *Instance* has this *Instance ID* stored in it.

Instant File Restore™: The Microlite-defined term for *Quick File Access* for optical or other random access media, or files containing archives. It means being able to position to any particular spot or spots on the archive and restore files or *Directories* without having to wait while the archive is read sequentially. Referred to as *IFR*.

Iomega REV™. See *REV*

Job: See *Scheduled Job*.

Job ID: an identifier that uniquely identifies a run of a *Scheduled Job*.

Every *Instance* created by a single run of a *Scheduled Job* shares a *Job ID*. If a *Scheduled Job* is supposed to back up the `System` and `mysql` *Domains*, both *Instances* would share the same *Job ID*, but no other *Instance* would.

*Label: Backup**EDGE*** includes information about every *Segment* at the start of that *Segment*. This *Label* tells roughly what the *Backup* contains, when it was made, what *Instance* this *Segment* belongs to, the order of this *Segment* relative to the other *Segments* in this *Instance*, etc.

If two *Instances* of the same *Archive* exist, it is not the case that one can necessarily interchange the *Segments* which comprise them. For example, one cannot generally read the first *Segment* of *Instance 1* then the second *Segment* of *Instance 2*, and expect to get anything useful from it. While they contain the same data if extracted, that data might be stored differently between the two *Instances*. The number of *Segments* might not even be the same.

Lazy Reclamation: A *Backup**EDGE*** exclusive! When an archive's *Retention Time* has expired it won't automatically be deleted if *Lazy Reclamation* is enabled. Instead, it will only be deleted if additional free space is required on the chosen storage *Resource*.

Legacy Backup: An archive made by a version of *Backup**EDGE*** prior to 03.00.00.

Legacy Mode: An option for performing tasks in *EDGEMENU* which bypass the normal screen controls and display the direct output of the backup formatter in a format similar to older versions of *Backup**EDGE***. In *Legacy Mode* it is possible to interrupt and restart *Jobs*.

Level 1 Verify: A method of reading back an archive and checking for media readability and file header integrity.

Level 2 Verify: A method of reading back an archive and comparing each file on a character by character basis against the actual file on the hard disk. Also known as a *Bit-Level Verify*.

Library: See *Autochanger*.

Link: The technical term for the human readable name for a *File* or *Directory*. A single real file may have more than one *Link*, or filename. To remove a *File* and re-allocate its space, you remove all *Links*.

Locate Threshold: A measurement of the relationship between the read speed of a tape *Device* and the locate, or positioning speed. Used to optimize *Fast File Restore*.

Master Backup: A full backup of a complete *Domain*.

Medium: something that holds data, such as a tape, Blu-ray Disc cartridge, NAS folder, etc.

MySQL Hot Backups: The process of archiving a MySQL database, table-by-table, without shutting it down.

Network Attached Storage: A server or appliance accessible over the network or Internet. Used for remote backups.

NFS Backups. Backups using the Network FileSystem network transport protocol.

Notifier: A definition for a method of disseminating backup status information. Information may be sent via email to a user or group of users. It may be formatted as a full page text or HTML report, as an abbreviated message for alpha-numeric pagers, cell phones and PDAs, or as a coded numeric pager message. It may also be formatted as a printer report.

One Button Disaster Recovery: Also called *OBDR*. A Hewlett Packard trade name for tape drives that can be booted for *Disaster Recovery* purposes as if the were CD-ROM drives. Referred to in this manual simply as *Bootable Tape*.

Pathname: A description of the full name or a *File* or *Directory*, including the names of any *Directories*, or folders, that the file resides in. For example, the *Pathname* of the *EDGEMENU* program is `/usr/lib/edge/bin/edgemenu`.

Quota: the maximum amount of data *Backup**EDGE*** will attempt to store on a *URL*, *S3CLOUD* or *FSP Resource*. Archives past their expiration time will be deleted to stay under the quota.

Raw Filesystem Partition: A disk partition managed by an application program instead of a *UNIX* filesystem. Applications such as Oracle, Informix and Sybase sometimes store their data in *Raw Filesystem Partitions*.

> *Backup**EDGE*** can properly archive and restore *Raw Filesystem Partitions*, but they MUST be identified as raw in advance. See “Raw Filesystem Partition Backups” on page 353 for more information and instructions on identifying virtual files.

Regular File: A standard file whose actual size (in bytes) is always reported by the operating system correctly. Regular files may contain programs or data.

Relative Pathname: A filename beginning with a dot (.). A file saved with a relative pathname (such as `./etc/termcap`) will be restored relative to the current *Working Directory* at the time of the restore.

Resource: A named set of properties describing one *Device* used by *Backup**EDGE***. For example, a *Resource* may represent a tape drive, and include the appropriate *Device Node(s)* for it, the *Hardware Block Size*, default *Edge Block Size*, special commands needed for use with *Backup**EDGE***, and so on.

Retention Time: Also known as *TTL*, or *Time-to-Live*. This is the minimum time an archive must be saved before being over-written or erased. It is possible to set a retention time such that

*Backup**EDGE*** will never erase the archive without manual intervention. Archives past their Retention Time are known as *Expired Archives*.

REV. The Iomega trade name for their line of storage devices and media using RRD, or *Removable Rigid Disk*, technology. REV is now discontinued and unavailable and the REV section of the User Guide has been removed.

Root: The *Superuser*, or *System Administrator*, of a *UNIX* or *Linux* system. The root user has complete system privileges. As most *Backup**EDGE*** tasks require this, full system backups and *Scheduling* require the user to be logged in as `root`.

S3 Backups. Backups using the object storage protocol now widely used but originally designed by Amazon for the *Amazon **S**imple **S**torage **S**ervice* (S3).

Segment: a unit of storage on a *Medium*. A NAS, for example, might hold many *Segments*. An *Instance* is composed of one or more *Segments*, possibly contained on more than one *Medium*. The different *Media* can be of different types (tape, NAS, etc.). A *Segment* belongs to exactly one *Instance*. Each *Segment* is given a number, starting from 1, that records the order that it is to be used when reading that *Instance*.

> This may sound complicated, but it isn't. A *Backup* using more than tape, for example, may be said to have one *Segment* on each tape. When writing to a NAS, SharpDrive, etc., *Backup**EDGE*** typically breaks a single *Backup* into *Segments* of 1GB each, which gets around file size limits. When S3CLOUD or re-startable NAS backups are performed, the *Backup* is broken (by default) into small 50MB *Segments*. In the event of a network failure, this provides for a smaller amount of data that needs to be cached and re-transmitted after a re-start.

Scheduled Job: A *Scheduled Job* describes all of the actions necessary to archive one or more *Domains* through a single *Sequence* (in other words, perform a backup). Once defined, *Jobs* can be run via the *Scheduler* at prescribed times, directly from *EDGEMENU*, or upon demand by using **EDGE.NIGHTLY** (see "The EDGE.NIGHTLY Program" on page 326).

Sequence: An organizational unit for backups of a *Domain*. It is possible to create multiple *Sequences* which each backup the same *Domain*. Each *Sequence* keeps separate history information, so that it is possible to keep (for example) off-site *Master Backups* from interfering with on-site *Differential Backups*.

Shell: The *UNIX* Operating System command interpreter, normally run when the user logs in. Typified by the prompt commands `%`, `$`, or `#`.

Seeking Device: A *Device* capable of reading and writing data to any spot on the medium non-sequentially. For example, tape drives are never seeking *Devices*. Floppy disks are seeking *Devices*.

Shell Program or Shell Script: A series of shell commands run sequentially from a file list.

Sparse File: See *Virtual File*.

Symbolic Link: A *File* with a special *Link* type. The *File* contains the *Pathname* to a *File* located elsewhere on the system or across a network. Reading and writing data to and from the *Symbolic Link* is the same as reading and writing to and from the real file. The *Symbolic Link* was originally designed to create *Links* to the same actual data or program *File* across *Filesystems*. They also work within a *Filesystem*.

Tape Block Size: The *Hardware Block Size* of a *Tape Device*. See *Hardware Block Size*.

Tar: tape archiver, a backup utility program included with *UNIX*.

Time-to-Live: See *Retention Time*.

Virtual File: A special kind of *File* used by some application programs. The *Filesystem* interprets this *File* type as being quite large, while a special technique is employed to prevent currently

empty sections of the *File* from consuming actual disk space. *Virtual Files* cannot be copied, archived or restored with standard operating system commands without consuming large amounts of space.

> *Backup**EDGE*** can properly archive and restore *Virtual Files*, but they MUST be identified as *Virtual* in advance. See “Using EDGE.TAPE for Hardware Status / Control” on page 319 for more information and instructions on *Virtual Files*.

Volume: One disk, tape, cartridge, etc. from a full backup set.

Volume Size: The storage capacity of one *Volume*. This is detected automatically for all optical and SharpDrive media, and most tape drives.

3.2 - Specific Operating System Release Support

Operating systems add releases, patches and updates too rapidly to be included in tables in this User Guide. The Microlite Web Site (`http://www.microlite.com`) has two sections to keep users apprised of currently supported operating systems and releases. From the home page, see the links for:

- Linux Support Tables.
- UNIX Support Tables.

3.3 - Specific Device Support

This manual cannot hope to keep up with the capabilities of various devices on each operating system. The Microlite Web Site (`http://www.microlite.com`) has a full support section, plus a Device Compatibility section under `Device Support Tables`. Please see the web site for technical details on device issues.

4 - Anatomy of a *BackupEDGE* Backup

Understanding what "Backup" means is the key to understanding how *Backup**EDGE*** works.

NOTE: *Backup**EDGE*** establishes defaults during the installation process that provide very useful on-site full-system backups and reports **without** a working knowledge of all the information and concepts described below. In particular, it selects defaults that emulate the action "backup up every file every night". The more you know, however, the better you will be able to extend the usefulness of the product.

In its simplest form, a backup means "take these data and make a copy of them over there". This is the method used by the *UNIX* `tar`, `cpio`, and `dump` commands for years: data (in the form of individual files) are copied to a tape, and can be restored from a tape. There is no notification or summary of results, no easy way to schedule backups regularly, and rarely any way to verify that the operation actually worked. To these programs, a backup is an *action*: that of copying data.

This works well, as long as your backup strategy is simple, your data is easy to access, and your tape drive is reliable. Unfortunately, these assumptions are far too restrictive for most production environments.

Ultimately, anything that does a backup must "copy ... them over there", at some level. However, that is only the beginning of what the average system administrator needs to protect the data in his or her care. To be truly useful, a backup solution must allow easy management of what data is copied, when it is copied, and to what *Device* is it sent. It must determine, reliably, the success or failure of the copy operation, and produce reports on the results. It must provide a clear path to restoring that data later, with a minimum of fuss or hassle. In short, protecting data in a production environment is a *process*, only a small part of which is the single *action* of copying data from one storage system to another.

*Backup**EDGE*** provides this process, which is described in the rest of this manual. If you usually think about a backup as an *action*, then by adjusting that view slightly, you may be able get much more out of *Backup**EDGE***.

In *Backup**EDGE***, typically a *Backup* happens when a *Scheduled Job* creates a backup in a *Sequence* of a *Domain* to a particular a *Resource* (which represents some physical *Device*). That seems very complicated when compared to the *action* of copying files to tape, but the added complexity is only a superficial side-effect of viewing a backup as a *process*. Let's break it down and show you how simple, logical, and powerful it is.

- The *Device* is the physical thing, such as a tape drive or NAS, that you will be using to store data. In some cases, a *Device* can also be a disk file. *Device* may be locally attached or network accessible.
- The *Resource* is the *Backup**EDGE*** software representation for your storage *Device*. It knows all about how to **control** the *Device*, **write** to it, and **read** from it, and erase or overwrite things stored on it. It records the appropriate settings for the *Device* to force data to be written and managed in a consistent way.
- The *Domain* defines data that is to be protected by a backup, and how *Backup**EDGE*** should treat that data. It specifies which files or filesystems are to be treated specially, and what if any special actions are to be taken before and after the backup to prepare those files to be archived. You may specify as many *Domains* as you like to allow *Backup**EDGE*** to protect different subsets of your data separately. A *Domain* stands in contrast to "a list of files" as seen by `tar` or `cpio`, since it includes information about *how* the data in those files are to be accessed beyond simply the filename that is used to find that data.
- The *Sequence* defines and tracks a unique group of *Master*, *Differential* and *Incremental Backups* for exactly one *Domain*. To maintain, for example, on-site and off-site backups that

protect your entire system, a different *Sequence* would be used for each (although both *Sequences* would refer to the same *Domain*, since both protect the same data). This keeps the on-site and off-site backups separate, which is especially useful when performing *Differential* or *Incremental Backups*. When a scheduled backup is performed, it contributes a backup to exactly one *Sequence*, of the *Domain* referred to by that *Sequence*. In contrast, the *action* of copying data generally keeps no records at all!

- The *Scheduled Job* is a complete specification for a backup. It contains a list of one or more *Domains* to be backed up, allows selection of a *Sequence* for tracking, and defines which *Resource* will be used for it. It also specifies:
  - when the backup is to be done.
  - what type of *Verify* pass (if any) is to be run.
  - whether the backup should be indexed for *Fast File Restore*.
  - whether the backup should or can be made bootable for *Disaster Recovery*.
  - when the archive created may be erased /or overwritten (expiration).
  - promotion strategies, which define the circumstances under which a *Differential Backup* may be promoted to a *Master Backup*, or an *Incremental Backup* to a *Differential Backup*.
  - autoloader medium selection.
  - media unload / eject strategies.

  It also records whom to notify if the backup passes, and whom else to notigy if the backup fails. Notification may be by printer, text email, HTML email, or SMS short text message.
- The *Quota* defines the maximum amount of data that can be written to a disk-based storage *Resource* such as a cartridge disk drive (*FSP*), network attached storage device (*URL*), or to the Amazon S3 internet storage cloud (*S3CLOUD*).

Each of the major *Backup**EDGE*** concepts has been designed and organized to control its own part of the backup process in logical steps. Let's break them down a little further.

4.1 - Resources

*Backup**EDGE*** controls every *Device* that it uses by looking at the *Resource* for it. This is simply a collection of all the things *Backup**EDGE*** needs to know about the *Device*. Whereas `tar` or `cpio` simply needs to know the read/write *Device Node* for a file, *Backup**EDGE*** needs to know a lot more. Why? Because *Backup**EDGE*** can do a lot more. Fortunately, most *Devices* are autodetected during installation of *Backup**EDGE***, so you do not need to set up *Resources* for them manually.

Here is an example of a *Backup**EDGE*** tape *Resource* for a standard SCSI tape drive...

```
+-------------------------------------------------------------------------+
|- General Resource Information -------------------------------------------|
|Resource Type       Tape Drive                                           |
|Resource Name       [tape0            ] Change as appropriate            |
|Description         [QUANTUM ULTRIUM 4 2210      ]                       |
|Changer Assoc       [web2v.microlite.com:changer0:dt0]                    |
|Interface           [SCSI       ]                                        |
|                                                                         |
|- Tape Drive Information -------------------------------------------------|
|Data Node           [/dev/st0                    ] [A] TapeAlert(tm) Support |
|No Rewind Node      [/dev/nst0                   ] [X] Multiple Archives? |
|Tape Block Size     [-1                          ] [C] Partition          |
|Locate Threshhold   [30                          ] [ Manual Check ]       |
|                                                                         |
|                                                                         |
|- Default Backup Properties ----------------------------------------------|
|Volume Size         [0           ] [H] Compression                       |
|Edge Block Size     [256         ] [Y] Double Buffering                  |
|[Next]                             [Prev]                        [Cancel]|
+-------------------------------------------------------------------------+
```

In this example from a system running Linux, *Backup**EDGE*** knows that this *Device* is a SCSI tape drive, and that it is part of an *Autochanger*.It also knows which *Device Node* is the standard read/write node, and which node to use when writing without rewinding the tape.

*Backup**EDGE*** will not attempt to set a *Tape Block Size* for this device (the `-1`). It will ensure that hardware compression is enabled before writing to it or reading from it. It will allow multiple archives per tape. It will by default not attempt to use the partitioning feature of the *Device*, but will try to check the *Device* for *TapeAlert* diagnostics messages during scheduled backups.

If you don't understand what all of these parameters mean, don't be alarmed. Pressing `[F1]` on any of the fields will bring up more information about it. Usually, however, you will not need to modify the settings detected during installation.

Here is another example, this time for a *Blu-ray Disc Device* on a *Linux* system...

```
|- General Resource Information ------------------------------------------------|
|Resource Type       Optical Drive                                               |
|Resource Name       [optical0          ] Change as appropriate                  |
|Description         [HL-DT-ST BD-RE GGW-H20L YL05]                              |
|Changer Assoc                                                                   |
|Interface           [IDE / ATAPI]                                               |
|                                                                                |
|- CD / DVD / Optical Information ----------------------------------------------|
|Data Node           [/dev/hdc                    ] [ ] Buffer Whole Disc?       |
|Mount Device Node   [/dev/hdc                    ] [X] BurnProof(tm)?           |
|Record Buffer (K)   [2048                        ] [X] Multiple Archives?       |
|Needs Eject?        [ ]                                                         |
|Writable Media:     CD-R[W], DVD-RAM, DVD+/-R[W], BD-RE                         |
|                                                                                |
|- Default Backup Properties ---------------------------------------------------|
|Volume Size         [0             ] [S] Compression Level  [5]                |
|Edge Block Size     [64            ] [Y] Double Buffering                      |
|[Next]                                                              [Cancel]    |
+--------------------------------------------------------------------------------+
```

Most *UNIX* systems do not have an operating system driver that allows you to open an optical *Device* and write to it like a tape drive. This would normally make a *Blu-ray Disc, DVD* or *CD* drive unusable as a backup *Device*. The `tar`, `cpio` and `dump` programs can't use it. *Backup**EDGE*** uses a special program to create archives on the optical *Device*, and then reads them using either the CD-ROM driver built into the operating system or a special *Backup**EDGE*** reader as appropriate. This is true for Blu-ray Disc, DVD-RAM, DVD-RW, DVD-R, DVD+RW and DVD+R and CD-R/CD-RW *Devices*.

To reiterate, a *Resource* is simply the *Backup**EDGE*** construct that describes advanced capabilities for storage *Devices* along with your preferences for how they should be configured before use.

4.2 - Domains

A *Domain* (also called a *Backup Domain*) describes data that may be protected by a backup, and what special actions occur along with such a backup. It provides *Backup**EDGE*** with information about how to properly and safely archive the data described by the *Domain*.

Let's look at an example, the default backup *Domain* (called `system`), created by *BackupEDGE* during installation.

```
+Edit Backup Domain-------------------------------------------------------+
|Machine:            web2v.microlite.com                                  |
|Name:               [system                                            ]|
|Description:        [Entire System                                     ]|
|                                                                         |
|-Edit Filesystem Backup Domain---------------------------------------------|
|Include:            [/                                                 ]|
|Exclude:            [/proc                                             ]|
|Exclude Netmounts:  [N]                                                  |
|Exclude Readmounts: [N]                                                  |
|Exclude Allmounts:  [N]                                                  |
|Incl. Filelist:     [                                                  ]|
|Excl. Filelist:     [/etc/edge.exclude                                 ]|
|Encryption List     [                                                  ]|
|                    [Advanced Properties]                                |
|[Save]                        [Back To Select]                 [Cancel]|
+-------------------------------------------------------------------------+
```

Advanced Properties

```
+Edit Advanced Domain Properties------------------------------------------+
|Machine:            web2v.microlite.com                                  |
|Virtual Filelist:   [/etc/edge.virtual                                 ]|
|Start/Stop Script:  [/usr/lib/edge/bin/edge.bscript                    ]|
|Raw Dev Filelist:   [/etc/edge.raw                                     ]|
|Raw Script:         [/usr/lib/edge/bin/edge.rawscript                  ]|
|No-check Filelist:  [/etc/edge.nocheck                                 ]|
|Config Script:      [                                                  ]|
|Follow Symlinks     [N]                                                  |
|Read Locking        [U]                                                  |
|Preserve Atime      [N]                                                  |
|Diff/Incr Level     [2]                                                  |
|[Save]                                                       [Cancel]|
+-------------------------------------------------------------------------+
```

This *Backup Domain* backs up an entire system. It starts in the `/` *Directory*, and includes all files and *Directories* except `/proc` and any pathnames that appear in the file `/etc/edge.exclude`.

Files (if any) listed in `/etc/edge.virtual` will be treated as *Virtual* (sometimes called *Sparse*) *Files*. Partitions (if any) listed in `/etc/edge.raw` will be treated as *Raw Filesystem Partitions*. Files listed in `/etc/edge.nocheck` will be excluded from being checked by the *Level 2 Verify* process. A program or script called *EDGE.BSCRIPT* will be run before and after every backup.

Finally, there are special flags for handling *Symbolic Links*, locking and time stamping of files.

Next, let's look at an example of a *Domain* used to backup an individual application....

```
+Edit Backup Domain-------------------------------------------------------+
|Machine:            web2v.microlite.com                                  |
|Name:               [filePro                                           ]|
|Description:        [All filePro Programs and Database                 ]|
|                                                                         |
|-Edit Filesystem Backup Domain---------------------------------------------|
|Include:            [/u/appl /etc/default/fppath /usr/bin/P /usr/bin/p ]|
|Exclude:            [                                                  ]|
|Exclude Netmounts:  [N]                                                  |
|Exclude Readmounts: [N]                                                  |
|Exclude Allmounts:  [N]                                                  |
|Incl. Filelist:     [                                                  ]|
|Excl. Filelist:     [                                                  ]|
|Encryption List     [                                                  ]|
|                    [Advanced Properties]                                |
|[Save]                        [Back To Select]                 [Cancel]|
+-------------------------------------------------------------------------+
```

```
 Advanced Properties

+Edit Advanced Domain Properties-----------------------------------------------+
|Machine:            web2v.microlite.com                                       |
|Virtual Filelist:   [                                                       ]|
|Start/Stop Script:  [/u/appl/fp/fpclean                                     ]|
|Raw Dev Filelist:   [                                                       ]|
|Raw Script:         [                                                       ]|
|No-check Filelist:  [                                                       ]|
|Config Script:      [                                                       ]|
|Follow Symlinks     [N]                                                      |
|Read Locking        [U]                                                      |
|Preserve Atime      [N]                                                      |
|Diff/Incr Level     [2]                                                      |
|[Save]                                                          [Cancel]    |
+-----------------------------------------------------------------------------+
```

In this example, The *Domain* consists of all the files used by the **filePro** database program. Note that in the simple example, all the files/directories to be included happened to fit on one line (which scrolls). In a larger example, they might have been placed one-per-line in an file used as the `Incl. Filelist`. Note the start/stop script which might be added to log out users, remove lock files, etc. It could potentially trim indexes to save space before the backup, and re-build them after the backup completed.

Notice that a *Domain* is more than just a "list of files". It is better described as "data to be protected, and how to access it". A *Domain* does ***not*** specify whether you will perform *Master Backups*, *Differential Backups*, *Incremental Backups*, or indeed **any** backups of that data; it just specifies what data are included and how that data are accessed.

NOTE: *BackupEDGE 3.x* has special support for MySQL Hot Backups and can create a specialized backup Domain. See "MySQL / MariaDB Backups" on page 177 for MySQL information.

4.3 - Sequences

A *Sequence* keeps track of individual backups of exactly one *Domain*. It allows you to separate backups by purpose, even if they protect the same data. It also keeps track of how recent the newest backup in that *Sequence* is, so it knows what data in the *Domain* has not been archived yet. This permits *Differential* and *Incremental Backups* to be performed.

```
+-----------------------------------------------------------------------------+
|                          Edit Backup Sequence                               |
|                                                                             |
|Machine:            web2v.microlite.com                                      |
|Name:               [onsite                                                ]|
|Description:        [On-Site Backups                                       ]|
+-----------------------------------------------------------------------------+
```

This is the default *Sequence* created during the installation of *BackupEDGE*, called `onsite`. It provides a control mechanism for backing up the *Domain* called `system`, which is the default *Domain* for your entire system. It is assumed that this *Sequence* will be used to keep track of on-site backups that can restore your entire system. All backups in this *Sequence* will work towards providing archived copies of the *Domain* called `system`.

Backups performed using the *Sequence* `onsite` keep a complete set of log files and time stamps for the latest *Master*, *Differential* and *Incremental Backups* separate from all other *Sequences*, even other *Sequences* of `system` backups.

A second sequence is also automatically created called `offsite`; If you wish to maintain off-site backups as well, you can (and should) create a separate *Schedule* for those, using the same *Domain* as `onsite`.

```
+-------------------------------------------------------------------------+
|                            Edit Backup Sequence                         |
|                                                                         |
|Machine:            web2v.microlite.com                                  |
|Name:               [offsite                                           ]|
|Description:        [Offsite Backups                                   ]|
+-------------------------------------------------------------------------+
```

This *Sequence* (`offsite`) may also be used to backup the *Domain* `system`. However, *Master* and *Differential Backups* created using this *Sequence* would have no effect on *Differential* or *Incremental Backups* created through `onsite`. This is quite desirable; if you are performing *Differential Backups* daily for on-site storage (recall that a *Differential Backup* is all and only those files which changed since the last *Master Backup*), you do not want those *Differential Backups* to be based on an off-site *Master Backup*. This would be very confusing.

As mentioned earlier, notice the distinction between "data to be protected" (i.e., the *Domain*) and "files backed up". *Master*, *Differential*, and *Incremental Backups* **in the same *Sequence***, when taken together, all protect the same data. However, they do not all necessarily back up each file in the *Domain* every time. It is the *Sequence* that keeps track of which file(s) need to be backed up to keep the data stored in a *Domain* archived safely for each backup type.

Separate *Sequences* maintain entirely separate accounting for this, so performing a *Master Backup* in `offsite` does not affect a *Differential Backup* in `onsite`. To put it another way, a *Differential Backup* in `onsite` is in no way related to or dependent on any *Master Backups* that may exist in `offsite`; one only needs the backups from `onsite` to restore the data in the *Domain* to the state of the last `onsite` backup!

4.4 - Scheduled Jobs

The *Scheduled Job* is the basic unit of work for *Backup**EDGE***. It records a "snapshot" of everything necessary to perform a complete, verified, possibly unattended backup. Everything that needs backed up should be backed up through a *Scheduled Job*. Consider the following *Scheduled Job*...

```
+ Edgemenu for BackupEDGE ---------------------------------------------------+
+ Edit Backup Schedule -------------------------------------------------------+
| Schedule Name:     simple_job                                               |
|          Time:     [00:30 ] (00:27:38)  Enabled: [X]                        |
| Sequence:                   web2v.microlite.com:esequence/onsite            |
| Backup Domain:              system mysql                                    |
| Primary Resource:  [Change] web2v.microlite.com:url!url0                    |
|                                                                             |
| +-----------------------------------------------+     September 2019        |
| | Every Sunday of the week                (None) |  Su Mo Tu We Th Fr Sa    |
| | Every Monday of the week               Master |   1 M  M  M  M  M   7    |
| | Every Tuesday of the week              Master |   8 M  M  M  M  M  14    |
| | Every Wednesday of the week            Master |  15 M  M  M  M  M  21    |
| | Every Thursday of the week             Master |  22 M  M  M  M  M  28    |
| | Every Friday of the week               Master |  29 M                    |
| | Every Saturday of the week              (None) |                          |
| +-----------------------------------------------+                           |
| Notify / Advanced: [Change]  [Reset Dates]                                  |
| Mail Summary To:   root                  Print Summary To:   optra1         |
| Mail Failures To:  tom@microlite.com     Print Failures To:  NONE           |
|[Save]                                                          [Cancel]|
+-------------------------------------------------------------------------+
|+Local Machine: web2v.microlite.com  Administering: web2v.microlite.com  ----+|
+Modify Backup Schedule-------------------------------------------------------+
```

This *Scheduled Job* says "Add a *Master Backup* to the *Sequence* `onsite` every weekday morning at 30 minutes after midnight. Use the *Device* described by the *Resource* known as `url0`. Include

a `mysql` backup. Notify `root` of the backup status via an email message, and send results to printer `optra1`. If a failure occurs, send an **additional** email notification to `tom@microlite.com`." Recall that `onsite` (described earlier) records backups of the whole-system *Domain* system by default, so this *Scheduled Job* will perform a backup designed to protect that *Domain*.

A look at the `Notify / Advanced:` window for this *Scheduled Job* would reveal...

```
+ Edgemenu for BackupEDGE ------------------------------------------------+
+ Edit Backup Advanced Properties ----------------------------------------+
|                    Backup Schedule Advanced Properties                  |
|                                                                         |
| Schedule Name:     simple_job                                           |
|                                                                         |
| Verify Type:       [B]                 Checksumming:  [X]               |
| Attempt Index:     [X]                                                  |
| Attempt Bootable:  [ ]                                                  |
| Promote A:         [ ]                 Retention:     [1 Weeks]         |
| Promote B:         [X]                 Copy to:       [NONE]            |
| Eject/Vol Switch:  [ ]                 Copy Retention:[Forever]         |
| Eject/Verify:      [ ]                 Copy Sequence: [ ]               |
|                                                                         |
| Mail Summary To:   [root                                              ]|
| Print Summary To:  [optra1                                            ]|
| Mail Failures To:  [tom                                               ]|
| Print Failures To: [                                                  ]|
|                                                                          |
|                                                                          |
|                                                                          |
|[Next]                                                          [Cancel]|
+--------------------------------------------------------------------------+
|+Local Machine: web2v.microlite.com  Administering: web2v.microlite.com  ----+|
+Modify Backup Schedule-------------------------------------------------------+
```

So, during this *Scheduled Job*, a *Level 2 (bit-level) Verify* will be performed, as well as an *Index* for *FFR* or *IFR*. The archive created will not be erased for **at least** 6 days, and there is no second copy of the archive being sent to another *Resource*.

Detailed logs for the backup operations are kept on a per-*Scheduled Job* basis. If you are performing more than one backup operation automatically, the logs for different *Scheduled Jobs* will not interfere with each other.

That's the basic summary of what happens during a backup, but in describing the screens we left a lot of things out. These will be described later in this manual, and you'll see how to extend these features into a truly advanced data protection system.

Now that you have an understanding of the basic concepts, let's install *Backup**EDGE***.

5 - Installing BackupEDGE

Please note that *Backup**EDGE*** may only be installed while logged in as `root` on a character terminal, console or xterm client.

5.1 - What Can I Expect From An Installation?

The installer is designed so that, when finished, your system is set up to perform nightly system backups[1]. During a normal *Backup**EDGE*** installation the following will occur...

- The installer will unpack and place all *Backup**EDGE*** program and data files in their proper places within the `/usr/lib/edge` *Directory*[2].
- *Symbolic Links* will be made to any files or programs which require access from normal *UNIX* search paths.
- The installer will attempt to detect all of your Tape, optical media, and *Autochanger Devices* and create *Resource* entries with default names for them.
- The installer will ask if you wish to create a url *Resource* for *FTP Backups* (unless this is an update install and at least one url *Resource* has already been defined).
- If *Autochangers* are detected, the installer will allow you to identify which tape drive(s) are associated with (i.e., installed in) which *Autochangers*.
- The installer will create a default backup *Domain* and *Sequence* automatically, and offer to *Schedule* a *Job* to back up your entire system each night. A default *Schedule Job* should **always be created**, even if it is not going to be used.
- If MySQL is detected, the installer will offer to configure for MySQL backups and add them to the default schedule.
- Icons will be placed on the root graphical desktop allowing the user to launch the Java interface (if Java is detected during installation) or character interface (through an xterm client) if Java is not detected.
- The installer will offer to scan your entire system for *Virtual* (*Sparse)* files, and note their pathnames in the `/etc/edge.virtual` file.

During an installation, only the base product is configured. Some features, such as Encryption, require a separate serial number and license, and are set up elsewhere. For more information about how to set up a specific feature, please consult the appropriate section of this manual for that feature.

If you wish to launch a *Web Services* daemon, you may complete this task after installation. See “Configuring Web Services and X11 Interfaces” on page 186 for more information.

1. Users wanting to store data on removable hard disk devices or to the Amazon S3 cloud will need to do additional setup.
2. Beginning with 02.01.03 build 2, BackupEDGE for Linux conforms to the Filesystem Hierarchical Standard. /usr/lib/edge is itself a symbolic link to appropriate entries in the /opt and /var/opt.

5.2 - Installation Pre-requisites

Prior to beginning a *Backup**EDGE*** installation, the system, devices and network should be set up properly.

NOTE: The installers for many operating systems, including OSR6, UW7 and Linux, recognize host adapters and install drivers and start-up programs during initial system load (ISL). If possible, make sure that all of your desired storage devices are attached during ISL so that the operating system can detect and install the drivers. Many support calls come from clients who install new host adapters after ISL and don't know how to get them recognized by their operating system.

- All storage devices should be properly recognized by the operating system, including tape drives, changers/libraries/autoloaders, and optical devices.

  Under Linux, OpenServer 6 and UnixWare 7, all SCSI, SAS, ATAPI, SATA and USB devices should be detected automatically by the operating system.

  Under OpenServer 5, this involves running "`mkdev tape`" (tape drives), "`mkdev juke`" (changers/libraries/autoloaders) and "`mkdev cdrom`" (optical drives), then relinking the kernel and rebooting. 5.0.6 and 5.0.7 users wishing to use ATAPI optical devices should be running the latest maintenance packs and "wd" driver supplements which can be found at `ftp://ftp.xinuos.com/pub/openserver5`

  OpenServer 6 users wishing to use ATAPI optical devices should be running at least ide driver supplement 7.1.4h (ide714h) which can be found in the Maintenance Pack 4 Driver Supplement at `ftp://ftp.xinuos.com/pub/openserver6/600/drivers/mp4drivers`

  UnixWare 7 release 7.1.4 users wishing to use ATAPI optical devices should be running at least ide driver supplement 7.1.4h (ide714h) which can be found at `ftp://ftp.xinuos.com/pub/unixware7/714/drivers/`

  Under Linux 2.4.x kernels (now deprecated), all ATAPI devices, including optical and tape drives, ***must*** be running under the "ide-scsi" driver with DMA enabled. When configured properly, all Linux storage devices to be used by *Backup**EDGE*** will be shown by typing the following at a *root* prompt: `cat /proc/scsi/scsi`

  Under Linux 2.6.x and later kernels, all ATAPI optical devices ***must*** be running with DMA enabled. ATAPI tapes must run with ide-scsi and DMA enabled.

  SATA devices may in most cases be used in IDE/ATAPI emulation mode. If your operating system has a native SATA AHCI driver, the PC BIOS should be configured accordingly and the drive used.

- Under some operating systems, all devices except floppies must have media inserted. Optical drives may not have blank media inserted. It must contain some data. You will be informed if this is required during the installation process.
- If the Linux Java GUI is to be used under X11, Java 1.4.2 or later must be installed prior to installation so that *Backup**EDGE*** can find it.
- Linux users must log in as root at least once to either the KDE or Gnome desktop (or both) prior to installation. This is necessary for the window manager to create the proper icon directories.

5.3 - Installing over a previous release of BackupEDGE

NOTE: This section has changed for *Backup**EDGE** 3.x*. You MUST remove all 02.0x and prior releases or beta releases of *Backup**EDGE*** before installing 3.x. See “Removing BackupEDGE” on page 192 for removal instructions.

Any *Backup**EDGE*** 03.0x release may be installed directly over any prior 03.0x release. All 01.0x or 02.0x releases must be removed completely before an 03.0x release may be installed.

5.4 - How Do I Install BackupEDGE?

*Backup**EDGE*** may be installed using one of three methods...

- From the Installation CD-ROM that ships as a media kit or is downloaded.
- From a downloaded, self-extracting executable (recommended method).
- From a Tar Format or Custom Archive.

Each of these methods ultimately unpacks the installation files, places them in the appropriate *Directories*, and the runs an *Installation Wizard* to detect and configure *Devices*, check for special file types, and schedule a simple *Scheduled Job* to back up your entire system.

NOTE: You should **ALWAYS** allow the installation wizard to create a default *Schedule*. You may later modify or even disable it if desired.

From The Installation CD-ROM

The *Installation CD-ROM* contains:

- Versions of *Backup**EDGE*** for multiple *UNIX* and *Linux* systems, in multiple distribution formats.
- On line documentation including manuals, white papers and “How To” guides.
- Tools for accessing the CD-ROM from Microsoft Windows.
- Tools for checking for newer versions of *Backup**EDGE*** from the Microlite Corporation website.

The *Master Install Program* detects your operating system type and selects the proper version of *Backup**EDGE*** to be installed automatically.

The basic installation procedure from CD-ROM is:

1. Mount the Installation CD-ROM.
2. Run the CD-ROM install program.
3. Unmount the CD-ROM.

Using the CD-ROM With Automounters

On many newer systems, the CD-ROM is automatically mounted when you insert it. In this case, you simply need to run the installation program.

NOTE: If you intend to do backups to optical or SharpDrive *media*, we highly recommend that you disable any automount daemons on your system. They will try to mount your backup media when inserted, with unpredictable results.

Newer *Linux* systems have both **automount** and **autorun** capabilities when running under *GUI* desktops.

If you are logged in as `root` under the KDE desktop and insert the CD-ROM, the *Backup**EDGE*** installation menu will appear automatically if **autorun** is enabled (or you will be prompted to confirm that you want to **autorun** the `install` program).

If **autorun** is not enabled but **automount** is, and upon CD-ROM insertion you get a *File Manager* popup window, you may click on the `install.sh` *Icon* to install or upgrade *Backup**EDGE***.

If **automount** is not enabled, but a CD-ROM *Icon* is available, insert the CD-ROM, click the CD-ROM *Icon*, and then click the `install.sh` *Icon* when it appears.

If none of the above work, simply follow the manual mounting instructions below.

Manually Mounting The CD-ROM

Linux

```
mount -r /dev/cd0 /mnt
/mnt/install.sh
umount /mnt
```

OpenServer 6/6V/6 Definitive (OSR6)

```
mount -r /dev/cd0 /mnt
/mnt/install.sh
umount /mnt
```

OpenServer 5.0.5-5.0.7, 5.0.7V/5 Definitive (OSR5)

```
mount -r -f HS,lower /dev/cd0 /mnt
/mnt/install.sh
umount /mnt
```

UnixWare 7.1.4, 7.1.4+ (UW7)/7 Definitive

```
mount -r -F cdfs /dev/cdrom/cdrom1 /mnt
/mnt/install.sh
umount /mnt
```

The CD-ROM Installation Screen

The CD-ROM install program displays a splash screen, then attempts to detect the operating system and release you are using and set the install program to install it.

```
  Microlite BackupEDGE CDROM Installation Menu              Version 03.03.01
  Copyright 1998 - 2020 by Microlite Corporation         All Rights Reserved
                                                 BackupEDGE Version 03.03.01
  Installation of these products is subject to your agreement to the terms
  of the License Agreement contained in the top directory of this CD-ROM!

  Thanks for trying or buying Microlite BackupEDGE!

  This CD-ROM contains BackupEDGE version:     03.03.01
  This CD-ROM was mastered on:               2020-08-13
  Evaluation copies may be installed until:  2021-08-12

  Please note that, due to production schedules, more recent releases
  of our products may be available on our ftp site. You may install
  from this CD-ROM, or you may wish to browse our site for the most
  recent BackupEDGE releases.

  Licensed copies may always be re-installed.

  Thanks - Microlite Development Team:  http://www.microlite.com
                                        ftp://ftp.microlite.com
Press [Enter] To Continue _ Press [Enter] To Continue _
```

Press `[Enter]` at this prompt to continue.

You will next be given the option to check the Microlite Corporation website for newer versions of *Backup**EDGE*** before installing anything. You must have a functioning Internet connection on the UNIX or Linux machine for this to work.

You may skip this check by pressing [Enter], in which case proceed to "The Installation Manager" on page 53. If you elect to perform this check by pressing `Y [Enter]`, however, *Backup**EDGE*** will check for a newer version.

If no newer version exists, you will be informed of this. Installation will continue with the CD-ROM version as if you did not check for a newer version.

From time to time, newer versions of *Backup**EDGE*** may require different licenses and serial numbers than older versions. When this happens, the first number in the version will change. The second and third number in the version is not related to the license[1]. See "The Indispensable BackupEDGE QA Guide" on page 365 for general rules on updates and upgrades.

If the version on the CD-ROM uses a different license than the newest version found on the website, you will be informed of this, and given the option to choose between it and the newest version that does not require a new license. Of course, if you are installing *Backup**EDGE*** in "demo mode", and do not have a serial number yet, you should choose the newest version regardless of license or serial number.

If you are presented with such a choice, whichever version you select will be treated as the "newer version", while the other version will be ignored.

Assuming some newer version is found, the Change Log for it will be displayed. This will provide information about exactly what is different between the newer version and the version found on the CD-ROM.

Once you have viewed the Change Log, you will be given the option to download and install the newer version, or stay with the version on the CD-ROM.

Whichever you select, installation will now proceed as described in "The Installation Manager" on page 53.

Alternate Distribution File Format Types

There are three different file format types used to distribute *Backup**EDGE***...

- Self Installing Binaries (recommended).
- VOL format. Used by Custom+ / Software Manager in *OSR5 and OSR6*.
- TAR Format.

These formats will be explained in the following sections. Here are the default filenames we use for most of the various distribution types...

Operating System	TAR or Custom+	Self Installing	DOS/Win Executables	Comments
Linux 5.x	`edgelx50_64.tar`	`edgelx50_64.elf`	`EDGELX50_64.EXE`	Linux systems running 5.x kernels under the EM64T and AMD64 architectures
Linux 4.x / 64	`edgelx40_64.tar`	`edgelx40_64.elf`	`EDGELX40_64.EXE`	Linux systems running 4.x kernels under the EM64T and AMD64 architectures
Linux 4.x / 32	`edgelx40_32.tar`	`edgelx40_32.elf`	`EDGELX40_32.EXE`	Linux IA32 systems running 4.x kernels

1. In the 01.0x.0x series, changing the second number pair required a new license.

Operating System	TAR or Custom+	Self Installing	DOS/Win Executables	Comments
Linux 3.x / 64	`edgelx30_64.tar`	`edgelx30_64.elf`	`EDGELX30_64.EXE`	Linux systems running 3.x kernels under the EM64T and AMD64 architectures
Linux 3.x / 32	`edgelx30_32.tar`	`edgelx30_32.elf`	`EDGELX30_32.EXE`	Linux IA32 systems running 3.x kernels
Linux 2.6.x / 64	`edgelx64.tar`	`edgelx64.elf`	`EDGELX64.EXE`	Linux systems running 2.6.x kernels under the EM64T and AMD64 architectures
Linux 2.6.x / 32	`edgelx26.tar`	`edgelx26.elf`	`EDGELX26.EXE`	Linux IA32 systems running 2.6.x kernels
OpenServer 6.0.x/6V, 6 Definitive	`edgesco6.tar`	`edgesco6.elf`	`EDGESCO6.EXE`	OpenServer 6 02.02.00 and later install / remove through Custom / Software Manager
OpenServer 5.0.5-5.0.7V, 6 Definitive	`VOL.000.000`	`edgesco5.elf`	`EDGESCO5.EXE`	Installs / removes through Custom / Software Manager
UnixWare 7.1.4/7.1.4+, 7 Definitive	`edgesc71.tar`	`edgesc71.elf`	`EDGESC71.EXE`	

Please note that the `.elf` extension does not always mean that the file is an *ELF* executable. All `.elf` files are self-extracting executables, but they are in whatever format is appropriate for the operating system on which they will be installed. The `.elf` extension is used for all of them only for consistency.

In the examples that follow, we'll use `edgedist.tar`, `edgedist.elf` or `EDGEDIST.EXE` to refer to the above files. In actual use, substitute `dist` / `DIST` with the proper four characters referring to the distribution you are using.

Installing From Self-Installing Binaries

Self-Installing Binaries are complete, single product distributions with a `tar` or `custom` archive wrapped up in a compressed executable file. When executed, these files extract their contents, then run either `tar` or `custom` as necessary to install the distribution and begin running the *Installation Manager* program. To use them, copy them into any *Directory* (`/tmp` is recommended), then from that *Working Directory* type...

```
chmod 755 edgedist.elf
./edgedist.elf
```

The *Installation Manager* will start. Proceed to "The Installation Manager" on page 53.

Installing From TAR Archives

`Tar` archives, whether downloaded from the web or copied off the installation CD, are very simple to use. Simply...

```
cd /
tar xvf edgedist.tar
/tmp/init.edge
```

Or, if the `tar` archive has been placed on a floppy, just...

```
cd /
tar xvf [floppy_device_name]
/tmp/init.edge
```

Substitute the correct name for the floppy *Device* on your system. If there is more than one floppy diskette in the distribution, extract them all using `tar` commands before running the `init.edge` program.

NOTE: *You must be in the / (not /root) directory before extracting the files!*

The *Installation Manager* will start. Proceed to "The Installation Manager" on page 53.

NOTE: On *OSR5*, we use the Custom+ / Software Manager format. Do not use these instructions for *OSR5*. Follow the Custom+ / Software Manager instructions in the following section.

Using Custom+ / Software Manager Archives

The download filename for *OSR5* and OSR6 systems is called `VOL.000.000`. It is a `tar` archive, but cannot be installed using the `tar` instructions given above.

It is meant to be used under *OSR5* or OSR6 by typing `custom` from a character interface or running **Software Manager** from the *GUI* or `scoadmin`. Use the `Software -> Install New` option, choose `Media Device -> Media Images` and type the name of the *Directory* where you've placed the `VOL.000.000` file. Or, if you are using a floppy archive, choose `Media Device -> Floppy Disk Drive 0`.

Alternately, you may run `custom` from the command line. The following example assumes that the `VOL.000.000` file is in the `/tmp` *Directory*...

```
custom -p misc:edgesco5 -F /tmp/VOL.000.000 -i
```

The *Installation Manager* will start. Proceed to "The Installation Manager" on page 53.

From Internet Downloads

Download the `EDGEDIST.EXE` file directly from the Microlite web site to your desktop. Double-Click on the resulting *Icon* to launch the installer.

The installer will prompt you for the number of floppies you'll need, and ask you to insert each one in turn and press `[Enter]`. They MUST be formatted, although it doesn't matter if they are DOS formatted or *UNIX* formatted.

When complete, take them to the *UNIX* system and follow the `tar` or `custom` installation instructions mentioned previously, as appropriate.

You may also download the file to any folder and double-click on it, or type `EDGEDIST.EXE [Enter]` from a DOS prompt.

Remember to replace `DIST` with the proper four characters referring to the distribution you are using.

5.5 - The Installation Manager

The *Installation Manager* is presented in a "Wizard" format. If there is any problem starting the installation manager program, any previous installation of *Backup**EDGE*** will be unaffected. Unlike older versions, simply extracting the distribution does not immediately overwrite an existing *Backup**EDGE*** installation. The *Installation Manager* will warn you before it causes your old installation to be overwritten.

If you wish to run an installation or upgrade non-interactively, you may do so as described in "BackupEDGE from the Command Line" on page 315.

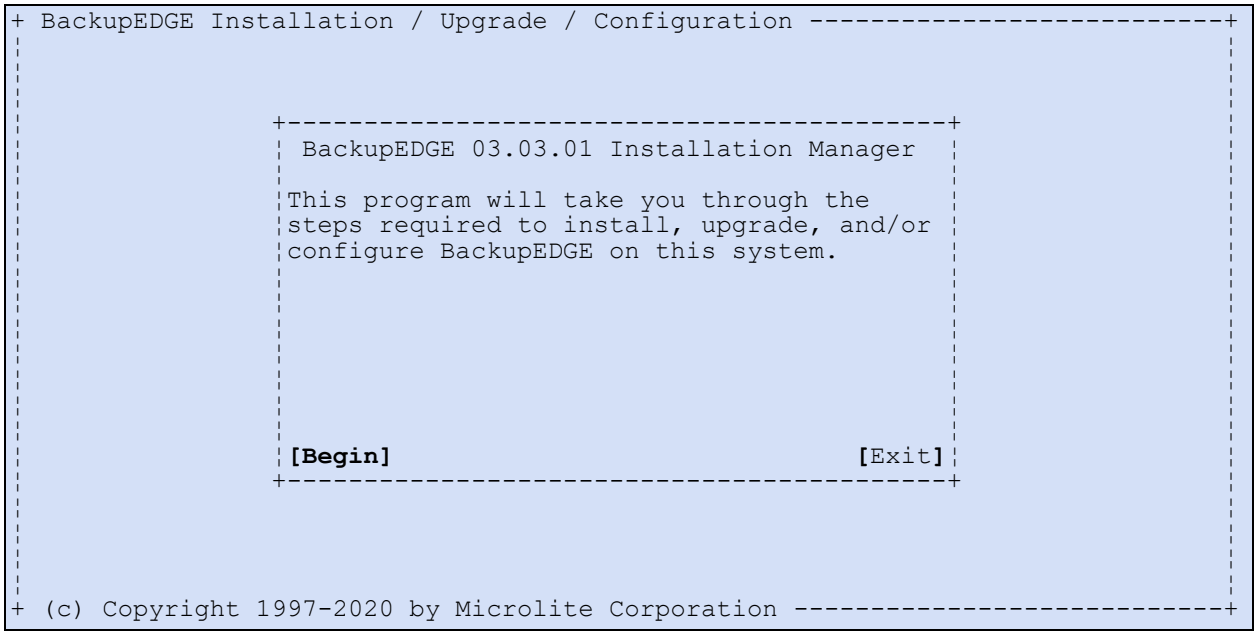
You may install and configure the base product using the following steps. If you wish to enable or configure features that require a separate serial number, such as Encryption, then you must consult the section of the manual on that particular feature.

Navigation

Use the [Arrow Keys] and / or [Tab] to **switch** fields. [Enter] generally selects things / presses buttons / etc. If you want to change a text field, simply highlight it and start typing. On color screens the current window will have red border lines and the inactive windows will have white border lines. To switch windows (sections of the screen) press [Tab]. Pressing a button means using the arrow or [Tab] keys until the indicated text is highlighted, then pressing [Enter].

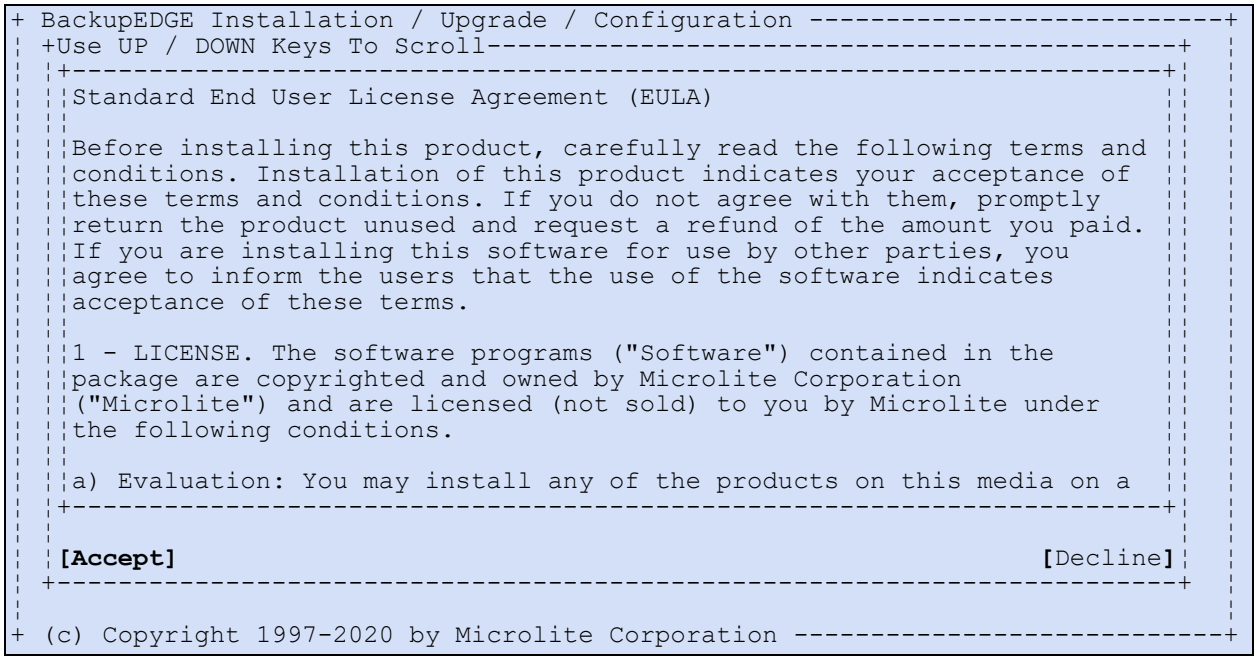
This section goes through a typical installation, screen-by-screen.

Initial Installation Manager Screen



Press [Begin] to begin (press [Enter] while [Begin] is highlighted). The first part of installation deals with actually copying files onto your system, overwriting any previous installation of *Backup**EDGE***. You will be prompted for confirmation before anything irreversible happens during this phase. Your only options are to proceed or abort the whole process. If you press [Exit] here, some distribution files will remain in /usr/lib/edge but no files will be installed or overwritten.

End User License Agreement



Installation of and upgrades to this product are subject to acceptance of an End User License Agreement (EULA). You may use the up and down arrow keys to scroll through the agreement. Press `[Accept]` to accept the terms (press `[Enter]` while `[Accept]` is highlighted). Press `[Decline]` to terminate the installation or upgrade. If you press `[Decline]` here, some distribution files will remain in `/usr/lib/edge` but no files will be installed or overwritten.

A complete copy of the EULA is incorporated into this manual. See “End User License Agreement (EULA)” on page 393.

On some operating systems, you may be given the choice to select between the “Large File” and “Non-Large File” version of *Backup**EDGE***. The Large File version allows you to back up files that are larger than 2GB (Gigabytes). The Non-Large File version does not. Assuming your operating system meets whatever requirements are stated in the question when it is asked, it is recommended that you select the Large File version as it has no disadvantages.

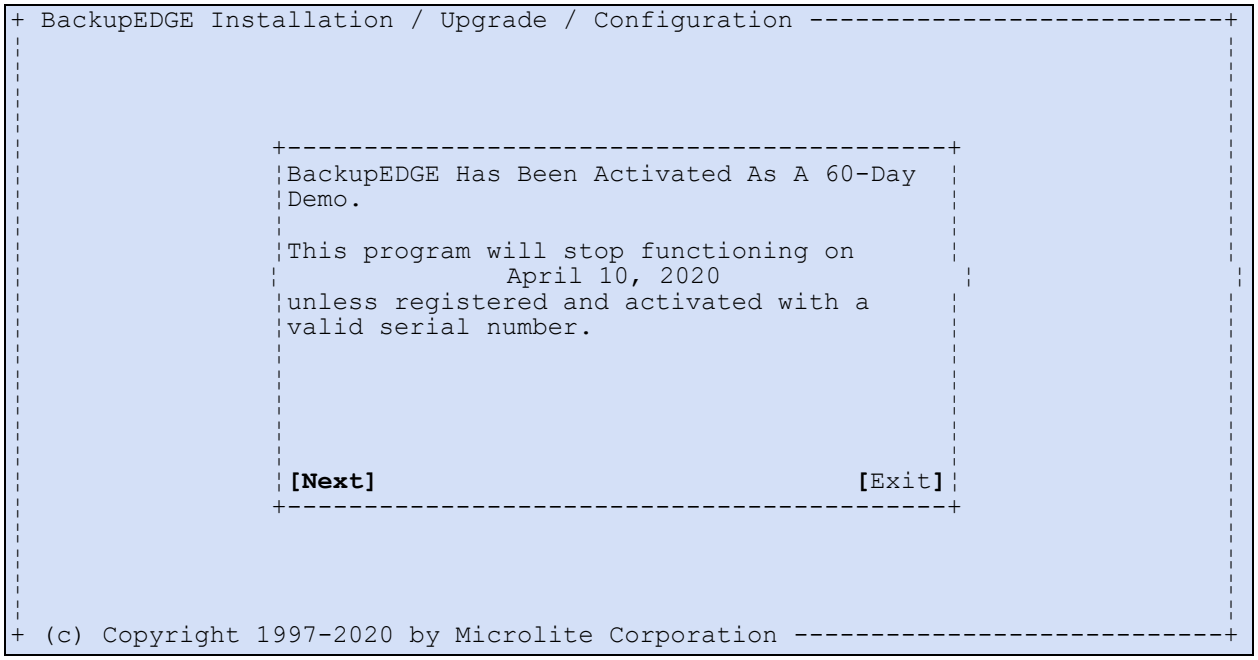
After selecting this, you will not be prompted for it again unless *Backup**EDGE*** is removed and re-installed. If you wish to change your mind later for some reason, you must run the installation in non-interactive mode:

```
./edgelnx.elf -terse -2
```

This would select the Large File version. Use `-1` (one) in place of `-2` to select the Non-Large File version. See “BackupEDGE from the Command Line” on page 315 for more information on non-interactive installations.

Activation Notice

Unless this is an upgrade to a licensed and activated release of *Backup**EDGE*** 03.00.00 or later, the product will be enabled in 60 day demo / evaluation mode.



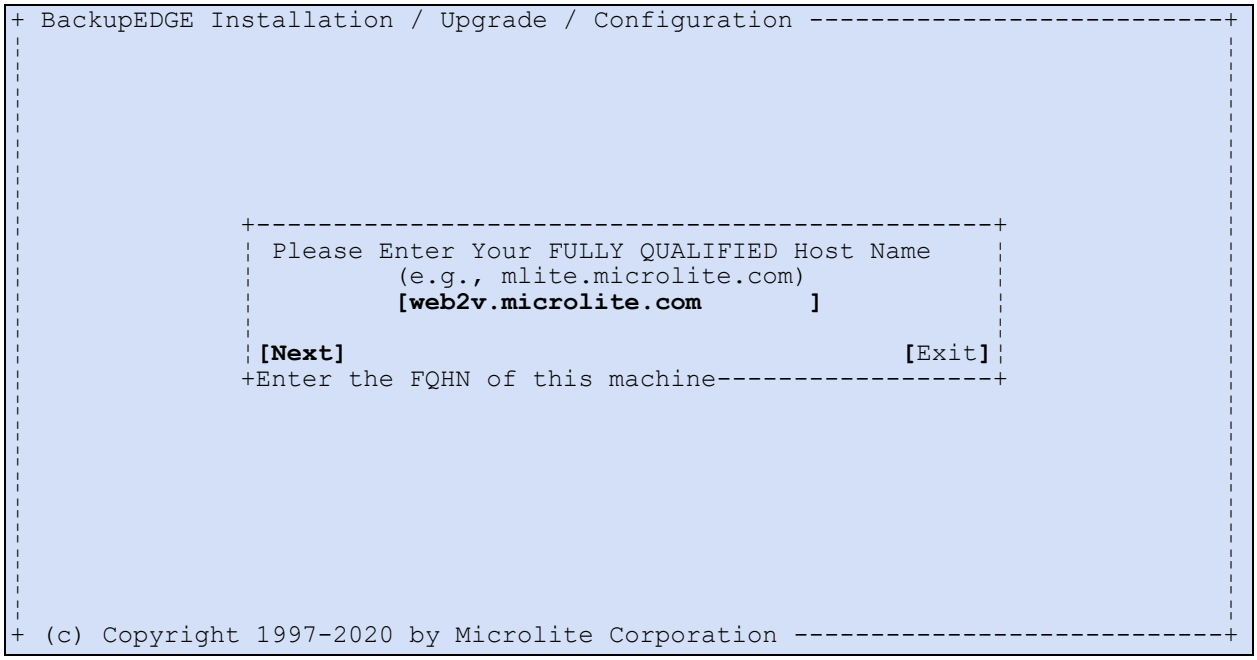
New *Backup**EDGE*** installations are activated automatically for 60 days. During this time, you MUST register and activate the program for it to continue to function.

*Backup**EDGE*** serial numbers for release 01.0x and 02.02.0x are not valid for release 03.00.00 and later. Upgrades are no longer available. You must purchase a new retail license to obtain a serial number compatible with this release of *Backup**EDGE***.

Registration and permanent activation may be performed at any time after the installation is complete by running *EDGEMENU* and selecting `Admin -> Activate BackupEDGE`.

Press `[Next]` to continue to the network settings screen. The `[Exit]` button on this screen is ignored.

Network Settings

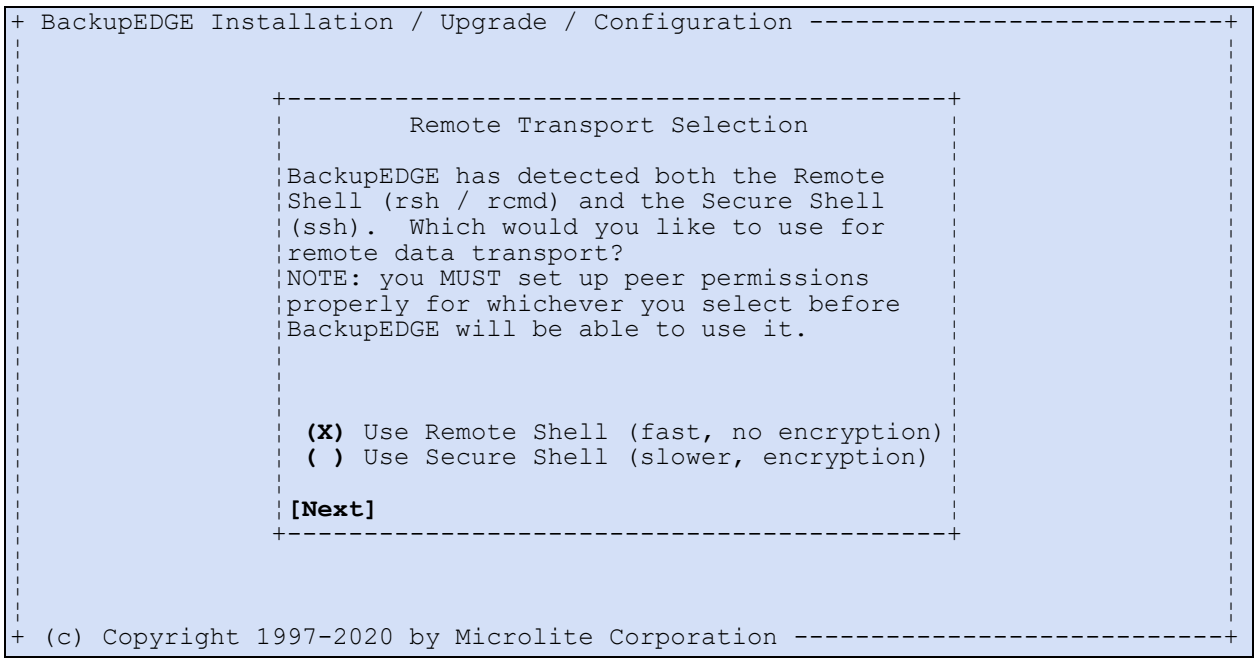


If you are asked to enter your system's Fully Qualified Host Name (FQHN), you should do so. This name must have both a host name and a domain name, such as "`mlitedfs.microlite.com`".

Once you have done this, select `[Next]` to continue with the installation.

NOTE. If the machine is not on a network and only the hostname appears, simply add "`localhost.com`" or "`yourcompany.com`" to give it a usable domain name.

Network Transport



This screen allows to change the way that *BackupEDGE* sends data across the network when doing *BackupEDGE* to *BackupEDGE* device backups. If you will be doing *FTP Backups* (see page 90), or if you do not create backups across the network, this setting is irrelevant. Just press `[Next]`. This setting does ***not*** affect *FTP Backups*.

For *BackupEDGE* to *BackupEDGE Network Backups*, the two most popular transports for sending data across the network are the *Remote Shell* (*rsh*, also called *rcmd* under some OpenServer 5 systems) and the *Secure Shell* (*ssh*). *BackupEDGE* typically configures itself to use *rsh/rcmd*. If *ssh* is detected, you are prompted to choose your transport layer through this screen.

FastSelect

This screen introduces and demonstrates the concept of **FastSelect** within the user interface. The `[Up-Arrow]` and `[Down-Arrow]` keys can be used while the cursor is on the `[Next]` button to choose between **Use Remote Shell** and **Use Secure Shell**. When the `(X)` is displayed next to the transport you wish to use, press `[Next]`.

FastSelect is available from many prompts within *BackupEDGE*, typically while the cursor is on a `[Next]` prompt and a series of choices are displayed.

If only the *Remote Shell* is detected, *BackupEDGE* will select it automatically and skip this screen. If only the *Secure Shell* (*ssh*) is detected, you will be notified that it has been selected as the default.

For *BackupEDGE* to *BackupEDGE Network Backups* to work, the following must be true...

- A system somewhere on the network must exist that has a storage *Device* and the same release of *BackupEDGE* installed. Let's call this system `tapehost`.
- The system to be backed up must also have a copy of *BackupEDGE* installed. Let's call this system `myhost`.
- Remote communications with `root` peer permissions must be set up such that `myhost` can execute commands on `tapehost`. For instance...

```
rcmd tapehost ls
rsh tapehost ls
ssh tapehost ls
```

These commands must be executable without prompting for a password.

Backups via FTP do not require this; Network Backups refers to backups from one *BackupEDGE* system to a resource on another system with *BackupEDGE* installed. *FTP Backups* cause *BackupEDGE* to talk to an FTP server directly, without using RSH / RCMD / SSH.

It is not necessary for `tapehost` to be able to execute commands on `myhost`.

NOTE: *RecoverEDGE* for *OSR6*, *UW7* and *Linux* will use *ssh* or *rsh* as defined here for restoring from remote tape drives. *RecoverEDGE* for *OSR5* will always be configured to use *rcmd*. Remote access **into** a system booted from *RecoverEDGE* media is always done using the *telnet* protocol regardless of the operating system type or network transport selection.

The user can switch *Network Transports* at any time by logging in as `root` and executing the following command...

```
/usr/lib/edge/bin/edge.install -network
```

This will re-run only the *Remote Transport Selection* section of the installer.

NOTE: You will not be prompted to select the Network Transport again during subsequent upgrades unless *BackupEDGE* is removed first. To force *BackupEDGE* to ask, run `edge.install -network` as directed above.

See "Network Backups - BackupEDGE to BackupEDGE" on page 257 for more information.

NOTE: Selection of the Network Transport is not related to the optional Encryption feature of *BackupEDGE*. It does not affect how data is stored on an archive; just how it is transported across the network. Files that are encrypted with the Encryption feature are always transported

across the network in encrypted form, even if *rsh*/*rcmd* is the Network Transport. The Network Transport also does not affect *FTP Backups*.

Device Autodetection

```
+ BackupEDGE Installation / Upgrade / Configuration ---------------------------+
|                                                                              |
|                  +-----------------------------------------+                 |
|                  |           Device Autodetection          |                 |
|                  |                                         |                 |
|                  |Ready to scan for valid resources.       |                 |
|                  |Previously configured resources will be  |                 |
|                  |unaffected.                              |                 |
|                  |                                         |                 |
|                  |                                         |                 |
|                  |                                         |                 |
|                  |                                         |                 |
|                  |                                         |                 |
|                  |                                         |                 |
|                  |                                         |                 |
|                  |  (X) Perform Autodetection              |                 |
|                  |  ( ) Skip Autodetection                 |                 |
|                  |                                         |                 |
|                  |[Next]                             [Exit]|                 |
|                  +-----------------------------------------+                 |
|                                                                              |
|                                                                              |
+ (c) Copyright 1997-2020 by Microlite Corporation ----------------------------+
```

*Backup**EDGE*** can scan your system and create *Resource* entries for each of Tape and Optical drives, as well as for any *Autochangers*. If this has not been done before, you will be given the option to do so.

NOTE: After autodetection has been completed successfully, you will not be prompted to do so again during future upgrades, unless *Backup**EDGE*** is completely removed or additional device support has been added to *Backup**EDGE***. To force autodetection again, you should use the option `Setup -> Configure BackupEDGE -> Autodetect New Devices` from *EDGEMENU*.

You **must** have one piece of media in each *Device* in order for *Backup**EDGE*** to properly detect the characteristics of the *Device*. *Backup**EDGE*** will not attempt to write on any *Devices* (unless `[Manual Check]` for tape drives is pressed specifically), but many *Devices* on many operating systems can not be autodetected unless they have media present.

NOTE: Optical drives may be probed only with a CD-ROM or with other non-blank media inserted. Do NOT use a factory blank *CD*, DVD or Blu-ray Disc during probing.

This screen again uses the concept of **FastSelect** within the user interface. The `[Up-Arrow]` and `[Down-Arrow]` keys can be used while the cursor is on the `[Next]` button to choose quickly between **Perform Autodetection** and **Skip Autodetection**. The normal response is the default (**Perform Autodetection**) so just press `[Next]`.

Each *Resource* that is detected is given a nickname, or *Resource Name*. There is a naming convention for these *Resources*. For instance, the first tape drive detected will generate a *Resource* called `tape0`, the second `tape1`, the third `tape2`, etc.

Optical *Resources* of all types are nicknamed `optical0`, `optical1`, etc. *Autochangers* are `changer0`, `changer1`, etc.

NOTE: *Resource Names* may be changed as desired. For instance, you can change the name for `tape0` to `sony` if it is easier to remember. Most people leave the names at the default. It is possible to rename a *Resource* after installation, but you must also update any *Scheduled Job* that references it by name. The easiest way is to pick the right name during installation and keep it. (Of course, you may modify any parameters other than the name, and all *Scheduled Jobs* will automatically use the new settings.)

Users of older versions of *Backup**EDGE*** will note that the older optical drive *Resources* were named `cdrom0`, `dvd0`, etc. These have all been changed to `optical0`, `optical1`, etc. in *Backup**EDGE*** 3.0 and later..

If you choose to skip **Device Autodetection** and already have *Resources* available, proceed to “Scheduling A Default Backup” on page 64. This is not recommended.

Pressing `[Exit]` on this screen will result in a complete fresh installation, but without *Device Resources* being created, a default backup schedule, or a sparse file scan. The first time you run *EDGEMENU* you’ll need to manually define at least one *Resource*.

If you have no URL resources defined, you will be given the option to create one for backups to an FTP server. If you elect to do this, you must provide the machine name, destination directory name (relative to ‘/’), and optionally the FTP username and password to use. Please refer to “Setting Up FTP Backups” on page 92 for more information.

If for any reason no *Resources* are found and you are not doing *Network, SharpDrive, or FSP/AF Backups*, proceed with the installation. Before you schedule your first backup job, you will have to create a new *Resource* to use with it. Refer to “Defining Resources Manually” on page 355 for information on manually defining *Resources* when you get to this point.

Remember, however, that *Backup**EDGE*** cannot detect or use a *Device* that has not been configured into your operating system. For tape drives, this means that operating system utilities such as `tar` and `cpio` must be able to access the *Device*. For optical drives, the operating system must at least see a CD-ROM drive, even if it is not capable of writing to the *Device* natively.

Navigating Resource Screens

`[F1]` - Field Help
`[F8]` - Refresh key. Redraws the display in the event it gets corrupted.
`[Up-Arrow]`/`[Down-Arrow]` - Scroll through fields.
`[Left-Arrow]`/`[Right-Arrow]` - Change values in scrollable fields, edit text fields. Switch between menu options.
`[Tab]` - Fast navigate to first field in a section.
`[Enter]` - Commit a change or press the highlighted button.

Examples of Storage Resources

Sample Tape Drive Resource

```
+-------------------------------------------------------------------------+
|- General Resource Information -------------------------------------------|
|Resource Type       Tape Drive                                           |
|Resource Name       [tape0            ] Change as appropriate            |
|Description         [QUANTUM ULTRIUM 4 2210      ]                       |
|Changer Assoc       [changer0:dt0]                                       |
|Interface           [SCSI       ]                                        |
|                                                                         |
|- Tape Drive Information -------------------------------------------------|
|Data Node           [/dev/st0                    ] [A] TapeAlert(tm) Support |
|No Rewind Node      [/dev/nst0                   ] [ ] Multiple Archives? |
|Tape Block Size     [-1                          ] [C] Partition         |
|Locate Threshhold   [30                          ] [ Manual Check ]      |
|                                                                         |
|                                                                         |
|- Default Backup Properties ----------------------------------------------|
|Volume Size         [0           ] [H] Compression                       |
|Edge Block Size     [256         ] [Y] Double Buffering                  |
|[Next]                             [Prev]                        [Cancel]|
+-------------------------------------------------------------------------+
```

BackupEDGE automatically detects tape drives and prepares a *Resource* for them. See “Configuring a Tape Resource” on page 69 for more information.

Sample Autochanger Resource

```
+-------------------------------------------------------------------------+
|- General Resource Information -------------------------------------------|
|Resource Type       AutoChanger                                          |
|Resource Name       [changer0         ] Change as appropriate            |
|Description         [DELL PV-124T 0070          ]                       |
|Changer Assoc       [Modify Associated Devices]                          |
|Interface           [SCSI       ]                                        |
|Control Node        [/dev/sg2         ]                                  |
|- Media Jukebox Information ----------------------------------------------|
|[ ]    Load after changer op.                                            |
|[X]    Unload before changer op.                                         |
|[A]    Barcode Support                                                   |
|[Y]    Wait for Device Ready                                             |
|[0   ] Load Delay                                                        |
|[Next]                           [Prev]                        [Cancel]|
+-------------------------------------------------------------------------+
```

BackupEDGE automatically detects tape autoloaders and prepares a *Resource* for them. It is necessary for the user to establish an *Association* between the autoloader and the storage *Resource* (or *Resources*) for which it will be handling media. See “Configuring an Autoloader Resource” on page 74 for more information.

Sample Optical Drive Resource

```
+ BackupEDGE Resource Information ------------------------------------------+
|- General Resource Information ----------------------------------------------|
|Resource Type       Optical Drive                                           |
|Resource Name       [optical0          ] Change as appropriate              |
|Description         [HL-DT-ST BD-RE GGW-H20L YL05]                          |
|Changer Assoc                                                               |
|Interface           [IDE / ATAPI]                                           |
|                                                                            |
|- CD / DVD / Optical Information --------------------------------------------|
|Data Node           [/dev/hdc                    ] [ ] Buffer Whole Disc?   |
|Mount Device Node   [/dev/hdc                    ] [X] BurnProof(tm)?       |
|Record Buffer (K)   [2048                        ] [X] Multiple Archives?   |
|Needs Eject?        [ ]                                                     |
|Writable Media:     CD-R[W], DVD-RAM, DVD+/-R[W], BD-RE                     |
|                                                                            |
|- Default Backup Properties -------------------------------------------------|
|Volume Size         [0            ] [S] Compression Level  [5]              |
|Edge Block Size     [64           ] [Y] Double Buffering                    |
|[Next]                              [Prev]                          [Cancel]|
+----------------------------------------------------------------------------+
```

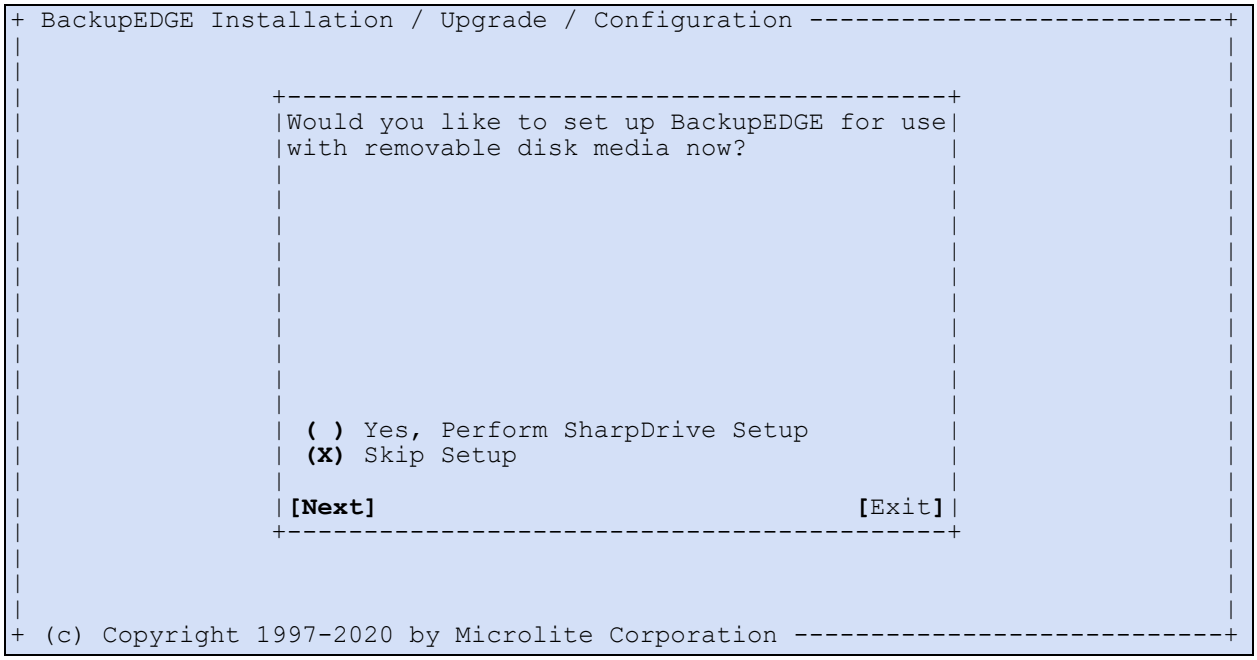
BackupEDGE automatically detects optical drives and prepares a *Resource* for them. See “Configuring an Optical Drive Resource” on page 77 for more information.

Configuring a URL for FTP Backups

```
+ BackupEDGE Installation / Upgrade / Configuration ---------------------------+
|                                                                              |
|                                                                              |
|                +-----------------------------------------+                   |
|                |Would you like to create a BackupEDGE URL|                   |
|                |resource for FTP backups now?            |                   |
|                |                                         |                   |
|                |                                         |                   |
|                |                                         |                   |
|                |                                         |                   |
|                |                                         |                   |
|                |                                         |                   |
|                |                                         |                   |
|                |                                         |                   |
|                |                                         |                   |
|                | (X) Yes, create one                     |                   |
|                | ( ) No                                  |                   |
|                |                                         |                   |
|                |[Next]                             [Exit]|                   |
|                +-----------------------------------------+                   |
|                                                                              |
|                                                                              |
|                                                                              |
+ (c) Copyright 1997-2020 by Microlite Corporation ---------------------------+
```

The installer asked if you wish to configure a *URL Resource* for FTP / FTPS backups. If you do, select `Yes` and see “Configuring FTP/FTPS Backups” on page 90 for more information. Otherwise, select `No`.

Configuring for SharpDrive Backups



On supported platforms, the installer asked if you wish to configure a *SharpDrive Resource* for removable / cartridge disk backups. If you do, select `Yes` and see “Configuring SharpDrive Backups” on page 80 for more information. Otherwise, select `No`.

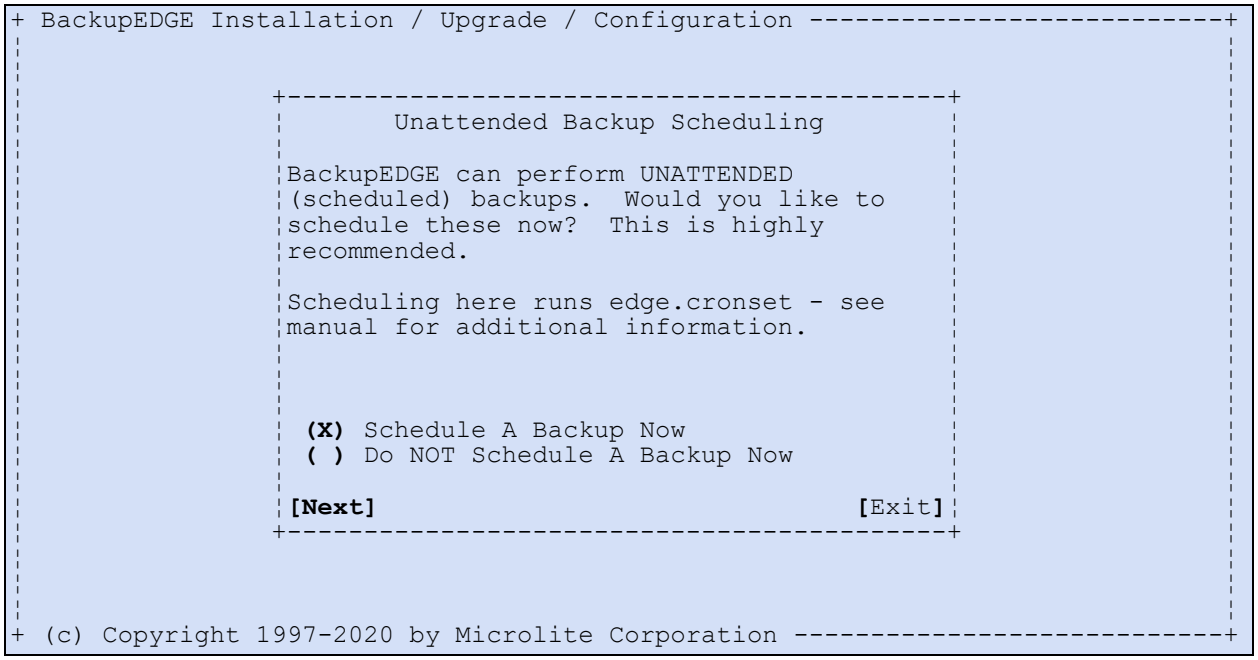
Configuring for S3-Compatible Cloud Backups

Although not configured during installation, It is possible to configure *Backup**EDGE*** to back up to the S3-compatible cloud services such as Amazon Simple Storage Service (S3), Google Cloud Storage, Wasabi and more. This may be done after installation is complete. See “Configuring S3 API Cloud Backups (S3CLOUD)” on page 113.

Configuring for NFS Backups

Although not configured during installation, It is possible on many operating systems to configure *Backup**EDGE*** to back up to *NFS servers* after installation is complete. See “Configuring NFS Backups” on page 98.

Scheduling A Default Backup



After all *Devices* have been defined, the installer will allow you to create or modify your unattended backup *Schedules*.

For more information on this, please refer to "BackupEDGE Licensing" on page 363.

Next you will be prompted to create a default Backup *Schedule*. Use **Fast Select** to choose whether or not to *Schedule* a backup now. If you choose not to *Schedule* a backup, proceed to "Virtual File Check" on page 67.

NOTE: Microlite recommends **always** choosing to allow the installer to create a default backups schedule, even if you intend to disable it later.

If you choose to `Schedule a Backup Now`, the **Basic Scheduler Wizard** will run. First, you'll need to choose a *Resource* for the *Schedule*.

Schedule Job Wizard - Select Primary Resource

```
+ Select Primary Device ------------------------------------------------------+
|You are selecting the Destination Resource(s) to use for this Backup / Verify.|
|  This will be the Primary Resource used.                                     |
|                                                                              |
|+ Resource List -------+                                                      |
||-> optical0           | Resource :   optical0                                |
||   sdrive0             |              HL-DT-ST BD-RE GGW-H20L YL05             |
||   tape0               | Machine :    [web2v.microlite.com                  ]|
||   url0                |                                                      |
||   floppy0             | To select a different resource, use the Up / Down    |
||   NullDevice          | arrow keys while the Next button is highlighted.  To |
||   [NEW]               | view resources on a different machine, press the TAB |
||                       | key and type the system name in the "Machine" field, |
||                       | and press ENTER.                                     |
|+----------------------+                                                      |
|                                                                              |
|[Next]                                [Prev]                          [Cancel]|
+------------------------------------------------------------------------------+
```

Using **FastSelect** from the `[Next]` button, highlight the appropriate *Resource* and press `[Enter]`. We'll use `tape1` in this example.

NOTE: You may choose a *Resource* from a different system by pressing `[Tab]` to get to the `Machine:` prompt and typing in the proper system name. Remote command permissions must be active, and the remote system must have the same release of *Backup**EDGE*** installed. The remote system must also have the desired *Resources* defined. If these criteria are met, then the `Resource List` above will display remote *Resources* in this instance. The **FastSelect** process is the same. See "Network Backups - BackupEDGE to BackupEDGE" on page 257 for more information.

NOTE: If no *Resources* were detected during autodetection, and none were defined previously (if this is an upgrade), then you will be presented with two choices: `NullDevice` and `[NEW]`. Using the `NullDevice` will simply ***discard the data***, so you will probably want to define a new *Resource* with `[NEW]` or enter a different machine for remote backups.

Schedule Job Wizard - Select Backup Time

```
+Scheduled Job Wizard - Select Backup Time------------------------------------+
|At what time (24 hour clock) would you like to run this scheduled job?        |
|[23:00                                                                      ]|
|                                                                              |
|                                                                              |
|                                                                              |
|                                                                              |
|[Next]                                [Prev]                          [Cancel]|
+------------------------------------------------------------------------------+
```

If the default time (`23:00`, or `11:00pm` local time) is acceptable, press `[Next]`. Otherwise, press `[Up-Arrow]` and type in the desired time, then press `[Next]`.

Schedule Job Wizard - Select Backup Days

```
+Scheduled Job Wizard - Select Backup Days-------------------------------------+
¦Pick which days you'd like to run this scheduled job.                         ¦
¦Sunday              [ ]                                                       ¦
¦Monday              [X]                                                       ¦
¦Tuesday             [X]                                                       ¦
¦Wednesday           [X]                                                       ¦
¦Thursday            [X]                                                       ¦
¦Friday              [X]                                                       ¦
¦Saturday            [ ]                                                       ¦
¦                                                                              ¦
¦[Next]                              [Prev]                             [Cancel]¦
+--------------------------------------------------------------------------------+
```

Use the arrows to position the cursor to the proper day of the week, and use `[Space]` to toggle the **X** off or on for each day of the week you'd like to run the backup. Then press `[Next]`.

Schedule Job Wizard - Edit Backup Schedule

```
+ Edit Backup Schedule ------------------------------------------------------+
| Schedule Name:     simple_job                                              |
|          Time:     [23:00 ] (14:58:46)  Enabled: [X]                       |
| Sequence:                   web2v.microlite.com:esequence/onsite           |
| Backup Domain:              system                                         |
| Primary Resource:  [Change] web2v.microlite.com:optical!optical0           |
|                                                                            |
| +-------------------------------------------------+     September 2019      |
| | Every Sunday of the week                (None) |  Su Mo Tu We Th Fr Sa  |
| | Every Monday of the week               Master |   1 M  M  M  M  M   7  |
| | Every Tuesday of the week              Master |   8 M  M  M  M  M  14  |
| | Every Wednesday of the week            Master |  15 M  M  M  M  M  21  |
| | Every Thursday of the week             Master |  22 M  M  M  M  M  28  |
| | Every Friday of the week               Master |  29 M                  |
| | Every Saturday of the week              (None) |                        |
| +-------------------------------------------------+                        |
| Notify / Advanced: [Change]  [Reset Dates]                                 |
| Mail Summary To:   root                    Print Summary To:   NONE        |
| Mail Failures To:  NONE                    Print Failures To:  NONE        |
|[Save]                                                          [Cancel]|
+----------------------------------------------------------------------------+
```

Here you have a final chance to change the `Time`, `Primary Resource`, `Day of the week`, and `Notification / Advanced` fields before selecting `[Next]` to save the schedule.

On the `Day of the week` lines (such as `Every Sunday of the week`) you may press the space bar to toggle the backup type between `Master`, `Differential`, `Incremental` and `(None)`. Days of the week with a backup occurring will show `M`, `D`, or `I` on the calendar to the right. Days with no backup scheduled will show the date. After installation, enabling the *Advanced Scheduler* provides many more options. See "Scheduling - Basic" on page 210 for more information.

You may also uncheck the `Enabled:` flag. This allows you to save the entire *Scheduled Job*, without submitting it to the scheduler. It is in effect an ON/OFF switch for pre-defined jobs.

NOTE: The `[Tab]` key is very useful for switching between fields in the *Scheduler*.

If you are configuring NAS backups, please refer to "Setting Up FTP Backups" on page 92 for additional information.

It is very important to set up at least one email address or printer to be *Notified* of the results of the *Scheduled Job*. This is done by pressing the `[Change]` button identified as `Notify / Advanced`.

Schedule Job Wizard - Notify / Advanced

```
+ Edit Backup Advanced Properties ------------------------------------------+
|                    Backup Schedule Advanced Properties                     |
|                                                                            |
| Schedule Name:     simple_job                                              |
|                                                                            |
| Verify Type:       [B]                 Checksumming:  [X]                  |
| Attempt Index:     [X]                 Retention:     [6 Days]             |
| Attempt Bootable:  [ ]                 Copy to:       [NONE]               |
| Promote A:         [ ]                 Copy Retention:[Forever]            |
| Promote B:         [X]                                                     |
| Eject/Vol Switch:  [ ]                                                     |
| Eject/Verify:      [ ]                                                     |
|                                                                            |
| Mail Summary To:   [root                                               ]   |
| Print Summary To:  [                                                   ]   |
| Mail Failures To:  [                                                   ]   |
| Print Failures To: [                                                   ]   |
|                                                                            |
|                                                                            |
|[Next]                                                          [Cancel]    |
+----------------------------------------------------------------------------+
```

Enter at least one user name in the `Mail Summary To` field. Preferably, add a print spooler name to the `Print Summary To` field, then press `[Next]`. Multiple user names and printers are separated by spaces.

By default, *Backup**EDGE*** will mail the results of all successful and unsuccessful *Scheduled Jobs* to the addresses listed using the system mailer, and will print summaries of all successful and unsuccessful *Scheduled Jobs* to the specified printer using the appropriate `lpr` or `lp` command for the operating system being used.

However, that is just the beginning of the reporting capabilities available with *Backup**EDGE***. *Notifiers* allow a wide variety of options for putting messages in users' hands. See "Working with Notifiers" on page 235 for additional information.

There are other fields in the *Advanced Properties* section of the *Basic Schedule*. For now, the defaults are fine.

Saving The Backup Schedule

When all advanced entries are created, press `[Next]` to return to the **Edit Backup Schedule** screen. Press `[Next]` from this screen to save the *Schedule*.

NOTE: The *Scheduler* will warn you if no *Notifications* have been defined, and strongly recommend that you create at least one. It will only let you continue in this case if you confirm that you do not want any *Notifications* sent or printed. This is highly discouraged.

See "Scheduling - Basic" on page 210 for additional information on the basic and advanced scheduling capabilities of *Backup**EDGE***.

Virtual File Check

The last phase of the installation is the *Virtual File Check*. *Backup**EDGE*** contains a scanner that will run as a *Background Task*, checking each file on your system and adding it to a list of files to be treated specially if it appears to be a *Virtual*, or *Sparse* file. Most users do not need to run this check, and the default is to `[Skip]` the check. See "Virtual File Identification" on page 345 for more information on this subject.

MySQL Backup Setup

If MySQL is detected, the installer will offer to configure for MySQL backups and add them to the default schedule. See "MySQL / MariaDB Backups" on page 177 for more information.

Finishing The Installation

The installer will congratulate you on your successful installation and ask you to press the `[Exit]` button. If you have launched the installer from an autorun session or from a *GUI Icon*, the window will close. If you ran from a command line, you'll be returned to a `root` prompt. Installation is now complete.

NOTE: Remember to un-mount the CD-ROM and eject it if this was a CD-ROM based installation.

5.6 - Notes on Changing Backup Device Hardware

*Backup**EDGE*** treats a *Resource* as a reference to the physical device, rather than to a device node. When attempting to access a *Resource*, *Backup**EDGE*** will try to find the same physical device that the *Resource* describes. Generally, this requires no action on your part, other than ensuring that the device in question really is attached to the system, and that the operating system can acces it.

*Backup**EDGE*** identifies devices by their manufacturer, model, and serial number. This information is recorded with the *Resource*. If *Backup**EDGE*** can find a device that matches these for the *Resource* it is trying to access, then it is assumed to be the correct physical device for that *Resource*, and is used. For older devices that do not provide such information, *Backup**EDGE*** generally assumes that they do not move from their original device node. In some cases, it may be able to determine by the process of elimination if such a device has moved, but in general it cannot tell the difference between devices without serial numbers.

Under OpenServer 5, optical devices are identified only by device node, not by serial number or other information. No attempt to find the same physical device is provided. This is caused by a limitation in some versions of the `Srom` driver. Tape drives under OpenServer 5 are not affected by this. Remember that for any device in OpenServer 5, tape or otherwise, you must make sure to run the appropriate `mkdev` script when you install it, or if you change its SCSI ID, ATAPI cable location, etc.

In most cases, the device will be configured once and never change. However, adding new hardware (such as an additional tape drive or optical drive) might cause the operating system to change the mapping between device node (e.g., `/dev/rStp0`, `/dev/st0`, or `/dev/rmt/ctape1`) and physical device. In this case, *Backup**EDGE*** will adjust automatically, subject to the exceptions listed above.

If a device is not available when *Backup**EDGE*** tries to use it, then *Backup**EDGE*** will try to find a substitute. This substitute will be chosen from all devices for which there is a corresponding *Resource* that is the same type (tape drive, optical, etc.) as the original. If *Backup**EDGE*** finds such a device, then it will ask for confirmation before using the device in place of the original, if possible. If *Backup**EDGE*** is running unattended, such as from a *Scheduled Job*, then it will allow the substitution automatically. Either way, the backup summary will note that a substitution has been made, along with information about the original and new device model and serial numbers.

If a substitution is in use for one or more *Resources* when *EDGEMENU* is started, then you will be notified about it. You will also be given the option to make the substitution permanent. This is useful if you have permanently switched hardware. For example, if a tape drive fails and is replaced by a new one, *Backup**EDGE*** will notice this, and create a substitution. You would then want to tell it to use this new device permanently.

6 - Configuring a Tape Resource

6.1 - General Concepts

Tape drives are the traditional storage device for server protection, although many users prefer the newer storage *Resources* available with *Backup**EDGE***.

NOTE: *Backup**EDGE** 3.0* and later supports multiple archives per medium on tape drives. This is a change in behaviour from our older products. Tapes used in single archive mode or initialized for single archive mode **must be re-initialized** for use with multiple archives per medium. The default may be over-ridden for legacy behaviour or for One Button Disaster Recovery (OBDR) support. See See “Multiple Archives Per Tape” on page 69..

NOTE 2: *Backup**EDGE** 03.00.03b4* and later **default** to having multiple archives per medium disabled, emulating legacy behaviour. However, if upgrading a prior 03.00.0x release, the currently defined behaviour will remain in place. If multiple domains per backup schedule (including MySQL) are to be configured, be sure to enable this feature and set appropriate archive expiration times.

6.2 - Compatibility Matrix

Operating System(s)	SCSI/SAS/USB	IDE/SATA[a]	Notes[b]
Linux	YES	YES	
OpenServer 6	YES	Limited	Sony devices only, using the SATA AHCI driver.
UnixWare 7	YES	Limited	Sony devices only, using the SATA AHCI driver.
OpenServer 5	YES	NO	IDE / SATA devices are not supported by *Backup**EDGE***.

a. IDE and SATA tape drives are no longer available in the marketplace. This information is for legacy purposes only.
b. These are due to operating system device driver issues, not strictly *Backup**EDGE*** issues. *Backup**EDGE*** advanced device management, tape positioning etc. require issuing commands beyond normal read/write commands and these require additional driver support.

6.3 - Multiple Archives Per Tape

*Backup**EDGE** 3.x* supports performing multiple backups onto tape media. By **default**, writing to a tape that has one or more *unexpired backups* will now result in *Backup**EDGE*** appending the new backup after the unexpired ones.

Append Behaviour

Multiple Archives Flag Set to **YES**	Multiple Archives Flag Set to **NO**
Backup will append to the tape starting after the last *expired* archive. If all archives have expired, Backup will start at beginning of tape	Backup will always start at *beginning of tape*. Backup will **FAIL** if tape contains an unexpired archive.
OBDR booting not supported	OBDR booting supported

*Backup**EDGE*** aggressively reclaims backups made on tape media, since a tape still must be written from front to back. This means that once a backup’s Time To Live has expired it can be reclaimed if it is the last backup on the tape or if the backups that were made after it also has an expired Time To Live which must include the last backup on the tape.

6.4 - Tape Notes

- Hardware compression is the default. and probably the fastest. Software compression will be slower but will probably increase net tape capacity.
- Optional encryption is supported.
- Full file checksumming, for maximum data integrity, is supported.
- *Fast File Restore* is available from any archive. It is not necessary to read through an entire archive to restore individual files and directories.
- MySQL™ hot backups are supported as a separate *Scheduled Job* when multiple archives per medium is disabled. When enabled, the MySQL backup will be appended after the full system backup.

6.5 - Initializing

`EDGEMENU -> Admin -> Initialize Medium` while the tape drive is selected as the *Primary Resource* will completely erase the tape and all archives on it, replacing them with a single tape label indicating that the medium has been initialized.

6.6 - Fast File Restore

*Backup**EDGE*** can restore any file from any archive on tape media using tape drive *Quick File Access* mode for the fastest possible media positioning.

6.7 - Resource Information

Sample Tape Drive Resource

```
+-------------------------------------------------------------------------------+
|- General Resource Information -------------------------------------------------|
|Resource Type       Tape Drive                                                 |
|Resource Name       [tape0             ] Change as appropriate                 |
|Description         [QUANTUM ULTRIUM 4 2210      ]                            |
|Changer Assoc       [changer0:dt0]                                             |
|Interface           [SCSI       ]                                              |
|                                                                               |
|- Tape Drive Information -------------------------------------------------------|
|Data Node           [/dev/st0                    ] [A] TapeAlert(tm) Support   |
|No Rewind Node      [/dev/nst0                   ] [X] Multiple Archives?      |
|Tape Block Size     [-1                          ] [C] Partition               |
|Locate Threshhold   [30                          ] [ Manual Check ]            |
|                                                                               |
|                                                                               |
|- Default Backup Properties ----------------------------------------------------|
|Volume Size         [0           ] [H] Compression                             |
|Edge Block Size     [256         ] [Y] Double Buffering                        |
|[Next]                             [Prev]                          [Cancel]    |
+-------------------------------------------------------------------------------+
```

Resource Type
This is automatically set.

Resource Name
The default name for the first drive is `tape0`, the second `tape1`, etc. Any name may be chosen, but no spaces are allowed in the name. We suggest keeping the default name. If you wish to rename the Resource, remember that the name is case-sensitive. Do not use the names "`tape`", "`changer`", "`optical`", "`rev`", "`url`", "`sccloud`", "`fsp`", "`af`", "`sdrive`", or "`other`" unless you add other characters also (e.g., "`tape0`").

Description
This defaults to the *Device* name, model number and firmware revision that are detected. It may be changed to any easy-to-remember description.

Changer Assoc
This field is only active if at least one *Autochanger* has been detected. If this *Device* is installed in an *Autochanger*, this field displays that relationship. In the example above, this is the first tape drive.

Interface Type
This tells *BackupEDGE* what type of commands to issue when communicating with the *Devices*. Options are: SCSI (use the SCSI /SAS / USB BUS), IDE/ATAPI, (use the IDE BUS), and Other (No *Device* control commands available. Open for read and write only). The default is almost always correct. Use `[Left-Arrow]`/`[Right-Arrow]` to change selections.

NOTE: *Linux* 2.4.x systems (now deprecated) with IDE/ATAPI *Devices* running under the `ide-scsi` driver show up as SCSI *Devices*. This is correct, and is the only recommended method for using them.

Devices which have trouble sending or receiving commands over the SCSI or IDE/ATAPI bus may be switched to `Resource Type: Other Device`. This tells *BackupEDGE* not to probe or set the *Device*, but to use read and write commands only. This disables SCSI inquiries and *Fast File Restore*.

Control Node
This field is *OSR5*-specific, and refers to a hardware control node which can be used to communicate with a *Device* without transferring any data to or from the loaded medium, possibly while the *Device* is in use by another program. The default is usually correct.

Data Node
This is the normal read/write, rewind-on-close *Device Node*. For operating systems that support them, you should be sure **not** to use "unload-on-close" *Device Nodes*. If a tape ejects immediately after a backup, it is very likely that the *Device Node* specified here is an "unload-on-close" type.

No Rewind Node
Used to open for read and write, without rewinding to beginning of tape on close.

Tape Block Size
There are three choices for this field. Setting it to `-1` tells *BackupEDGE* not to attempt to set the *Tape Block Size* before a backup. It will simply use the current setting of the *Device*. `0` tells *BackupEDGE* to place the *Device* in *Variable Block Mode*, where the block size is the write buffer size. Other positive numbers (typically `512`, `1024`, and `2048`) tell *BackupEDGE* to set the *Device* into a *Fixed Block Mode*. The *BackupEDGE* default is `-1`.

NOTE: If your tape drive will be doing *Bootable Backups*, the **Tape Block Size** MUST be set at `2048`.

Multiple Archives?
If checked, allows multiple archives to be stored per tape. If unchecked, only a single archive per tape will be written (this was the behavior in all previous *BackupEDGE* releases.

Locate Threshold
This value is the key to **Fast File Restore** (*FFR*). It sets a threshold (in Megabytes) for using high speed positioning commands, resulting in the fastest possible restore of files and *Directories* when needed. See "Notes on Tape Locate Threshold" on page 72 for additional details.

TapeAlert™ Support
BackupEDGE can check compatible storage *Devices* for *TapeAlert* messages before, during, and after *Scheduled* backups, as well as from within *EDGEMENU* or from the command line. Leave this field set to `A` to automatically check the tape drive for *TapeAlert* compatibility and messages.

Partition
Many DDS and other tape drives can be formatted into logical partitions, which are treated as separate tape drives. *BackupEDGE* supports this, and can switch between partitions if this field is set to `1` or `2`. Normally, leave it at `C` which means to use the `Current` partition.

We suggest that you do not partition tapes.

Manual Check
Pressing this button starts the process which writes, reads, and measures the positioning speed and capabilities of your tape drive, eventually generating a **Locate Threshold**. To skip this field, navigate through it with `[Up-Arrow]`/`[Down-Arrow]` instead of `[Enter]`. Please see "Notes on Changing Backup Device Hardware" on page 68 for further information and instructions on performing a **Manual Check** and setting the *Locate Threshold*.

Volume Size
0 means "Unlimited", i.e. *BackupEDGE* will not impose any volume size restrictions and will write to the entire tape. For *Devices* that do not support hardware compression, this may be set to the maximum capacity of the *Device* in Kilobytes. Pressing `[F1]` on this field will pop up a scrollable list of usable *Volume Sizes* for various *Devices*.

Edge Block Size
This is the size of the read/write buffer used by *BackupEDGE*. `64` is a good default, or any other number may be used. `20` provides compatibility with tar. Normally, larger numbers provide increased performance. Modern devices such as DLT, AIT and LTO require a **Tape Block Size** of `0` and an **Edge Block Size** of at least `256` for reasonable performance.

Compression
Options are [**H**]ardware, [**S**]oftware, or [**N**]one. If there is media in the drive, and the drive is set in compression ON mode when detection is done, this field will default to `H`. Otherwise it will be set to `S` or `N`. If it displays as `S` and you are sure you *Device* can perform hardware compression, change it to `H` here. Press the first character of the desired compression mode while the cursor is on this field in order to change it.

For *Devices* that *BackupEDGE* can control, this setting will be used to set up the *Device* before a backup. If *BackupEDGE* cannot control the *Device*, this setting will be used to tell *BackupEDGE* what to expect from the *Device*.

Double Buffering
Should always be set to [**Y**]es. This creates multiple, independent read and write processes to speed up backups. May be disabled (set to `N`) if memory problems result.

When all values are set appropriately, press `[Next]`.

6.8 - Notes on Tape Locate Threshold

In a nutshell, *Locate Threshold* tells *BackupEDGE* when to use read commands to get from one file to another on the tape while restoring, and when to use high speed positioning commands. *BackupEDGE* assigns a convenient default to the locate threshold. If you do not perform a lot of individual file or directory restores, it is more than adequate and no further reading here is required. If partial restores are frequent occurrences for you, this section will help you understand and optimize tape drive high speed positioning. This affects only tape.

You might think "If high speed positioning is available, why not just use it all the time?". The reason is that it will actually cause some restore operations to slow down, because of **overhead**.

It takes a noticeable amount of time for a tape drive to switch into and out of positioning mode. If two files that need to be restored are *relatively* close together, it is may be quicker to restore the first one, read and discard a little data, then restore the second one, than to incur the overhead of using a positioning command.

The definition of the *Locate Threshold* is “The nonnegative offset, in megabytes, where it becomes faster to use a position command instead of a read command.”.

For instance, if the *Locate Threshold* for a *Device* is *29*, then any time the end point of one file to be restored is within `29` megabytes of the starting point of the next file to be restored, it is faster *not* to use a positioning command.

If the *Locate Threshold* is set to `-1` (the default), attempts to use *FFR* with this *Resource* will operate at normal speed; *FFR* will be no faster than any other restore. This is treated as if the *Locate Threshold* were infinite.

NOTE: A *Locate Threshold* of `-1` is special; it means “Never use positioning commands.” This is in contrast with a *Locate Threshold* of `0`, which means “Always use a positioning command for any positive offset.” Notice that `-1` is a special case, while `0` is not.

Remember that this is a measurement of the capabilities of a *Device*. You may enter a *Locate Threshold* manually for a particular *Device* if you have already checked it with a previous version of *Backup**EDGE***. If you have never tested this *Device* for positioning capability, it is ***strongly*** recommended that you do so, even if you believe the drive can position reliably. This is because positioning depends on many things besides the tape drive, such as the operating system *Device* drivers. Performing a test of the *Device*'s fast positioning ability ensures that it is configured for reliable operation. The other benefit is that getting the right *Locate Threshold* can significantly improve the performance of *FFR*.

To determine the *Locate Threshold*, you will need a blank tape. Press the `[Manual Check]` button, located to the right of the *Locate Threshold* text box. You will be prompted to enter a test size (in Kilobytes), and the *Edge Block Size* size (in 512-byte blocks). The defaults are usually fine. If you begin the test, ***ALL DATA ON THE TAPE WILL BE ERASED***. Upon completion of the test, the *Locate Threshold* will be set to the appropriate value. If the test fails for some reason, you will be notified and the *Locate Threshold* will be set to `-1`.

If you do not wish to run the *Locate Threshold* test during initial installation, you may launch it at any time from within the `Admin -> Define Resources` section of *EDGEMENU*.

*Backup**EDGE*** uses a heuristic during *Device* detection. If the *Device* is a tape drive with hardware compression, the autodetector will set the *Locate Threshold* to 30 by default. While probably not the best *Locate Threshold* for your *Device*, it will function as a good starting point. Running the `[Manual Check]` can improve the performance of your restores.

6.9 - RecoverEDGE Reminder

After adding a new *Resource* to *Backup**EDGE*** and creating at least one successful backup, always remember to re-create your *Recover**EDGE*** media and / or images so that they will understand how to use the *Resource*. Test them to make sure you can read from the *Resource* if necessary.

7 - Configuring an Autoloader Resource

7.1 - General Concepts

*Backup**EDGE*** supports all SCSI and SAS tape libraries (also known as autochangers, autoloaders or just loaders). Media may be selected for insertion into a tape drive by storage slot name, or via barcode id.

7.2 - Autoloader Elements

A tape *Autochanger* is composed of up to four types of *Elements*.

- **dt** *Elements* are **D**ata **T**ransfer units. That's the tape drive or drives. There may be more than one tape drive in an autoloader.
- **st** *Elements* are called **St**orage units. Those are the slots or other places that media or cleaning cartridges are stored. There is no slot limit.
- **ie** *Elements* are **I**mport/**E**xport units. These are used to get a tape into and out of a larger *Library* without actually opening the case.
- Finally, **mt** *Elements* are **M**edium **T**ransport units. These are technically the robotic arms that move things around.

Only the largest *Libraries* have **ie** *Elements* that can be addressed. Desktop *Autochangers* typically only move cartridges between **dt** and **st** *Elements*, although **mt** *Elements* may be referenced.

7.3 - Resource Information

Sample Autochanger Resource

```
+-------------------------------------------------------------------------------+
|- General Resource Information -------------------------------------------------|
|Resource Type       AutoChanger                                                |
|Resource Name       [changer0          ] Change as appropriate                 |
|Description         [DELL PV-124T 0070           ]                             |
|Changer Assoc       [Modify Associated Devices]                                |
|Interface           [SCSI       ]                                              |
|Control Node        [/dev/sg2          ]                                       |
|- Media Jukebox Information ----------------------------------------------------|
|[ ]    Load after changer op.                                                  |
|[X]    Unload before changer op.                                               |
|[A]    Barcode Support                                                         |
|[Y]    Wait for Device Ready                                                   |
|[0   ] Load Delay                                                              |
|[Next]                              [Prev]                          [Cancel]|
+-------------------------------------------------------------------------------+
```

Here we have new fields...

Load after changer op.
Some larger *Autochangers* require that the tape *Device* issue a specific media load command after the changer has moved media to a tape drive, or **dt** *Element*. If your *Autochanger* requires this, then use the `[Space]` key to change this field to an [**X**].

Unload before changer op.
Some large *Autochangers* require that the tape *Device* issue a specific unload command before media can be removed from a **dt** *Element*. If your *Autochanger* requires this, then use the `[Space]` key to change this field to an [**X**]. (Most devices larger than desktop autoloaders require this flag to be set.)

Barcode Support
*Backup**EDGE*** probes for and reads *Private Volume Tags* (barcodes) from media [**A**]utomatically if your changer supports them. This field can also be set to [**Y**]es or [**N**]o to specifically enable or disable support.

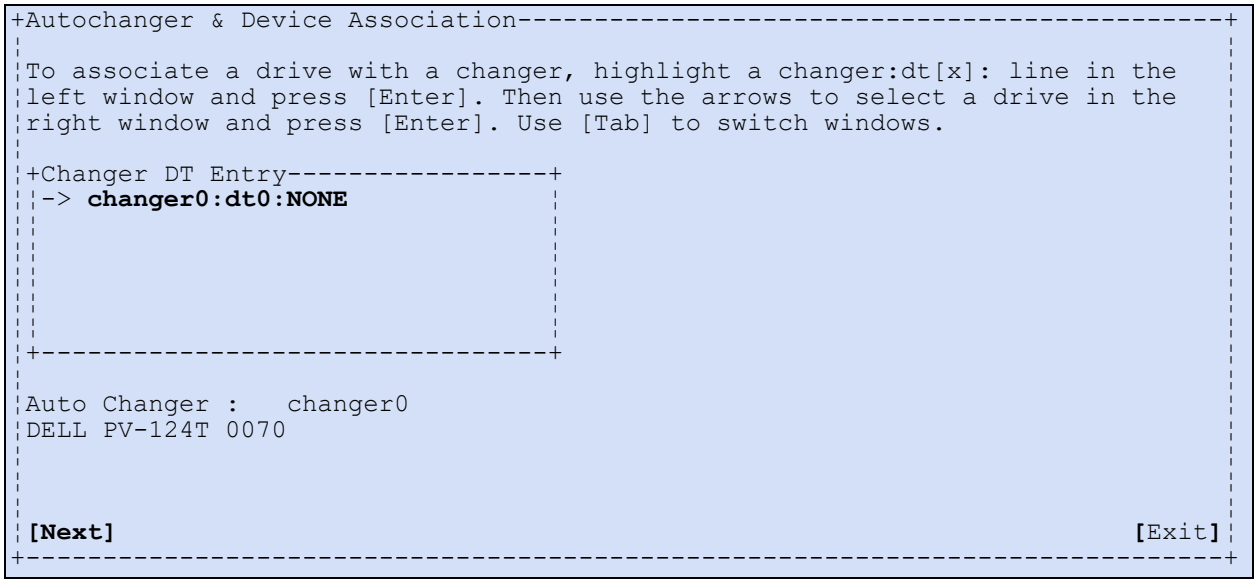
Wait for Device Ready
*Backup**EDGE*** attempts to poll the device after inserting media to determine when the load is complete.

Load Delay
*Backup**EDGE*** waits the specified number of seconds after inserting media, then assumes the load is complete.

Autochanger and Device Association

If you have an *Autochanger*, you must establish a relationship between it and any tape drives you may have. This allows *Backup**EDGE*** to know which tape drive(s) are attached to the *Autochanger*, and which are stand-alone *Devices*. When *Backup**EDGE*** needs to load a tape, this information allows it to do so.

*Backup**EDGE*** creates an **Association** to record this relationship.



During installation the above screen will appear. The *Autochanger* tells *Backup**EDGE*** how many tape drives (**dt** *Elements*) are contained within it. There will be one entry in the box for each tape drive (called `dt0`, `dt1` etc.). In this example there is only one tape drive installed in `changer0`.

To establish an *Autochanger / Tape Device* relationship, press [Tab] to place the cursor in the Changer DT Entry box, highlight the proper dt *Element*, and press [Enter].

```
+Autochanger & Device Association-----------------------------------------+
|                                                                          |
|To associate a drive with a changer, highlight a changer:dt[x]: line in the
|left window and press [Enter]. Then use the arrows to select a drive in the
|right window and press [Enter]. Use [Tab] to switch windows.              |
|                                                                          |
|+Changer DT Entry-----------------+  +Data Trans. Element-----+           |
||-> changer0:dt0:NONE              |  |   rev0                |           |
||                                  |  |-> tape0               |           |
||                                  |  |   optical0            |           |
||                                  |  |                       |           |
||                                  |  |                       |           |
|+----------------------------------+  +-----------------------+           |
|                                                                          |
|Auto Changer :   changer0             DT Element :   tape0                |
|DELL PV-124T 0070                     QUANTUM ULTRIUM 4 2210              |
|                                                                          |
|                                                                          |
|[Next]                                                          [Exit]    |
+--------------------------------------------------------------------------+
```

In the above example, pressing [Enter] when tape0 is highlighted would result in a Changer DT Entry that looked like this:

```
-> changer0:dt0:tape0
```

When the proper relationships are established, [Tab] down to and press the [Next] button.

When you later view the tape1 *Resource* from within *EDGEMENU*, the *Autochanger / Tape Device* relationship will be shown in the Changer Assoc field.

```
+-------------------------------------------------------------------------+
|- General Resource Information ------------------------------------------|
|Resource Type       Tape Drive                                           |
|Resource Name       [tape0             ] Change as appropriate           |
|Description         [QUANTUM ULTRIUM 4 2210      ]                       |
|Changer Assoc       [changer0:dt0]                                       |
|Interface           [SCSI       ]                                        |
|                                                                         |
|- Tape Drive Information ------------------------------------------------|
|Data Node           [/dev/st0                    ] [A] TapeAlert(tm) Support
|No Rewind Node      [/dev/nst0                   ] [X] Multiple Archives?
|Tape Block Size     [-1                          ] [C] Partition         |
|Locate Threshold    [30                          ] [ Manual Check ]      |
|                                                                         |
|                                                                         |
|- Default Backup Properties ---------------------------------------------|
|Volume Size         [0            ] [H] Compression                      |
|Edge Block Size     [256          ] [Y] Double Buffering                 |
|[Next]                              [Prev]                    [Cancel]   |
+-------------------------------------------------------------------------+
```

7.4 - Scheduled Media Insertion

See “Media List” on page 225 for more information about using automatic media insertion in the *Scheduler*.

7.5 - Manual Media Manipulation

See “Autochanger Media Manipulation” on page 250 for more information about using EDGEMENU to move cartridges between slots and drives.

See “The EDGE.CHANGER Program” on page 324 for more information about moving cartridges between slots and drives via the command line or within scripts.

8 - Configuring an Optical Drive Resource

8.1 - General Concepts

BackupEDGE supports all optical drives, and the following writable media types:

Write Once	Re-Writable
DVD-R, DVD+R, DVD+R DL, CD-R.	BD-RE, DVD-RAM, DVD+RW, DVD-RW, CD-RW

Write strategy and capacity are selected automatically. For multiple archive backups, multiple media types may be inserted in any order, i.e a DVD+R might be followed by a CD-RW.

NOTE: *BackupEDGE 3.0* and later supports multiple archives per medium on optical drives when using some re-writable media. This is a change in behaviour from our older products. The default may be over-ridden for legacy behaviour. See Multiple Archives Per Medium below.

8.2 - Compatibility Matrix

Operating System(s)	IDE / SATA	USB	Notes
Linux	YES	YES	
OpenServer 6	YES	YES	All Maintenance Packs + patchck updates required.
UnixWare 7	YES	YES	All Maintenance Packs + patchck updates required.
OpenServer 5	YES	5.0.7 Only	All Maintenance Packs + patchck updates required. 5.0.5 not supported.

8.3 - Multiple Archives Per Medium

BackupEDGE 3.x supports performing multiple backups onto BD-RE and DVD-RAM. By **default**, writing to media that has one or more *unexpired backups* will now result in *BackupEDGE* adding the new backup as shown below:

Medium	Multiple Archives Flag Set to **YES**	Multiple Archives Flag Set to **NO**
BD-RE, DVD-RAM	Backup will intersperse new archives with old archives, lazily reclaiming space as available.	Backup will always blank and start at beginning of medium. Archive will **FAIL** if a current unexpired backup exists on the medium.
DVD-RW DVD+RW	**Not Supported**. Currently behaves as if flag is set to **NO**.	Backup will always blank and start at beginning of medium. Archive will **FAIL** if a current unexpired backup exists on the medium.
DVD-R, DVD+R, DVD+R DL	**Not Supported**. Currently behaves as if flag is set to **NO**.	Backup will **FAIL** if another archive (or any other data) already exists on the medium.

8.4 - Pre-requisites

- All programs / daemons that automatically recognize and attempt to mount or otherwise use a CD DVD or BD-RE should be disabled before attempting to use this class of device for storage.

8.5 - Optical Media Notes

- Capacity detection is automatic. Quota or capacity is set to the size of each medium automatically.
- Multiple archives per medium utilize archive expiration times and lazy reclamation to maximize the number of archives stored for maximum safety. This may be disabled if only on archive per medium is desired (legacy behaviour).
- Compression and optional encryption are supported.
- Direct booting for *Recover**EDGE*** disaster recovery is supported.
- Full file checksumming, for maximum data integrity, is supported.
- *Instant File Restore* is available from any archive. It is not necessary to read through an entire archive to restore individual files and directories.
- MySQL™ hot backups are supported as a separate *Scheduled Job* when multiple archives per medium is disabled. When enabled, the MySQL backup will be appended after the full system backup.

8.6 - Initializing

All re-writable media is blanked automatically before initial use and as required. Running `EDGEMENU -> Admin -> Initialize Medium` while optical media is selected as the *Primary Resource* will blank BD-RE, DVD-RAM, DVD+RW and DVD-RW media and FAIL on all other media types.

8.7 - Resource Information

Sample Optical Drive Resource

```
+ BackupEDGE Resource Information ------------------------------------------+
|- General Resource Information ------------------------------------------- |
|Resource Type       Optical Drive                                          |
|Resource Name       [optical0          ] Change as appropriate             |
|Description         [HL-DT-ST BD-RE GGW-H20L YL05]                         |
|Changer Assoc                                                              |
|Interface           [IDE / ATAPI]                                          |
|                                                                           |
|- CD / DVD / Optical Information ----------------------------------------- |
|Data Node           [/dev/hdc                   ] [ ] Buffer Whole Disc?   |
|Mount Device Node   [/dev/hdc                   ] [X] BurnProof(tm)?       |
|Record Buffer (K)   [2048                       ] [X] Multiple Archives?   |
|Needs Eject?        [ ]                                                    |
|Writable Media:     CD-R[W], DVD-RAM, DVD+/-R[W], BD-RE                    |
|                                                                           |
|- Default Backup Properties ---------------------------------------------- |
|Volume Size         [0            ] [S] Compression Level  [5]             |
|Edge Block Size     [64           ] [Y] Double Buffering                   |
|[Next]                              [Prev]                        [Cancel] |
+---------------------------------------------------------------------------+
```

Data Node
This is the *Device Node* used when reading data from the CD-ROM.

Mount Device Node
This is the *Device Node* used when mounting a CD-ROM as a filesystem.

Record Buffer
The amount of space *Backup**EDGE*** will buffer before beginning a CD-Record or CD-ReWrite session. Increase this amount if you have problems with data under-runs running *Optical* backups.

Needs Eject?
In some instances, the capacity of a *Device* is checked by the operating system only when media is inserted. After writing to blank *optical media*, no data can be read because the driver is convinced it is still blank. Or, let's say you had a *CD-RW* with 100MB previously written to it. You do a 400MB backup, and during the verify you get a read error at the 100MB point. Your OS has cached the size.

In this instance, set the **Needs Eject?** flag to [**Y**]es. After each write, *BackupEDGE* will eject and re-insert the media to get the OS to detect the new media size.

NOTE: This typically happens when an automount daemon is monitoring the *Device* you are using form backups. We highly recommend shutting down automount daemons on *optical devices* which are used to create backups.

Writable Media
This is not editable, but instead indicates what *BackupEDGE* believes are the recordable media options for this *Device*. Read-only devices or Virtual devices will say `Device Cannot Write` here.

Buffer Whole Disc?
If this flag is set to [**Y**]es, *BackupEDGE* will buffer the entire *CD-R/RW* image before beginning to write it. This requires at least as much free disk space as the size of the optical drive. **Buffer Whole Disc** overrides any **Record Buffer** settings and is generally not necessary on any modern optical drive.

BurnProof™?
All modern optical drives incorporate technologies that prevent them from ruining media in the event of a data under-run. This flag should always be set to [**Y**]es.

Multiple Archives?
If checked, allows multiple archives to be stored per medium. If unchecked, only a single archive per medium will be written (this was the behavior in all previous *BackupEDGE* releases.

Volume Size
0 means "ask the media". *BackupEDGE* can normally autodetect the appropriate volume size for the type of media loaded into an optical drive at the time when a backup is made. For this to occur, the Volume Size must be set to `0` in the *Resource*. Autodetection will fill in the `Volume Size` field with `0`. It should almost **never** be changed.

Compression
The only compression available is [**S**]oftware. This ***will*** cause the data stream to stop and start. Make sure you have a buffer under-run proof *Device*, or have set a large **Record Buffer** size or the **Buffer Whole Disc** flag if you use software compression. Otherwise, use [**N**]one.

When compression is set to [**S**]oftware, a "Level" field appears to the right. The default compression level is 5. Available options are 1 through 9. 1 provides the highest performance and the least compression, 9 the most compression and the slowest performance. 1 is usually sufficient. See "Software Compression and Performance" on page 255 for a discussion of compression values.

8.8 - RecoverEDGE Reminder

After adding a new *Resource* to *BackupEDGE* and creating at least one successful backup, always remember to re-create your *RecoverEDGE* media and / or images so that they will understand how to use the *Resource*. Test them to make sure you can read from the *Resource* if necessary.

9 - Configuring SharpDrive Backups

9.1 - General Concepts

The proliferation, performance, and pricing of hot pluggable USB and SATA hard drives, cartridge drives and flash drives has quickly made them a force in the backup and disaster recovery storage space as a direct replacement to tape storage.

*Backup**EDGE 3.0*** (beginning with 03.00.03) recognizes this and defines a new storage *Resource* type to handle them all called "**SharpDrive™ Media**".

*Backup**EDGE 3.1*** (beginning with 03.01.02) and later supports both FDISK partitioning (under 2TB) and GPT Partitioning (any Size Media) under Linux systems that support GPT.

9.2 - Compatibility Matrix

Operating System SharpDrive Medium	Linux	UW7	OSR 6	OSR 5.0.7
SATA Quantum GoVault	YES	NO	NO	NO
SATA RDX/RD1000	YES	NO	NO	NO
USB Quantum GoVault	YES	YES	YES	NO
USB RDX/RD1000	YES	YES	YES	NO
USB Standard Hard Drives	YES	YES	YES	NO
USB Standard Flash Drives. Pen Drives, etc.	YES	YES	YES	NO

OpenServer 5 users should consult "Configuring Legacy Disk-to-Disk Backups" on page 158, as *SharpDrive* media is not supported. Users of other operating systems may also choose our legacy disk preparation system, but *SharpDrive* tends to be faster and easier to set up and use.

The SATA driver in UnixWare 7 and OpenServer 6 systems has limited functionality with SharpDrive media. Users should go to "Configuring Legacy Disk-to-Disk Backups" on page 158 when using SATA devices.

9.3 - Multiple Archives Per Medium

*Backup**EDGE*** supports performing multiple backups onto *SharpDrive Media*. By **default**, the quota for a *SharpDrive* is the entire free space of its filesystem. This is the general behaviour:

Medium	Archive Behaviour
SharpDrive	The process will attempt to create a new archive. If starting a new segment would cause the quota to be reached, the oldest expired archive will be erased in its entirety (all segments). If starting a new segment would exceed the quota and no more expired archives exist, the *Scheduler* will prompt for a new volume.

9.4 - Pre-requisites

- All programs / daemons that automatically recognize and mount a hard / flash drive should be disabled before attempting to use this class of device for storage. *Backup**EDGE*** will handle all mounting as needed.
- All media to be used, i.e. removable disks, cartridges, and flash drives, must be initialized one time. This is performed in an automated, wizard-style fashion either by the *Backup**EDGE***

installer or from within *EDGEMENU*. This is much easier than the media preparation required in our legacy D2D feature.

9.5 - SharpDrive Notes

- Capacity detection is automatic. Quota is set to the size of each medium automatically, and media may be mixed at random, i.e. a hard drive may be followed by a flash drive and *Backup**EDGE*** will understand each.
- Multiple archives per medium utilize archive expiration times and lazy reclamation to maximize the number of archives stored for maximum safety.
- Compression and optional encryption are supported.
- Direct booting for *Recover**EDGE*** disaster recovery is supported.[1]
- Full file checksumming, for maximum data integrity, is supported.
- *Instant File Restore* is available from any archive. It is not necessary to read through an entire archive to restore individual files and directories.
- MySQL™ hot backups are supported.
- Cases where two or more devices are left plugged in are handled automatically. The *SharpDrive* with the most available space is used. Available space is defined as a combination of free space plus expired archive space.
- If the “GDISK” utility is installed, EDGEMENU will assume that all things necessary to support GPT partitions are installed.

Linux has the ability to boot directly from *SharpDrive* media if FDISK partitioning is used. UnixWare 7 and OpenServer 6 servers do not support booting directly from these devices, but are fully disaster recovery compliant when booting from other media types such as CDROM. Linux media partitioned as GPT is not bootable. Other boot media, such as optical or PXE, must be used.

During disaster recovery, *Recover**EDGE*** automatically scans all connected *SharpDrive*-formatted media and shows all archives available for restore.

9.6 - First time Use

As far as the operating system is concerned, *SharpDrives* are really just plain hard drives. So no autodection is available. To use *SharpDrives*...

- A one-time setup is required. This creates the *SharpDrive Resource* (`sdrive0` by default) and begins the media initialization process.
- Each piece of media to be used must be initialized as a *SharpDrive* so that *Backupe**EDGE*** can recognize it. During initialization...
  - All previous information on the medium is erased.
  - The medium is formatted with a filesystem and a *Backup**EDGE*** signature is placed in the superblock.
  - The medium may be given a unique name, such as “Tuesday” or “Week 7" or whatever fits your storage strategy and should be externally labeled as such.

Media may be also non-destructively re-initialized at a later date to check consistency and update the index control file (`CTL`).

1. Linux 2.6.x 32bit and 64bit kernel distributions only.

Under *EDGEMENU*, choose `[Setup]`, then `[Configure BackupEDGE]`. Select `Configure SharpDrive Media`.

```
+BackupEDGE Configuration-------------------------------------------------+
|             Please select the BackupEDGE subsystem to configure.        |
|                                                                         |
|Machine:            ml310.microlite.com                                  |
|                                                                         |
|+------------------------------------------------------------------------+|
||   Autodetect New Devices                                               ||
||-> Configure SharpDrive Media                                           ||
||   Schedule Nightly Backups                                             ||
||   Configure BackupEDGE Web Interface                                   ||
||   Configure BackupEDGE Encryption                                      ||
||   Autodetect Virtual (Sparse) Files                                    ||
||   Configure MariaDB/MySQL(tm) Backups                                  ||
||   Configure Java Paths                                                 ||
||                                                                        ||
||                                                                        ||
||                                                                        ||
||                                                                        ||
|+------------------------------------------------------------------------+|
|                                                                         |
|[Configure]                                                      [Done]  |
+-------------------------------------------------------------------------+
```

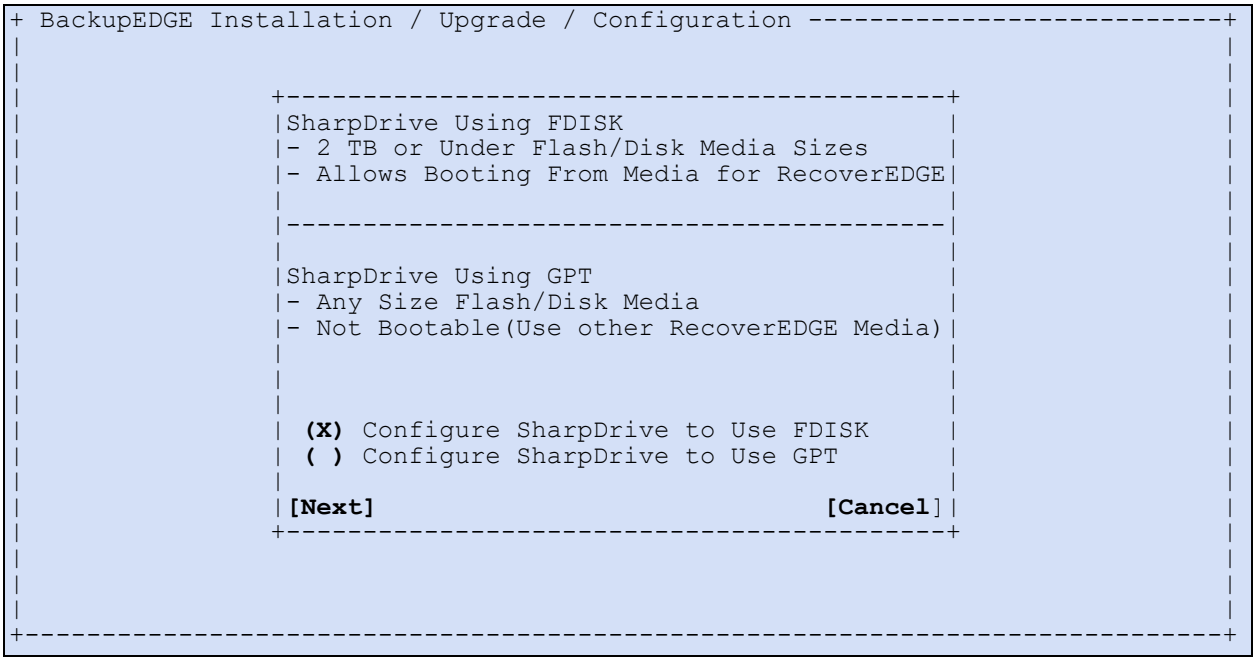
The first time this menu item is run, the *SharpDrive Resource* will be created. If the *SharpDrive Resource* already exists, the menu will jump to "SharpDrive Medium Selector" on page 84 so that additional media can be initialized.

SharpDrive Resource Setup

```
+BackupEDGE Configuration-------------------------------------------------+
|             Please select the BackupEDGE subsystem to configure.        |
|                +----------------------------------------+               |
|Machine:        |         SharpDrive Resource Setup      |               |
|                |                                        |               |
|+---------------|This will allow you to configure BackupEDGE|-------------+|
||   Autodetect N|for use with removable disk/flash media,   |             ||
||-> Configure Sh|and format new media to be compatible with |             ||
||   Schedule Nig|BackupEDGE.                               |             ||
||   Configure Ba|                                        |               ||
||   Configure Ba|                                        |               ||
||   Autodetect V|                                        |               ||
||   Configure My|                                        |               ||
||   Configure Ja|                                        |               ||
||   Configure Am|                                        |               ||
||               | (X) Perform SharpDrive Setup           |               ||
||               | ( ) Skip Setup                         |               ||
||               |                                        |               ||
|+---------------|[Next]                          [Cancel]|-------------+|
|                +----------------------------------------+               |
|[Configure]                                                      [Done]  |
+-------------------------------------------------------------------------+
```

Select `Perform SharpDrive Setup` when prompted, and go through the acknowledgement screens until you reach the medium selector.

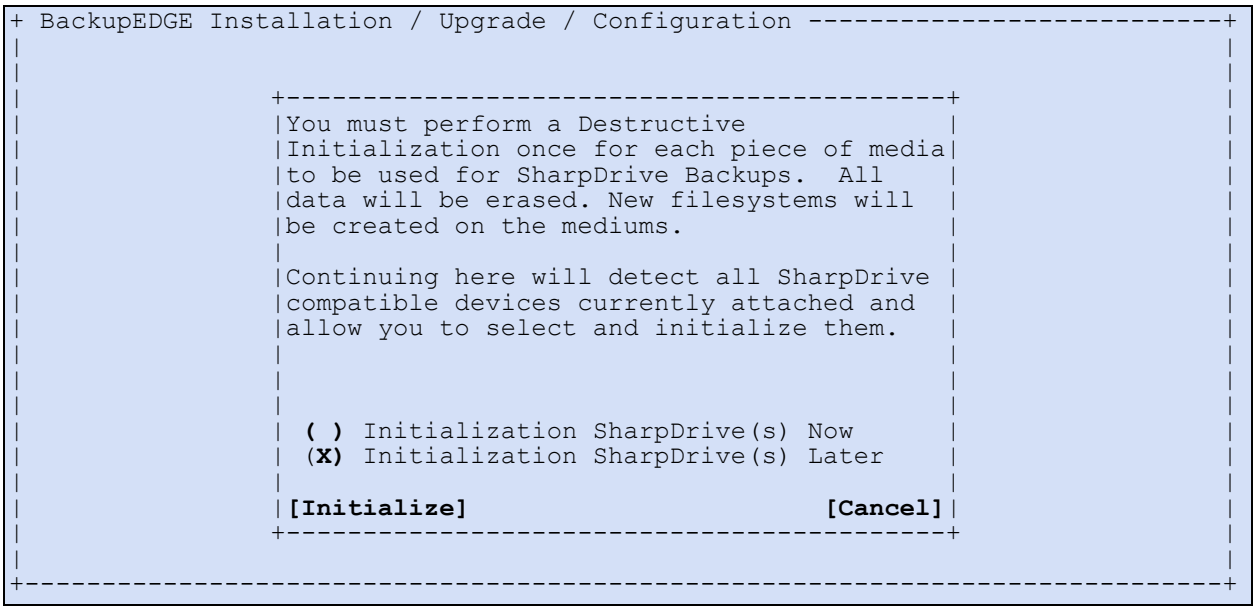
Linux Server GPT Option



Select `Configure SharpDrive To Use FDISK` if all of your media are under 2TB in size and you wish to use FDISK. This preserves the ability to boot the media using *Recover**EDGE*** if desired.

Select `Configure SharpDrive To Use GPT` if any of your media is greater than 2TB in size. All media of any size will be initialized with GPT partitioning. Media cannot be booted using *Recover**EDGE***. You will have to create separate CD, ISO image or PXE boot images.

SharpDrive Medium Acknowledgement



Select `Initialize SharpDrives Now` and `[Continue]`. if you wish to initialize. Nothing will be erased or written until you have selected the proper media. Select `Initialize Later` if you don't currently have media available.

SharpDrive Medium Selector

```
+Select disk(s) to ERASE and use with sdrive0 ('space' selects)----------------+
|+-------------------------------------------------------------------------------+|
||->  [1] (7 GB) 'PNY USB2.0FD  8.02'                                            ||
||    [2] (7 GB) 'Kingston DataTraveler16  PMAP'                                 ||
||    [3] (465 GB) 'WD 5000AAJExterna  1.65'                                     ||
||                                                                               ||
||                                                                               ||
||                                                                               ||
||                                                                               ||
||                                                                               ||
||                                                                               ||
||                                                                               ||
||                                                                               ||
||                                                                               ||
|+-------------------------------------------------------------------------------+|
|Desc:                                                                          |
|Vend: PNY                                Dnode: /dev/sdb                       |
|Model: USB2.0FD                          S/N:                                  |
|Cap: 7GB                                 Resc: sdrive0                         |
|                                                                               |
|[Next]                                                              [Cancel]|
+-------------------------------------------------------------------------------
```

Note that it is possible to initialize more than one *SharpDrive* concurrently. If you have more than one pieces of media connected, use the space bar to select each desired medium before selecting `[Next]`. An * will appear next to all *SharpDrives* selected for initialization.

If the `Desc:` field is not blank, this *SharpDrive* has been initialized at least once.

Confirm Selections

```
+Select disk(s) to ERASE and use with sdrive0 ('space' selects)----------------+
|+-------------------------------------------------------------------------------+|
||->  [1] (7 GB) 'PNY USB2.0FD  8.02'                                            ||
||    [2] (7 GB) 'Kingston DataTraveler16  PMAP'                                 ||
||    [3] (465 GB) 'WD 5000AAJExterna  1.65'                                     ||
||             +Selection Box-----------------------------------+                ||
||             |                                                |                ||
||             |Are you sure you want to ERASE ALL DATA on this |                ||
||             |                  1 device?                     |                ||
||             |                                                |                ||
||             |                                                |                ||
||             |                                                |                ||
||             |                                                |                ||
||             |                                                |                ||
||             |                                                |                ||
|+-------------|   [No]                              [Yes]      |-------------+|
|Desc:         |                                                |               |
|Vend: PNY     +------------------------------------------------+               |
|Model: USB2.0FD                          S/N:                                  |
|Cap: 7GB                                 Resc: sdrive0                         |
|                                                                               |
|[Next]                                                              [Cancel]|
+-------------------------------------------------------------------------------+
```

You must **manually select** `[Yes]` to continue.

SharpDrive Medium Description

```
+Question-------------------------------------------------------------------+
|Please enter a short descriptive phrase for /dev/sdc (PNY)                |
|                                                                          |
|[BackupEDGE Monday Nightly Backups                                       ]|
|                                                                          |
|                                                                          |
|                                                                          |
|                                                                          |
|[Continue]                                                      [Cancel]|
+-------------------------------------------------------------------------+
```

The above prompt will appear once for each *SharpDrive* selected for initialization. Any text in the description will appear in all reports using this medium. When you select `[Continue]` the medium / media will be initialized:

- The device will be blanked and formatted.
- A filesystem will be created.
- A signature unique to *Backup**EDGE*** will be placed in the boot block, along with the *Descriptive Phrase* used above. These are used to confirm to *Recover**EDGE*** that this device may contain archives. *Recover**EDGE*** will never attempt to erase it.

SharpDrive Initialization

```
+Question-------------------------------------------------------------------+
|Please enter a+NOTICE-----------------------------------------+           |
|              |                                               |           |
|[BackupED+Plea|           Initialization Successful          |----+     ]|
|          |   |                                               |    |      |
|          |   |                                               |    |      |
|          |   |                                               |    |      |
|          +---|                                               |----+      |
|[Continue]    |                     [ Ok ]                    |     [Cancel]|
+--------------+-----------------------------------------------+-------------+
```

Repeat this procedure if additional media needs to be formatted.

9.7 - Theory of Operation

For the most part, *SharpDrive Resources* are very similar to more conventional ones such as tape or optical media. However, there are a few points you should be aware of before using them.

Segments

In a tape backup, *Backup**EDGE*** streams the data directly on to the media. In *SharpDrive* backups, *Backup**EDGE*** streams the data into *archive files* on the target medium. This potentially subjects the files to filesystem size limitations and ulimit or other arbitrary operating system limitations.

To work around these limits, *Backup**EDGE*** automatically segments archives; that is, it divides one logically long archive into short archive files (called *segments*) that can be managed by the operating system managing the storage device. By default, these segments are 1 gigabyte -1 block in length.

*Backup**EDGE*** can write multiple archives to *SharpDrive Resources*, and each archive may contain multiple segments. *Backup**EDGE*** handles segments automatically, and provides tools for managing the segments. To maintain consistent archives, the individual segments should never be manipulated by operating system commands. This is why segments do not have names that make sense to humans.

Quotas

Each *SharpDrive Resource* is assigned a default storage quota which is the size of the created filesystem.

Retention Times

By default, all archives created to a *SharpDrive Resource* using the *Scheduler* have a retention time (or expiration time) of one week. They will not be erased automatically until the retention time is up, but will not necessarily be erased just because its retention time is up. An archive past its retention time is called an *Expired Archive*.

Space Reclamation

Archives are retained on *SharpDrive Media* at least until their expiration time has passed. After that, they are deleted in one of two ways...

Lazy Reclamation Enabled (Default)

If *Lazy Reclamation* is enabled, archives will remain on media as long as possible, just in case they may be needed even after their retention time is up. This allows maximum space utilization on the media. For an archive to be deleted...

- The retention time must be up, i.e. it must be an *Expired Archive*.
- Adding a segment to a new archive would cause the defined quota (usually the device capacity automatically calculated by *Backup**EDGE***) to be exceeded.

If both conditions are true, the oldest *Expired Archive* will be deleted in its entirety. This process ensures that a maximum number of older archives are available on the *SharpDrive Resource*.

If the quota is reached and none of the archives has expired, the backup will prompt for additional media.

By default, each backup in a *Scheduled Job* has a *Retention Time* of 1 week. This is may be changed on a per-schedule basis in the default simple *Scheduler*, and on a per-backup basis in the advanced *Scheduler*.

Lazy Reclamation Disabled

Disabling *Lazy Reclamation* (un-checking the `Lazy Reclamation` field in the *Resource Definition*) configures *Backup**EDGE*** to check for and immediately erase all expired archives any time a new backup is started to the *SharpDrive Media*. Only unexpired archives will be retained.

9.8 - Modifying the SharpDrive Resource

```
+ BackupEDGE Resource Information ------------------------------------------+
|- General Resource Information ------------------------------------------|
|Resource Type       SharpDrive Media                                      |
|Resource Name       [sdrive0          ] Change as appropriate             |
|Description         [SharpDrive Removable Media  ]                        |
|Changer Assoc       [Standalone Device]                                   |
|Interface           [Other      ]                                         |
|                                                                          |
|- SharpDrive Information ------------------------------------------------|
|Dir Suffix          [/backupedge                                      ]   |
|Segment Size (K)    [1048544                    ] [X] Lazy Reclamation    |
|                                                                          |
|                                                                          |
|                                                                          |
|                                                                          |
|- Default Backup Properties ---------------------------------------------|
|Quota               [0            ] [S] Compression Level  [5]            |
|Edge Block Size     [64           ] [Y] Double Buffering                  |
|[Next]                              [Prev]                    [Cancel]    |
+--------------------------------------------------------------------------+
```

The 'Directory Suffix' field is the directory on the SharpDrive Media where archives are stored. The default is /backupedge and should not generally be changed.

The 'Segment Size' field is the maximum size of a single archive segment and should not be changed.

'Lazy Reclmation' controls the behavior of space reclamation (deleting archives) on the *SharpDrive Resource*. See "Space Reclamation" on page 86 for additional information. The default behaviour is *Enabled*.

The 'Quota' field represents the storage quota, or total amount of space that *Backup**EDGE*** will use for all archives stored on this medium. The default of 0 means that BackupEDGE should auto-detect the free space, and should not generally be changed.

9.9 - Scheduling

Be sure to make sdrive0 the *Resource* in both the *Scheduler* and as the *Primary Resource* in *EDGEMENU*. In the Notify/Advanced screen, select Attempt Bootable if you want to be able to boot from the *SharpDrive* media (Linux only).

9.10 - Multiple Inserted SharpDrives

*Backup**EDGE*** will handle multiple, currently inserted *SharpDrives*.

Read /Restore Operations

During normal Read / Restore operations, *Backup**EDGE*** will automatically scan and have access to all archives on all *SharpDrive* media for the selected *Resource*, i.e. sdrive0. The user doesn't need to worry about where the archive is, as long as the removable medium on which it is stored is currently plugged in. All archives from all media will be listed for selection.

Write Operations

During backups, *Backup**EDGE*** will scan all available media initialized for a particular *Resource* and attempt to use the one with the most available space. This is a combination of free space and space available for reclamation, i.e. the total space used by archives that have expired. It's goal is to silently avoid splitting archives across different physical media.

We strongly recommend that the user has only one medium plugged in when performing a backup; this makes *Backup**EDGE***'s job entirely unambiguous and eliminates the possibility of a misunderstanding.

There are exceptions to this behaviour which are outlined in “What else do I need to know about SharpDrives?” on page 388. These only apply when multiple *SharpDrives* are inserted concurrently.

9.11 - General Notes

ALWAYS wait a sufficient time for the *SharpDrive* media to become ready after insertion.

9.12 - RecoverEDGE with SharpDrive

Medium Creation

Under *EDGEMENU*, choose `[Setup]`, then `[Make RecoverEDGE Media]`.

Select `SharpDrive Boot Files for SharpDrive Booting`. Choose `[Make Media]` to create the boot files necessary. In the Notify / Advanced screen of the Scheduler, select `Attempt Bootable`. This must be done prior to any backups.

NOTE SharpDrives must have communicated with the machine during this booted session to ensure that all modules required to read data from them are loaded into the RecoverEDGE image. Best practice for this is to read a label from the SharpDrive. (Initializing the media works as well but may take much longer)

(It is also possible to select `Boot Media on sdrive0` to immediately create a bootable *SharpDrive* with no backups, i.e. one which can be used to restore from other *Resource* types.)

Disaster Recovery

All *SharpDrives* (except the one you are booting from if you are booting from a *SharpDrive*) should be ejected / unplugged until you are completely booted and reach the *Recover**EDGE*** main menu.

Make sure your PC BIOS is set to boot from the USB bus (or correct SATA drive in the event you are using SATA cartridge media).

During the boot process, you’ll be asked to unplug / eject the *SharpDrive* media. You **MUST** complete this task within 30 seconds. **All** *SharpDrives* must be unplugged or ejected at this time. After the recovery system is prepared, you’ll be asked to re-plug / re-insert it (or them).

During recovery, *Backup**EDGE*** will ignore the resource name when looking at *SharpDrive* media. It will pretend that all media has been initialized for use with whatever *SharpDrive* resource it has been told to access.

9.13 - Moving SharpDrive Media Between Machines

SharpDrive media may be moved between machines, as long as some rules are followed:

- The machines must have a similar operating system. Linux machines cannot read UnixWare/OpenServer 6 *SharpDrives*, for example, even if your Linux has vxfs support (which it probably does).
- There must be an identically-named *Resource* on the machine as the one on which the medium was initialized. For example, if you initialize a medium for use with *Resource* on *Server A*, then *Server B* must have a *Resource* named *Resource* to read from it or write to it.

9.14 - Copying Archives

After the backup and verify portion of a scheduled job, *Backup**EDGE*** can optionally copy the archive(s) to some other resource. This resource may be a *SharpDrive*, if desired.

If the original resource is also a *SharpDrive*, you must use two different *Resources* with appropriately defined media. In other words, do not attempt to create a job that writes to `sdrive0` and also copies to `sdrive0`. Instead, one may write to `sdrive0` and copy to `sdrive1`.

To do this, media must be plugged in for both `sdrive0` and `sdrive1`. The `sdrive1` media will be ignored during the backup and verify, since the *Resource* name does not match.

9.15 - RecoverEDGE Reminders

After adding a new *Resource* to *Backup**EDGE*** and creating at least one successful backup, always remember to re-create your *Recover**EDGE*** media and / or images so that they will understand how to use the *Resource*. Test them to make sure you can read from the *Resource* if necessary.

When using *Recover**EDGE*** with *SharpDrive* backups that are not bootable, you must make sure all *SharpDrive* media is UNPLUGGED when booting. When you get to the main *Recover**EDGE*** menu, you may plug in any SharpDrives, then wait 10 or more seconds for them to start and go “ready” before continuing.

When using *Recover**EDGE*** with bootable *SharpDrive* media, you must boot from the media, eject or unplug it when requested, then re-attach it after getting to the main *Recover**EDGE*** menu. Wait 10 or more seconds for them to start and go “ready” before continuing.

10 - Configuring FTP/FTPS Backups

10.1 - General Concepts

FTP backups are backups that treat a remote FTP server as if it were a locally attached storage device. They are also known as URL backups, since the remote address of the FTP server is expressed to *Backup**EDGE*** as an industry-standard internet Uniform Resource *L*ocator format. The *Backup**EDGE** Resource* name used to define and reference FTP backups is called a *URL Resource*.

When transferring data, *Backup**EDGE*** FTP backups can use either the standard FTP protocol, or the encrypted FTP over SSL protocol, also known as FTPS.

10.2 - Multiple Archives Per Medium

*Backup**EDGE*** supports performing multiple backups onto *URL Resources*. The quota for a *URL Resource* is defined by the user during setup. This is the general behaviour:

Medium	Archive Behaviour
URL	The process will attempt to create a new archive. If starting a new segment would cause the quota to be reached, the oldest expired archive will be erased in its entirety (all segments). If starting a new segment would exceed the quota and no more expired archives exist, the backup will **FAIL**.

10.3 - FTP Notes

- Quota (maximum capacity) must be entered in the *URL Resource* definition. This may be changed as needed. The quota should be set to less than the available free space on the FTP server.
- Multiple archives per medium utilizes archive expiration times and lazy reclamation to maximize the number of archives stored for maximum safety.
- Compression and optional encryption are supported.
- Full file checksumming, for maximum data integrity, is supported.
- *Instant File Restore* is available from any archive. It is not necessary to read through an entire archive to restore individual files and directories.
- MySQL™ hot backups are supported.
- When specifying and FTP Server in the *URL Resource Definition*, we recommend using an IP address, if possible, instead of a hostname. This can shorten access times by eliminating DNS lookups, and can be especially useful during disaster recovery cases where DNS service may not be available.

10.4 - Theory of Operation

For the most part, these backup resources are very similar to more conventional ones such as tape or DVD. However, there are a few points you should be aware of before using them.

Segments

In a tape backup, *Backup**EDGE*** streams the data directly on to the media. In FTP backups, *Backup**EDGE*** streams the data into *archive files* on the FTP site. This potentially subjects the files to filesystem size limitations and ulimit or other arbitrary operating system limitations.

To work around these limits, *BackupEDGE* automatically segments archives; that is, it divides one logically long archive into short archive files (called *segments*) that can be managed by the operating system using the storage device. By default, these segments are 1 gigabyte -1 block in length[1].

BackupEDGE can write multiple archives to FTP servers, and each archive may contain multiple segments. *BackupEDGE* handles segments automatically, and provides tools for managing the segments. To maintain consistent archives, the individual segments should never be manipulated by operating system commands. This is why segments do not have names that make sense to humans.

Quotas

Each *URL Resource* is assigned a storage quota. *BackupEDGE* will not attempt to use more storage on the FTP server than that assigned by the quota.

Retention Times

By default, all archives created to a *URL Resource* using the *Scheduler* have a retention time (or expiration time) of one week. They will not be erased automatically until the retention time is up, but will not necessarily be erased just because its retention time is up. An archive past its retention time is called an *Expired Archive*.

Space Reclamation

Archives are retained on *FTP* servers at least until their expiration time has passed. After that, they are deleted in one of two ways...

Lazy Reclamation Enabled (Default)

If *Lazy Reclamation* is enabled, archives will remain on the server as long as possible, just in case they may be needed even after their retention time is up. This allows maximum space utilization on the server. For an archive to be deleted...

- The retention time must be up, i.e. it must be an *Expired Archive*.
- Adding a segment to a new archive would cause the defined quota to be exceeded.

If both conditions are true, the oldest *Expired Archive* will be deleted in its entirety. This process ensures that a maximum number of older archives are available on the *URL Resource*.

If the quota is reached and none of the archives has expired, the backup will prompt for additional media.

By default, each backup in a *Scheduled Job* has a *Retention Time* of 1 week. This is may be changed on a per-schedule basis in the default simple *Scheduler*, and on a per-backup basis in the advanced *Scheduler*.

Lazy Reclamation Disabled

Disabling *Lazy Reclamation* (un-checking the `Lazy Reclmatation` field in the *Resource Definition*) configures *BackupEDGE* to check for and immediately erase all expired archives any time a new backup is started to the *URL Resource*. Only unexpired archives will be retained. This allows only the minimum required amount of space to be used, while still retaining as many archives as are needed.

1. Selecting the re-startable option changes the segment size to 50MB.

Note that usually, if you are backing up multiple machines and/ or schedules to the same FTP site, you will create multiple *Resources*, one per machine/schedule combination. Each *Resource* would use a different directory on the FTP server and have a different quota. A typical schedule would look like this:

Sample FTP Backup Schedule

```
+ Edit Backup Schedule ------------------------------------------------------+
| Schedule Name:     simple_job                                              |
|          Time:     [23:00] (14:58:46)  Enabled: [X]                        |
| Sequence:                  web2v.microlite.com:esequence/onsite            |
| Backup Domain:             system                                          |
| Primary Resource:  [Change] web2v.microlite.com:url!url0                   |
|                                                                            |
| +---------------------------------------------+     September 2019         |
| | Every Sunday of the week              (None) |  Su Mo Tu We Th Fr Sa     |
| | Every Monday of the week              Master |   1 M  M  M  M  M   7     |
| | Every Tuesday of the week             Master |   8 M  M  M  M  M  14     |
| | Every Wednesday of the week           Master |  15 M  M  M  M  M  21     |
| | Every Thursday of the week            Master |  22 M  M  M  M  M  28     |
| | Every Friday of the week              Master |  29 M                     |
| | Every Saturday of the week             (None) |                          |
| +---------------------------------------------+                            |
|                                                                            |
| Notify / Advanced: [Change]  [Reset Dates]                                 |
| Mail Summary To:   root                    Print Summary To:   NONE        |
| Mail Failures To:  NONE                    Print Failures To:  NONE        |
|[Save]                                                          [Cancel]|
+----------------------------------------------------------------------------+
```

This *Schedule* will perform Monday through Friday backups. In the example, a five backup rotation will be created. Because of the one week default retention, *Expired Archives* (those older than one week old) will be retained on the FTP server at least one week, and possibly longer based on the *Lazy Reclamation* flag in the *Resource* definition. If the quota is reached and none of the archives has expired, the backup will fail.

Changing the retention time in the Schedule to 2 weeks, three weeks, etc. allows easy creation of multiple minimal storage rotations.

10.5 - Setting Up FTP Backups

To have *Backup**EDGE*** back up to an FTP server, you must:

1 Configure the FTP server with a directory (folder) prepared to accept FTP backups.

2 Configure a URL Resource on the server being backed up.

3 Test the FTP server connection.

4 Initialize the FTP backup resource.

5 Select the FTP backup resource from *EDGEMENU* or within a Schedule.

Initializing the FTP backup resource does NOT erase any data. If there are no current files in the backup directory, *Backup**EDGE*** will create a control file (named `CTL`) indicating that it is ready to accept *Backup**EDGE*** archives. If *Backup**EDGE*** detects a control file, it will scan the directory for any current archives and re-build its index of available archives and their sizes. This may take a while on some FTP servers. FTP backups cannot commence until the FTP server directory has been initialized one time.

NOTE: Do not place any other files in the *Backup**EDGE*** directory on the FTP server. Do not manually remove any *Backup**EDGE*** files. The only way to manipulate these files other than from within edgemenu without corrupting the control file database is by using the `edge.segadm` command. See “EDGE.SEGADM” on page 330 for more information on using this program.

Preparing the FTP Server

Set up the FTP server correctly to allow access by *BackupEDGE*. This can be anonymous FTP, or it can use a username / password. You must also create a directory for *BackupEDGE* to write to. For proper management, only *BackupEDGE* should use or access this directory.

The recommended directory structure for FTP backups is:

```
/backup_dir/hostname/schedule_name
```

where `backup_dir` is the home directory for FTP backups, `hostname` is the name of the system being backed up, and `schedule_name` is the backup schedule being used (the default nightly backup schedule named is: `simple_job`).

BackupEDGE must be allowed to create files, overwrite files, delete files, and read files in this directory. This step does not involve *BackupEDGE*; you must configure your FTP server using whatever methods are appropriate. See "NAS Configuration Guide" on page 327 for instructions on configuring FTP backups to a variety of different commercial NAS devices. Any FTP server or NAS appliance will have similar configuration information.

Creating the URL Resource

```
+ BackupEDGE Resource Information ------------------------------------------+
|- General Resource Information ------------------------------------------- |
|Resource Type       URL Resource                                           |
|Resource Name       [url0             ] Change as appropriate              |
|Description         [FTP Resource                ]                         |
|Changer Assoc       [Standalone Device]                                    |
|Interface           [Other      ]                                          |
|                                                                           |
|- URL Resource Information ----------------------------------------------- |
|Protocol            [FTP                         ] [Test URL]              |
|Machine             [localhost                   ] [ ] Lazy Reclamation    |
|Directory           [~                                                  ] |
|Username            [                            ]                         |
|Password            [                            ]                         |
|URL                 ftp://localhost/~                                      |
|- Default Backup Properties ---------------------------------------------- |
|Quota               [0            ] [S] Compression Level  [5]             |
|Edge Block Size     [64           ] [Y] Double Buffering                   |
|[Next]                              [Prev]                        [Cancel]|
+---------------------------------------------------------------------------+
```

Create the FTP resource in *BackupEDGE*. During installation, you may be asked if you want to create an *URL* (FTP) resource. After installation, use `edgemenu:Admin->Define Resources` to do this. Select '`[NEW]`', and use the down-arrow keys to change the resource type to '*FTP Server (url)*'. Press *[Enter]*, give the *Resource* a name (or leave the default) and press *[Enter]*, then *[Next]*.

The '`Protocol`' field lets you select between *FTP* and two forms of *FTPS (FTP over SSL)*.

FTP

Authenticate a standard un-encrypted FTP session.

FTPS (FTP Data+Ctrl via SSL)

This is used to encrypt both the session authentication and the actual data transferred.

FTPS (FTP Ctrl via SSL)

This is used to encrypt only session authentication information. The actual data is unencrypted. This may provide a performance benefit in situations where you are already encrypting the data with *BackupEDGE* encryption.

If you try to write to a resource that uses one of these combinations and the server does not support it, the backup operation will fail and produce an error.

For the '`Machine`' field, you put the hostname or IP address of the machine running the FTP server, such as such as '`ftp.server.com`' or '`192.168.168.22`'. Optionally you may specify a connection port other than the default by using a colon at the end of the server name, as in '`ftp.server.com:2000`'

In the '`Directory`' field, you put the directory *Backup**EDGE*** should use, as it appears in the URL. This directory must start with a leading `/` or the results will be unpredictable.

The '`Username`' and '`Password`' fields are optional. If you don't fill them in, *Backup**EDGE*** will try to use *anonymous FTP*. (Note that for many servers you can also use '`ftp`' and whatever email address you like for these fields.)

'`Lazy Reclmation`' controls the behavior of space reclamation (deleting archives) on the *URL Resource*. See "Space Reclamation" on page 91 for additional information. The default behaviour is *Enabled*.

The '`Quota`' field represents the storage quota, or total amount of space that *Backup**EDGE*** will use for all archives stored on this FTP site. It **MUST be specified**, and may be specified in megabytes (type `4096M` for example) or gigabytes (type `64G` for example).

There is a separate limit for the amount of space that any single file created by *Backup**EDGE*** on this resource can consume that is not affected directly by the '`Quota`'. These files are called *segments* and *Backup**EDGE*** automatically creates them as necessary. (This setting is not controllable from the *Resource Manager* screen. It defaults to a value that is slightly smaller than 1GB, which should be fine for most situations.)

Here is an example of the *Resource* screen with a typical FTP backup definition.

```
+ BackupEDGE Resource Information ------------------------------------------+
|- General Resource Information ------------------------------------------- |
|Resource Type       URL Resource                                           |
|Resource Name       [url0              ] Change as appropriate             |
|Description         [FTP Resource                ]                         |
|Changer Assoc       [Standalone Device]                                    |
|Interface           [Other      ]                                          |
|                                                                           |
|- URL Resource Information ----------------------------------------------- |
|Protocol            [FTP                         ] [Test URL]              |
|Machine             [ds508.microlite.com         ] [ ] Lazy Reclamation    |
|Directory           [/backupedge/web2v/simple_job                       ] |
|Username            [backupedge                  ]                        |
|Password            [**********                  ]                        |
|URL                 ftp://ds508.microlite.com/backupedge/web2v/simple_job  |
|- Default Backup Properties ---------------------------------------------- |
|Quota               [40G          ] [S] Compression Level  [5]             |
|Edge Block Size     [64           ] [Y] Double Buffering                   |
|[Next]                              [Prev]                        [Cancel]|
+---------------------------------------------------------------------------+
```

Note that as you select the protocol type and type in the machine name and directory name, *EDGEMENU* formulates the URL line.

Testing the URL Resource

Test the FTP server connection from the machine with *Backup**EDGE*** installed. The `[Test URL]` button uses the information on the *URL Resource* screen to create a connection with the FTP server and test transferring files back and forth to the appropriate directory. If a failure occurs, the reasons will be displayed on the screen to help with debugging. For reference, a copy of the most recent test failure log (if any) will be saved in the file `/usr/lib/edge/tmp/testurl.log`.

Initialize the URL Resource

When you press `[Next]` to save the resource, you will be asked if you want to '*Initialize*' it. You **must** let *Backup**EDGE*** initialize the resource. This tests the connection again and creates a control file named `CTL` in the destination directory. To initialize at a later time, use `edgemenu:Admin->Initialize Medium`. Note that initializing the resource will **not** erase any existing backups. If backups exist, the `CTL` file, which contains information about the individual archive segments, will be re-calculated.

Switching to Active Mode FTP

By default, *Backup**EDGE*** will use passive FTP. If you require active FTP, append `,p` to the machine field, such as `ftp.server.com,p` or `ftp.server.com:2000,p`. Many FTP connections that go through a firewall will require this mode. If `[Test URL]` appears to hang, it may be necessary to kill the edgemenu process, append `,p`, and try again.

Re-startable FTP Backups

By default, *Backup**EDGE*** expects a reliable FTP connection. It streams backups and verifies live. For less reliable connections, a re-startable mode is provided. It breaks up the backup into 50MB segments, and transmits them sequentially. If the segment fails to transfer, it will automatically be re-sent. If you require re-startable FTP, append `,r` to the machine field, such as `ftp.server.com,r` or `ftp.server.com:2000,r`. This is also compatible with active mode FTP. Use `ftp.server.com,p,r` or `ftp.server.com:2000,p,r`.

Selecting the URL Resource

Select the FTP resource as you would any other resource in EDGEMENU or in the Scheduler.

When you set up a new schedule, it's a good idea to use `edgemenu:Verify->Show Archive Label` to see how many archives are actually present after a few days and check the amount of space used.

10.6 - Backup Granularity

Be creative. Backups to devices with a lot of random access storage space provide the opportunity to increase backup frequency. One possible use is doing *Master Backups* each night, and *Differential Backups* at midday.

As an example, the "Sample FTP Backup Schedule" on page 92 will perform your nightly backup of the default *Domain* (`system`) through the default *Sequence* (`onsite`). Enable the advanced scheduler, then create a new *Schedule* called `midday_backups`. When prompted, have the new *Schedule* use the same *Domain* and *Sequence* as the default *Schedule*. You may also have to choose whether or not to include a MySQL backup. Set the time to noon or so.

When you are finished, you'll have a very fast midday backup and be able to increase the reliability of your data.

Midday Backup Example

```
+ Edit Backup Schedule ------------------------------------------------------+
| Schedule Name:     [midday_backup]                                          |
|          Time:     [12:01 ] (14:28:24)  Enabled: [X]                        |
| Sequence:          [Change] web2v.microlite.com:esequence/onsite            |
| Backup Domain:     [Change] system                                          |
| Primary Resource:  [Change] web2v.microlite.com:url!url0                    |
|                                                                             |
| +-------------------------------------------------+     September 2019       |
| | Every Sunday of the week                (None) |  Su Mo Tu We Th Fr Sa    |
| | Every Monday of the week                Differ |   1 D  D  D  D  D   7    |
| | Every Tuesday of the week               Differ |   8 D  D  D  D  D  14    |
| | Every Wednesday of the week             Differ |  15 D  D  D  D  D  21    |
| | Every Thursday of the week              Differ |  22 D  D  D  D  D  28    |
| | Every Friday of the week                Differ |  29 D                    |
| | Every Saturday of the week              (None) |                          |
| +-------------------------------------------------+                          |
|                                                                             |
| Notify / Advanced: [Change]  [Reset Dates]                                  |
| Mail Summary To:   root                    Print Summary To:   NONE         |
| Mail Failures To:  NONE                    Print Failures To:  NONE         |
|[Next]                        [Back To Select]                      [Cancel]|
+-----------------------------------------------------------------------------+
|+Local Machine: web2v.microlite.com  Administering: web2v.microlite.com  ----+|
```

This will create 5 separate *Differential Backups*. If you only care about having the last one around, you could just change `Retention Time` to `[1 Days]` in the `Notify / Advanced` screen. This would allow at least one *Differential Backup* to remain current at all times. Expired ones would be erased only if the *Scheduler* needs to reclaim the space.

The scheduler provides great flexibility. Extending the above example, it is possible to create hourly *Differential Backups* or *Incremental Backups* every day, providing an even greater safety margin by increasing backup frequency.

Deleting archives manually is discussed in “Deleting Backups” on page 253.

10.7 - FTP Backups and Firewalls

Switching to Active Mode FTP

By default, *Backup**EDGE*** will use passive FTP. If you require active FTP, append `,p` to the machine field, such as `ftp.server.com,p` or `ftp.server.com:2000,p`. Many FTP connections that go through a firewall will require this mode. If `[Test URL]` appears to hang, it may be necessary to kill the edgemenu process, append `,p`, and try again.

Connection Timeouts

Many firewalls terminate inactive connections after 15 minutes (the default, but usually selectable). While a data transfer connection is almost always transmitting something, the FTP control connection remains open and quiescent, and can time out, causing the transfer to close. *Backup**EDGE*** 02.03.01 build 2 and later implement keep-alive packets on the control connection to prevent this.

Gateway Anti-Virus FTP Inhibition

*Backup**EDGE*** utilizes the FTP “`REST`” command to perform Instant File Restore. This command allows an archive segment to be opened at the exact block where a file begins.

By default, some Firewall / UTMs (Unified Threat Management Systems) block the FTP “`REST`” command. This must be enabled.

Examples...

- On modern Sonicwall firmware, go into the `Security Services`, `Gateway Anti-Virus` menu, and click on `Configure Gateway AV Settings`. Make sure `Enable FTP 'REST' requests with Gateway AV` is checked, and click `Ok`.
- On legacy Sonicwall firmware, you must log in to the Sonicwall, then manually change the URL from the home page URL (usually `main.html`) to "`diag.html`". Find the '`Enable FTP 'REST' requests with Gateway AV`' checkbox and enable it, then save the settings.

10.8 - RecoverEDGE Reminder

After adding a new *Resource* to *Backup**EDGE*** and creating at least one successful backup, always remember to re-create your *Recover**EDGE*** media and / or images so that they will understand how to use the *Resource*. Test them to make sure you can read from the *Resource* if necessary.

11 - Configuring NFS Backups

11.1 - General Concepts

NFS Backups are similar to *D2D Backups*, except that the mount command used mounts a directory on an NFS server instead of a filesystem on a local hard drive. Two *Resources* combine to make *NFS Backups* function:

- *FSP Resource*, or FileSystem Partition Resource, defines and controls the directory on remote filesystem where archives are stored. No other files may be in this directory except those created by *Backup**EDGE***.
- *AF Resource*, or Attached FileSystem Resource, defines the commands *Backup**EDGE*** must use to mount and unmount the remote filesystem containing the FSP Resource. No other user or process should mount and unmount the remote filesystem.

11.2 - Multiple Archives Per Medium

*Backup**EDGE*** supports performing multiple backups using *NFS Backups*. The quota for *NFS Backups* is defined by the user during setup. This is the general behaviour:

Medium	Archive Behaviour
NFS via FSP/AF	The process will attempt to create a new archive. If starting a new segment would cause the quota to be reached, the oldest expired archive will be erased in its entirety (all segments). If starting a new segment would exceed the quota and no more expired archives exist, the backup will **FAIL**.

11.3 - Compatibility Matrix

Operating System / **NFS Backup Compatibility**	**Linux**	**OSR 5.0.7**	**OSR 6**	**UW7**
Automatic mount / unmount	YES	YES	YES	YES
Backup / Restore / Instant File Restore	YES	YES	YES	YES
Multiple archives per medium	YES	YES	YES	YES
Quotas and Lazy Retention	YES	YES	YES	YES
Disable Lazy Retention	YES	YES	YES	YES
*Recover**EDGE*** Bare Metal DIsaster Recovery	YES	YES	NO	NO

11.4 - NFS Backup Notes

- Quota (maximum capacity) **must** be entered in the *FSP Resource* definition.
- Multiple archives per medium utilizes archive expiration times and lazy reclamation to maximize the number of archives stored for maximum safety.
- Compression and optional encryption are supported.
- Full file checksumming, for maximum data integrity, is supported.
- *Instant File Restore* is available from any archive. It is not necessary to read through an entire archive to restore individual files and directories.
- MySQL™ hot backups are supported.

11.5 - Theory of Operation

For the most part, *NFS Backup Resources* are very similar to more conventional ones such as tape or DVD. However, there are a few points you should be aware of before using them.

Segments

In a tape backup, *Backup**EDGE*** streams the data directly on to the media. In *NFS Backups*, *Backup**EDGE*** streams the data into *archive files* on the remote server. This potentially subjects the files to filesystem size limitations and ulimit or other arbitrary operating system limitations.

To work around these limits, *Backup**EDGE*** automatically segments archives; that is, it divides one logically long archive into short archive files (called *segments*) that can be managed by the operating system using the storage device. By default, these segments are 1 gigabyte -1 block in length.

*Backup**EDGE*** can write multiple archives to *NFS Backup Resources*, and each archive may contain multiple segments. *Backup**EDGE*** handles segments automatically, and provides tools for managing the segments. To maintain consistent archives, the individual segments should never be manipulated by operating system commands. This is why segments do not have names that make sense to humans.

Quotas

Each *NFS Backup Resource* is assigned a storage quota. *Backup**EDGE*** will not attempt to use more storage on the target medium than that assigned by the quota.

Retention Times

By default, all archives created to an *NFS Backup Resource* using the *Scheduler* have a retention time (or expiration time) of one week. They will not be erased automatically until the retention time is up, but will not necessarily be erased just because its retention time is up. An archive past its retention time is called an *Expired Archive*.

Space Reclamation

Archives are retained on *NFS Backup Resources* at least until their expiration time has passed. After that, they are deleted in one of two ways...

Lazy Reclamation Enabled (Default)

If *Lazy Reclamation* is enabled, archives will remain on media as long as possible, just in case they may be needed even after their retention time is up. This allows maximum space utilization on the media. For an archive to be deleted...

- The retention time must be up, i.e. it must be an *Expired Archive*.
- Adding a segment to a new archive would cause the defined quota (as defined by the user when defining the *Resource*) to be exceeded.

If both conditions are true, the oldest *Expired Archive* will be deleted in its entirety. This process ensures that a maximum number of older archives are available on the target media.

If the quota is reached and none of the archives has expired, the backup will prompt for additional media.

By default, each backup in a *Scheduled Job* has a *Retention Time* of 1 week. This is may be changed on a per-schedule basis in the default simple *Scheduler*, and on a per-backup basis in the advanced *Scheduler*.

Lazy Reclamation Disabled

Disabling *Lazy Reclamation* (un-checking the `Lazy Reclamation` field in the *Resource Definition*) configures *BackupEDGE* to check for and immediately erase all expired archives any time a new backup is started to the *FSP Resource*. Only unexpired archives will be retained.

By default, each backup in a scheduled job has a *Retention Time* of 1 week. Note that usually, if you are backing up multiple machines and / or schedules to the same data store, you will create multiple *Resources*, one per machine/schedule combination. Each *FSP Resource* would use a different directory on the NFS server and have a different quota, where combined quotas should not exceed available free space. A typical schedule would look like this:

Sample NFS Backup Schedule

```
+ Edit Backup Schedule ------------------------------------------------------+
| Schedule Name:     simple_job                                              |
|          Time:     [23:00] (14:58:46)  Enabled: [X]                        |
| Sequence:                  myserver.microlite.com:esequence/onsite         |
| Backup Domain:             system                                        |
| Primary Resource:  [Change] myserver.microlite.com:fsp!fsp0               |
|                                                                           |
| +---------------------------------------------+     September 2019         |
| | Every Sunday of the week                (None) |  Su Mo Tu We Th Fr Sa     |
| | Every Monday of the week               Master |   1 M  M  M  M  M   7     |
| | Every Tuesday of the week              Master |   8 M  M  M  M  M  14     |
| | Every Wednesday of the week            Master |  15 M  M  M  M  M  21     |
| | Every Thursday of the week             Master |  22 M  M  M  M  M  28     |
| | Every Friday of the week               Master |  29 M                     |
| | Every Saturday of the week              (None) |                          |
| +---------------------------------------------+                           |
|                                                                           |
| Notify / Advanced: [Change]  [Reset Dates]                                |
| Mail Summary To:   root                    Print Summary To:   NONE       |
| Mail Failures To:  NONE                    Print Failures To:  NONE       |
|[Save]                                                          [Cancel]|
+---------------------------------------------------------------------------+
```

This *Schedule* will perform Monday through Friday backups. In the example, a five backup rotation will be created. Because of the one week default retention, *Expired Archives* (those older than one week old) will be retained on the target medium at least one week, and possibly longer based on the *Lazy Reclamation* flag in the *Resource* definition. If the quota is reached and none of the archives has expired, the backup will fail.

Changing the retention time in the Schedule to 2 weeks, three weeks, etc. allows easy creation of multiple minimal storage rotations.

11.6 - Setting Up NFS Backups

To have *BackupEDGE* backup to an NFS Resource you must:

1. Configure an *AF Resource* to mount and unmount the *NFS Server* on demand.
2. Configure an *FSP Resource* to read and write to a particular directory on the *NFS Server* and associate it with the proper *AF Resource* for mounting / unmounting.
3. Initialize the *FSP Resource*.
4. Select the *FSP Resource* from *EDGEMENU* or within a *Schedule*.

Initializing the *FSP Backup Resource* does NOT erase any data. If there are no current files in the backup directory, *BackupEDGE* will create a control file (named `CTL`) indicating that it is ready to accept *BackupEDGE* archives. If *BackupEDGE* detects a control file, it will scan the directory

for any current archives and re-build its index of available archives and their sizes. *FSP Backups* cannot commence until the *FSP Resource* has been initialized one time.

NOTE: Never place any other (non-*BackupEDGE*-created) files in the *BackupEDGE* directory on the *FSP Resource*. Never manually remove any *BackupEDGE* files. The **only** way to manipulate these files other than from within *EDGEMENU* without corrupting the control file database is by using the `edge.segadm` command. See "EDGE.SEGADM" on page 330 for more information on using this program.

Preparing the NFS Server

NFS Servers generally have permissions setting that must be configured to allow other servers to attach to them. This is called "exporting" a file system or directory. This is usually done by changing the exports file via GUI or from the command line.

Setting Up an Attached Filesystem Resources for NFS

The *AF* (Attached Filesystem) *Resource* is a special *Resource* handling the remote *NFS Server*. It is responsible for management and concurrence. It knows how to mount and unmount it, etc. and understands when more than one local schedule is accessing the remote server. A backup cannot be written directly to the *AF Resource*.

Setting up the *AF Resource* requires using `edgemenu:Admin->Define Resources`. Select '`[NEW]`', then select '`Attached Filesystem (AF)`'. Change the resource name to something suitable if desired. (the default is '`af0`' and is fine).

Unedited AF Resource.

```
+ BackupEDGE Resource Information ------------------------------------------+
|- General Resource Information ------------------------------------------- |
|Resource Type       Attached Filesystem                                     |
|Resource Name       [af0               ] Change as appropriate              |
|Description         [Attached Filesystem Resource]                          |
|Changer Assoc       [Standalone Device]                                     |
|Interface           [Other      ]                                           |
|                                                                            |
|- Attached Filesystem Information ---------------------------------------- |
|Mount Dir           [/usr/lib/edge/system/mnt/af0                          ]|
|Mount Device Node   [/dev/null                                             ]|
|Mount Command       [/etc/mount %m %M                                      ]|
|Unmount Command     [/etc/umount %M                                        ]|
|Exclude Node        [                                                      ]|
|                                                                            |
|[Next]                              [Prev]                          [Cancel]|
+----------------------------------------------------------------------------+
```

Usually, the *only fields you must modify* for NFS mounting are the `Mount Device Node`, the `Mount Command`, and the `Exclude Node`. The other fields, `Mount Dir` and `Unmount Command`, will work without modification. The default mount directory is in a *BackupEDGE* directory that gets automatically excluded from backups, and should not be changed.

The `Mount Device Node` is the directory you've created on the remote server as the root directory of all backups, such as '`remote_server:/backupedge`'. You may use the format `IP_address:/mountpoint` or `hostname:/mountpoint` as desired. It may be desirable to use an IP address to ensure valid connections even if name services aren't working.

The `Exclude Node` is the device node that will be excluded by *RecoverEDGE* during disk preparation for disaster recovery. Please use "`/dev/null`" in this field.

The `Mount Command` must be modified for the particular NFS mount command for the operating system you are using. Here are some examples...

NFS Mount Commands for different Operating Systems

Linux
```
/etc/mount %m %M -o nolock
```

Xinuos / SCO OpenServer 5
```
/etc/mount -f NFS %m %M
```

Xinuos / SCO OpenServer 6
```
/etc/mount -f nfs -o vers=2 %m %M
```

Xinuos / SCO UnixWare 7.1.4
```
/etc/mount -f nfs -o vers=2 %m %M
```

The `Exclude Node` is the device node that will be excluded by *RecoverEDGE* during disk preparation for disaster recovery. Please use "`/dev/null`" in this field.

Completed AF Resource Example (Linux).

```
+ BackupEDGE Resource Information ------------------------------------------+
|- General Resource Information ------------------------------------------- |
|Resource Type       Attached Filesystem                                     |
|Resource Name       [af0               ] Change as appropriate              |
|Description         [Attached Filesystem Resource]                          |
|Changer Assoc       [Standalone Device]                                     |
|Interface           [Other      ]                                           |
|                                                                            |
|- Attached Filesystem Information ---------------------------------------- |
|Mount Dir           [/usr/lib/edge/system/mnt/af0                         ] |
|Mount Device Node   [192.168.100.114:/backupedge ]                          |
|Mount Command       [/etc/mount %m %M -o nolock                           ] |
|Unmount Command     [/etc/umount %M                                       ] |
|Exclude Node        [/dev/null                                            ] |
|                                                                            |
|[Next]                              [Prev]                          [Cancel]|
+----------------------------------------------------------------------------+
```

Press `[Next]` to save the AF resource.

NOTE: OpenServer 6 and UnixWare 7 NFS Resources are not compatible with RecoverEDGE. You must use another Resource type, such as FTP/FTPS backups, to be able to perform remote backups with bare metal recovery on these operating systems.

Setting Up a FileSystem Partition Resource for NFS

After you have saved the AF resource, you must create one or more *Filesystem Partition* (FSP) resources to write to it. Essentially these are simply directories created under the master mount point defined by the AF Resource.

Setting up an FSP resource is very simple. Use `edgemenu:Admin->Define Resources` to create a Resource. Select '`[NEW]`' and then select `Directoy (fsp)`. Change the resource name to something suitable if desired. (the default is '`fsp0`' and is fine).

All of the fields in the "`General Resource Information`" section of this form have excellent defaults except "`AF Association`". Press **[Enter]** on this field and select the *AF Resource* that

will be handling the mounting and un-mounting of the filesystem. This tells *BackupEDGE* to make sure that the remote filesystem is mounted before trying to access the FSP.

```
+ BackupEDGE Resource Information ------------------------------------------+
|- General Resource Information ------------------------------------------- |
|Resource Type       FS Partition                                           |
|Resource Name       [fsp0              ] Change as appropriate             |
|Description         [Directory Resource          ]                         |
|AF Association      [myserver:af0]                                         |
|Interface           [Other      ]                                          |
|                                                                           |
|- FS Partition Information ----------------------------------------------- |
|Dir Suffix          [/myserver                                          ]  |
|Segment Size (K)    [1048544                    ] [X] Lazy Reclamation     |
|                                                                           |
|                                                                           |
|                                                                           |
|- Default Backup Properties ---------------------------------------------- |
|Quota               [120G          ] [S] Compression Level  [5]            |
|Edge Block Size     [64            ] [Y] Double Buffering                  |
|[Next]                               [Prev]                        [Cancel]|
+---------------------------------------------------------------------------+
```

NOTE: *BackupEDGE* handles concurrent access multiple FSPs that share one AF correctly. You may write more than one backup at a time using a single AF.

'Dir Suffix' is the subdirectory under the remote mount point defined in the AF Resource where the backups will be saved. This value can be altered to reflect the host name or schedule name of the server that is being backed up if desired.

'Segment Size', controls the maximum file size that *BackupEDGE* will create. The default is slightly less than 1GB. Note that this does **not** limit the maximum archive size; *BackupEDGE* will automatically split the archive up into multiple files (*segments*) if needed. Generally, the user will not know (or care) about this, as it will be handled for you automatically. The 'Segment Size' field does not need to be altered in most cases.

'Lazy Reclmation' controls the behavior of space reclamation (deleting archives) on the FSP media. See "Space Reclamation" on page 160 for additional information. The default behaviour is *Enabled*.

Do not confuse 'Segment Size' with 'Quota'. 'Quota' limits the total space consumed by all *BackupEDGE* archives on this resource. If the 'Quota' is 100GB, then no more than 100GB will be written by *BackupEDGE* to this FSP until something is erased, or a new medium is loaded.

The [S]oftware compression level from 1 to 9, or choose [N]one for no compression. Do not attempt to set compression to [H]ardware.

Initialize the FSP Resource

When you press [Next] to save the *FSP Resource*, you will be asked if you want to '*Initialize*' the *Resource*. You must let *BackupEDGE* initialize the *Resource* before use. This mounts the remote filesystem, creates the subdirectory and adds a control file named CTL in the destination directory. To initialize at a later time, use edgemenu:Admin->Initialize Medium. while the Primary Resource is set to the correct *FSP*. Note that initializing the *Resource* will **not** erase any existing backups. If existing backups exits, the CTL file, which contains information about the individual archive segments, will be re-calculated.

11.7 - Backup Granularity

Be creative. Remote backups to *NFS Servers* with a lot of space provide the opportunity to increase backup frequency. One possible use is doing *Master Backups* each night, and *Differential Backups* at midday.

As an example, the "Sample NFS Backup Schedule" on page 100 will perform a nightly backup of the default *Domain* (`system`) through the default *Sequence* (`onsite`). Enable the advanced scheduler, then create a new *Schedule* called `midday_backups`. When prompted, have the new *Schedule* use the same *Domain* and *Sequence* as the default *Schedule*. The user may also have to choose whether or not to include a MySQL backup. Set the time to noon or so.

When completed, there will be a very fast midday backup and the reliability of the data will be increased.

Midday Backup Example

```
+ Edit Backup Schedule ------------------------------------------------------+
| Schedule Name:     [midday_backup]                                          |
|          Time:     [12:01 ] (14:28:24)  Enabled: [X]                        |
| Sequence:          [Change] myserver.microlite.com:esequence/onsite         |
| Backup Domain:     [Change] system                                          |
| Primary Resource:  [Change] myserver.microlite.com:fsp!fsp0                 |
|                                                                             |
| +---------------------------------------------+     September 2019         |
| | Every Sunday of the week                (None) |  Su Mo Tu We Th Fr Sa     |
| | Every Monday of the week                Differ |   1 D  D  D  D  D   7     |
| | Every Tuesday of the week               Differ |   8 D  D  D  D  D  14     |
| | Every Wednesday of the week             Differ |  15 D  D  D  D  D  21     |
| | Every Thursday of the week              Differ |  22 D  D  D  D  D  28     |
| | Every Friday of the week                Differ |  29 D                     |
| | Every Saturday of the week              (None) |                           |
| +---------------------------------------------+                             |
|                                                                             |
| Notify / Advanced: [Change]  [Reset Dates]                                  |
| Mail Summary To:   root                    Print Summary To:   NONE         |
| Mail Failures To:  NONE                    Print Failures To:  NONE         |
|[Next]                          [Back To Select]                      [Cancel]|
+-----------------------------------------------------------------------------+
|+Local Machine: myserver.microlite.com  Administering: myserver.microlite.com+|
```

This will create 5 separate *Differential Backups*. If there is only a need to save the latest one, simply set the `Retention Time` to `[1 Days]` in the `Notify / Advanced` screen. This would allow at least one *Differential Backup* to remain current at all times. Expired ones would be erased only if the *Scheduler* needs to reclaim the space.

The scheduler provides great flexibility. Extending the above example, it is possible to create hourly *Differential Backups* or *Incremental Backups* every day, providing an even greater safety margin by increasing backup frequency.

Deleting archives manually is discussed in "Deleting Backups" on page 253.

11.8 - RecoverEDGE Reminders

After adding a new *Resource* to *Backup**EDGE*** and creating at least one successful backup, always remember to re-create your *Recover**EDGE*** media and / or images so that they will understand how to use the *Resource*. Test them to make sure you can read from the *Resource* if necessary.

NOTE: OpenServer 6 and UnixWare 7 NFS Resources are NOT compatible with RecoverEDGE. A different *Resource* type must be used, such as *FTP/FTPS Backups*, to be able to perform remote backups with bare metal recovery on these operating systems.

To boot *Recover**EDGE*** media and initialize it at a different IP address, for testing or cloning, remember to make sure that the *NFS Server*'s exports file has had the new IP address added. Otherwise you won't be able to mount the remote server from the new IP address.

12 - Configuring CIFS (SMB) Backups - Linux

12.1 - General Concepts

CIFS *Backups* are backups where the storage *Resource* is a remotely mounted server or NAS using the Common Internet FileSystem (*CIFS*). CIFS has in the past been known as SMB or Samba. *CIFS Backups* are similar to *D2D Backups*, except that the mount command used mounts a directory on a *CIFS Server* instead of a filesystem on a local hard drive. Two *Resources* combine to make *CIFS Backups* function:

- *FSP Resource*, or FileSystem Partition Resource, defines and controls the directory on remote filesystem where archives are stored. No other files may be in this directory except those created by *Backup**EDGE***.
- *AF Resource*, or Attached FileSystem Resource, defines the commands *Backup**EDGE*** must use to mount and unmount the remote filesystem containing the FSP Resource. No other user or process should mount and unmount the remote filesystem.

12.2 - Multiple Archives Per Medium

*Backup**EDGE*** supports performing multiple backups using *CIFS Backups*. The quota for *CIFS Backups* is defined by the user during setup. This is the general behaviour:

Medium	Archive Behaviour
CIFS via FSP/AF	The process will attempt to create a new archive. If starting a new segment would cause the quota to be reached, the oldest expired archive will be erased in its entirety (all segments). If starting a new segment would exceed the quota and no more expired archives exist, the backup will **FAIL**.

12.3 - CIFS Backup Compatibility

CIFS Backups are compatible with any computer from which a *CIFS Server* can be mounted with standard username and password authentication.

NOTE: *Recover**EDGE*** bare metal disaster recovery for *CIFS Backups* is **ONLY** supported under *Backup**EDGE** 03.01.03 build 2* and later, and only under the following operating systems...

- Red Hat Enterprise Linux 8.x family, including Oracle Linux Server 8.x, and CentOS 8.x.
- Red Hat Enterprise Linux 7.x family, including Oracle Linux Server 7.x, CentOS 7.x, and Scientific Linux 7.x.
- Red Hat Enterprise Linux 6.x family, including Oracle Linux Server 6.x, CentOS 6.x, and Scientific Linux 6.x.
- Ubuntu Ubuntu 14.04 and later Server.
- SuSE Linux Enterprise Server 11 with Service Pack 2 (SP2) and later.

Other Linux variants may work, but these are the only ones tested and supported at the time of this release.

12.4 - CIFS Backup Notes

- Your Linux system must have the **cifs-utils** package installed to be able to properly support *CIFS Backups*. Even if CIFS mounting works without it, this package will be required for DNS support.

- Quota (maximum capacity) **must** be entered in the *FSP Resource* definition.
- Multiple archives per medium utilizes archive expiration times and lazy reclamation to maximize the number of archives stored for maximum safety.
- Compression and optional encryption are supported.
- Full file checksumming, for maximum data integrity, is supported.
- *Instant File Restore* is available from any archive. It is not necessary to read through an entire archive to restore individual files and directories.
- MySQL™ hot backups are supported.

12.5 - Theory of Operation

For the most part, *CIFS Backup* resources are very similar to more conventional ones such as tape or DVD. However, there are a few points you should be aware of before using them.

Segments

In a tape backup, *Backup**EDGE*** streams the data directly on to the media. In *CIFS Backups*, *Backup**EDGE*** streams the data into *archive files* on the remote server. This potentially subjects the files to filesystem size limitations and ulimit or other arbitrary operating system limitations.

To work around these limits, *Backup**EDGE*** automatically segments archives; that is, it divides one logically long archive into short archive files (called *segments*) that can be managed by the operating system using the storage device. By default, these segments are 1 gigabyte -1 block in length.

*Backup**EDGE*** can write multiple archives to *CIFS Backup Resources*, and each archive may contain multiple segments. *Backup**EDGE*** handles segments automatically, and provides tools for managing the segments. To maintain consistent archives, the individual segments should never be manipulated by operating system commands. This is why segments do not have names that make sense to humans.

Quotas

Each *CIFS Backup Resource* is assigned a storage quota. *Backup**EDGE*** will not attempt to use more storage on the target medium than that assigned by the quota.

Retention Times

By default, all archives created to an *CIFS Backup Resource* using the *Scheduler* have a retention time (or expiration time) of one week. They will not be erased automatically until the retention time is up, but will not necessarily be erased just because its retention time is up. An archive past its retention time is called an *Expired Archive*.

Space Reclamation

Archives are retained on *CIFS Backup Resources* at least until their expiration time has passed. After that, they are deleted in one of two ways...

Lazy Reclamation Enabled (Default)

If *Lazy Reclamation* is enabled, archives will remain on media as long as possible, just in case they may be needed even after their retention time is up. This allows maximum space utilization on the media. For an archive to be deleted...

- The retention time must be up, i.e. it must be an *Expired Archive*.

- Adding a segment to a new archive would cause the defined quota (as defined by the user when defining the *Resource*) to be exceeded.

If both conditions are true, the oldest *Expired Archive* will be deleted in its entirety. This process ensures that a maximum number of older archives are available on the target media.

If the quota is reached and none of the archives has expired, the backup will prompt for additional media.

By default, each backup in a *Scheduled Job* has a *Retention Time* of 1 week. This is may be changed on a per-schedule basis in the default simple *Scheduler*, and on a per-backup basis in the advanced *Scheduler*.

Lazy Reclamation Disabled

Disabling *Lazy Reclamation* (un-checking the `Lazy Reclamation` field in the *Resource Definition*) configures *Backup**EDGE*** to check for and immediately erase all expired archives any time a new backup is started to the *FSP Resource*. Only unexpired archives will be retained.

By default, each backup in a scheduled job has a *Retention Time* of 1 week. Note that usually, if you are backing up multiple machines and / or schedules to the same data store, you will create multiple *Resources*, one per machine/schedule combination. Each *FSP Resource* would use a different directory on the *CIFS Server* and have a different quota, where combined quotas should not exceed available free space. A typical schedule would look like this:

Sample CIFS Backup Schedule

```
+ Edit Backup Schedule ------------------------------------------------------+
| Schedule Name:     simple_job                                               |
|          Time:     [23:00 ] (14:58:46)  Enabled: [X]                        |
| Sequence:                  myserver.microlite.com:esequence/onsite          |
| Backup Domain:             system                                         |
| Primary Resource:  [Change] myserver.microlite.com:fsp!fsp0                 |
|                                                                             |
| +-----------------------------------------------+     September 2019        |
| | Every Sunday of the week                (None) |  Su Mo Tu We Th Fr Sa     |
| | Every Monday of the week               Master |   1 M  M  M  M  M   7     |
| | Every Tuesday of the week              Master |   8 M  M  M  M  M  14     |
| | Every Wednesday of the week            Master |  15 M  M  M  M  M  21     |
| | Every Thursday of the week             Master |  22 M  M  M  M  M  28     |
| | Every Friday of the week               Master |  29 M                     |
| | Every Saturday of the week              (None) |                          |
| +-----------------------------------------------+                           |
|                                                                             |
| Notify / Advanced: [Change]  [Reset Dates]                                  |
| Mail Summary To:   root                    Print Summary To:   NONE         |
| Mail Failures To:  NONE                    Print Failures To:  NONE         |
|[Save]                                                            [Cancel]|
+-----------------------------------------------------------------------------+
```

This *Schedule* will perform Monday through Friday backups. In the example, a five backup rotation will be created. Because of the one week default retention, *Expired Archives* (those older than one week old) will be retained on the target medium at least one week, and possibly longer based on the *Lazy Reclamation* flag in the *Resource* definition. If the quota is reached and none of the archives has expired, the backup will fail.

Changing the retention time in the Schedule to 2 weeks, three weeks, etc. allows easy creation of multiple minimal storage rotations.

12.6 - Setting Up CIFS Backups

To have *BackupEDGE* backup to a *CIFS Resource* you must:

1 Configure an *AF Resource* to mount and unmount the *CIFS Server* on demand.

2 Configure an *FSP Resource* to read and write to a particular directory on the *CIFS Server* and associate it with the proper AF Resource for mounting / unmounting.

3 Initialize the *FSP Resource*.

4 Select the *FSP Resource* from *EDGEMENU* or within a *Schedule*.

Initializing the *FSP Backup Resource* does NOT erase any data. If there are no current files in the backup directory, *BackupEDGE* will create a control file (named `CTL`) indicating that it is ready to accept *BackupEDGE* archives. If *BackupEDGE* detects a control file, it will scan the directory for any current archives and re-build its index of available archives and their sizes. FSP backups cannot commence until the FSP Resource has been initialized one time.

NOTE: Never place any other (non-*BackupEDGE*-created) files in the *BackupEDGE* directory on the FSP Resource. Never manually remove any *BackupEDGE* files. The **only** way to manipulate these files other than from within *EDGEMENU* without corrupting the control file database is by using the `edge.segadm` command. See "EDGE.SEGADM" on page 330 for more information on using this program.

Preparing the CIFS Server

CIFS Servers generally have permissions setting that must be configured to allow other servers to attach to them. This varies per *CIFS Server* type and is the responsibility of the user.

Setting Up an Attached Filesystem Resources for CIFS

The *AF* (Attached Filesystem) *Resource* is a special *Resource* handling the remote CIFS server. It is responsible for management and concurrence. It knows how to mount and unmount it, etc. and understands when more than one local schedule is accessing the remote server. A backup cannot be written directly to the AF resource.

Setting up the *AF Resource* requires using `edgemenu:Admin->Define Resources`. Select '`[NEW]`', then select '`Attached Filesystem (AF)`'. Change the resource name to something suitable if desired. (the default is '`af0`' and is fine).

Unedited AF Resource.

```
+ BackupEDGE Resource Information ------------------------------------------+
|- General Resource Information ------------------------------------------- |
|Resource Type       Attached Filesystem                                     |
|Resource Name       [af0               ] Change as appropriate              |
|Description         [Attached Filesystem Resource]                          |
|Changer Assoc       [Standalone Device]                                     |
|Interface           [Other      ]                                           |
|                                                                            |
|- Attached Filesystem Information ---------------------------------------- |
|Mount Dir           [/usr/lib/edge/system/mnt/af0                          ]|
|Mount Device Node   [/dev/null                                             ]|
|Mount Command       [/etc/mount %m %M                                      ]|
|Unmount Command     [/etc/umount %M                                        ]|
|Exclude Node        [                                                      ]|
|                                                                            |
|[Next]                              [Prev]                          [Cancel]|
+----------------------------------------------------------------------------+
```

Usually, the *only fields you must modify* for CIFS mounting are the `Mount Device Node`, the `Mount Command`, and the `Exclude Node`. The other fields, `Mount Dir` and `Unmount Command`,

will work without modification. The default mount directory is in a *BackupEDGE* directory that gets automatically excluded from backups, and should not be changed.

You'll need three pieces of information to create this *Resource*...

`Mount Device Node`
This is a **combination** of the **host name** or **IP address**, and the **directory** to be used for backups on the *CIFS Server*. The form for this is: `//hostname/drectory_tree` or `//IP_address/directory_tree`. This directory should already be created on the server. In our example the hostname will be `cifs.microlite.com` and the directory will be `/backupedge/cifsdir`. This yields a `Mount Device Node` of: `//cifs.microlite.com/backupedge/cifsdir`. If you do not expect DNS (name service) to be running, especially in the case of a bare metal recovery, use the IP address instead of the hostname for the *CIFS Server*.

`USERNAME`
The user name for authentication to the *CIFS Server*.

`PASSWORD`
The password required for authentication to the *CIFS Server*.

The `Mount Device Node` is the directory you've created on the remote server as the root directory of all backups, such as '`remote_server:/backupedge`'. You may use the format `IP_address:/mountpoint` or `hostname:/mountpoint` as desired. It may be desirable to use an IP address to ensure valid connections even if name services aren't working.

The `Exclude Node` is the device node that will be excluded by *RecoverEDGE* during disk preparation for disaster recovery. Please use "`/dev/null`" in this field.

The `Mount Command` must be modified for the particular CIFS mount command for the operating system you are using. Here is an example for Linux...

CIFS Mount Command for Linux

Linux

```
mount -t cifs -o username=USER,password=PASSWORD %m %M
```

The `%m` variable is replaced by the `Mount Device Node` and the `%M` variable is replaced by the local mount directory node.

The `Exclude Node` is the device node that will be excluded by *RecoverEDGE* during disk preparation for disaster recovery. Please use "`%M`" in this field.

Completed AF Resource Example (Linux).

```
+ BackupEDGE Resource Information ------------------------------------------+
|- General Resource Information -------------------------------------------|
|Resource Type       Attached Filesystem                                    |
|Resource Name       [af0               ] Change as appropriate             |
|Description         [Attached Filesystem Resource]                         |
|Changer Assoc       [Standalone Device]                                    |
|Interface           [Other      ]                                          |
|                                                                           |
|- Attached Filesystem Information ----------------------------------------|
|Mount Dir           [/usr/lib/edge/system/mnt/af0                        ] |
|Mount Device Node   [//cifs.microlite.com/backupedge/cifsdir             ] |
|Mount Command       [mount -t cifs -o username=USER,password=PASSWORD %m %M ] |
|Unmount Command     [/etc/umount %M                                      ] |
|Exclude Node        [%M                                                  ] |
|                                                                           |
|[Next]                            [Prev]                          [Cancel]|
+---------------------------------------------------------------------------+
```

Press `[Next]` to save the AF resource.

NOTE: OpenServer 5, OpenServer 6 and UnixWare 7 CIFS Resources are not compatible with RecoverEDGE. You must use another *Resource* type, such as *FTP/FTPS Backups*, to be able to perform remote backups with bare metal recovery on these operating systems.

Setting Up a FileSystem Partition Resource for CIFS

After you have saved the AF resource, you must create one or more *Filesystem Partition* (FSP) resources to write to it. Essentially these are simply directories created under the master mount point defined by the AF Resource.

Setting up an FSP resource is very simple. Use `edgemenu:Admin->Define Resources` to create a Resource. Select '`[NEW]`' and then select `Directoy (fsp)`. Change the resource name to something suitable if desired. (the default is '`fsp0`' and is fine).

All of the fields in the "`General Resource Information`" section of this form have excellent defaults except "`AF Association`". Press **[Enter]** on this field and select the *AF Resource* that will be handling the mounting and un-mounting of the filesystem. This tells *Backup**EDGE*** to make sure that the remote filesystem is mounted before trying to access the FSP.

```
+ BackupEDGE Resource Information ------------------------------------------+
|- General Resource Information -------------------------------------------|
|Resource Type       FS Partition                                           |
|Resource Name       [fsp0              ] Change as appropriate             |
|Description         [Directory Resource          ]                         |
|AF Association      [myserver:af0]                                         |
|Interface           [Other      ]                                          |
|                                                                           |
|- FS Partition Information -----------------------------------------------|
|Dir Suffix          [/myserver                                          ]  |
|Segment Size (K)    [1048544                    ] [X] Lazy Reclamation     |
|                                                                           |
|                                                                           |
|                                                                           |
|- Default Backup Properties ----------------------------------------------|
|Quota               [120G          ] [S] Compression Level  [5]            |
|Edge Block Size     [64            ] [Y] Double Buffering                  |
|[Next]                              [Prev]                          [Cancel]|
+---------------------------------------------------------------------------+
```

NOTE: *Backup**EDGE*** handles concurrent access multiple FSPs that share one AF correctly. You may write more than one backup at a time using a single AF.

'Dir Suffix' is the subdirectory under the remote mount point defined in the AF Resource where the backups will be saved. This value can be altered to reflect the host name or schedule name of the server that is being backed up if desired.

'Segment Size', controls the maximum file size that *BackupEDGE* will create. The default is slightly less than 1GB. Note that this does **not** limit the maximum archive size; *BackupEDGE* will automatically split the archive up into multiple files (*segments*) if needed. Generally, the user will not know (or care) about this, as it will be handled for you automatically. The 'Segment Size' field does not need to be altered in most cases.

'Lazy Reclmation' controls the behavior of space reclamation (deleting archives) on the FSP media. See "Space Reclamation" on page 160 for additional information. The default behaviour is *Enabled*.

Do not confuse 'Segment Size' with 'Quota'. 'Quota' limits the total space consumed by all *BackupEDGE* archives on this resource. If the 'Quota' is 100GB, then no more than 100GB will be written by *BackupEDGE* to this FSP until something is erased, or a new medium is loaded.

The [S]oftware compression level from 1 to 9, or choose [N]one for no compression. Do not attempt to set compression to [H]ardware.

Initialize the FSP Resource

When you press [Next] to save the *Resource*, you will be asked if you want to '*Initialize*' the *Resource*. You must let *BackupEDGE* initialize the *Resource* before use. This mounts the remote filesystem, creates the subdirectory and adds a control file named CTL in the destination directory. To initialize at a later time, use edgemenu:Admin->Initialize Medium. while the Primary Resource is set to the correct FSP.Note that initializing the resource will **not** erase any existing backups. If existing backups exits, the CTL file, which contains information about the individual archive segments, will be re-calculated.

12.7 - Backup Granularity

Be creative. Remote backups to *CIFS Servers* with a lot of space provide the opportunity to increase backup frequency. One possible use is doing *Master Backups* each night, and *Differential Backups* at midday.

As an example, the "Sample CIFS Backup Schedule" on page 107 will perform a nightly backup of the default *Domain* (system) through the default *Sequence* (onsite). Enable the advanced scheduler, then create a new *Schedule* called midday_backups. When prompted, have the new *Schedule* use the same *Domain* and *Sequence* as the default *Schedule*. The user may also have to choose whether or not to include a MySQL backup. Set the time to noon or so.

When completed, there will be a very fast midday backup and the reliability of the data will be increased.

Midday Backup Example

```
+ Edit Backup Schedule ------------------------------------------------------+
| Schedule Name:     [midday_backup]                                          |
|          Time:     [12:01 ] (14:28:24)  Enabled: [X]                        |
| Sequence:          [Change] myserver.microlite.com:esequence/onsite         |
| Backup Domain:     [Change] system                                          |
| Primary Resource:  [Change] myserver.microlite.com:fsp!fsp0                 |
|                                                                             |
| +---------------------------------------------+     September 2019         |
| | Every Sunday of the week              (None) |  Su Mo Tu We Th Fr Sa      |
| | Every Monday of the week             Differ |   1 D  D  D  D  D   7      |
| | Every Tuesday of the week            Differ |   8 D  D  D  D  D  14      |
| | Every Wednesday of the week          Differ |  15 D  D  D  D  D  21      |
| | Every Thursday of the week           Differ |  22 D  D  D  D  D  28      |
| | Every Friday of the week             Differ |  29 D                      |
| | Every Saturday of the week            (None) |                           |
| +---------------------------------------------+                             |
|                                                                             |
| Notify / Advanced: [Change]  [Reset Dates]                                  |
| Mail Summary To:   root                  Print Summary To:   NONE           |
| Mail Failures To:  NONE                  Print Failures To:  NONE           |
|[Next]                        [Back To Select]                      [Cancel]|
+-----------------------------------------------------------------------------+
|+Local Machine: myserver.microlite.com  Administering: myserver.microlite.com+|
```

This will create 5 separate *Differential Backups*. If there is only a need to save the latest one, simply set the `Retention Time` to `[1 Days]` in the `Notify / Advanced` screen. This would allow at least one *Differential Backup* to remain current at all times. Expired ones would be erased only if the *Scheduler* needs to reclaim the space.

The scheduler provides great flexibility. Extending the above example, it is possible to create hourly *Differential Backups* or *Incremental Backups* every day, providing an even greater safety margin by increasing backup frequency.

Deleting archives manually is discussed in “Deleting Backups” on page 253.

12.8 - RecoverEDGE Reminders

After adding a new *Resource* to *Backup**EDGE*** and creating at least one successful backup, always remember to re-create your *Recover**EDGE*** media and / or images so that they will understand how to use the *Resource*. Test them to make sure you can read from the *Resource* if necessary.

NOTE: OpenServer 5, OpenServer 6 and UnixWare 7 CIFS Resources are not compatible with RecoverEDGE. You must use another *Resource* type, such as *FTP/FTPS Backups*, to be able to perform remote backups with bare metal recovery on these operating systems.

*Recover**EDGE*** media / images when booted will not automatically enable networking to deal with CIFS mounts. Please remember to enable Networking from the *Recover**EDGE*** main menu before selecting `Test Media` or `Restore`.

If you need to edit a *Resource* while in *Recover**EDGE***, go to `Utilities`, then `Shell`, then type `/tmp/resource` at the shell prompt to start the *Resource Manager*.

13 - Configuring S3 API Cloud Backups (S3CLOUD)

13.1 - General Concepts

Cloud (Internet-based) *Object Storage* is one of the most popular methods of off-site data protection.

A growing number of cloud (Internet) based storage services have standardized on the **application programming interface (API)** for *Object Storage* originally developed and used worldwide by storage retailer amazon.com's the *Amazon Web Services*™ S3 Simple Storage Service. *Backup**EDGE*** is compatible with that connectivity API through a *Resource* type called "*S3CLOUD*".

We've tested the *S3CLOUD Resources* with multiple on-line *Object Storage* providers, including **Amazon S3**, **Google Cloud Storage**, **Wasabi, Digital Ocean Spaces, Backblaze B2**[1], and more.

We've also tested **MIN**IO[2], popular open-source object storage software for a variety of Linux, BSD, Windows and macOS-based servers. With **MIN**IO you may create your own *Object Storage* server.

Later sub-sections of this **User Guide** describe use of *Backup**EDGE*** with the products listed above in additional detail, beginning with "Using Amazon Web Services S3 Cloud" on page 122.

*Backup**EDGE** 03.01.01* and later has *S3CLOUD* support, opening up a world of inexpensive on-line backup services.

Once configured, backups to *S3CLOUD Resources* work just as if they were being done to a locally attached storage device. Your internet connection speed will generally be the biggest limitation when using *S3CLOUD Resources*.

NOTE: *S3CLOUD Resources* were optimized beginning with *Backup**EDGE** 03.02.01 build 3*. If you have a prior release and are using *S3CLOUD Resources*, see the tech note at: https://www.microlite.com/support/s3cloudfaster.ts.html

13.2 - Multiple Archives Per Medium

*Backup**EDGE*** supports performing multiple backups onto *S3CLOUD Resources*. The quota for an *S3CLOUD Resource* is defined by the user during setup, and defaults to 100GB. This is the general behaviour:

Medium	Archive Behaviour
S3CLOUD	The process will attempt to create a new archive. If starting a new segment would cause the quota to be reached, the oldest expired archive will be erased in its entirety (all segments). If starting a new segment would exceed the quota and no more expired archives exist, the backup will **FAIL**.

13.3 - Prerequisites

- **DNS:** Valid *Domain Name Service* (DNS) must be used, as the IP addresses of the S3 *Endpoints* used to contact S3-compatible services may be changed at any time by the providers.

1. **Backblaze B2** is supported in *Backup**EDGE** 03.04.02 build 1* and later.
2. **MIN**IO is supported in *Backup**EDGE** 03.04.02 build 1* and later.

- **Time:** Accurate *Time Service* is required for secure authentication. You should be running an NTP (Network Time Protocol) daemon on the server for the most accurate timekeeping.
- **Service Provider Account:** You must have a standard account with a valid credit card attached for billing to use their services.

13.4 - Terminology

There is unique terminology related to S3-compatible storege.Here is a brief description of some of these terms:

- **Account**: This is the name of the top level account at *Amazon* or another S3-compatible provider, i.e. the one you log in to in order to manage all services purchased from the *amazon.com* web site, etc. All billing is handled by the provider under their pricing and terms of service.
- **Account Holder**: This refers to the name on the *Account*, and is usually an email address. Access to the *Account* by the *Account Holder* is usually via email address and password, although multi-factor authentication may also be added.
- **Bucket**: All *S3*-compatible storage resides within unique storage entities called *Buckets*. An unlimited number of files can be created within a single *Bucket*. Each *Bucket* entry has two parts: a unique *Bucket Name* and the *Region* of the world (or a specific datacenter) where the *Bucket* will be located.

NOTE: *Buckets* may be created using multiple access tiers on some S3-compatible services. *Backup**EDGE*** is only compatible with frequent access tiers. Do not attempt to use infrequent access or “Glacier-type” tiers.

- **Region**: *S3* providers store information in worldwide networks of data centers. For many reasons, including location security, latency, and performance, users may choose the location, or *Region*, where their data is stored. *Regions* are accessed by sending data to specific *Endpoints*.
- **Endpoint**. *S3 Cloud Endpoint* is essentially the access address for storing data in a particular *S3 Region*. The *Endpoint* name for a *Region* is a specific server name.
- **Port**[1]. *S3CLOUD* services such as **MIN**IO that use a communications port other than the default https port (443) require `:PORT` to be appended to the *Endpoint* in *Backup**EDGE***.
- **User**. Within a single *Account*. many providers allow multiple individual *Users* to be created. A *User* may be given individual access to a *Bucket*. Secure program access to the *Bucket* is managed via an *Access Key ID* and *Secret Key ID* pair, and optionally one or more security *Policies*.
- **Group**. Multiple *Users* may be added to a *Group*, and the items below may be controlled at the *Group* level rather than the *User* level.
- **Policy**. A method for ensuring which *Users* or *Groups* get access to a *Bucket* or *Buckets*, and under what levels and circumstances. For instance, you may limit access to a bucket to particular times of day or from specific IP addresses or ranges of addresses.
- **Access Key ID**. A special non-intuitive, vendor generated ID string created once for each *User* or *Group*. It is always available to the *Account Holder*.
- **Secret Key ID**. A special private code (like a secure password) created for an *Access Key ID*. It is automatically generated by the vendor. This *Secret Key ID* ***must*** be written down and saved when created. For maximum security, many vendors will never display it again.

1. Specifying a communications port number in the *Endpoint* is supported in *Backup**EDGE** 03.04.02 build 1* and later.

13.5 - Security

The *Account Holder* has full access to all storage *Buckets*. For this reason, some vendors (including Amazon) allow individual *Users* to be created under the *Account*, and *BackupEDGE* should be configured using the unique credentials (*Access Key ID* and *Secret Key ID*) of those *Users*. More than one *User* and security *Policy* may be created under a single *Account*. As long as the unique credentials are used properly, individual *Amazon Users* will have access only to archives stored in their own private *Buckets*.

All communications between *BackupEDGE* and S3-compatible providers are performed over an encrypted link. Strict authentication and policy management ensures that data is kept secure from unauthorized access.

Optional *BackupEDGE Encryption* may be used to encrypt archives that are stored on S3-compatible services.

13.6 - Setup Summary

S3-Compatible Storage Provider

Before configuring *BackupEDGE*, you must create a *Bucket* in the proper *Region* at your S3-compatible storage provider, either though an on-line user interface for sites like Amazon, or through third party software for sites without a web-based *Bucket Manager* tool.

Microlite Corporation has successfully used the S3 Browser and the Cloudberry Explorer for Amazon S3 to manage *Buckets* on Amazon and other S3-compatible sites.

- For specific setup instructions for ***Amazon Simple Storage Service (s3)***, see “Using Amazon Web Services S3 Cloud” on page 122.
- For specific setup instructions for ***Google Cloud Storage***, see “Using Google Cloud Storage” on page 136.
- For specific setup instructions for ***Wasabi Hot Cloud Storage***, see “Using Wasabi Hot Cloud Storage” on page 143.
- For specific setup instructions for ***dinCloud***, see “Using Backblaze B2” on page 150.
- For specific setup instructions for ***Dunkel***, see “Using Dunkel Cloud Storage” on page 155.
- For ***generic S3-compatible*** storage providers, see “Using Digital Ocean Spaces” on page 156.

Within *BackupEDGE*

On the *BackupEDGE* side, the user must run the *EDGMENU* program, then:

- Create a new *S3CLOUD Resource* storage *Resource*. (See “Create a BackupEDGE S3CLOUD Resource” on page 118). Four pieces of information are required:
  - Unique directory name for this server and schedule.
  - *S3 Bucket* name.
  - *S3 Access Key ID*.
  - *S3 Secret Access Key*.
  - *S3 Cloud Endpoint* and optional *Port*.
- Initialize the *S3CLOUD Resource*.
- Select the new *S3CLOUD Resource* as the storage *Resource* in *EDGEMENU* or in a *Scheduled Job*.

As long as the *Account* remains open, stored archives may be retrieved. Closing the *Account* or deleting the *Bucket* within the account will result in the loss of all stored data.

By default, only the https port (443) needs to be open on the user firewall for *S3CLOUD Resources* to function. If you are using a different port, change the firewall appropriately.

13.7 - Important S3CLOUD Notes

- *S3CLOUD Resource* security protocols require very accurate time. You MUST either enable the NTP time daemon or use some other method of ensuring accurate time before attempting to use this service.
- Quota (maximum capacity) must be entered in the *S3CLOUD Resource* definition. The default for this *Resource* type is 100GB. This may be changed as needed. There is no limit. Multiple archives per medium utilizes archive expiration times and lazy reclamation to maximize the number of archives stored for maximum safety.
- Compression and optional encryption are supported. The connection and all data transported between *Backup**EDGE*** and *S3CLOUD Endpoints* is always encrypted.
- Full file checksumming, for maximum data integrity, is supported.
- *Instant File Restore* is available from any archive. It is not necessary to read through an entire archive to restore individual files and directories.
- MySQL™ hot backups are supported.

13.8 - Theory of Operation

*Backup**EDGE** S3CLOUD Resources* are very similar to the *URL Resources* used for *FTP Backups*. However, there are a few points you should be aware of before using them.

Segments

In a tape, DVD, or similar backup, *Backup**EDGE*** streams the data directly on to the media as a single complete archive. In *S3CLOUD* backups, as in FTP backups, *Backup**EDGE*** streams the data into *archive files*. One of the restrictions in *S3CLOUD* storage is that, before sending an archive file you must tell the cloud site length of the file you are sending.

To work with this restriction, *Backup**EDGE*** automatically segments archives; that is, it divides one logically long archive into many short archive files (called *segments*) that are small enough to keep from filling the hard drive while keeping the backup streaming at maximum network bandwidth. By default, these segments are 50 megabytes in length. This is configurable but usually not necessary.

*Backup**EDGE*** can write multiple archives to *S3CLOUD* servers, and each archive may contain multiple segments. *Backup**EDGE*** handles segments automatically, and provides tools for managing the segments. To maintain consistent archives, the individual segments should never be manipulated by operating system commands or *Bucket Manager* tools. This is why segments do not have names that make sense to humans.

Quotas

Each *S3CLOUD Resource* is assigned a storage quota. *Backup**EDGE*** will not attempt to use more storage in the *S3CLOUD* storage cloud than that assigned by the quota.

Retention Times

By default, all archives created to an *S3CLOUD Resource* using the *Scheduler* have a *Retention Time* (or expiration time) of one week. They will not be automatically erased until the *Retention*

Time is up, but will not necessarily be erased just because its *Retention Time* is up. An archive past its *Retention Time* is called an *Expired Archive*.

Space Reclamation

Archives are retained on *S3CLOUD* servers at least until their expiration time has passed. After that, they are deleted in one of two ways...

Lazy Reclamation Enabled (Default)

If *Lazy Reclamation* is enabled, archives will remain on the *S3CLOUD* server as long as possible, just in case they may be needed even after their retention time is up. This allows maximum space utilization on the server. For an archive to be deleted...

- The retention time must be up, i.e. it must be an *Expired Archive*.
- Adding a segment to a new archive would cause the defined quota to be exceeded.

If both conditions are true, the oldest *Expired Archive* will be deleted in its entirety. This process ensures that a maximum number of older archives are available on the *URL Resource*.

If the quota is reached and none of the archives has expired, the backup will prompt for additional media.

By default, each backup in a *Scheduled Job* has a *Retention Time* of 1 week. This is may be changed on a per-schedule basis in the default simple *Scheduler*, and on a per-backup basis in the advanced *Scheduler*.

Lazy Reclamation Disabled

Disabling *Lazy Reclamation* (un-checking the `Lazy Reclamation` field in the *Resource Definition*) configures *Backup**EDGE*** to check for and immediately erase all expired archives any time a new backup is started to the *s3cloud Resource*. Only unexpired archives will be retained. This allows only the minimum required amount of space to be used, while still retaining as many archives as are needed.

Note that usually, if you are backing up multiple machines and/ or schedules to the same cloud site, you will create multiple *Resources*, one per machine/schedule combination. Each *Resource* would use a different directory on the cloud server and have a different quota. A typical schedule would look like this:

Sample S3CLOUD Backup Schedule

```
+ Edit Backup Schedule ------------------------------------------------------+
| Schedule Name:     simple_job                                               |
|          Time:     [23:00 ] (15:20:21)  Enabled: [X]                        |
| Sequence:                   acme.microlite.com:esequence/onsite             |
| Backup Domain:              system                                         |
| Primary Resource:  [Change] acme.microlite.com:s3cloud!s3cloud0             |
|                                                                             |
| +-----------------------------------------------+     September 2019        |
| | Every Sunday of the week                (None) |  Su Mo Tu We Th Fr Sa     |
| | Every Monday of the week               Master |   1 M  M  M  M  M   7     |
| | Every Tuesday of the week              Master |   8 M  M  M  M  M  14     |
| | Every Wednesday of the week            Master |  15 M  M  M  M  M  21     |
| | Every Thursday of the week             Master |  22 M  M  M  M  M  28     |
| | Every Friday of the week               Master |  29 M                     |
| | Every Saturday of the week              (None) |                           |
| +-----------------------------------------------+                           |
|                                                                             |
| Notify / Advanced: [Change]  [Reset Dates]                                  |
| Mail Summary To:   root                    Print Summary To:   NONE         |
| Mail Failures To:  NONE                    Print Failures To:  NONE         |
|[Save]                                                          [Cancel]|
+-----------------------------------------------------------------------------+
```

This *Schedule* will perform Monday through Friday backups. In the example, a five backup rotation will be created. Because of the one week default retention, *Expired Archives* (those older than one week old) will be retained on the cloud server at least one week, and possibly longer based on the *Lazy Reclamation* flag in the *Resource* definition. If the quota is reached and none of the archives has expired, the backup will fail.

Changing the retention time in the Schedule to 2 weeks, three weeks, etc. allows easy creation of multiple minimal storage rotations.

Create a BackupEDGE S3CLOUD Resource

Use `edgemenu:Admin->Define Resources` to do this. Select '`[NEW]`', and use the down-arrow keys to change the resource type to '*S3 Cloud Storage (s3cloud)*'. Press *[Enter]*, give the *Resource* a name (or leave the default) and press *[Enter]*, then *[Next]*.

```
+ BackupEDGE Resource Information -------------------------------------------+
|- General Resource Information -------------------------------------------|
|Resource Type       Amazon S3 and Compatible S3 Cloud Resource              |
|Resource Name       [s3cloud0          ] Change as appropriate             |
|Description         [S3CLOUD                    ]                          |
|Changer Assoc       [Standalone Device]                                    |
|Interface           [Other      ]                                          |
|                                                                           |
|-S3 INFO -----------------------------------------------------------------|
|Directory           [/backups                   ] [Test URL]               |
|Bucket              [YOURS3BUCKET               ] [X] Lazy Reclamation     |
|Access Key          [                           ]                          |
|Secret Access Key   [                                                  ] |
|S3 Cloud Endpoint   [endpoint_url[:PORT]                               ] |
|                                                                           |
|- Default Backup Properties ----------------------------------------------|
|Quota               [100G         ] [S] Compression Level  [5]            |
|Edge Block Size     [64           ] [Y] Double Buffering                   |
|[Next]                              [Prev]                        [Cancel]|
+-----------------------------------------------------------------------------+
```

Directory

The default backup directory is "`/backups`", which is in reality a directory stored in the *Bucket* within your Amazon account.

Bucket

This is the name of the *Bucket* you created in the appropriate *Region* of your *Account*.

Access Key
This is the *Access Key ID* of the *User* you created in your *Amazon Account*.

Secret Access Key
This is the *Secret Access Key ID* for the *Access Key ID* of the *User* you created in your *Amazon Account*.

S3 Cloud Endpoint[:PORT][1]
This is the *Access Address* for the *Region* where you created the *Bucket* in your *Account*.

For ***Amazon S3***, you will find a list of available *Endoints* on page 122.

For **Google Cloud Storage** you will find a list of available *Endpoints* on page 136.

For ***dinCloud D3***, you will find a list of available *Endpoints* on page 150.

For **Dunkel Cloud Storage**, you will find a list of available Endpoints on page 155.

For other S3-compatible providers, please see their own on-line documentation for *Region* and *Endpoint* information.

S3CLOUD services such as **MIN**IO that use a communications port other than the default https port (443) require `:PORT` to be appended to the *Endpoint* in *Backup**EDGE***.

Lazy Reclamation
This controls the behavior of space reclamation (deleting archives) on the *s3cloud Resource*. See "Space Reclamation" on page 117 for additional information. The default behaviour is *Enabled*.

As with *URL Resources*, we recommend that you set the directory to reflect your system name and schedule name. Here is an example of an *s3cloud Resource* set for use with the default backup scheduled (**simple_job**) for system **acme**.

```
+ BackupEDGE Resource Information ------------------------------------------+
|- General Resource Information ------------------------------------------- |
|Resource Type       Amazon S3 and Compatible S3 Cloud Resource              |
|Resource Name       [s3cloud0          ] Change as appropriate             |
|Description         [S3CLOUD                    ]                          |
|Changer Assoc       [Standalone Device]                                    |
|Interface           [Other      ]                                          |
|                                                                           |
|-S3 INFO ----------------------------------------------------------------- |
|Directory           [/acme-simple-job           ] [Test URL]               |
|Bucket              [/backupedge-acme-uss       ] [X] Lazy Reclamation     |
|Access Key          [AKIAIIJGSX3TBOFZPODA       ]                          |
|Secret Access Key   [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              ] |
|S3 Cloud Endpoint   [s3.amazonaws.com                                      ] |
|                                                                           |
|- Default Backup Properties ---------------------------------------------- |
|Quota               [100G         ] [S] Compression Level  [5]             |
|Edge Block Size     [64           ] [Y] Double Buffering                   |
|[Next]                              [Prev]                        [Cancel] |
+---------------------------------------------------------------------------+
```

Testing the S3CLOUD Resource

Test the *s3cloud* server connection from the machine with *Backup**EDGE*** installed. The `[Test URL]` button uses the information on the *S3CLOUD Resource* screen to create a connection with *the S3 ENdpoint* and tests transferring files back and forth to the appropriate directory. If a failure occurs, the reasons will be displayed on the screen to help with debugging. For reference, a copy of the most recent test failure log (if any) will be saved in the file `/usr/lib/edge/tmp/testurl.log`.

1. Specifying a communications port number in the *Endpoint* is supported in *Backup**EDGE** 03.04.02 build 1* and later.

Initialize the S3CLOUD Resource

When you press `[Next]` to save the resource, you will be asked if you want to '*Initialize*' it. You must let *BackupEDGE* initialize the resource. This tests the connection again and creates a control file named `CTL` in the destination directory. To initialize at a later time, use `edgemenu:Admin->Initialize Medium`. Note that initializing the resource will **not** erase any existing backups. If existing backups exits, the `CTL` file, which contains information about the individual archive segments, will be re-calculated.

Selecting the S3CLOUD Resource

Select the *S3CLOUD Resource* as you would any other resource in *EDGEMENU* or in the *Scheduler*.

When you set up a new schedule, it's a good idea to use `edgemenu:Verify->Show Archive Label` to see how many archives are actually present after a few days and check the amount of space used.

13.9 - Creating Additional S3CLOUD Resources

Use `edgemenu:Admin->Define Resources` to do this. Select '`[NEW]`', and use the down-arrow key to change the resource type to *'S3 Cloud Storage (s3cloud)'*. This would typically be done to create a separate *Resource* directory for use with a different schedule, but it is also possible to create *S3CLOUD Resources* in different *Regions* or even with completely different providers.

13.10 - Backup Granularity

Be creative. Backups to devices with a lot of random access storage space provide the opportunity to increase backup frequency. One possible use is doing *Master Backups* each night, and *Differential Backups* at midday.

As an example, the "Sample S3CLOUD Backup Schedule" on page 118 will perform your nightly backup of the default *Domain* (`system`) through the default *Sequence* (`onsite`). Enable the advanced scheduler, then create a new *Schedule* called `midday_backups`. When prompted, have the new *Schedule* use the same *Domain* and *Sequence* as the default *Schedule*. You may also have to choose whether or not to include a *MySQL* backup. Set the time to noon or so.

When you are finished, you'll have a very fast midday backup and be able to increase the reliability of your data.

Midday Backup Example

```
+ Edit Backup Schedule ------------------------------------------------------+
| Schedule Name:     [midday_backup]                                          |
|          Time:     [12:01 ] (14:28:24)  Enabled: [X]                        |
| Sequence:          [Change] acme.microlite.com:esequence/onsite             |
| Backup Domain:     [Change] system                                          |
| Primary Resource:  [Change] acme.microlite.com:s3cloud!s3cloud              |
|                                                                             |
| +-----------------------------------------------+     September 2019       |
| | Every Sunday of the week                (None) |  Su Mo Tu We Th Fr Sa    |
| | Every Monday of the week                Differ |   1 D  D  D  D  D   7    |
| | Every Tuesday of the week               Differ |   8 D  D  D  D  D  14    |
| | Every Wednesday of the week             Differ |  15 D  D  D  D  D  21    |
| | Every Thursday of the week              Differ |  22 D  D  D  D  D  28    |
| | Every Friday of the week                Differ |  29 D                    |
| | Every Saturday of the week              (None) |                          |
| +-----------------------------------------------+                          |
|                                                                             |
| Notify / Advanced: [Change]  [Reset Dates]                                  |
| Mail Summary To:   root                    Print Summary To:   NONE         |
| Mail Failures To:  NONE                    Print Failures To:  NONE         |
|[Next]                        [Back To Select]                      [Cancel]|
+-----------------------------------------------------------------------------+
|+Local Machine: web2v.microlite.com  Administering: web2v.microlite.com  ----+|
```

This will create 5 separate *Differential Backups*. If you only care about having the last one around, you could just change `Retention Time` to `[1 Days]` in the `Notify / Advanced` screen. This would allow at least one *Differential Backup* to remain current at all times. Expired ones would be erased only if the *Scheduler* needs to reclaim the space.

The scheduler provides great flexibility. Extending the above example, it is possible to create hourly *Differential Backups* or *Incremental Backups* every day, providing an even greater safety margin by increasing backup frequency.

Deleting archives manually is discussed in “Deleting Backups” on page 253.

13.11 - S3CLOUD Backups and Firewalls

Gateway Anti-Virus HTTP/HTTPS Inhibition

*Backup**EDGE*** utilizes HTTP/HTTPS byte-range requests to perform *Instant File Restore* on *S3CLOUD Resources*. These requests allows an archive segment to be opened at the exact block where a file begins.

Some Firewall / UTMs (Unified Threat Management Systems) can block these requests.

As an example, on Sonicwall products, go into the `Security Services`, `Gateway Anti-Virus` menu, and click on `Configure Gateway AV Settings`. Make sure `Enable HTTP Byte-Range requests with Gateway AV` is checked, and click `Ok`.

13.12 - RecoverEDGE Reminder

After adding a new *Resource* to *Backup**EDGE*** and creating at least one successful backup, always remember to re-create your *Recover**EDGE*** media and / or images so that they will understand how to use the *Resource*. Test them to make sure you can read from the *Resource* if necessary.

13.13 - Using Amazon Web Services S3 Cloud

To use *Backup**EDGE*** with the ***Amazon Web Services S3 Cloud***, a working knowledge of *Amazon* and *Amazon S3* is expected. There are initial setup steps required on both the *Amazon* web site and via the *EDGEMENU Backup**EDGE*** user interface.

The following information from ***Amazon Web Services*** is required to create an *s3cloud Resource*...

- *Bucket* name.
- *Access Key ID*.
- *Secret Access Key*.
- *Cloud Endpoint*.

For *EDGEMENU*, please see “Create a BackupEDGE S3CLOUD Resource” on page 118.

On initial setup, the users logs into the *Amazon S3 Console* and:

- creates a storage container, called a *Bucket*, through the **S3** control panel menu. The *Bucket* is created in one of the supported **Amazon S3 Regions** throughout the world.
- creates a *User* through the AWS Identity and Access Management (*IAM*) control panel menu and adds a default *Security Policy*. This creates two credentials called an *Access Key ID* and a *Secret Access Key* which MUST be copied down and saved.
- optionally creates and applies a custom *Security Policy* to further restrict access to the *Bucket* .

Amazon S3 Regions and Endpoints

Amazon has storage clouds on multiple continents; you can store data locally at your choice of multiple locations in...

- The United States
- Africa
- Asia Pacific
- Canada
- The European Union
- The Middle East
- South America

Amazon tracks and bills the user for this service, not Microlite Corporation. Rates vary by **Amazon S3 Region**. Pricing can be found at: https://aws.amazon.com/s3/pricing.

*Backup**EDGE*** 03.01.01 through 03.01.04 were capable of using the original eight worldwide **Amazon S3 Regions** (storage locations) throughout the wold. These are listed on the next page.

*Backup**EDGE*** 03.01.05 and later are capable of using all of the worldwide **Amazon S3 Regions** (storage locations) throughout the world (23 at the time of this writing). These are also listed on the next page.

Here is a list of the available **Amazon S3 Regions** where *Buckets* may be created. The *Endpoint* is essentially the access address of the servers in the **Amazon S3 Region**. The **Amazon S3 Region** name is in **Bold**.

Current S3 Regions[1]

Amazon S3 Region	*Region Coverage*	*Amazon S3 Endpoint*
Africa (Cape Town)	Africa	s3-accesspoint.af-south-1.amazonaws.com
Asia Pacific (Hong Kong)	Hong Kong	s3-ap-east-1.amazonaws.com
Asia Pacific (Mumbai)	India	s3-ap-south-1.amazonaws.com
Asia Pacific (Seoul)	Southeast Asia - South Korea	s3-ap-northeast-2.amazonaws.com
Asia Pacific (Singapore)	Southeast Asia	s3-ap-southeast-1.amazonaws.com
Asia Pacific (Sydney)	Australia / New Zealand	s3-ap-southeast-2.amazonaws.com
Asia Pacific (Osaka-Local)[a]	Japan	s3-ap-northeast-3.amazonaws.com
Asia Pacific (Tokyo)	Japan	s3-ap-northeast-1.amazonaws.com
Canada (Central)	Canada	s3-ca-central-1.amazonaws.com
CN (Beijing)[b]	China - Beijing	s3.cn-north-1.amazonaws.com.cn
CN (Ningxia)[c]	China - Ningxia	s3.cn-northwest-1.amazonaws.com.cn
EU (Frankfurt)	European Union - Germany	s3-eu-central-1.amazonaws.com
EU (Ireland)	European Union - Ireland	s3-eu-west-1.amazonaws.com
EU (London)	European Union - UK	s3-eu-west-2.amazonaws.com
EU (Paris)	European Union - France	s3-eu-west-3.amazonaws.com
EU (Stockholm)	European Union - Sweden	s3-eu-north-1.amazonaws.com
EU (Milan)	European Union - Italy	s3-eu-south-1.amazonaws.com
ME (Bahrain)	Middle East	s3-me-south-1.amazonaws.com
South America (Sao Paulo)	South America	s3-sa-east-1.amazonaws.com
US East (N. Virginia)	Entire United States	s3.amazonaws.com or s3.us-east-1.amazonaws.com
US East (Ohio)	Ohio	s3-us-east-2.amazonaws.com
US West (N. California)	California	s3-us-west-1.amazonaws.com
US West (Oregon)	US Pacific Northwest	s3-us-west-2.amazonaws.com

a. Requires a special Amazon-Osaka Account.
b. Requires a special Amazon China Account.
c. Requires a special Amazon China Account.

Choose the most desirable of the **Amazon S3 Regions** listed.

S3 Signature Version 2 Regions - BackupEDGE 03.01.01 - 03.01.04

Legacy versions of *BackupEDGE* supported fewer *Regions*; ap-southeast-1, ap-southeast-2, ap-northeast-1, eu-west-1, sa-east-1, us-=east-1, us-west-1 and us-west-2 only.

1. All regions support Amazon Signature Version 4 for use with *BackupEDGE 03.01.05* and later.

Amazon S3 Initial Setup[1]

NOTE: Amazon Web Services changes web interfaces frequently. The screen shots on these pages reflect the user interface at the time this Guide was published. The interface look may change in the future.

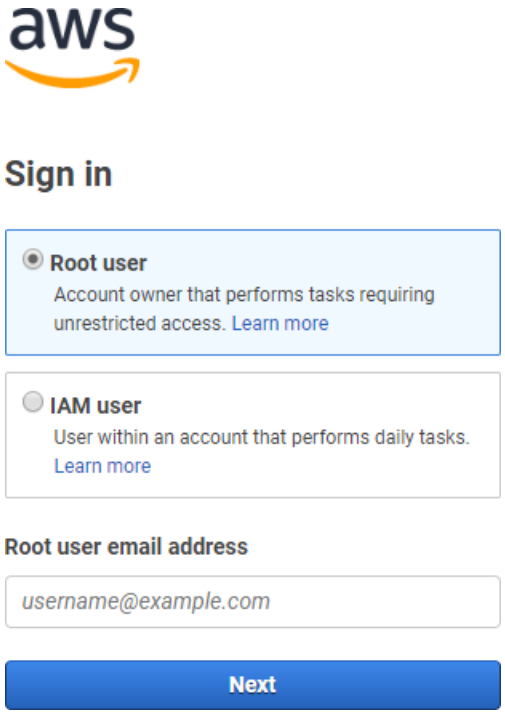
To have *BackupEDGE* back up to Amazon **S3**, you must:

1 Create an account on http://www.amazon.com.

2 Make sure you add **Amazon Web Services** to the Amazon *Account*.

3 Log in to the Amazon AWS Management Console by browsing to: https://aws.amazon.com/console

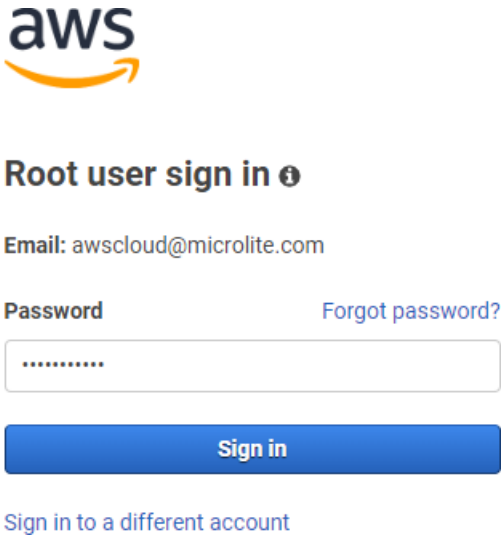
4 Click on *My Account*, then *AWS Management Console*. Select *Root User*, type the **account email address**, and click *Next*.



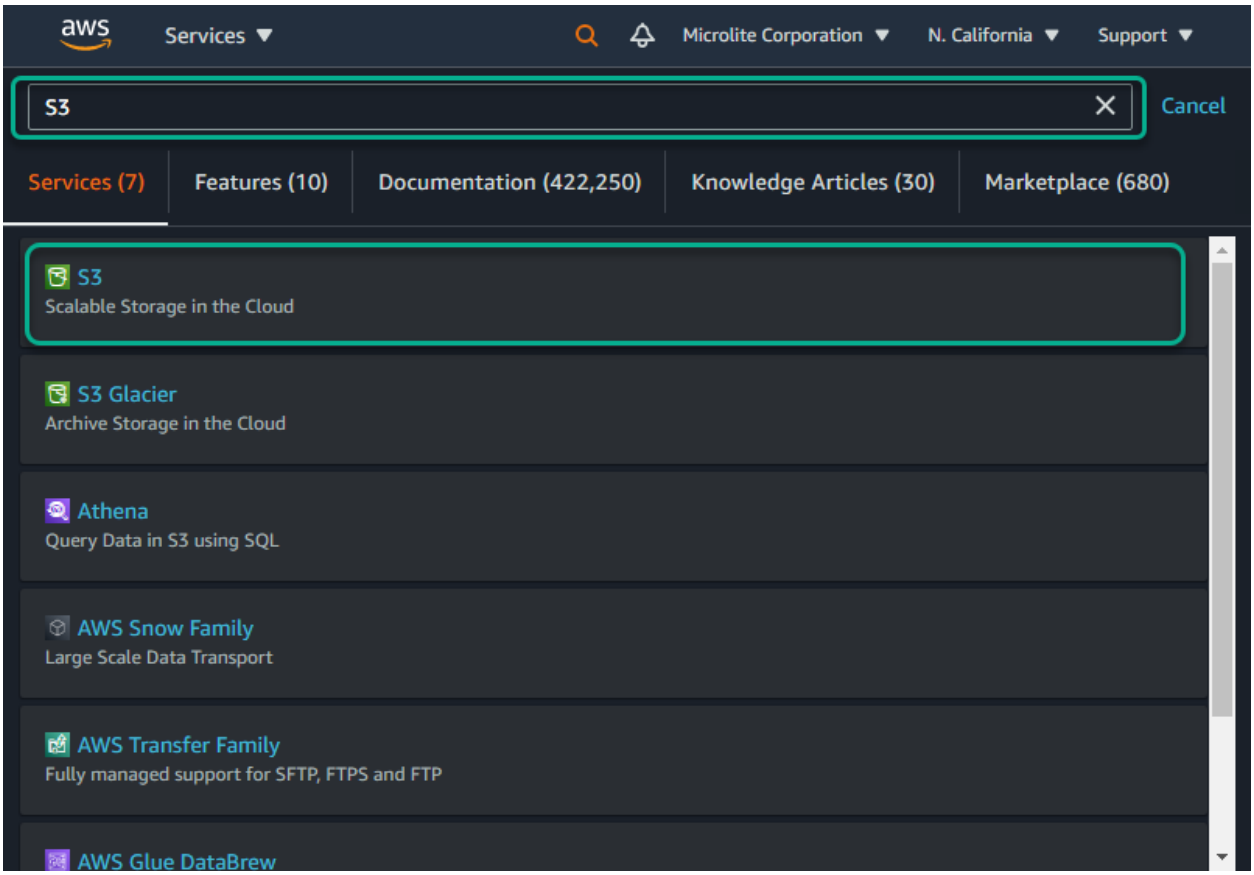
1. Amazon may change the functionality of their web-based management system without notice. The exact steps described here may also change in this instance.

5 Follow the instructions in the Security Check, if prompted.

6 Type the **Password** and click *Sign in*.

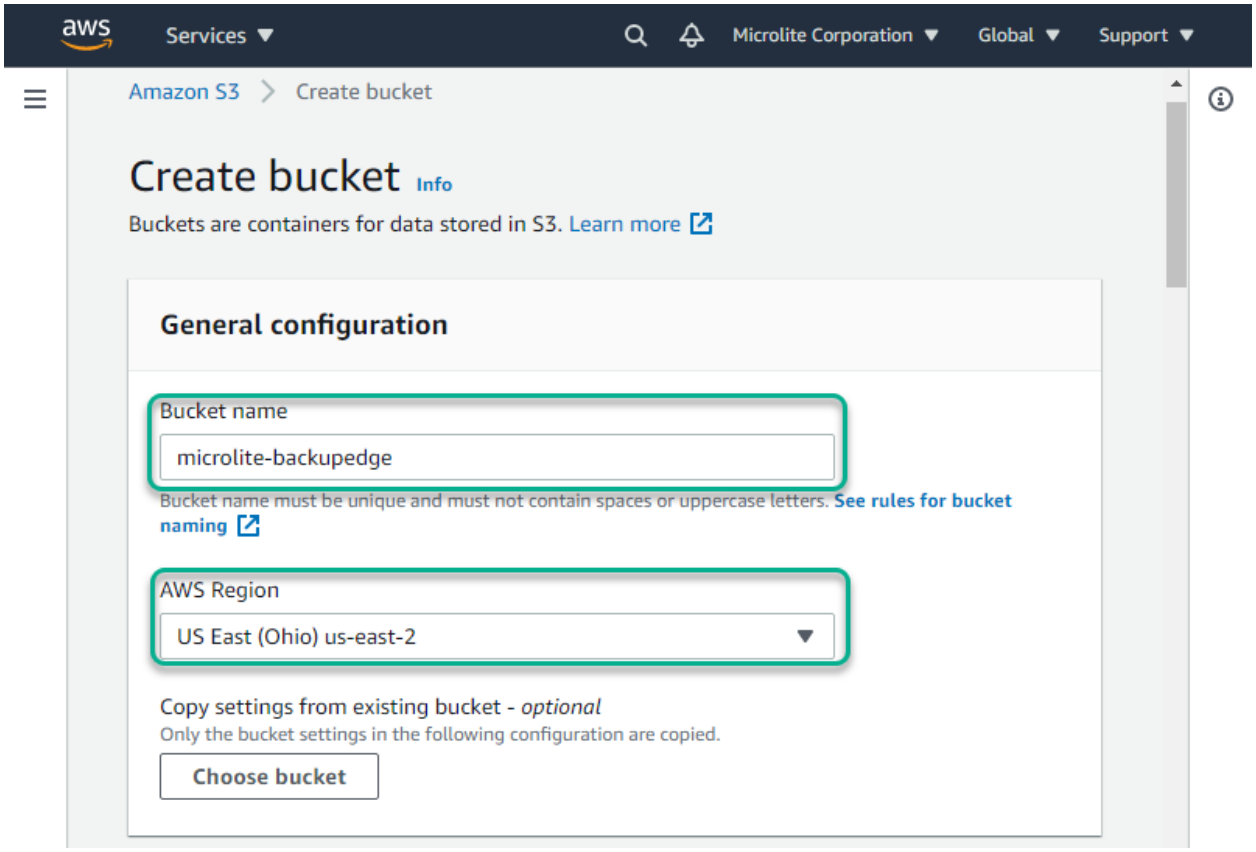


7 At the *AWS Management Console*, at the top of the screen, click the ***Search*** icon. Type **S3** and then select ***S3*** - *Scalable Storage in the Cloud*, from the available choices.



8 A list of your current *Buckets* will be displayed, or No Buckets will be shown if you have none. Choose **Create Bucket**. This will start the *Bucket Wizard*.

9 Provide a *Bucket name* and select the appropriate **Region Name**. Write down the *Bucket Name*. You can use any name, like the one below, but you may want to use a *Bucket Name* format like `backupedge dash company / schedule dash region`.



NOTE: *Bucket Names* are unique for all of *Amazon S3*. You may not use a *Bucket Name* that is currently in use by anyone else. For consistency, Microlite recommends basing the *Bucket Name* on the server you'll be backing up and the *Region Name* you'll be using.

NOTE: *Buckets* may be created using multiple access tiers on Amazon S3. *Backup**EDGE*** is only compatible with frequent access tiers. Do not attempt to use infrequent access or "Glacier-type" tiers.

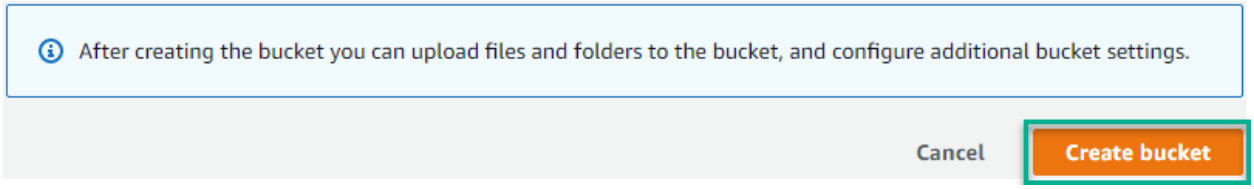
The example above is **microlite-backupedge**. If you want to add the *Schedule* name to the *Bucket Name*, it might look like **backupedge-simple-job-us-west-2**. *Bucket Names* may only contain letters and dashes (-). Good practice is to replaces underlines with dashes.

Select one of the **Region** names shown in the drop down list (based on your physical location). The **Region Name** you choose will determine the **Amazon S3 Endpoint**.

Whichever **Region Name** you choose, write down the **Amazon S3 Endpoint** from the list on page 123.

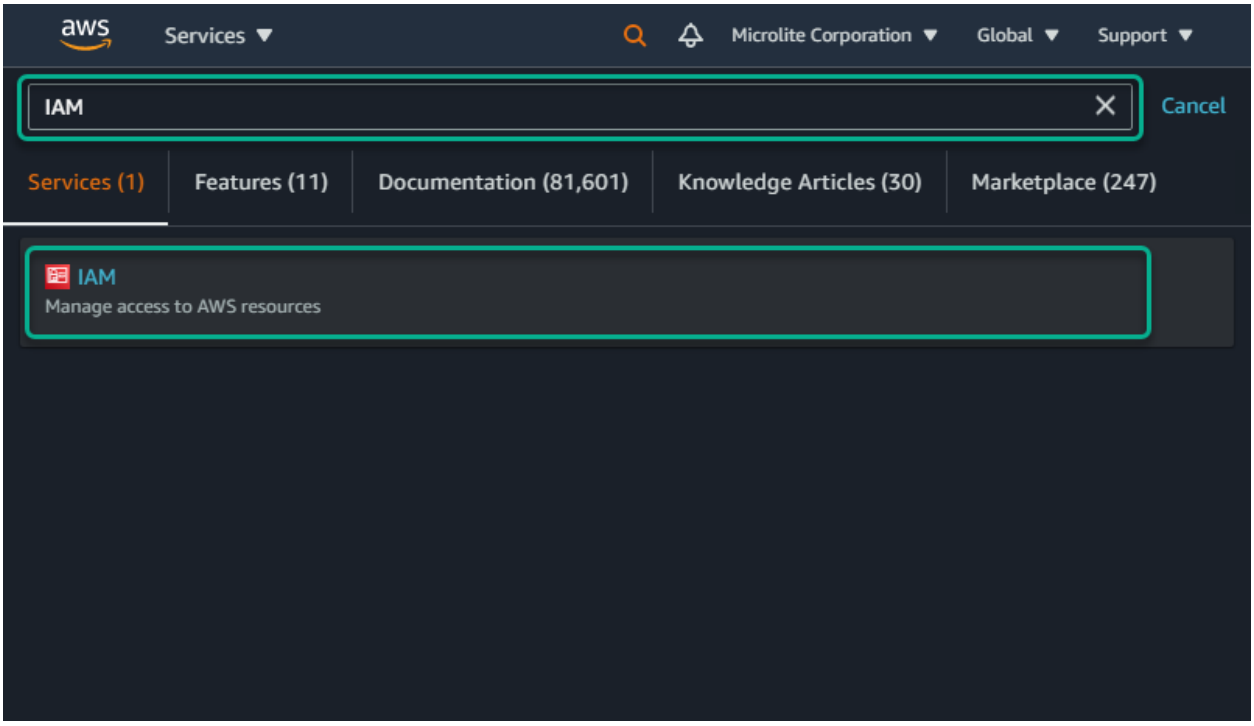
NOTE: Make sure you write down the *Bucket Name* and **Region Name** before proceeding. The **Region Name** translates to an **Amazon S3 Endpoint** as shown in the table on page 123. In the example above, the US East 2 (Columbus, Ohio USA) Region was used.

10 There is no need to click ***Next*** or any other Amazon options. After typing the *Bucket Name* and selecting the *Region*, scroll to the bottom of the page and click ***Create*** to create the bucket.

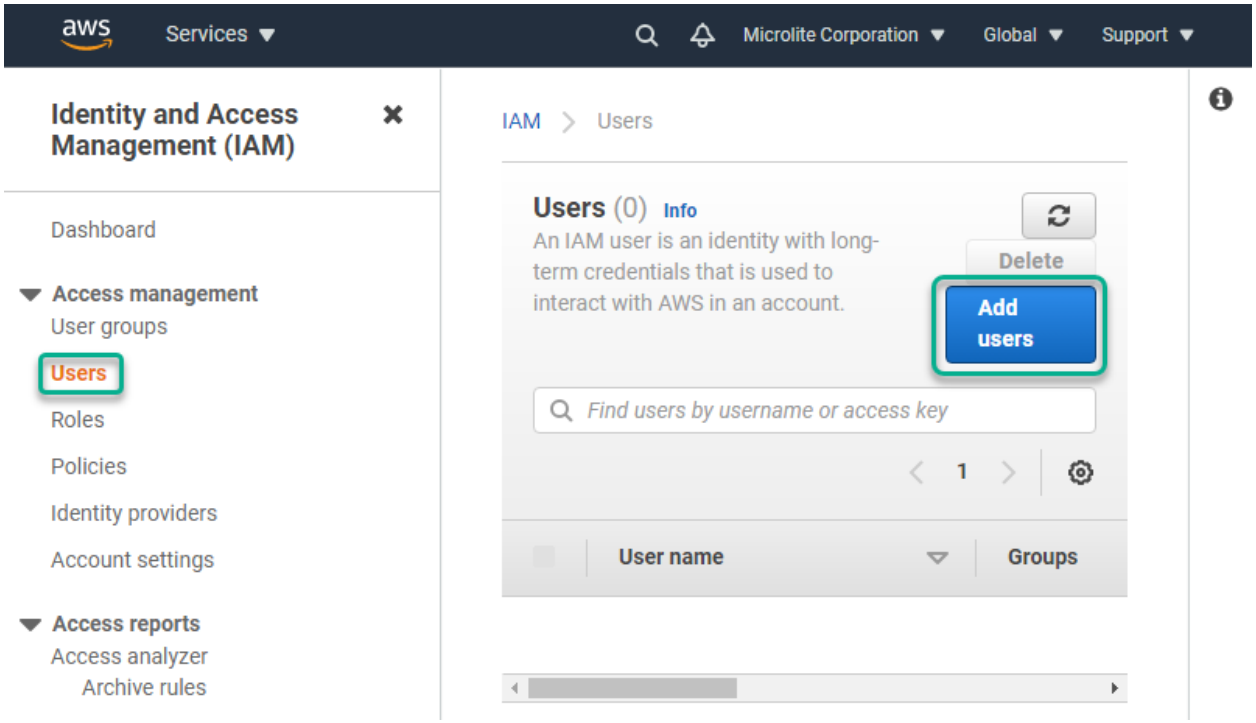


11 The *Bucket Wizard* will confirm the *Bucket Name* and the *Region* by returning to the main list, which will now include the created *Bucket*. You may create any number of *Buckets* in any number of *Regions*.

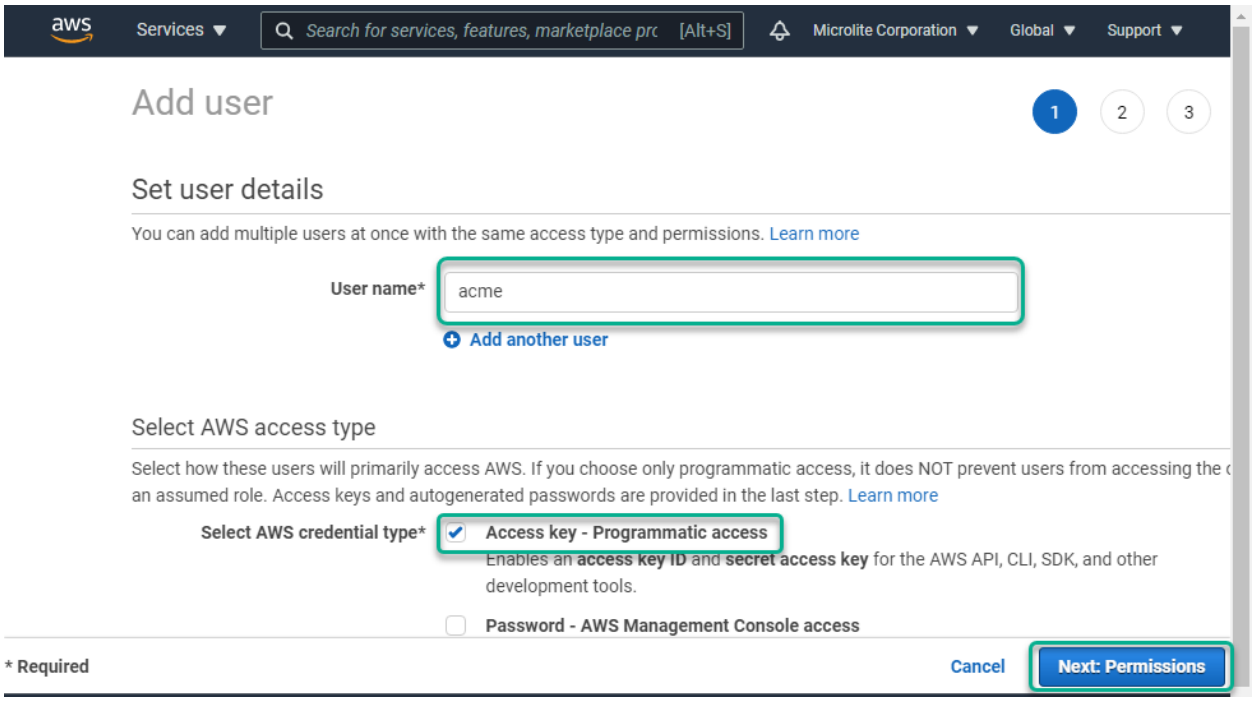
12 Click the *Console Home* icon at the upper left corner of the screen (see icon symbol at right). At the top of the screen, click the ***Search*** icon. Type **IAM** and then select ***IAM*** - *Manage access to AWS resources*, from the available choices.



13 Create a User by clicking on **Users** on the left, then the **Add User** button.

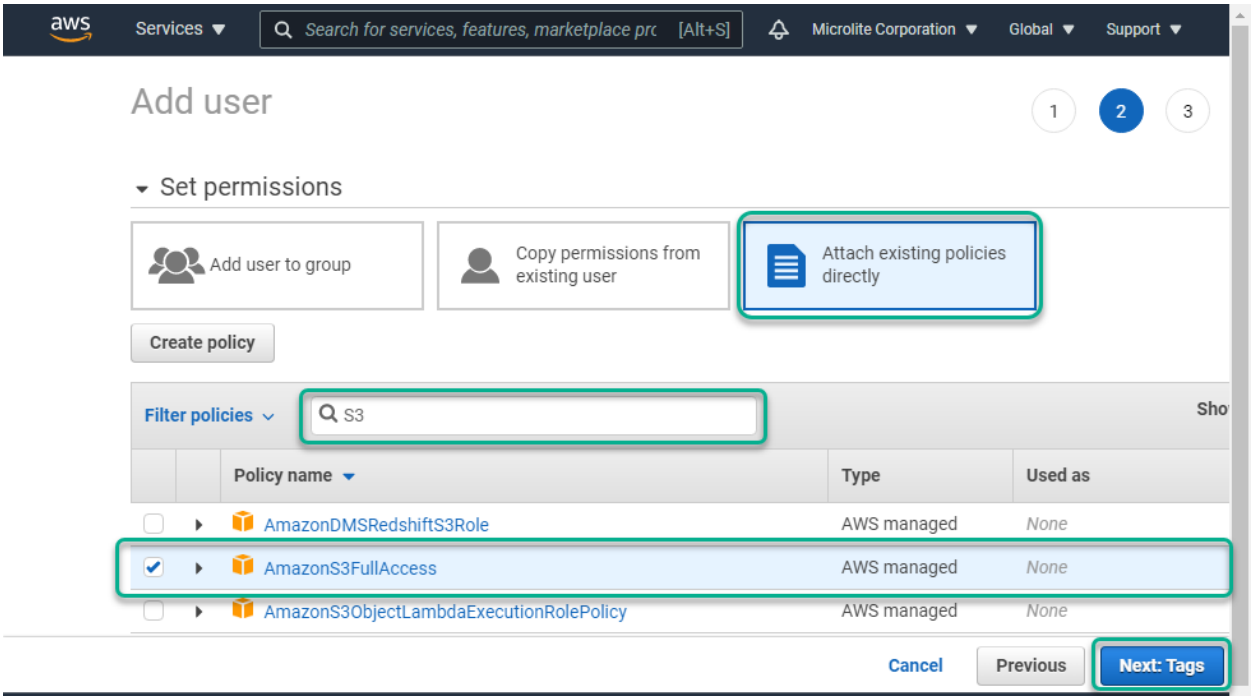


14 Type the *User name*. Under *Select AWS credential* type select "*Access Key - Programatic access*". Click **Next: Permissions**.



15 Select "**Attach existing policies directly**". In the *Filter policies* search bar type **`s3`** to narrow the list of available policies. Then check the **`AmazonS3FullAccess`** policy and click

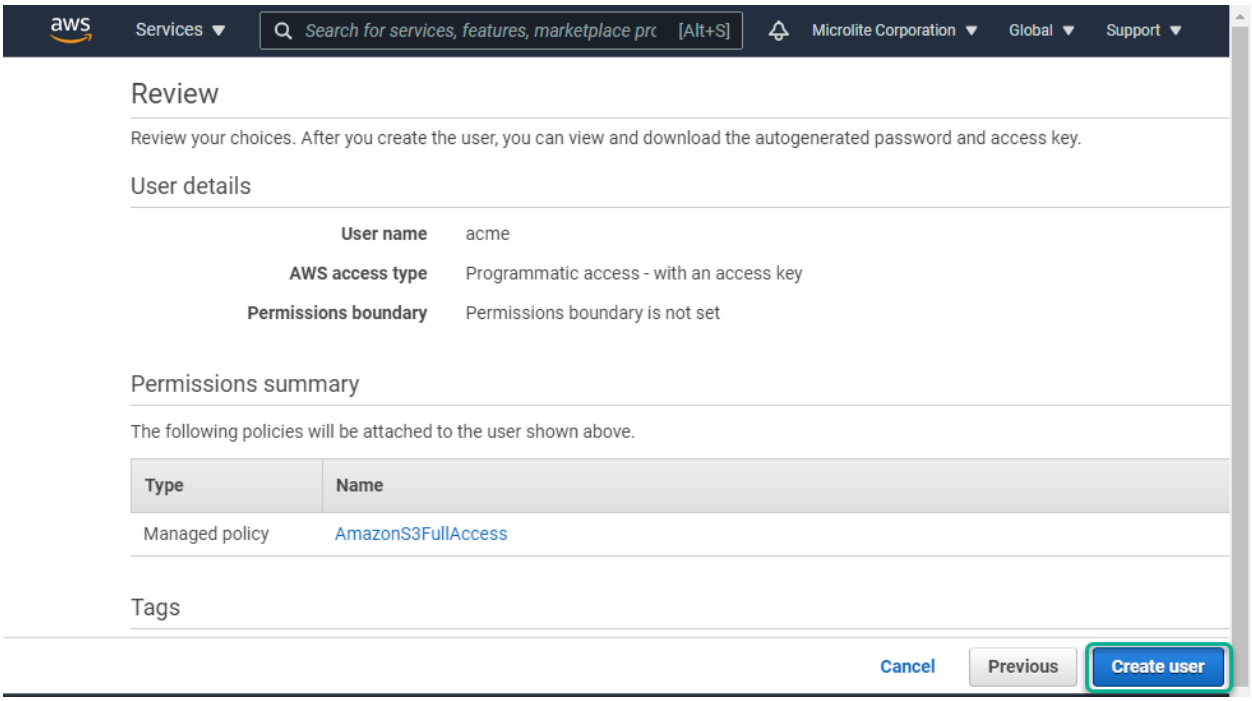
Next: Tags.



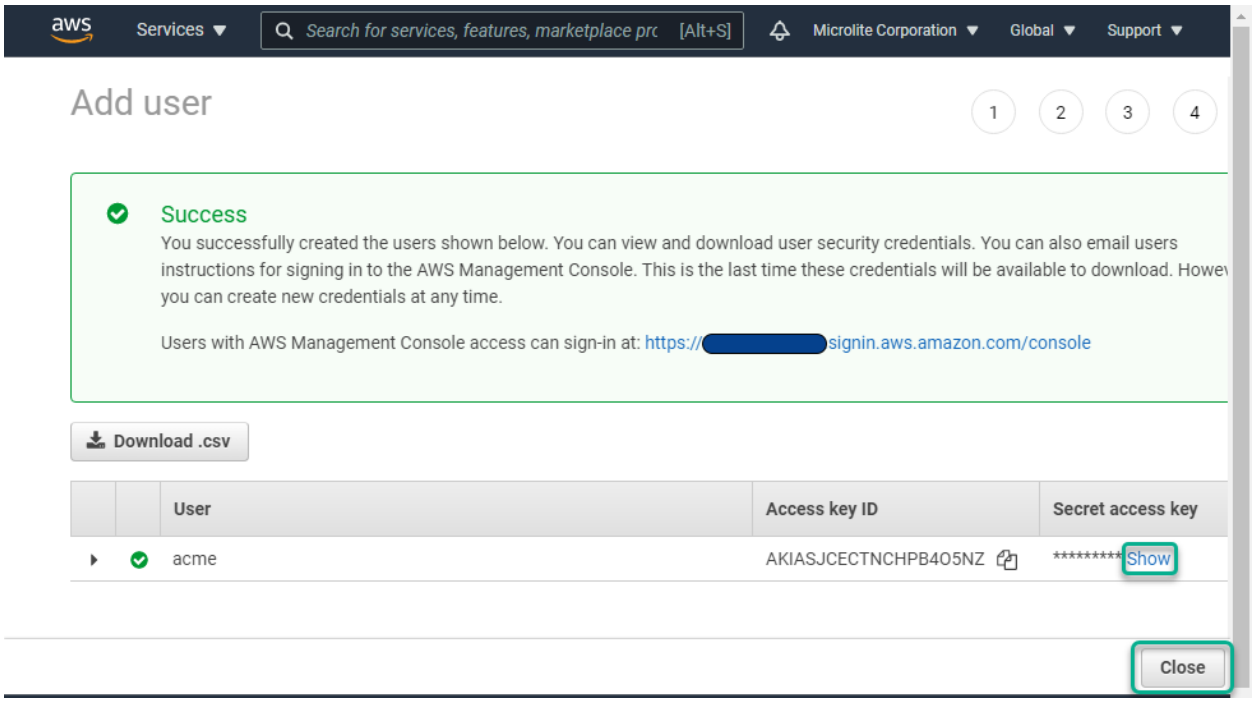
Please note that you may create your own, tighter security policies. Please see “Creating Additional Amazon AWS Security Policies” on page 132 for additional information.

16 No entries are necessary on the Add tags (optional) screen. Ignore this screen and click **Next: Review**.

17 Verify the **User name** and **Managed policy** is correct, then click **Create User**.



18 When the user has been created (acme in the examples shown here), you'll get a screen that allows you to view the *Access Key ID* and, when you click **Show**, the *Secret Key ID*. There is also an option to **download a .CSV** file containing this information.



You **MUST, MUST, MUST** copy or download and **secure these keys**. *The Secret access key* will never be available again. If you need it again and don't have a copy, you must create a new key and replace it in all currently configured servers.

19 Only after the keys have been secured, click **Close** to continue. You'll see the created user, number of active keys, and creation date.

You now have the **Bucket Name**, **Region Name**, **Access Key ID** and **Secret Key ID** you need to place into *BackupEDGE*. The **Region Name** translates to an **Amazon S3 Endpoint** as shown in the table on page 123.

This is all of the setup required to use set up ***Amazon Web Services*** for use with *BackupEDGE*. Using the default security policy, only users with the proper **Access Key ID** and **Secret Key ID** may use *BackupEDGE* to access your data. It is, however, possible to further restrict access by using additional security policies. While not strictly necessary, you may learn more about **Security Policies** on page 132.

Creating Additional Amazon AWS Security Policies

Instead of using the *Default Security Policy*, you may wish to restrict individual *Users* to individual *Buckets* under the Account.

From the **IAM** menu, select **Policies**, then **Create Policy**, then **Create Your Own Policy**. Follow the instructions below, then see "Attaching Specific Security Policies" on page 135.

The first policy and below restricts access to any user to a single *Bucket*. Typically this is used when more than one server is using the same Amazon Account, and individual Bucket security is required.

The second is for access to a second *Bucket* with the same credentials. One possible use would be to create a second *Bucket*, possibly even in another *Region*, accessible via a second *Resource* using the same credentials but a different *Bucket Name*.

The third adds IP Range security to the first policy. Access will only be allowed to a bucket from a single IP address or IP address range. This provides the additional security of requiring the proper credentials AND coming from a specific location in order to have access to the *Amazon Buckets*.

NOTE: The *Version* line and date referenced in the Policies defined below identify a specific *Amazon Policy Version*. Do not attempt to change the date.

SECURITY POLICY WITH SINGLE ACCESSIBLE BUCKET

Please note that you must replace `your_bucket_name` below with the actual bucket name you created at the beginning of this section (our example was `backupedge-acme-uss`). This is done in two places.

Policy Name	`BackupEDGE_S3_Single_Bucket_Access_Policy`
Description	`Restrict BackupEDGE Access to a Single Bucket`

```
{
  "Version":"2012-10-17",
    "Statement": [
    {
      "Effect": "Allow",
      "Action":[
         "s3:ListAllMyBuckets",
         "s3:DeleteBucket"
        ],
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action":[
        "s3:ListBucket"
      ],
      "Resource": [ "arn:aws:s3:::your_bucket_name"]
    },
    {
      "Effect": "Allow",
      "Action":[
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": [ "arn:aws:s3:::your_bucket_name/*"]
    }
  ]
}
```

Please note that you must replace `your_bucket_name` above with the actual bucket name you created at the beginning of this section (our example was `backupedge-acme-uss`). This is done in two places.

SECURITY POLICY WITH TWO ACCESSIBLE BUCKETS

Please note that you must replace `your_bucket_name` and `your_other_bucket_name` below with the actual *Bucket Names* you created at the beginning of this section (our example was `backupedge-acme-uss`). This is done in two places for each *Bucket*.

Policy Name	BackupEDGE_S3_Two_Bucket_Access_Policy
Description	Restrict BackupEDGE S3 Access to Two Buckets

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action":[
         "s3:ListAllMyBuckets",
         "s3:DeleteBucket"
        ],
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action":[
        "s3:ListBucket"
      ],
      "Resource": [ "arn:aws:s3:::your_bucket_name",
                    "arn:aws:s3:::your_other_bucket_name"
      ]
    },
    {
      "Effect": "Allow",
      "Action":[
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": [ "arn:aws:s3:::your_bucket_name/*",
                    "arn:aws:s3:::your_other_bucket_name/*"
      ]
    }
  ]
}
```

SECURITY POLICY WITH IP ADDRESS / RANGE LIMITATION

This *Policy* allows access to one *Bucket* only from a specific IP address or sub-net range.

Policy Name	BackupEDGE_S3_IP_Range_Access_Policy
Description	Restrict BackupEDGE S3 Bucket Access to IP Range

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action":[
         "s3:ListAllMyBuckets",
         "s3:DeleteBucket"
        ],
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "XXX.XXX.XXX.0/24"
        }
      },
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action":[
        "s3:ListBucket"
      ],
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "XXX.XXX.XXX.0/24"
        }
      },
      "Resource": [ "arn:aws:s3:::your_bucket_name"]
    },
    {
      "Effect": "Allow",
      "Action":[
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "XXX.XXX.XXX.0/24"
        }
      },
      "Resource": [ "arn:aws:s3:::your_bucket_name/*"]
    }
  ]
}
```

Replace `your_bucket_name` in the example above the actual bucket name you created, and replace `XXX.XXX.XXX.0/24` with either a full subnet like `192.174.123.0/24` or a single address like `192.174.123.123` as appropriate. This occurs in three places in the *Policy*.

Either give *Policies* your own name in the *Policy Name* field, or cut and paste one from the manual above. Cut and paste one of the three security policies, then change *Bucket Names* and IP addresses as appropriate.

An unlimited number of *Policies* may be created within *Amazon S3*, but the default *Policy* or one of the three above are sufficient for most users.

Attaching Specific Security Policies

To attach a *Security Policy* of your own creation...

1 From the **IAM** menu, select **Users**.

2 Click on the appropriate **User name** (not the checkbox next to it).

3 Click **Add Permissions**, then **Attach existing policies directly**.

4 Type enough of the **Policy Type** name to see it, or scroll down until you see it.

5 Check the selection box and click **Next: Review**.

6 Click **Add permissions**.

The final step is to detach the **Full Access** policy...

1 From the **IAM** menu, select **Users**.

2 Click on the appropriate **User name** (not the checkbox next to it).

3 Click on the **AmazonS3FullAccess - AWS Managed Policy** to open it.

4 Click **Detach Policy** to remove it.

13.14 - Using Google Cloud Storage

To use *BackupEDGE* with the ***Google Cloud Storage*** (https://cloud.google.com/storage), a working knowledge of *Google* and ***Google Cloud Storage*** is expected. There are initial setup steps required on both the *Google* web site and via the *EDGEMENU BackupEDGE* user interface.

Google Cloud Storage is capable of single-location-or multi-location hosting in *Regions* around the world.

NOTE: The `[Test URL]` command in `Define Resources` takes a very long time to run under *BackupEDGE 03.00.03 build 3* and earlier. It is safe to ignore this test and run "`Initialize Media`" when setting up an *S3CLOUD Resource* with ***Google Cloud Storage***.

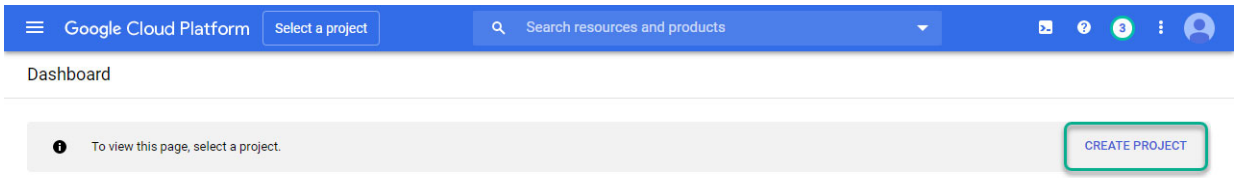
Google Cloud Storage Initial Setup[1]

The following information from ***Google Cloud Storage*** is required to create an *S3CLOUD Resource*...

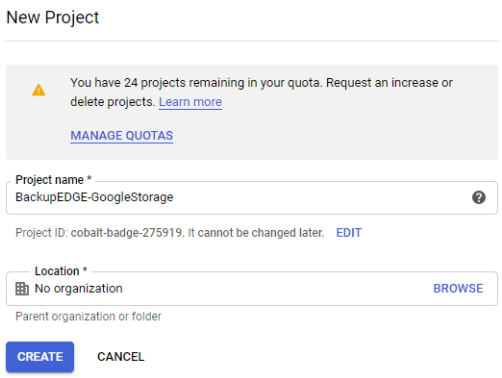
- *S3 Bucket Name*.
- *S3 Access Key ID*.
- *S3 Secret Access Key*.
- *S3 Cloud Endpoint*. This is always the same.

For *EDGEMENU*, please see "Create a BackupEDGE S3CLOUD Resource" on page 118.

On initial setup, the users logs into the ***Google Cloud Storage*** *URL* and clicks **Go to Console**.

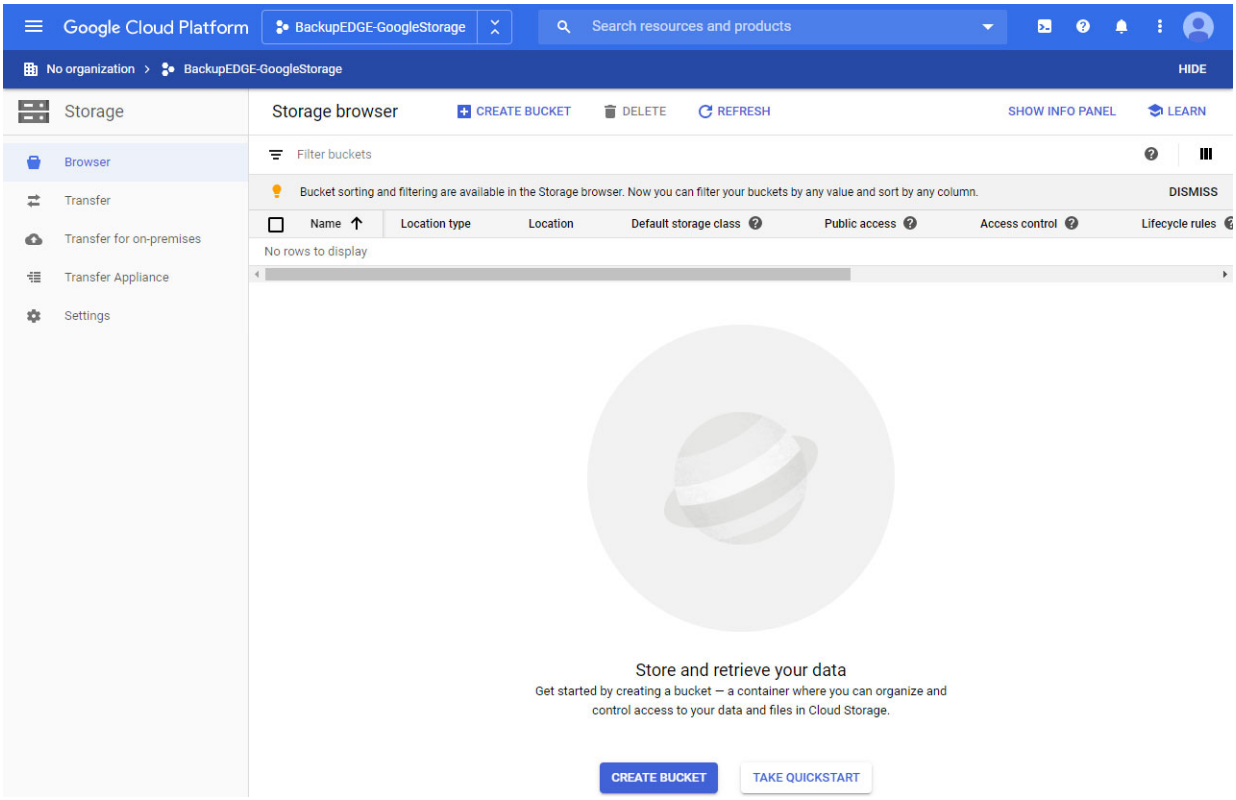


- Click *Create Project*. Note that if there are already *Projects* in your ***Google Cloud Storage*** account, one of them will be shown in the upper left of the screen where "`Select a Project`" is shown above. You may click this to display a dropdown menu allowing you to select a current project or click "`Create Project`" to create another new project.

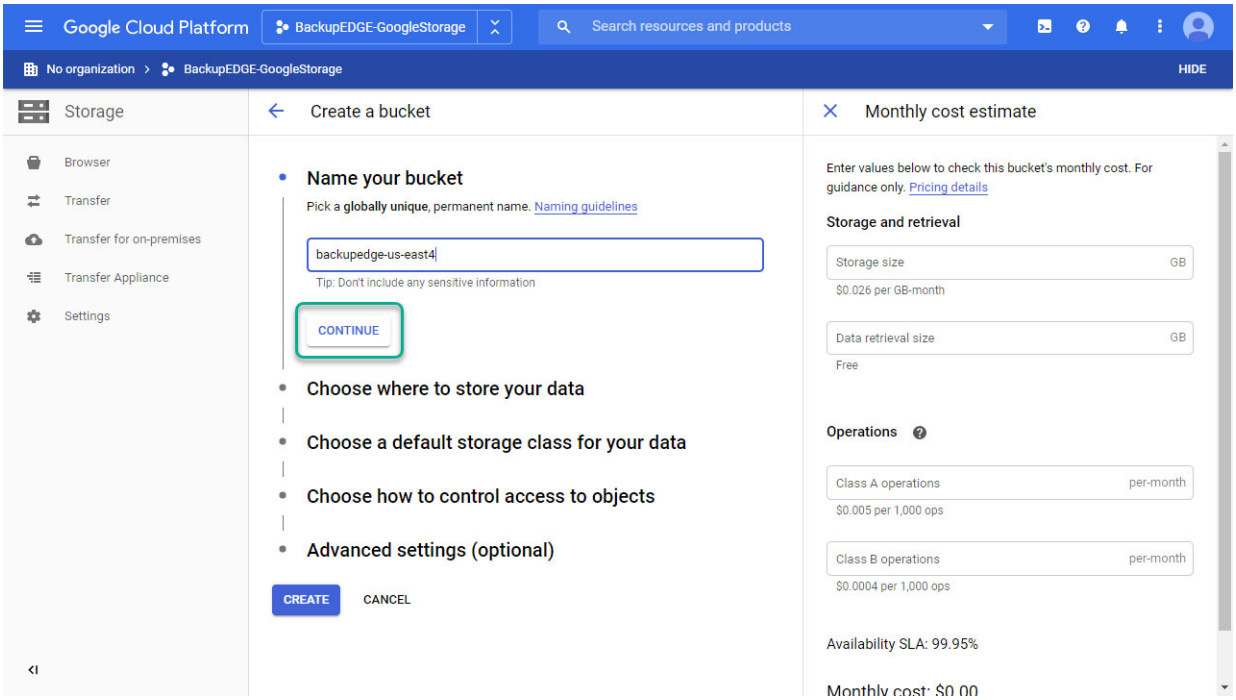


1. Google may change the functionality of their web-based management system without notice. The exact steps described here may also change in this instance.

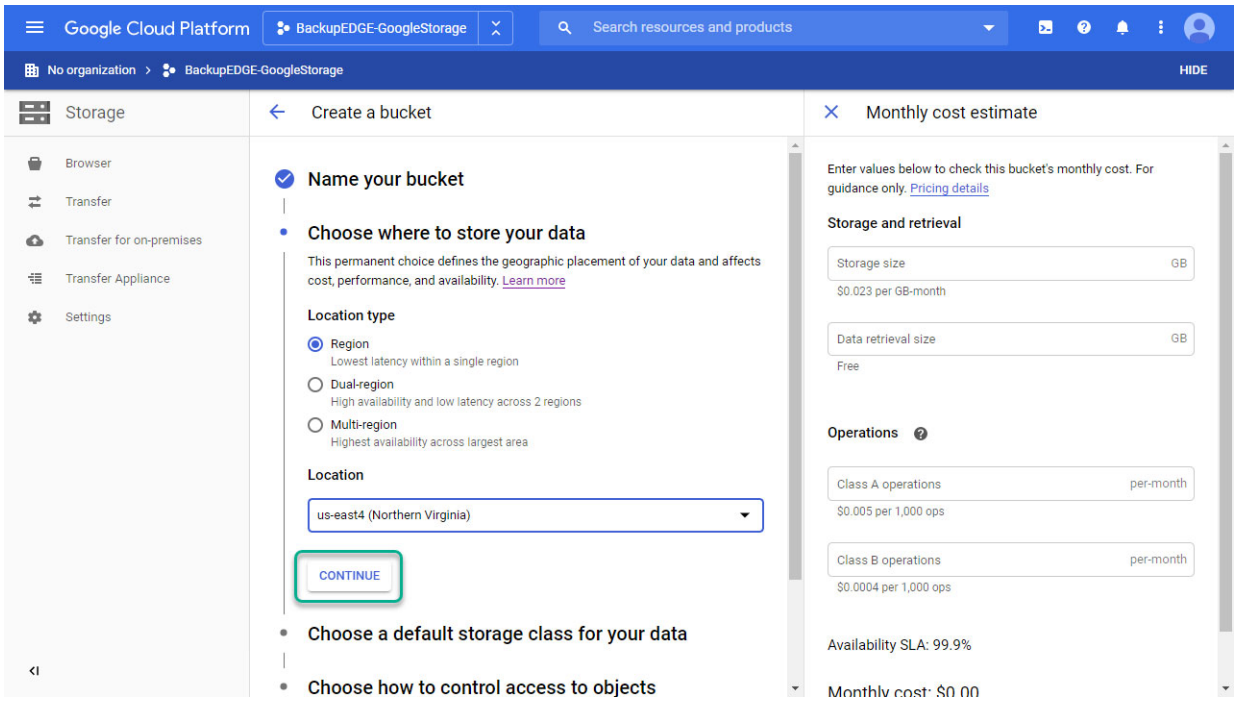
- Type the name of the project (example above is `BackupEDGE-GoogleStorage` and click `CREATE`.
- Click the *Menu Icon* in the upper left corner of the screen (see icon symbol at right). Scroll down the list of items on the left and select **Storage**. (A "Learn" panel may appear on the right side of the screen. You may close it.)



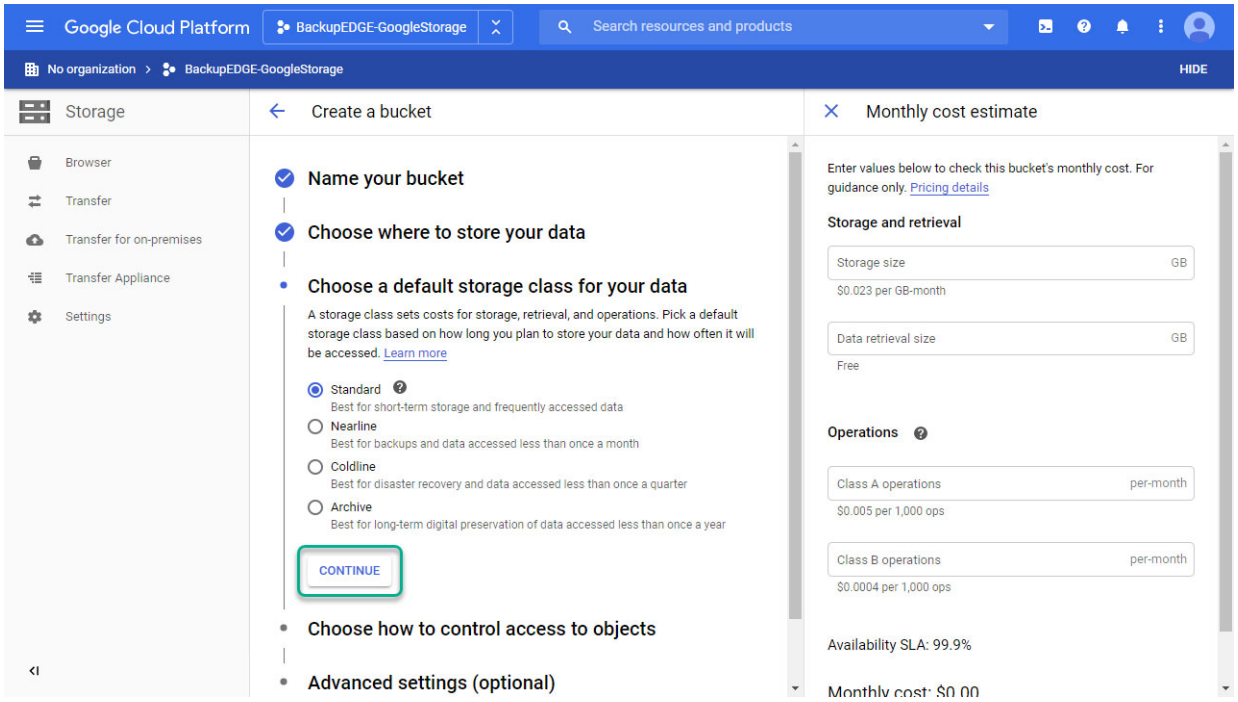
- Click **Create Bucket**. Type a unique bucket name as shown below and click **`Continue`** (not **`Create`**).



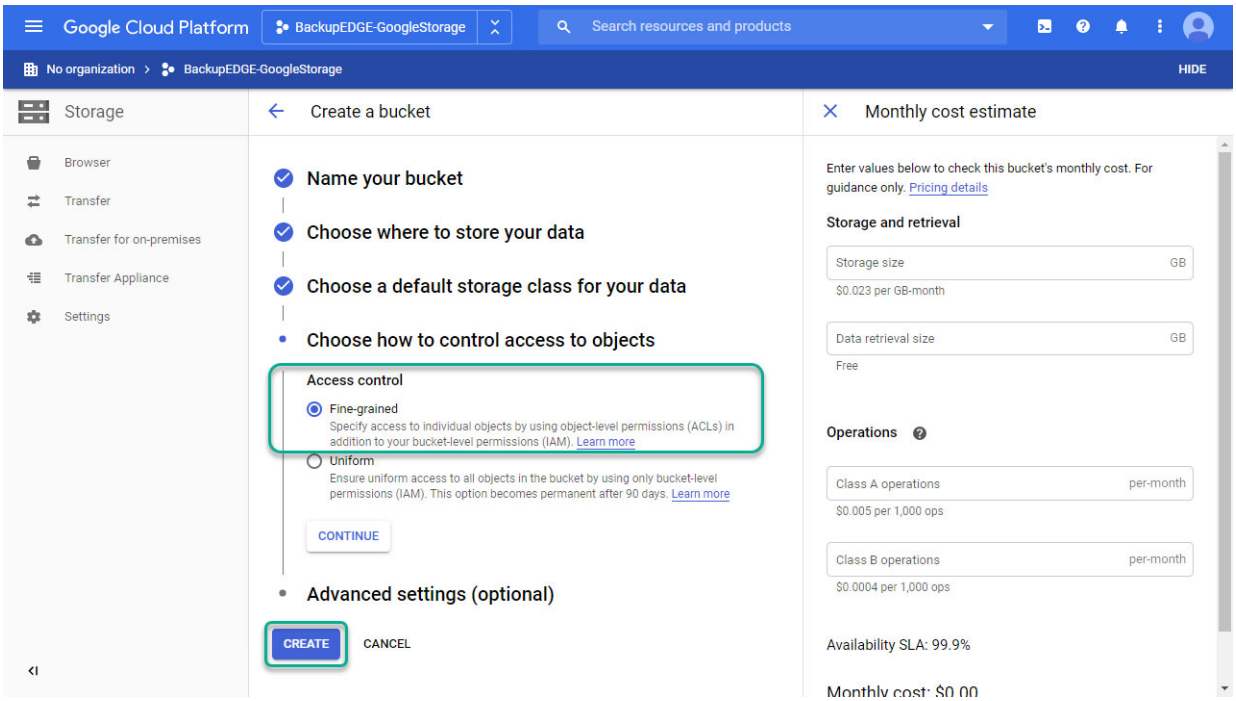
- Select **`REGION`**, as the **Location type**, then select the **Location** (from the drop-down list) in which to store your data. Typically the region nearest you is chosen to reduce latency, but any **Location** may be selected. It is also possible to select the **`Dual-region`** or **`Multi-region`** **Location type**, then select two or more regions where your data will be automatically replicated for redundancy purposes. This is at a higher cost per megabyte, which may be estimated on the right side of the web page. In this example we will choose the `us-east4 (Northern Virginia)` **Location**. Choose the location and click **`Continue`** (not **`Create`**).



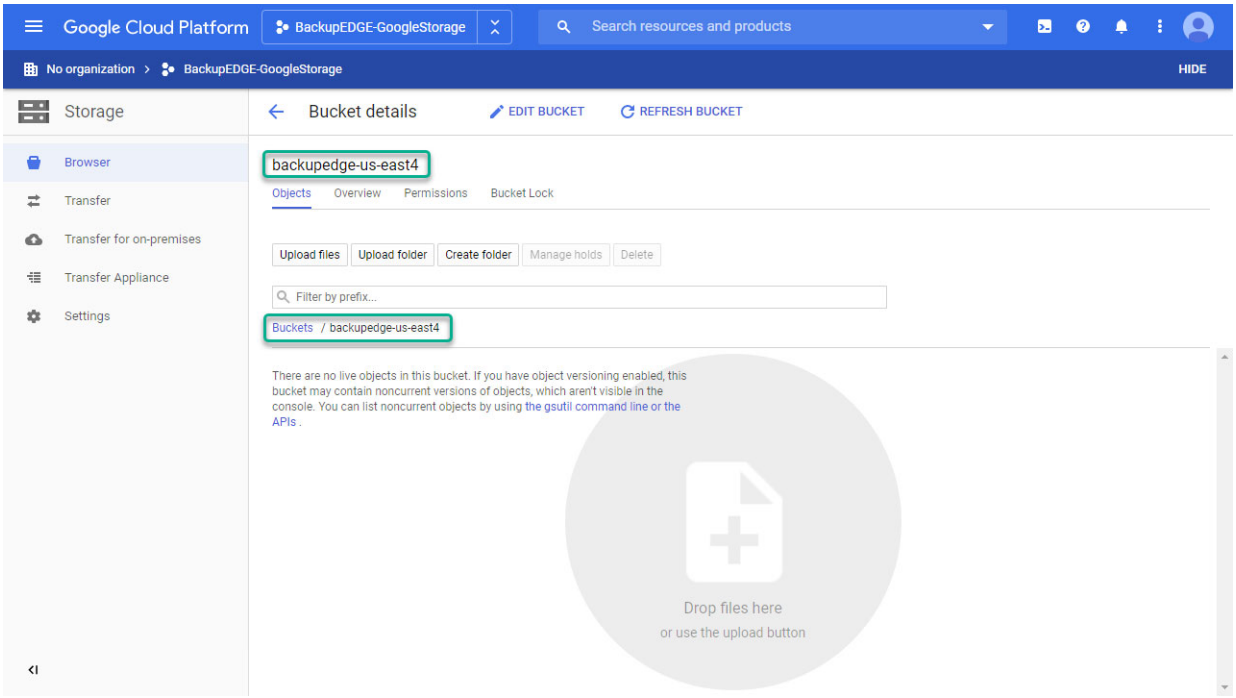
- Choose **Standard** as the Default Storage Class and click **`Continue`** (not **`Next`**). **No other storage classes are supported!**



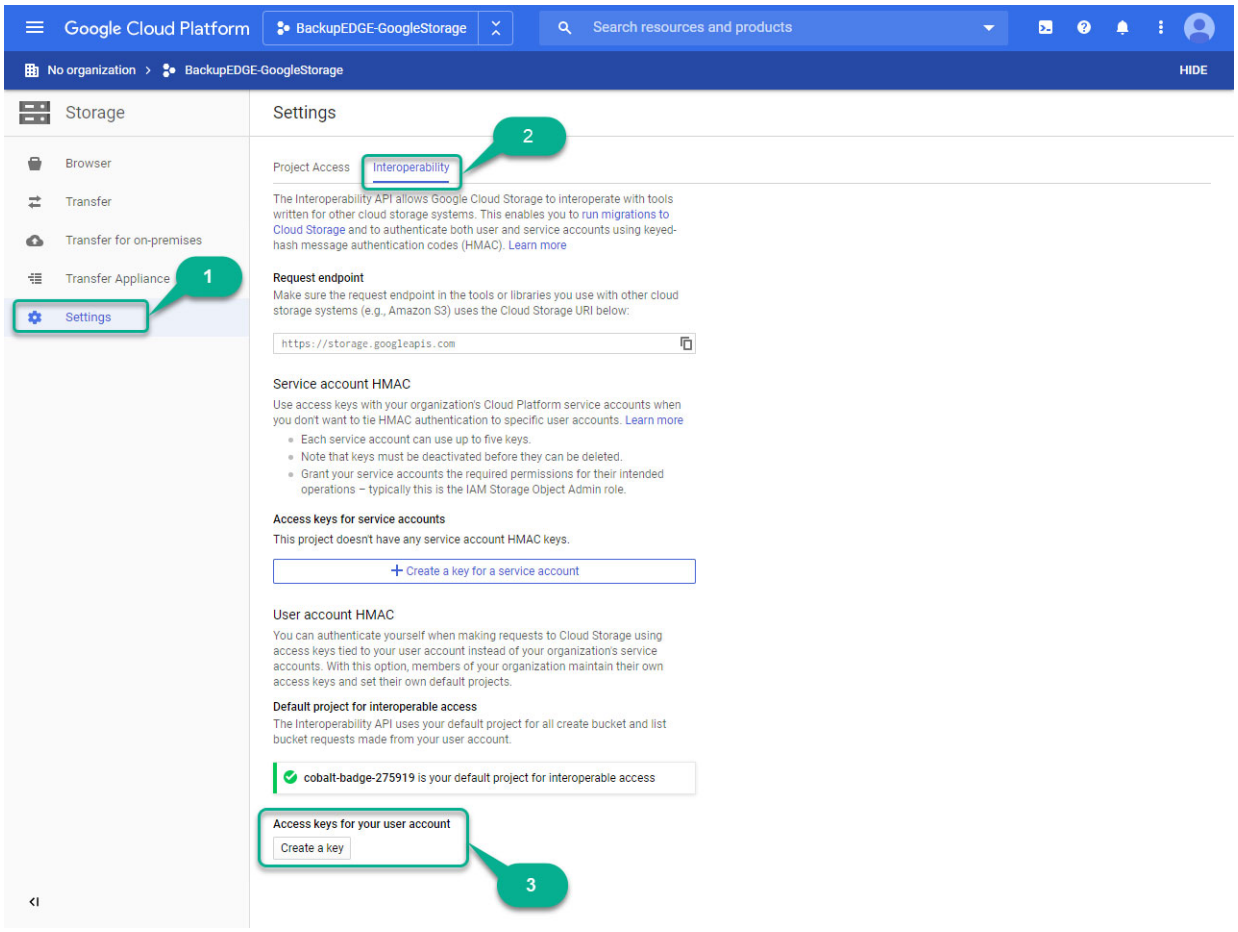
- Under **Choose how to control access to objects**, select **`Fine-grained`**. As no **Advanced settings** are required, you may now click **`Create`** to create the bucket.



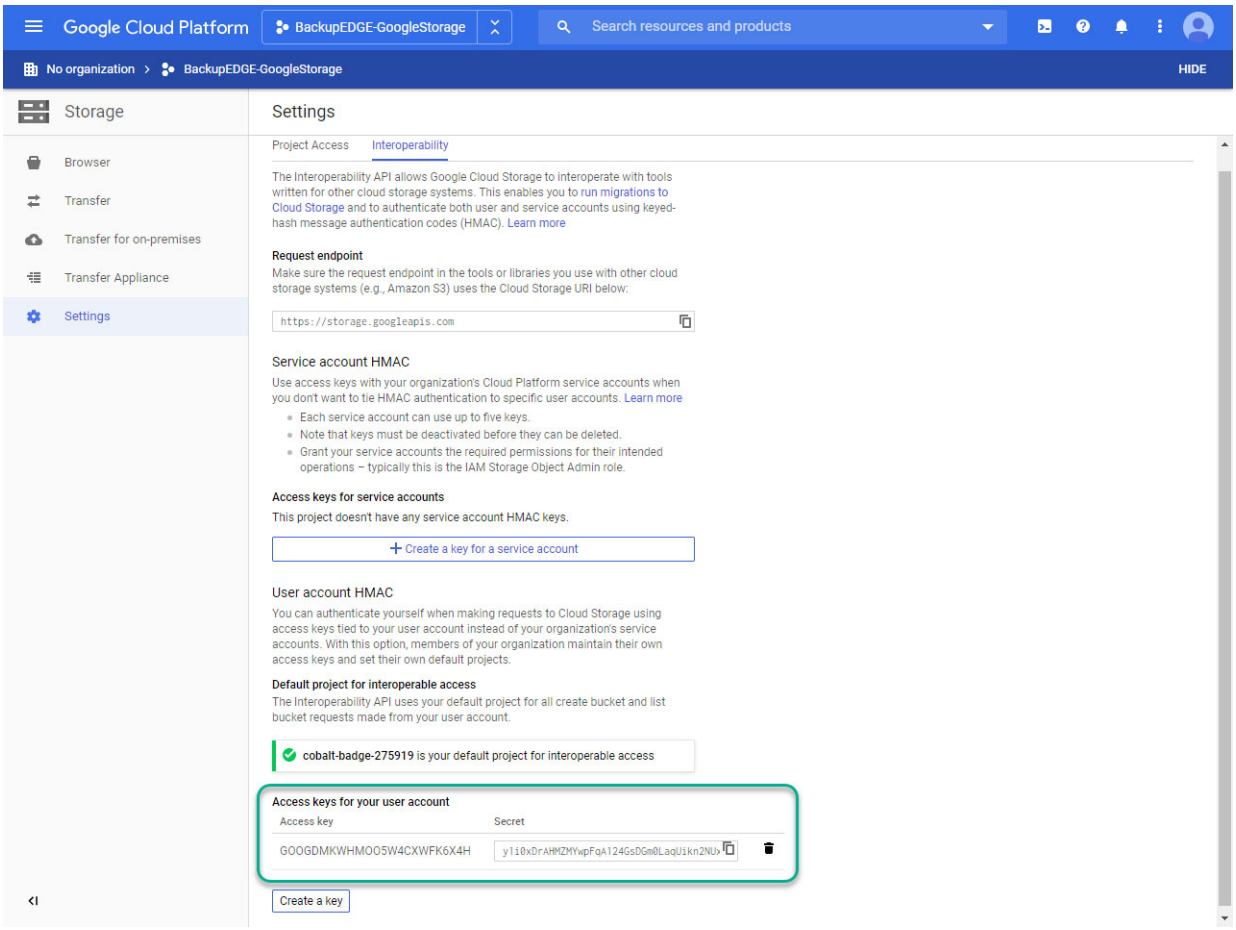
- The **Bucket Browser** will be displayed. The new bucket, and any future buckets you create, will be shown.



- Click the *Menu Icon* in the upper left corner of the screen (see icon symbol at right). Scroll down the list of items on the left and select **Storage**., then **Settings**, then **Interopability**, then **Create a key**.



- The keys will be generated. You'll see the **Access Key** and the **Secret Key** at the bottom web page.



You **MUST, MUST, MUST** copy or download and **secure these keys**. *The Secret Key ID* will never be available again. If you need it again and don't have a copy, you must create a new key and replace it in all currently configured servers.

You may now **Sign Out** of the *Google Cloud Platform*. You will need the **Bucket** name, **Access Key**, and **Secret Key**, along with the default Endpoint from the table on the next page, to create a ***Resource*** in *EDGEMENU*.

Google Cloud Storage Regions and Endpoints

Google has a single storage *Endpoint* for all *Regions* around the world.

Google tracks and bills the user for this service, not Microlite Corporation. Pricing can be found at: (https://cloud.google.com/storage/pricing).

Here is a list of the available *Regions* where *Buckets* may be created. The *Endpoint* is essentially the access address of the servers in the *Region*.

Google Cloud Storage Region	*Location*	*Endpoint*
North America		
northamerica-northeast1	Montréal, Quebec, CA	storage.googleapis.com
us-central1	Council Bluffs, IA, USA	
us-east1	Moncks Corner, SC, USA	
us-east4	Ashburn, VA, USA	
us-west1	The Dalles, OR, USA	
us-west2	Los Angeles, CA USA	
us-west3	Salt Lake City, UT USA	
us-west4	Not Known	
South America		
southamerica-east1	São Paulo, Brazil	storage.googleapis.com
Europe		
europe-north1	Hamina, Finland	storage.googleapis.com
europe-west1	St. Ghislain, Belgium	
europe-west2	London, UK	
europe-west3	Frankfurt, Germany	
europe-west4	Eemshaven, Netherlands	
europe-west6	Zurich, Switzerland	
Asia		
asia-east1	Changhua County, Taiwan	storage.googleapis.com
asia-east2	Hong Kong	
asia-northeast1	Tokyo, Japan	
asia-northeast2	Osaka, Japan	
asia-northeast3	Seoul, South Korea	
asia-south1	Mumbai, India	
asia, southeast1	Jurong West, Singapore	
Australia		
australia-southeast1	Sydney, Australia	storage.googleapis.com

13.15 - Using Wasabi Hot Cloud Storage

To use *BackupEDGE* with the ***Wasabi Hot Cloud Storage*** (https://wasabi.com), a working knowledge of *BackupEDGE* and ***Wasabi Hot Cloud Storage*** is expected. There are initial setup steps required on both the *Wasabi* web site and via the *EDGEMENU BackupEDGE* user interface.

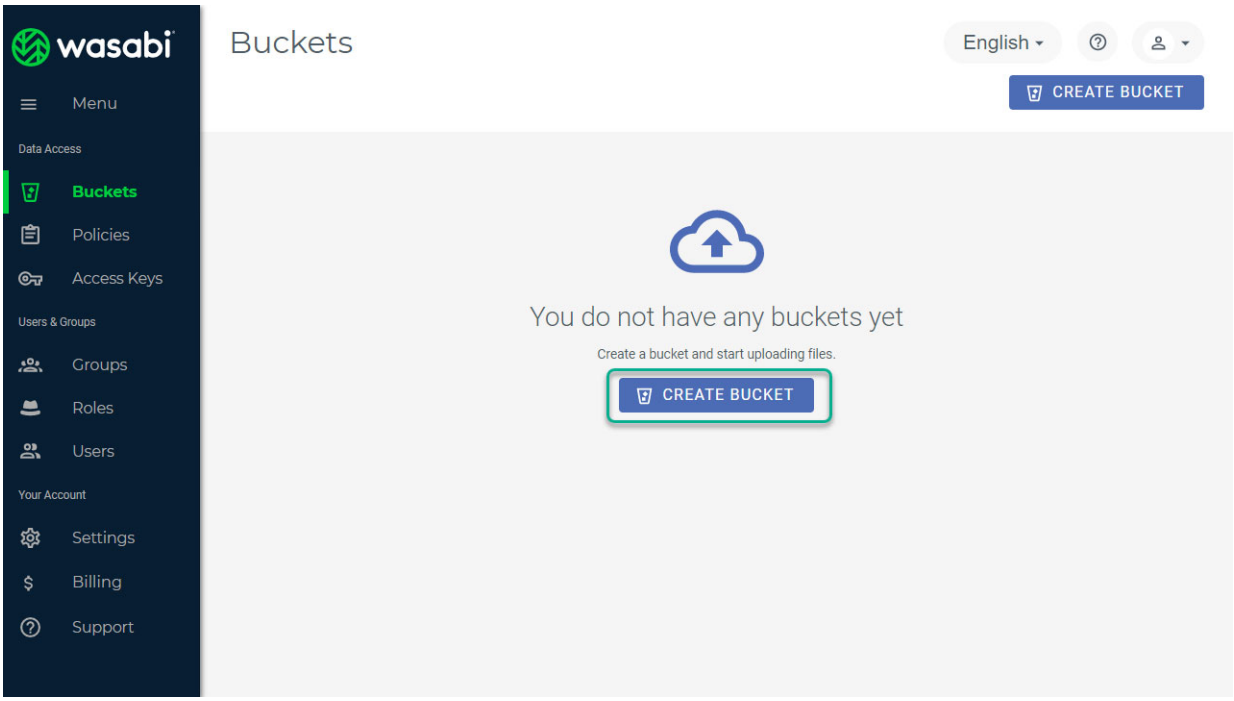
Wasabi Hot Cloud Storage Initial Setup[1]

The following information from ***Wasabi Hot Cloud Storage*** is required to create an *S3CLOUD Resource*...

- *S3 Bucket Name*.
- *S3 Access Key ID*.
- *S3 Secret Access Key*.
- *S3 Cloud Endpoint*.

For *EDGEMENU*, please see “Create a BackupEDGE S3CLOUD Resource” on page 118.

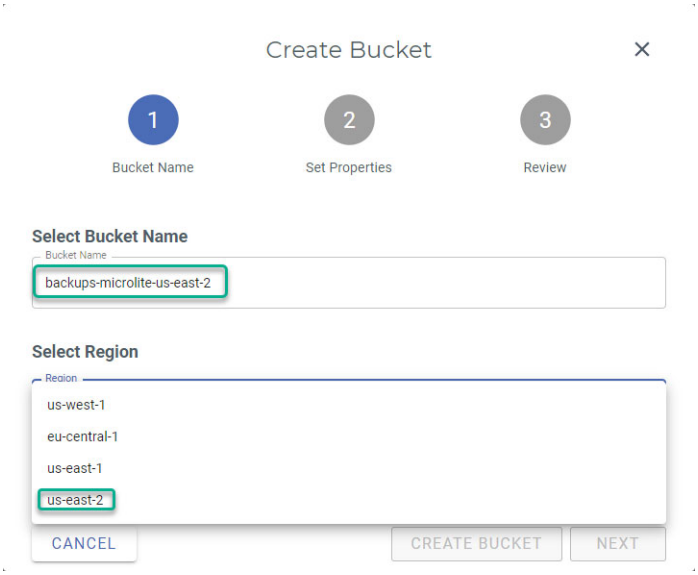
On initial setup, the user logs into the ***Wasabi Hot Cloud Storage*** *URL* (https://console.wasabisys.com). First time users will see the following...



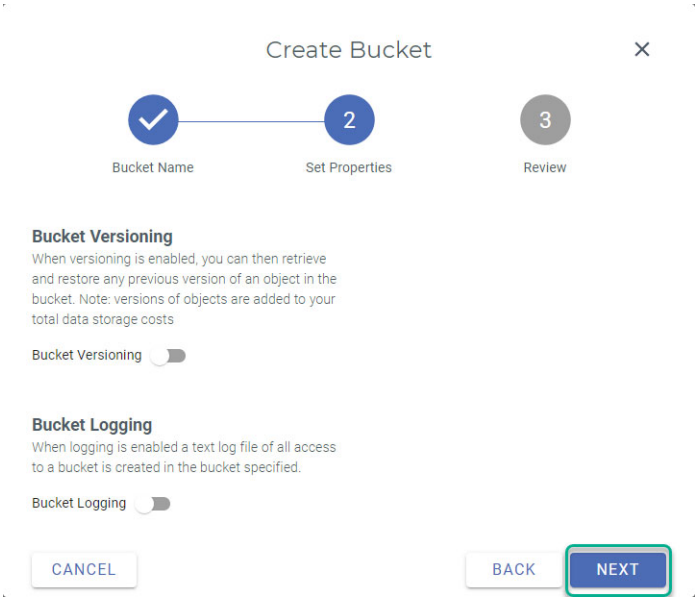
If one or more *Buckets* already exist, the list of *Buckets* will be shown.

1. Wasabi may change the functionality of their web-based management system without notice. The exact steps described here may also change in this instance.

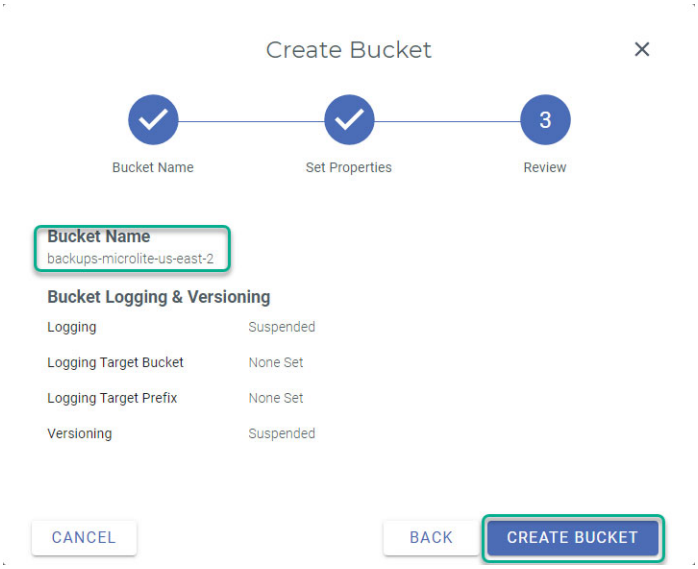
- Click *Create Bucket*. Type a unique *Bucket Name*. This name must be unique for all of *Wasabi*. You'll be notified if a *Bucket* with an identical name already exists. Select a *Region* (see "Wasabi Hot Cloud Storage Regions and Endpoints" on page 148) and Click *Next*. (You must match the *Endpoint* later).



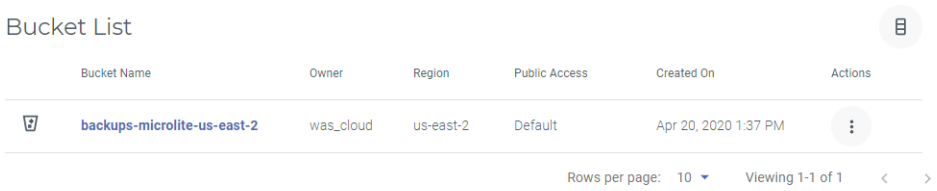
- Do not change the *Create Bucket* properties as shown below. Simply click *Next*.



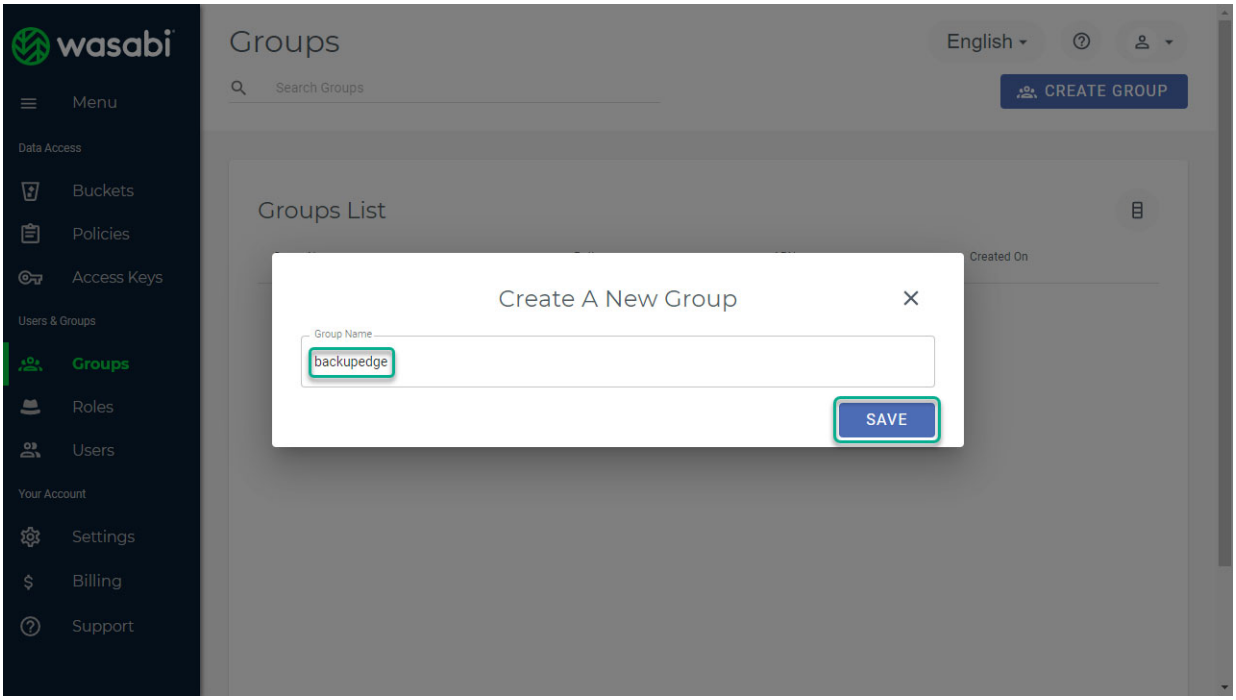
- Review the *Create Bucket* settings and click *Next*.



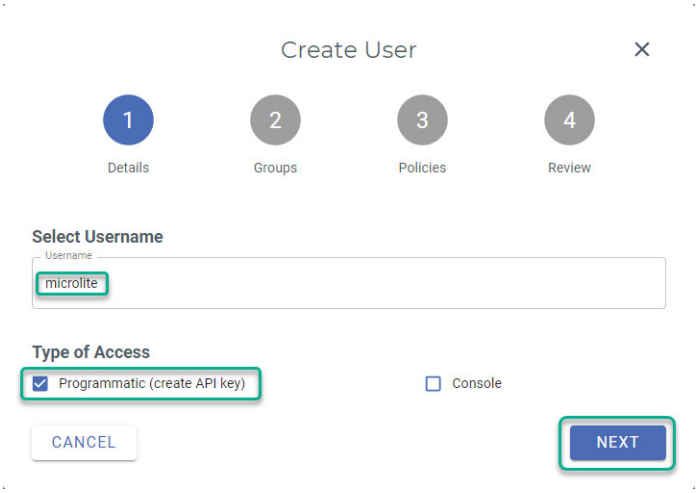
- When one or more *Buckets* have been successfully created, you'll see them displayed like this:



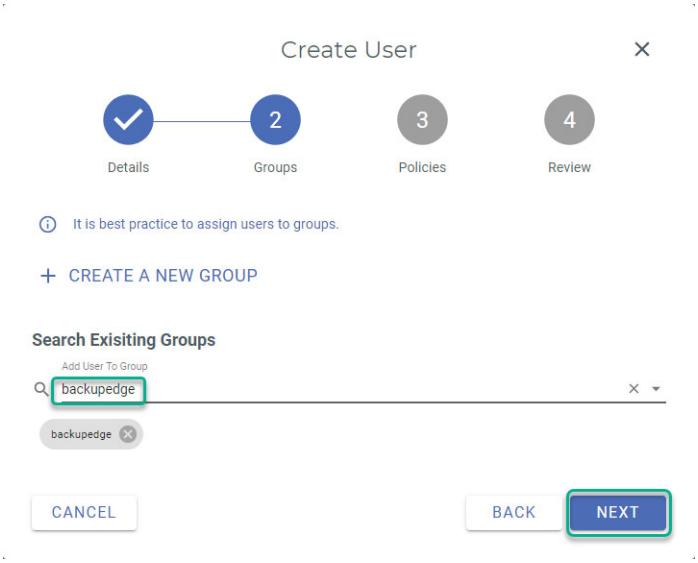
- Click *Groups* on the left-side menu, then click *CREATE GROUP*. Type a *Group Name* and click *Save*.



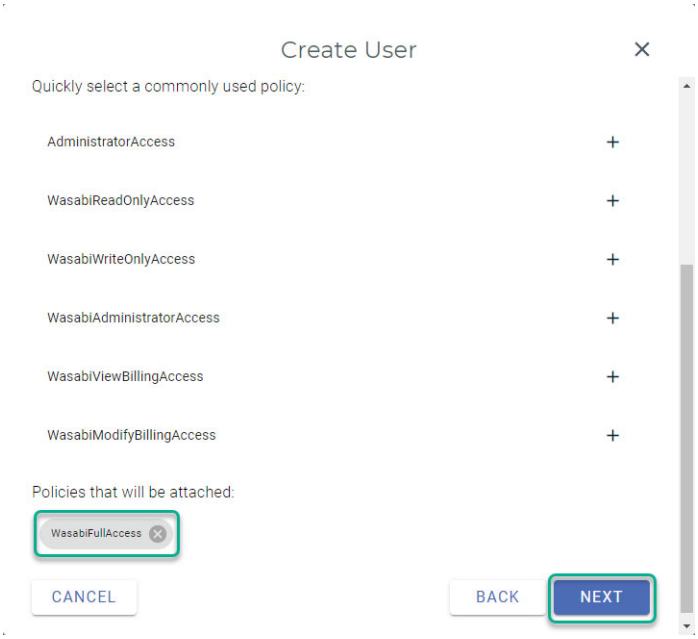
- Click *Users* on the left-side menu, then click *CREATE USER*.



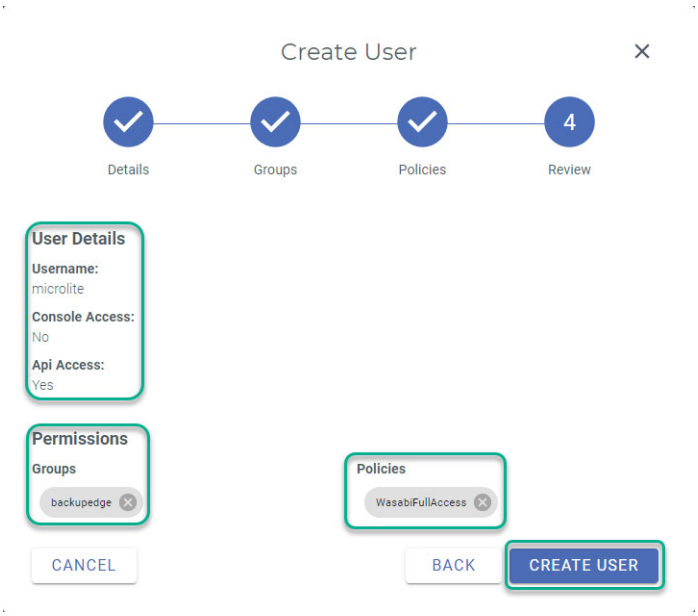
- Type a *Username* and select *Programmatic (create API key)* as shown above and click *Next*.
- The the *Group Name* you created earlier (or any other *Group Name* you've created) and click *Next*.



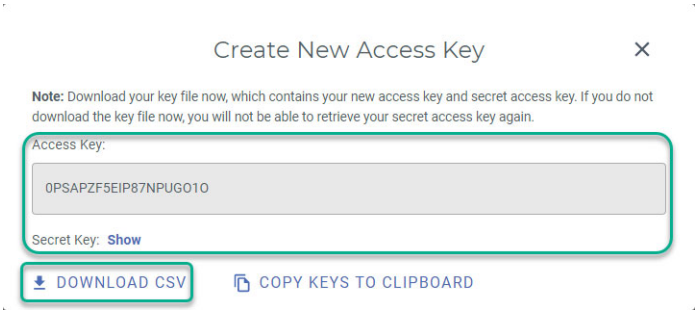
- Select the *Wasabi Full Access* Policy as shown below and click *Next*.



- Review the *Create User* information as shown below and click *CREATE USER*.



- This will add the new User to Wasabi and create a unique *Access Key* and *Secret Key*.



- You **MUST, MUST, MUST** copy or download and **secure these keys**. *The Secret Key ID* will never be available again. If you need it again and don't have a copy, you must create a new key and replace it in all currently configured servers.
- Only after the keys have been secured, click the **X** to close and continue. You'll see the created user, number of active keys, and creation date.

You now have the **Bucket Name**, **Region Name**, **Access Key ID** and **Secret Key ID** you need to place into *BackupEDGE*. The **Region Name** translates to an **Wasabi Hot Cloud Storage Endpoint** as shown in the table below.

Wasabi Hot Cloud Storage Bucket Policies

Wasabi has definable bucket policies in addition to the Full Access Policy shown previously. The Wasabi Management Console User Guide better defines those policies.

Wasabi Hot Cloud Storage Quotas

Wasabi has pricing defined in *Terabytes per month* (`TB/m`). *BackupEDGE Resource* quotas may be set as desired, but for typical single server use should be defined as `1TB`, `2TB`, `3TB` etc.

Wasabi Hot Cloud Storage Regions and Endpoints

Wasabi currently has a four storage *Endpoints*.

Wasabi tracks and bills the user for this service, not Microlite Corporation. Pricing can be found at: (https://wasabi.com/pricing/).

Here is a list of the available *Regions* where *Buckets* may be created. The *Endpoint* is essentially the access address of the servers in the *Region*.

Wasabi Cloud Storage Region	*Wasabi Cloud Storage Endpoint.*
Eastern United States (us-east-1)	s3.us-east-1.wasabisys.com[a]
Eastern United States (us-east-2)	s3.us-east-2.wasabisys.com
Central United States (us-central-1)	s3.us-central-1.wasabisys.com
Western United States (us-west-1)	s3.us-west-1.wasabisys.com
Central European Union (eu-central-1)	s3.eu-central-1.wasabisys.com
Western Europe (London)	s3.eu-west-1.wasabisys.com
Asia Pacific Tokyo (ap-northeast-1)	s3.ap-northeast-1.wasabisys.com
Asia Pacific Osaka (ap-northeast-2)	s3.ap-northeast-2.wasabisys.com

a. The legacyendpoint name `s3.wasabisys.com` may also be used.

NOTE: Access to the Wasabi Hot Cloud Storage Tokyo *Region* (ap-northeast-1) is currently only available to NTT Communication (NTT Com) customers that obtain the service from NTT Com as part of the NTT Com Enterprise Cloud service. Please contact Wasabi or NTT for more information.

Wasabi and FTP / FTPS Backups

NOTE: Wasabi FTPS support is Region-dependent.

Wasabi has the unique ability to allow FTP/FTPS (FTPS is recommended) backups through *Backup**EDGE***. The credentials required are the *account login name* (known as the *root account* on *Wasabi*), the *account login password*, and a *Bucket Name*.

```
+ BackupEDGE Resource Information ------------------------------------------+
|- General Resource Information ------------------------------------------- |
|Resource Type       URL Resource                                           |
|Resource Name       [url0              ] Change as appropriate             |
|Description         [FTP Resource - Wasabi       ]                         |
|Changer Assoc       [Standalone Device]                                    |
|Interface           [Other      ]                                          |
|                                                                           |
|- URL Resource Information ----------------------------------------------- |
|Protocol            [FTPS (FTP Data+Ctrl via SSL)] [Test URL]              |
|Machine             [s3.us-east-1.wasabisys.com  ] [ ] Lazy Reclamation    |
|Directory           [/backupedge-microlite/ftpbackups                    ] |
|Username            [was_cloud@microlite.com     ]                         |
|Password            [**********                  ]                         |
|URL                 ftps://s3.us-east-1.wasabisys.com/backupedge-microlite/ftp|
|- Default Backup Properties ---------------------------------------------- |
|Quota               [1T          ] [S] Compression Level  [5]              |
|Edge Block Size     [64          ] [Y] Double Buffering                    |
|[Next]                              [Prev]                          [Cancel]|
+---------------------------------------------------------------------------+
```

The *Machine* name is the same as the *Endpoint* of the *Region* where the *Bucket* was created.

The Directory is a combination of the *Bucket Name* you've created, and a storage directory (in our example *ftpbackups*). You must use an FTP client or the command line `ftp` program, manually log into the *Wasabi* server (*Machine*) using the *root account* credentials, change directories into the *Bucket Name*, them make a new blank directory for your FTP/FTPS backups.

13.16 - Using Backblaze B2

NOTE: Requires *Backup**EDGE** 03.04.02 build 1* and later.

To use *Backup**EDGE*** with the ***Backblaze B2*** (https://www.backblaze.com), a working knowledge of *Backup**EDGE*** and ***Backblaze B2*** is expected. There are initial setup steps required on both the ***Backblaze B2*** web site and via the *EDGEMENU Backup**EDGE*** user interface.

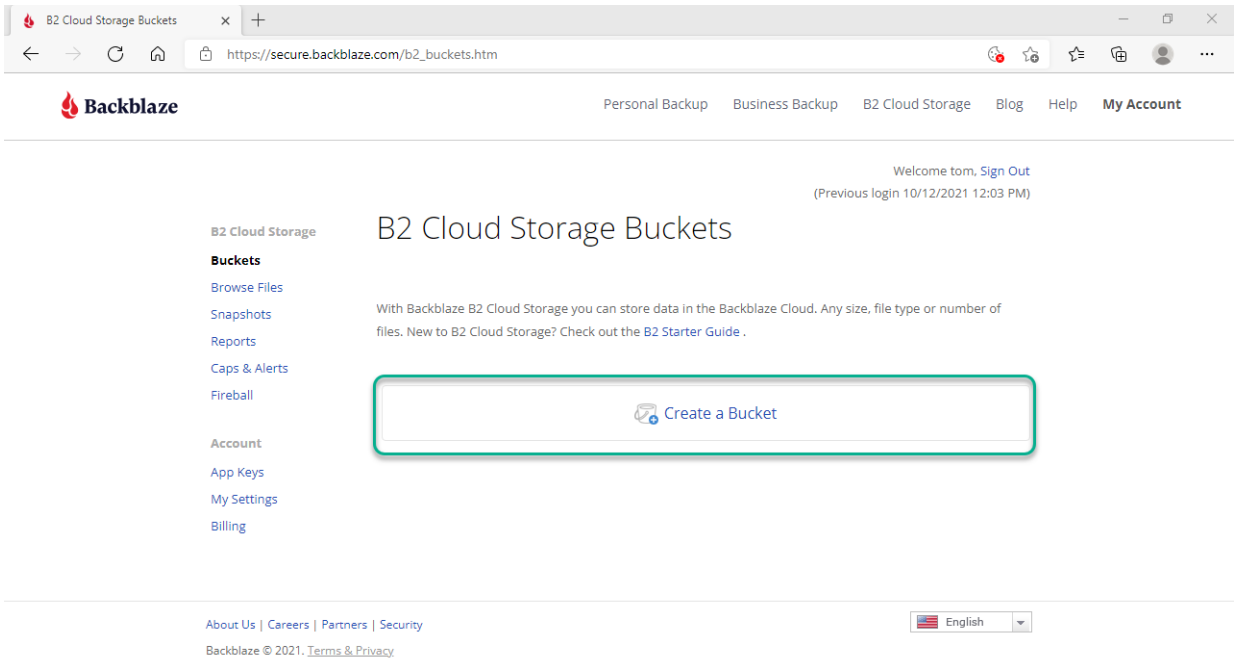
Backblaze B2 Initial Setup[1]

The following information from ***Backblaze B2*** is required to create an *S3CLOUD Resource*...

- *Bucket Name*
- *Endpoint*
- *Access Key ID*
- *Secret Access Key*

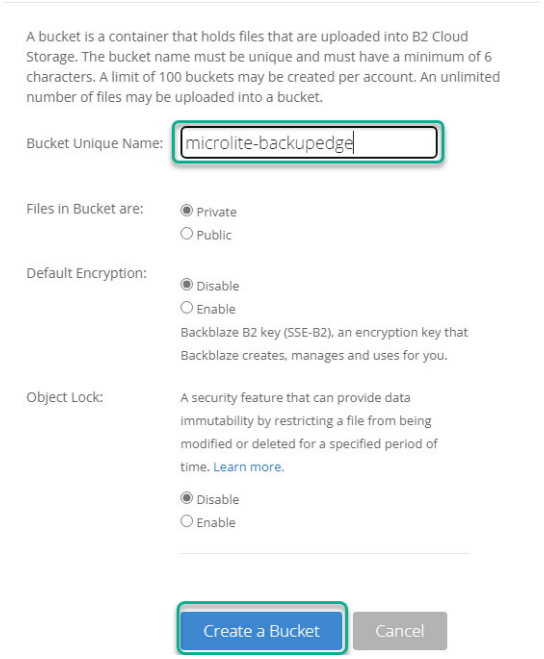
For *EDGEMENU*, please see “Create a BackupEDGE S3CLOUD Resource” on page 118.

On initial setup, the user must log into the following ***Backblaze B2*** *URL:* (https://secure.backblaze.com/b2_buckets.htm). First time users will see the following...

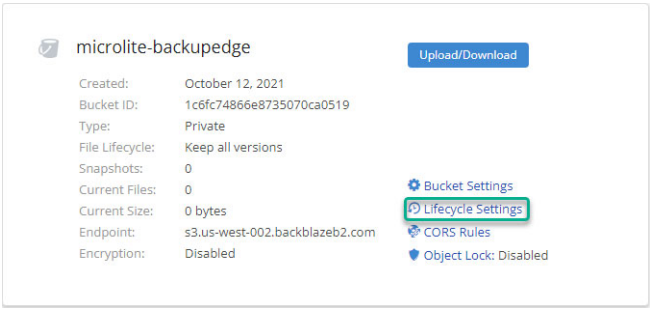


1. Backblaze may change the functionality of their web-based management system without notice. The exact steps described here may also change in this instance.

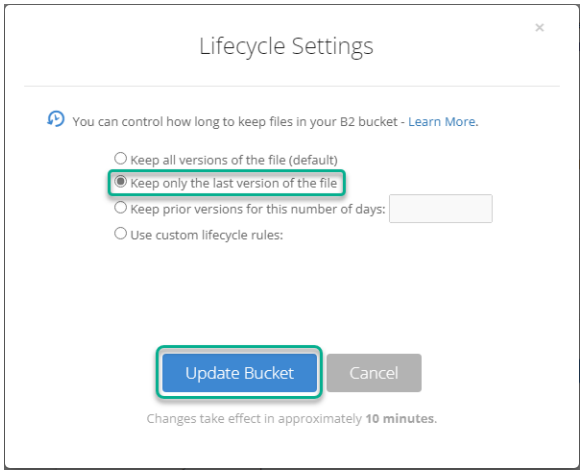
- Click *Create a Bucket*. In the *Bucket Unique Name* field, type the name you want to be your *BackupEDGE **Bucket Name***. This name must be unique for all of ***Backblaze B2***. You'll be notified if a *Bucket* with an identical name already exists. Leave the defaults for Privacy, Encryption, and Object Lock at their defaults and click *Create a Bucket*.



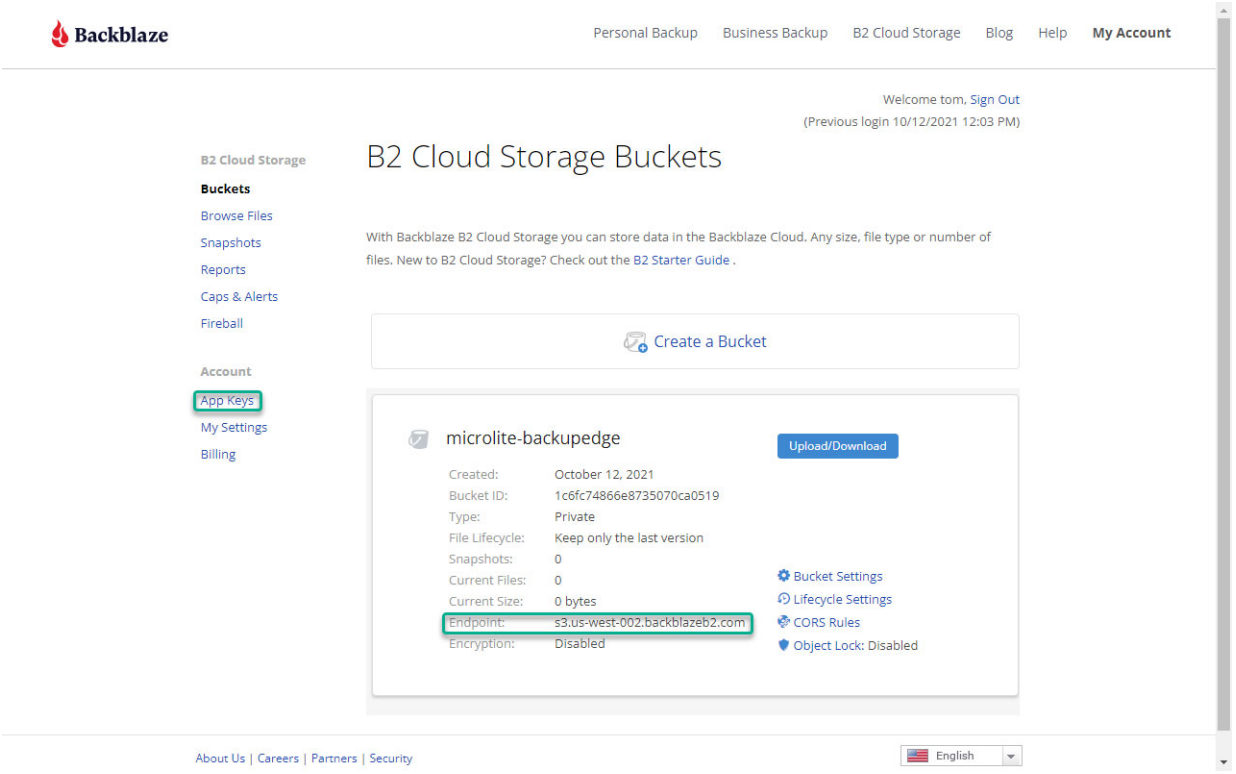
- You'll be returned to the main screen and the bucket will be created.



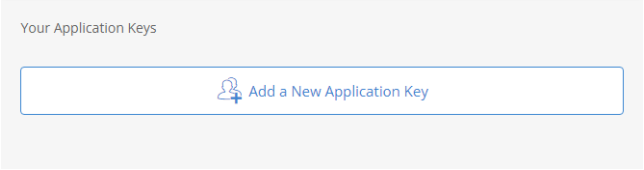
- Select *Lifecycle Settings*, then choose *Keep only the last version of the file*, then click *Update Bucket*.



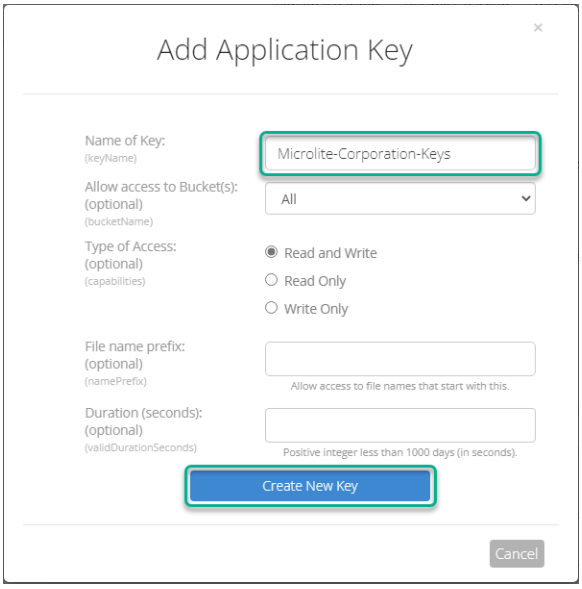
- The screen should look like as it does below:



- Record the ***Endpoint*** as assigned by ***Backblaze B2***.
- Click *App Keys* under the *Account* options on the left.
- Click *Add a New Application Key*.



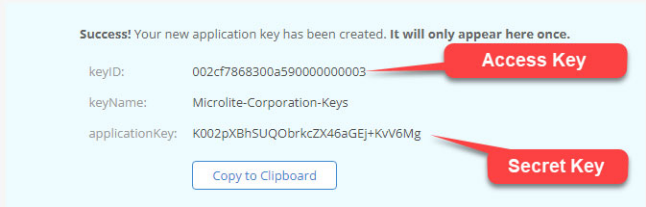
- Type a reference name for your Application Key, and click *Create New Key*.



- Your *Application Key* will be created and you'll be directed to copy the *applicationKey* to the clipboard. Preserve the *keyID* and the *applicationKey*.

NOTE: Application Keys may be set to allow access to individual buckets, or be used with all buckets. This example shows the all buckets setting.

- You **MUST, MUST, MUST** copy or download and **secure these keys**.
- The *applicationKey* will never be available again. If you need it again and don't have a copy, you must create a new key and replace it in all currently configured server.



The keys are used in the *Backup**EDGE** S3CLOUD Resource* as follow:

- The **keyID** is the *Backup**EDGE*** **Access Key ID**.
- The **applicationKey** is the *Backup**EDGE*** **Secret Key ID**.

After the keys have been secured, you may *Sign Out* of the ***Backblaze B2*** web site.

You now have the **Bucket Name**, **Endpoint**, **Access Key ID** and **Secret Key ID** you need to place into *Backup**EDGE***.

13.17 - Using dinCloud D3 Storage Services

To use *BackupEDGE* with the ***dinCloud D3 Cloud Storage*** (www.dincloud.com), a working knowledge of *dinCLoud* and *dinCloud D3* is expected. There are initial setup steps required on both the *dinCLoud D3* web site and via the *EDGEMENU BackupEDGE* user interface.

The following information is required to create an *S3CLOUD Resource*...

- *S3 Bucket* name.
- *S3 Access Key ID*.
- *S3 Secret Access Key*.
- *S3 Cloud Endpoint*.

For *EDGEMENU*, please see “Create a BackupEDGE S3CLOUD Resource” on page 118.

On initial setup, the users logs into the *dinCloud Console* using multi-factor authentication and:

- Tabs to “My D3 Storage”.
- Clicks “New D3 Storage Account”, enters a Label for the Storage Account, and selects a Datacenter.
- When “Create Account” is clicked, a *D3 Storage Account* is created, and an email is sent to the designated email account. This email contains the *S3 Cloud Endpoint* (identified as “**URL**”, The *S3 Access Key ID* (identified as “**Access Key**”) and the *S3 Secret Access Key* (identified as “**Secret Key**”). These should be stored and saved.

Next, you will need to create a *Bucket*. *dinCloud* does not have a web-based *Bucket* creation tool. Microlite Corporation has successfully used the S3 Browser and the Cloudberry Explorer for Amazon S3 to manage *Buckets* on *dinCloud*. Other products are available.

dinCloud D3 Regions and Endpoints

dinCloud has storage *Regions* and *Endpoints* the Midwest and Southwest areas of the United States.

dinCloud tracks and bills the user for this service, not Microlite Corporation. Pricing can be found at: https://www.dincloud.com/cloud-storage.

Here is a list of the available *Regions* where *Buckets* may be created. The *Endpoint* is essentially the access address of the servers in the *Region*. This information will be sent to you automatically when you create a new *D3 Storage Account*.

dinCloud D3 Region	***dinCloud D3 Endpoint***
US - Southwest	d3-lax.dincloud.com
US - Central	d3-ord.dincloud.com

13.18 - Using Dunkel Cloud Storage

To use *BackupEDGE* with the ***Dunkel Cloud Storage*** (www.dunkel.de/s3), a working knowledge of *Dunkel* and *Dunkel Cloud Storage* is expected. There are initial setup steps required on both the *Dunkel* web site and via the *EDGEMENU BackupEDGE* user interface.

The following information is required to create an *S3CLOUD Resource*...

- *S3 Bucket* name.
- *S3 Access Key ID*.
- *S3 Secret Access Key*.
- *S3 Cloud Endpoint*.

For *EDGEMENU*, please see “Create a BackupEDGE S3CLOUD Resource” on page 118.

On initial setup, the users logs into the *Dunkel Console* using multi-factor authentication and:

- Tabs to “Insert Location Here”.
- Clicks “New Dunkel Storage Account”, enters a Label for the Storage Account, and selects a Datacenter.
- When “Create Account” is clicked, a *Dunkel Storage Account* is created, and an email is sent to the designated email account. This email contains the *S3 Cloud Endpoint* (identified as “**URL**”, The *S3 Access Key ID* (identified as “**Access Key**”) and the *S3 Secret Access Key* (identified as “**Secret Key**”). These should be stored and saved.

Next, you will need to create a *Bucket*. *Dunkel* does not have a web-based *Bucket* creation tool. Microlite Corporation has successfully used the S3 Browser and the Cloudberry Explorer for Amazon S3 to manage *Buckets* on *Dunkel Cloud Storage*. Other products are available.

Dunkel Cloud Storage Regions and Endpoints

Dunkel has a single storage *Region* and *Endpoint* near Frankfurt, Germany.

dinCloud tracks and bills the user for this service, not Microlite Corporation. Pricing can be found at: (www.dunkel.de/s3).

Here is a list of the available *Regions* where *Buckets* may be created. The *Endpoint* is essentially the access address of the servers in the *Region*. This information will be sent to you automatically when you create a new *D3 Storage Account*.

Dunkel Cloud Storage Region	***dinCloud D3 Endpoint***
Germany	dcs.dunkel.de

13.19 - Using Digital Ocean Spaces

Under *BackupEDGE 03.04.02 build 1* and later S3 Signature Version 4 will be used.

Log into Digital Ocean. If two factor authentication is enabled, check your email and enter the authentication code provided.

Go to **Spaces** and click *Create* then *Spaces* to create a new *Bucket*. Digital Ocean will present a list of available datacenter *Regions*. Choose from the available *Regions*, then type a *Bucket* name into the *Choose a unique name* field.

Digital Ocean Spaces Region	*Digital Ocean Spaces Endpoint*
NYC1 - New York City 1	nyc1.digitaloceanspaces.com
NYC2 - New York City 2	nyc2.digitaloceanspaces.com
NYC3 - New York City 3	nyc3.digitaloceanspaces.com
SFO1 - San Francisco 1	sfo1.digitaloceanspaces.com
SFO2 - San Francisco 2	sfo2.digitaloceanspaces.com
SFO3 - San Francisco 3	sfo3.digitaloceanspaces.com
AMS1 - Amsterdam 1	ams1.digitaloceanspaces.com
AMS2 - Amsterdam 2	ams2.digitaloceanspaces.com
AMS3 - Amsterdam 3	ams3.digitaloceanspaces.com
FRA1 - Frankfort 1	fra1.digitaloceanspaces.com
SGP1 - Singapore 1	sgp1.digitaloceanspaces.com

Click on *Manage Keys*, then under *Spaces access keys* click *Generate New Key* to create a new `Access Key:` and `Secret Key:`.

13.20 - Using Other S3 API Compatible Storage Services

The *Backup**EDGE** S3CLOUD* storage *Resource* type is potentially compatible with many other cloud storage vendors in addition to the ones previously mentioned in this section. However, until tested by Microlite we can't officially support them.

The following information is required from the third party, *S3 API* compatible storage service to create an *S3CLOUD Resource* in *Backup**EDGE*...

- *S3 Bucket* name.
- *S3 Access Key ID*.
- *S3 Secret Access Key*.
- *S3 Cloud Endpoint*.

If the storage service does not have a web-based tool to create a *Bucket*. Microlite Corporation has successfully used the S3 Browser and the Cloudberry Explorer for Amazon S3 to manage *Buckets* on many *S3 API* compatible sites.

13.21 - Using Private Cloud Servers: NAS Devices and MINIO

Many Network-Attached-Storage (NAS) devices now have an *Object Storage* application or service. For instance:

- **TrueNAS** calls the *Object Storage Service* the **S3 Service**.
- **QNAP** calls the *Object Storage Service* the **QuObjects App**.

Beginning with *Backup**EDGE** 03.04.02 build 1* and later, a *Port* number may be appended to the *Endpoint* field, preceded by a *colon* (:), in an *S3CLOUD Resource*. This allows *Backup**EDGE** to be compatible with the *Object Storage* applications on many NAS devices, and with the **MIN**IO software-based *Object Storage* service.

14 - Configuring Legacy Disk-to-Disk Backups

14.1 - General Concepts

Most users will want to configure and use *SharpDrive Media* as described in “Configuring SharpDrive Backups” on page 80. This section is for OpenServer 5 users or those with a vested interest, such as combining them with URL backups for a various backup-restore combinations.

Disk-to-Disk Backups are also known as D2D Backups or Directory Backups.) These are backups using a (preferably removable) hard disk or flash storage device. Two *Resources* combine to make Disk-to-Disk backups function:

- *FSP Resource*, or FileSystem Partition Resource, defines and controls the directory on the filesystem where archives are stored. No other files may be in this directory except those created by *Backup**EDGE***.
- *AF Resource*, or Attached FileSystem Resource, defines the commands *Backup**EDGE*** must use to mount and unmount the device / filesystem containing the FSP Resource. No other user or process should mount and unmount the filesystem.

14.2 - Multiple Archives Per Medium

*Backup**EDGE*** supports performing multiple backups onto *FSP Resources*. The quota for an *FSP Resource* is defined by the user during setup. This is the general behaviour.:

Medium	Archive Behaviour
FSP	The process will attempt to create a new archive. If starting a new segment would cause the quota to be reached, the oldest expired archive will be erased in its entirety (all segments). If starting a new segment would exceed the quota and no more expired archives exist, the backup will **FAIL**.

14.3 - Compatibility Matrix.

Operating System / Medium	Linux	UW7	OSR 6	OSR 5.0.7
SATA Quantum GoVault	YES	YES	YES	NO[a]
SATA RDX/RD1000	YES	YES	YES	NO[a]
USB Quantum GoVault	YES	YES	YES	YES
USB RDX/RD1000	YES	YES	YES	YES
USB Standard Hard Drive / Flash Drive	YES	NO[b]	NO[b]	YES
CIFS / Samba Network Mounted Filesystems	YES	NO	NO	NO
NFS Network Mounted Filesystems	YES	PART	PART	YES
Local Filesystems / Directories	PART	PART	PART	PART

a. The OpenServer 5 IDE/ATAPI driver is incompatible with these SATA devices.
b. USB hard drives / flash drives which are hot plugged may not be used with these operating systems safely.

YES - Compatible with *Backup**EDGE*** and *Recover**EDGE***.

PART - Compatible with *Backup**EDGE*** but not *Recover**EDGE***.May be used for fast, temporary backups.

NO - Not compatible with *BackupEDGE* or *RecoverEDGE*, generally because of an operating system limitation.

Removable Disk Cartridge Systems

Removable disk cartridge systems such as the IBM / Quantum GoVault and the RDX / RD1000 are easy to use and compatible with *BackupEDGE* and *RecoverEDGE* when the operating system is marked **YES** above. Drive cartridges **must** be pre-formatted with the proper filesystem type for your operating system.

Removable Hard Drives / Flash Drives

Removable hard drives, including USB hard drives, flash drives, etc. make excellent D2D devices and are completely compatible with *BackupEDGE* and *RecoverEDGE*. Flash drives are treated exactly as hard drives and, like hard drives, must be pre-configured with the proper filesystem type for your operating system.

NOTE: Flash drives can be very slow.

Local Filesystem / Directory Backups

Mounting a local (permanently attached) hard drive or filesystem as a directory can be very useful for making fast data copies, but is not recommended for anything else. Its data is very likely to be lost if the server has a catastrophic event (fire/flood/earthquake etc.). The potential for either loss or accidental erasure during a disaster recovery is very high. Microlite never recommends the use of archive devices or media that cannot be taken off-site on a periodic basis.

14.4 - FSP Notes

- Quota (maximum capacity) must be entered in the *FSP Resource* definition.
- Multiple archives per medium utilize archive expiration times and lazy reclamation to maximize the number of archives stored for maximum safety.
- Compression and optional encryption are supported.
- Full file checksumming, for maximum data integrity, is supported.
- *Instant File Restore* is available from any archive. It is not necessary to read through an entire archive to restore individual files and directories.
- MySQL™ hot backups are supported.

14.5 - Potential Applications

There are many ways to use FSP and AF Resources. Some are compatible with *RecoverEDGE* disaster recovery, and some are not. It is important to understand which uses and devices server which purposes.

14.6 - Theory of Operation

For the most part, these backup resources are very similar to more conventional ones such as tape or DVD. However, there are a few points you should be aware of before using them.

Segments

In a tape backup, *BackupEDGE* streams the data directly on to the media. In D2D backups, *BackupEDGE* streams the data into *archive files* on the target medium. This potentially subjects the files to filesystem size limitations and ulimit or other arbitrary operating system limitations.

To work around these limits, *BackupEDGE* automatically segments archives; that is, it divides one logically long archive into short archive files (called *segments*) that can be managed by the operating system managing the storage device. By default, these segments are 1 gigabyte -1 block in length.

BackupEDGE can write multiple archives to *D2D Resources*, and each archive may contain multiple segments. *BackupEDGE* handles segments automatically, and provides tools for managing the segments. To maintain consistent archives, the individual segments should never be manipulated by operating system commands. This is why segments do not have names that make sense to humans.

Quotas

Each *D2D Resource* is assigned a storage quota. *BackupEDGE* will not attempt to use more storage on the target medium than that assigned by the quota.

Retention Times

By default, all archives created to an *FSP Resource* using the *Scheduler* have a retention time (or expiration time) of one week. They will not be erased automatically until the retention time is up, but will not necessarily be erased just because its retention time is up. An archive past its retention time is called an *Expired Archive*.

Space Reclamation

Archives are retained on *FSP Media* at least until their expiration time has passed. After that, they are deleted in one of two ways...

Lazy Reclamation Enabled (Default)

If *Lazy Reclamation* is enabled, archives will remain on media as long as possible, just in case they may be needed even after their retention time is up. This allows maximum space utilization on the media. For an archive to be deleted...

- The retention time must be up, i.e. it must be an *Expired Archive*.
- Adding a segment to a new archive would cause the defined quota (as decided by the user when defining the *Resource*) to be exceeded.

If both conditions are true, the oldest *Expired Archive* will be deleted in its entirety. This process ensures that a maximum number of older archives are available on the target media.

If the quota is reached and none of the archives has expired, the backup will prompt for additional media.

By default, each backup in a *Scheduled Job* has a *Retention Time* of 1 week. This is may be changed on a per-schedule basis in the default simple *Scheduler*, and on a per-backup basis in the advanced *Scheduler*.

Lazy Reclamation Disabled

Disabling *Lazy Reclamation* (un-checking the `Lazy Reclamation` field in the *Resource Definition*) configures *BackupEDGE* to check for and immediately erase all expired archives any time a new backup is started to the *FSP Resource*. Only unexpired archives will be retained.

By default, each backup in a scheduled job has a *Retention Time* of 1 week. Note that usually, if you are backing up multiple machines and / or schedules to the same target medium, you will create multiple *Resources*, one per machine/schedule combination. Each *Resource* would use a different directory on the *FSP Resource* and have a different quota, where combined quotas should not exceed available space. A typical schedule would look like this:

Sample D2D Backup Schedule

```
+ Edit Backup Schedule ------------------------------------------------------+
| Schedule Name:     simple_job                                               |
|          Time:     [23:00 ] (14:58:46)  Enabled: [X]                        |
| Sequence:                   web2v.microlite.com:esequence/onsite            |
| Backup Domain:              system                                         |
| Primary Resource:  [Change] web2v.microlite.com:fsp!fsp0                   |
|                                                                            |
| +-------------------------------------------------+     September 2019      |
| | Every Sunday of the week                (None) |  Su Mo Tu We Th Fr Sa    |
| | Every Monday of the week                Master |   1 M  M  M  M  M   7    |
| | Every Tuesday of the week               Master |   8 M  M  M  M  M  14    |
| | Every Wednesday of the week             Master |  15 M  M  M  M  M  21    |
| | Every Thursday of the week              Master |  22 M  M  M  M  M  28    |
| | Every Friday of the week                Master |  29 M                    |
| | Every Saturday of the week              (None) |                          |
| +-------------------------------------------------+                          |
|                                                                            |
| Notify / Advanced: [Change]  [Reset Dates]                                 |
| Mail Summary To:   root                    Print Summary To:   NONE        |
| Mail Failures To:  NONE                    Print Failures To:  NONE        |
|[Save]                                                          [Cancel]|
+----------------------------------------------------------------------------+
```

This *Schedule* will perform Monday through Friday backups. In the example, a five backup rotation will be created. Because of the one week default retention, *Expired Archives* (those older than one week old) will be retained on the target medium at least one week, and possibly longer based on the *Lazy Reclamation* flag in the *Resource* definition. If the quota is reached and none of the archives has expired, the backup will fail.

Changing the retention time in the Schedule to 2 weeks, three weeks, etc. allows easy creation of multiple minimal storage rotations.

14.7 - Setting Up D2D Backups

To have *Backup**EDGE*** back up to an D2D Device you must:

1. Prepare the removable storage device to accept backups.
2. Configure an AF Resource to mount and unmount the device on demand.
3. Configure an FSP Resource to read and write to the mounted device and associate it with the proper AF Resource.
4. Initialize the FSP Resource.
5. Select the FSP Resource from EDGEMENU or within a Schedule.

Initializing the FSP backup resource does NOT erase any data. If there are no current files in the backup directory, *Backup**EDGE*** will create a control file (named `CTL`) indicating that it is ready to accept *Backup**EDGE*** archives. If *Backup**EDGE*** detects a control file, it will scan the directory for any current archives and re-build its index of available archives and their sizes. FSP backups cannot commence until the FSP Resource has been initialized one time.

NOTE: Never place any other (non-*Backup**EDGE***-created) files in the *Backup**EDGE*** directory on the FSP Resource. Never manually remove any *Backup**EDGE*** files. The **only** way to manipulate these files other than from within *EDGEMENU* without corrupting the control file database is by using the `edge.segadm` command. See “EDGE.SEGADM” on page 330 for more information on using this program.

Preparing the Storage Device

Microlite recommends that your removable hard disk contain a single filesystem that is mounted and unmounted only by *BackupEDGE*. To prepare the hard drive, the following steps are usually necessary:

1 Attach the device and make sure it is seen by the operating system.

2 Run FDISK, erase all partitions, and create a single primary partition.

3 Create a valid filesystem on the partition.

NOTE: The filesystem MUST be of the same type as an existing, always mounted filesystem (like the root filesystem) on the running system. This is so that valid modules needed to mount it can be picked up by the disaster recovery media. For instance, on a Linux system if all your regular filesystems are `ext3`, do not create a `reiserfs` filesystem on the removable media.

See “Storage Device Preparation Example (Linux)” on page 166 for more detailed information.

See “Storage Device Preparation Example (OpenServer 6)” on page 168 for more detailed OpenServer 6 information.

See “Storage Device Preparation Example (OpenServer 5)” on page 171 for more detailed OpenServer 6 information.

Setting Up an Attached Filesystem Resources

The AF (Attached Filesystem) Resource is a handler for devices that must be mounted and unmounted prior to use, such as removable hard drives, flash memory cards, and so on. It is responsible for managing the entire removable medium. It knows how to mount and unmount it, etc. You cannot write a backup directly to the AF resource.

Setting up the AF resource requires using `edgemenu:Admin->Define Resources`. Select ‘`[NEW]`’, then change the type to ‘`Attached Filesystem`’ (use the down-arrow key), and change the resource name to something suitable (the default is ‘`af0`’ and is fine).

Unedited AF Resource.

```
+ BackupEDGE Resource Information ------------------------------------------+
¦- General Resource Information -------------------------------------------¦
¦Resource Type       Attached Filesystem                                    ¦
¦Resource Name       [af0               ] Change as appropriate             ¦
¦Description         [Attached Filesystem Resource]                         ¦
¦Changer Assoc       [Standalone Device]                                    ¦
¦Interface           [Other      ]                                          ¦
¦                                                                           ¦
¦- Attached Filesystem Information ---------------------------------------¦
¦Mount Dir           [/usr/lib/edge/system/mnt/af0                        ] ¦
¦Mount Device Node   [/dev/null                  ]                         ¦
¦Mount Command       [/etc/mount %m %M                                    ] ¦
¦Unmount Command     [/etc/umount %M                                      ] ¦
¦Exclude Node        [                                                    ] ¦
¦                                                                           ¦
¦[Next]                              [Prev]                          [Cancel]¦
+---------------------------------------------------------------------------+
```

Usually, the *only two fields you must modify* are the `Mount Device Node` and the `Exclude Node`. The other fields, `Mount Dir`, `Mount Command`, and `Unmount Command`, will probably work without modification. The default mount directory is in a *BackupEDGE* directory that gets automatically excluded from backups, and should not be changed.

The `Mount Device Node` is the device node that you will use to mount this attached filesystem, such as ‘`/dev/sdb1`’.

The `Exclude Node` is the device node that will be excluded by *RecoverEDGE* during disk preparation for disaster recovery. The idea is that you do not want *RecoverEDGE* re-creating the filesystem on your removable hard drive that previously held the backup you wanted to restore from.

The `Exclude Node` should be the '*whole disk*' node, even if you are mounting only a partition of it. For example, if the `Mount Device Node` is '`/dev/sdb1`', you would want to use '`/dev/sdb`' as the `Exclude Node`.

Completed AF Resource.

```
+ BackupEDGE Resource Information ------------------------------------------+
|- General Resource Information ------------------------------------------- |
|Resource Type       Attached Filesystem                                     |
|Resource Name       [af0               ] Change as appropriate              |
|Description         [Attached Filesystem Resource]                          |
|Changer Assoc       [Standalone Device]                                     |
|Interface           [Other      ]                                           |
|                                                                            |
|- Attached Filesystem Information ---------------------------------------- |
|Mount Dir           [/usr/lib/edge/system/mnt/af0                         ] |
|Mount Device Node   [/dev/sdb1                  ]                           |
|Mount Command       [/etc/mount %m %M                                     ] |
|Unmount Command     [/etc/umount %M                                       ] |
|Exclude Node        [/dev/sdb                                             ] |
|                                                                            |
|[Next]                              [Prev]                          [Cancel]|
+----------------------------------------------------------------------------+
```

Note that this means you cannot use one partition of a removable hard drive as a regular filesystem and another for *BackupEDGE*. If you do this, disaster recovery might not recover the other filesystem automatically, since the whole disk will be excluded. If you do not list the whole disk, the *BackupEDGE* partition might be erased during recovery. Generally, this is not restrictive because if you are doing disaster recovery with removable media, it must be possible to remove the media physically from the system. If you do not, then you stand a chance of losing your backups to whatever disaster that required your system to be recovered in the first place!

You may modify the `Mount Dir` to cause *BackupEDGE* to mount the *Attached Filesystem* elsewhere. If you do, you must also tell *BackupEDGE* to exclude it from backup, else a *Master Backup* will traverse into that directory. You can do this by adding the mount directory to `/etc/edge.exclude`. Note that the default mount directory does NOT require this, since *BackupEDGE* will exclude it by default.

The `Mount Command` and `Unmount Command` fields should be whatever commands are used to mount and unmount the attached filesystem, respectively. They accept the substitutions '`%m`' for the mount device node, and '`%M`' for the mount directory.

Press `[Next]` to save the AF resource.

NOTE: AF Resources can be problematic with hot plug devices. Many hot plug devices change device names between hot plugs, and there is no reliable way to search for the correct device, especially in cases where, for instance, more than one USB hard drive is used as a backup device, or more than one USB device is plugged in at a time. Please do extensive testing before deploying solutions using AF Resources.

Setting Up a FileSystem Partition Resource

After you have saved the AF resource, you must create one or more *Filesystem Partition* (FSP) resources to write to it. Setting up an FSP resource is very simple. Use `edgemenu:Admin->Define Resources` to create a Resource. Select '`[NEW]`' to do this. In the popup box, be sure to change the type to '`Filesystem Partition`' (use the right and left arrow keys), and optionally change the resource name (the default is '`fsp0`').

All of the fields in this form have excellent defaults except “AF Association”. Press **[Enter]** on this field and select the AF Resource that will be handling the mounting and un-mounting of the filesystem. This should be changed to the reflect This tells *BackupEDGE* to make sure that the filesystem is mounted before trying to access the FSP.

```
+ BackupEDGE Resource Information ------------------------------------------+
|- General Resource Information ---------------------------------------------|
|Resource Type       FS Partition                                            |
|Resource Name       [fsp0              ] Change as appropriate              |
|Description         [Directory Resource          ]                          |
|AF Association      [asusp1:af0]                                            |
|Interface           [Other      ]                                           |
|                                                                            |
|- FS Partition Information -------------------------------------------------|
|Dir Suffix          [/fsp0                                                ]  |
|Segment Size (K)    [1048544                    ] [X] Lazy Reclamation      |
|                                                                            |
|                                                                            |
|                                                                            |
|- Default Backup Properties ------------------------------------------------|
|Quota               [120G         ] [S] Compression Level  [5]              |
|Edge Block Size     [64           ] [Y] Double Buffering                    |
|[Next]                              [Prev]                          [Cancel]|
+----------------------------------------------------------------------------+
```

NOTE: *BackupEDGE* handles concurrent access to an FSP (or to multiple FSPs that share one AF) correctly. You may write more than one backup at a time to an FSP.

‘Dir Suffix’ is the directory where the backups will be saved, and should typically be left at the default. When used with an AF Resource, this suffix is appended to the Mount Dir (mount directory) in the AF Resource.

‘Segment Size’, controls the maximum file size that *BackupEDGE* will create. The default is slightly less than 1GB. Note that this does **not** limit the maximum archive size; *BackupEDGE* will automatically split the archive up into multiple files (*segments*) if needed. Generally, you will not know (or care) about this, as it will be handled for you automatically. You do not need to alter the ‘Segment Size’ field in most cases.

‘Lazy Reclmation’ controls the behavior of space reclamation (deleting archives) on the FSP media. See “Space Reclamation” on page 160 for additional information. The default behaviour is *Enabled*.

Do not confuse ‘Segment Size’ with ‘Quota’. ‘Quota’ limits the total space consumed by all *BackupEDGE* archives on this resource. (For FSPs that refer to removable media devices, as described below, the ‘Quota’ limits the amount of space that will be used on any single medium.) In other words, if the ‘Quota’ is 100GB, then no more than 100GB will be written by *BackupEDGE* to this FSP until something is erased, or a new medium is loaded. This is useful if one AF (*Attached Filesystem,* see below) is split into multiple FSPs, and you want to make sure that no single FSP consumes the whole AF. It should typically be set at the size of the filesystem on the device.

You may choose any [S]oftware compression level from 1 to 9, or choose N for no compression. Do not attempt to set compression to [H]ardware.

Initialize the FSP Resource

When you press [Next] to save the resource, you will be asked if you want to ‘*Initialize*’ it. You must let *BackupEDGE* initialize the resource. This mounts the filesystem, creates the directory and adds a control file named CTL in the destination directory. To initialize at a later time, use edgemenu:Admin->Initialize Medium. Note that initializing the resource will **not** erase any

existing backups. If existing backups exits, the `CTL` file, which contains information about the individual archive segments, will be re-calculated.

NOTE: If your AF refers to a device with removable media, or you are using a series of USB disk drives, you must *Initialize* **each FSP** on each medium. You may do this with `edgemenu:Admin->Initialize Medium`. If you insert media that has not been initialized for use with *Backup**EDGE***, the backup will not work. Initializing a medium that already has backups on it will not erase the backups.

14.8 - Unmounted FSP Resources

If you create an FSP Resource and do not control it with an AF resource, you are merely backing up to a local directory. Although a fine method for doing quick backups, *Backup**EDGE*** cannot use the local directories for disaster recovery.

14.9 - Backup Granularity

Be creative. Backups to devices with a lot of random access storage space provide the opportunity to increase backup frequency. One possible use is doing *Master Backups* each night, and *Differential Backups* at midday.

As an example, the “Sample D2D Backup Schedule” on page 161 will perform your nightly backup of the default *Domain* (`system`) through the default *Sequence* (`onsite`). Enable the advanced scheduler, then create a new *Schedule* called `midday_backups`. When prompted, have the new *Schedule* use the same *Domain* and *Sequence* as the default *Schedule*. You may also have to choose whether or not to include a MySQL backup. Set the time to noon or so.

When you are finished, you’ll have a very fast midday backup and be able to increase the reliability of your data.

Midday Backup Example

```
+ Edit Backup Schedule ------------------------------------------------------+
| Schedule Name:     [midday_backup]                                          |
|          Time:     [12:01 ] (14:28:24)  Enabled: [X]                        |
| Sequence:          [Change] web2v.microlite.com:esequence/onsite            |
| Backup Domain:     [Change] system                                          |
| Primary Resource:  [Change] web2v.microlite.com:fsp!fsp0                    |
|                                                                             |
| +-----------------------------------------------+     September 2019       |
| | Every Sunday of the week                (None) |  Su Mo Tu We Th Fr Sa    |
| | Every Monday of the week               Differ |   1 D  D  D  D  D   7    |
| | Every Tuesday of the week              Differ |   8 D  D  D  D  D  14    |
| | Every Wednesday of the week            Differ |  15 D  D  D  D  D  21    |
| | Every Thursday of the week             Differ |  22 D  D  D  D  D  28    |
| | Every Friday of the week               Differ |  29 D                    |
| | Every Saturday of the week              (None) |                          |
| +-----------------------------------------------+                          |
|                                                                             |
| Notify / Advanced: [Change]  [Reset Dates]                                  |
| Mail Summary To:   root                    Print Summary To:   NONE         |
| Mail Failures To:  NONE                    Print Failures To:  NONE         |
|[Next]                        [Back To Select]                      [Cancel]|
+-----------------------------------------------------------------------------+
|+Local Machine: web2v.microlite.com  Administering: web2v.microlite.com  ----+|
```

This will create 5 separate *Differential Backups*. If you only care about having the last one around, you could just change `Retention Time` to `[1 Days]` in the `Notify / Advanced` screen. This would allow at least one *Differential Backup* to remain current at all times. Expired ones would be erased only if the *Scheduler* needs to reclaim the space.

The scheduler provides great flexibility. Extending the above example, it is possible to create hourly *Differential Backups* or *Incremental Backups* every day, providing an even greater safety margin by increasing backup frequency.

Deleting archives manually is discussed in “Deleting Backups” on page 253.

14.10 - Storage Device Preparation Example (Linux)

On a Linux system with one SATA or SCSI hard drive, the full disk device would be `/dev/sda`. Plugging in a SATA removable cartridge shell, or a USB removable shell or disk drive, would automatically cause a device node of `/dev/sdb` to be created.

Here is an example configuring a 40GB hard drive on a Linux system called `asusp1`. All typing is **bold**.

```
asusp1:~ # fdisk /dev/sdb

The number of cylinders for this disk is set to 38150.
There is nothing wrong with that, but this is larger than 1024,
and could in certain setups cause problems with:
1) software that runs at boot time (e.g., old versions of LILO)
2) booting and partitioning software from other OSs
   (e.g., DOS FDISK, OS/2 FDISK)
```

(Print the current table if not empty use **d** to delete partitions until empty.)

```
Command (m for help): p

Disk /dev/sdb: 40.0 GB, 40003567616 bytes
64 heads, 32 sectors/track, 38150 cylinders
Units = cylinders of 2048 * 512 = 1048576 bytes

   Device Boot      Start         End      Blocks   Id  System
```

Create a new primary partition the entire size of the disk.

```
Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-38150, default 1): [Enter for default]
Using default value 1
Last cylinder or +size or +sizeM or +sizeK (1-38150, default 38150): [Enter]
Using default value 38150
```

Write the table and exit.

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
```

The first partition on `/dev/sdb` will always be called `/dev/sdb1`. Let’s make an **ext3** filesystem on it.

```
asusp1:~ # mkfs.ext3 -L BackupEDGE /dev/sdb1
mke2fs 1.39 (29-May-2006)
Filesystem label=BackupEDGE
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
```

```
4889248 inodes, 9766396 blocks
488319 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=4294967296
299 block groups
32768 blocks per group, 32768 fragments per group
16352 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632,
2654208,
        4096000, 7962624

Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 30 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
```

NOTE: The filesystem is built, with a notice that it will be checked automatically every 30 mounts. This can be overridden by issuing the following command, which will eliminate frequent log messages.

```
asusp1:~ # tune2fs -c 0 /dev/sdb1
tune2fs 1.39 (29-May-2006)
Setting maximal mount count to -1
```

Your hard disk and filesystem are now prepared.

Completed AF Example Resource.

```
+ BackupEDGE Resource Information ------------------------------------------+
|- General Resource Information -------------------------------------------|
|Resource Type       Attached Filesystem                                    |
|Resource Name       [af0               ] Change as appropriate             |
|Description         [Attached Filesystem Resource]                         |
|Changer Assoc       [Standalone Device]                                    |
|Interface           [Other      ]                                          |
|                                                                           |
|- Attached Filesystem Information ----------------------------------------|
|Mount Dir           [/usr/lib/edge/system/mnt/af0                        ] |
|Mount Device Node   [/dev/sdb1                  ]                          |
|Mount Command       [/etc/mount %m %M                                    ] |
|Unmount Command     [/etc/umount %M                                      ] |
|Exclude Node        [/dev/sdb                                            ] |
|                                                                           |
|[Next]                              [Prev]                          [Cancel]|
+---------------------------------------------------------------------------+
```

The *Mount Device Node* and *Exclude Node* are critical. Get the Mount Device Node wrong and you can't make backups. Get the Exclude node wrong and *Recover**EDGE*** won't know to always exclude this device from initialization (being erased) during disaster recovery.

Remember to create a matching Attached Filesystem (af) Resource, as shown i.n "Setting Up a FileSystem Partition Resource" on page 163, and associate it with the AF.

14.11 - Storage Device Preparation Example (OpenServer 6)

NOTE: Due to hot plugging issues, Microlite does not support the use of standard USB hard drives as backup devices on this operating system. This is because unplugging and re-plugging them changes the device nodes. Cartridge-based SATA and USB devices like the RDX / RD1000 and Quantum GoVault are supported, as long as cartridges only are inserted or removed. The device itself may not be plugged / unplugged during operation. Power up the server with the devices already connected and powered on.

Device Node Identification

OpenServer 6 uses a naming convention that is easy to decode. Device nodes are always of the form:

```
Controller
 Bus
  Target
   Logical Unit Number, or LUN, abbreviated as "d"
    Partition
     Slice (optional)
```

and are always in the same order

To identify your storage device(s), log in as `root` and run **`sdiconfig -l`**, looking for the `DISK` entries. Note the numbers below that are in **bold**. and that this is the letter **l**, not a **one**.

```
asusp1:~ # sdiconfig -l
0:0,2,0: HBA      : (ide,2) Generic IDE/ATAPI
  0,0,0: DISK     : ST3320620AS              3.AA
  0,1,0: CDROM    : ASUS     DRW-2014L1T     1.02
  1,0,0: DISK     : QUANTUM GoVault          0110
  1,1,0: CDROM    : Iomega  RRD2             P099
  1,2,0: HBA      : (ide,2) Generic IDE/ATAPI
1:0,7,0: HBA      : (usb_msto,1) USB     USB HBA
  0,0,0: DISK     : TANDBERGRDX              2040
```

Vendor ID	Device ID	Firmware Version	Controller (c)	Bus (b)	Target (t)	LUN (d)
(none)	ST3320620AS	3.AA	0	0	2	0
QUANTUM	GoVault	0110	0	1	0	0
TANDGERG	RDX	2040	1	0	0	0

In this example, the ST3320620AS device is the primary hard drive and doesn't concern us.

For the Quantum GoVault in this example, the controller is **0**, the bus is **1**, the target is **0**, and the LUN is **0**, yielding the following useful nodes:

Description	Device Node
Raw device node - Entire disk - Used for fdisk	`/dev/rdsk/c0b1t0d0p0`
Block Device Node - Entire disk - used in *af Resource* & *RecoverEDGE*.	`/dev/dsk/c0b1t0d0p0`
Block Device Node - Partition 1 - used for divvy command	`/dev/dsk/c0b1t0d0p1`
Block Device Node - Partition 1 - Disk Slice used for backups (mount device)	`/dev/dsk/c0b1t0d0p1s0`

For the Tandberg RDX Quikstor in this example, the controller is **1**, the bus is **0**, the target is **0**, and the LUN is **0**, yielding the following useful nodes:

Description	Device Node
Raw device node - Entire disk - Used for fdisk	`/dev/rdsk/c1b0t0d0p0`
Block Device Node - Entire disk - used in *af Resource* & *RecoverEDGE*.	`/dev/dsk/c1b0t0d0p0`
Block Device Node - Partition 1 - used for divvy command	`/dev/dsk/c1b0t0d0p1`
Block Device Node - Partition 1 - Disk Slice used for backups (mount device)	`/dev/dsk/c1b0t0d0p1s0`

We'll continue with the Quantum GoVault device nodes in this example.

Creating an FDISK Partition

```
asusp1:~ # fdisk /dev/rdsk/c0b1t0d0p0
```

If there are no existing partitions on the cartridge, you'll see...

```
The recommended default partition for your disk is:

  a 100% "Unix System" partition.

To select this, please type "y".  To partition your disk
differently, type "n" and the "fdisk" program will let you
select other partitions.
```

Select "**y**". The entire drive cartridge will be assigned to the fdisk partition and marked active.

If you select "**n**", or if the drive had a valid fdisk partition, the normal fdisk menu will be shown.

```
Total disk size is 38153 cylinders (38153.0 MB)

                                            Cylinders                  Approx
Partition   Status       Type          Start    End   Length    %      MB
=========   ======    ===========      =====    ===   ======   ===   ======
    1       Active    UNIX System          0   38152   38153    100    38153.1


SELECT ONE OF THE FOLLOWING:

     0.   Overwrite system master boot code
     1.   Create a partition
     2.   Change Active (Boot from) partition
     3.   Delete a partition
     4.   Exit (Update disk configuration and exit)
     5.   Cancel (Exit without updating disk configuration)
Enter Selection:
```

Delete all partitions, create a new one using the entire disk (100%), make the partition active, and type choose:

```
4. Exit (Update disk configuration and exit)
```

Creating an DIVVY Filesystem

```
asusp1:~ # divvy -m /dev/rdsk/c0b1t0d0p1
```

Make sure to use p1 as the partition in the command. You'll see...

```
There a 39056850 blocks available in the UNIX area.
Please enter the number of file systems you want this area
to be divided into, or press <Return> to get the default of 7 file system(s)
```

The number of blocks displayed will be dependent on the disk cartridge size. Type "**1**".

```
The layout of the filesystems and swap area are now prepared.

Do you wish to make any manual adjustments to the sizes or
names of the filesystems or swap area before they are created
on the hard disk? (y/n)
```

Type "**n**". The filesystem will be created.

Your hard disk cartridge and filesystem are now prepared. Use the correct nodes in *EDGEMENU* to create a new AF Resource.

Completed AF Example Resource.

```
+ BackupEDGE Resource Information ------------------------------------------+
|- General Resource Information ------------------------------------------- |
|Resource Type       Attached Filesystem                                     |
|Resource Name       [af0               ] Change as appropriate              |
|Description         [Attached Filesystem Resource]                          |
|Changer Assoc       [Standalone Device]                                     |
|Interface           [Other      ]                                           |
|                                                                            |
|- Attached Filesystem Information ---------------------------------------- |
|Mount Dir           [/usr/lib/edge/system/mnt/af0                         ] |
|Mount Device Node   [/dev/dsk/c1b0t0d0p1         ]                          |
|Mount Command       [/etc/mount %m %M                                     ] |
|Unmount Command     [/etc/umount %M                                       ] |
|Exclude Node        [/dev/dsk/c0b1t0d0p0                                  ] |
|                                                                            |
|[Next]                              [Prev]                          [Cancel]|
+----------------------------------------------------------------------------+
```

The **Mount Device Node** and **Exclude Node** are critical. Get the **Mount Device Node** wrong and you can't make backups. Get the **Exclude Node** wrong and *Recover**EDGE*** won't know to always exclude this device from initialization (being erased) during disaster recovery.

Remember to create a matching Attached Filesystem (af) Resource, as shown i.n "Setting Up a FileSystem Partition Resource" on page 163, and associate it with the AF.

OpenServer 6 D2D Backup Issues

Before booting from *Recover**EDGE*** media, you must have the correct disk cartridge inserted, and it can not be write protected. If you need to change the cartridge, you'll need to shut down *Recover**EDGE***, replace the cartridge, and boot again.

14.12 - Storage Device Preparation Example (OpenServer 5)

NOTE: Microlite does not support the use of SATA disk cartridge based drives as backup devices. This is because the OpenServer 5 "wd" driver cannot reference the drive during the second phase of the "mkdev hd" operation.

Device Node Creation

Use the "mkdev hd" command twice; once to create a kernel entry and, after rebooting, a second time to create device nodes and filesystems for the USB hard drive, flash drive, or disk cartridge drive. After that, **fdisk** and **divvy** should be run individually on any additional drives or cartridges.

```
# mkdev hd
```

```
Your root hard disk is attached to an IDE controller.
Pick one of the choices below or you may quit and
invoke mkdev hd -u for a detailed usage message.
                1) Add a hard disk to an IDE controller
                2) Add a hard disk to a SCSI controller
                3) Add a hard disk to an IDA controller (EISA)
                4) Add a hard disk to a  USB controller
Enter 1, 2, 3, 4 or enter 'q' to quit: 4

The Host Adapter parameters will be automatically configured
What is the USB Device ID for this device?
Select 0-15, or h for help, or q to quit: 0

What is the LUN of this device?
 Press <Return> to use the default: 0
Select 0-7, or h for help, or q to quit: 0

You are about to add the following USB device:
USB Hard Disk configured as USB Device ID 0, LUN 0
Update USB configuration? (y/n) y

The USB configuration file has been updated.
Disk already configured as disk number 1 (/dev/dsk/1s0)
A new kernel must be built and rebooted before disk configuration can
continue.
Would you like to relink at this time? (y/n) y

        The UNIX Operating System will now be rebuilt.
        This will take a few minutes.  Please wait.
        Root for this system build is /
        The UNIX Kernel has been rebuilt.
Do you want this kernel to boot by default? (y/n) y
Backing up unix to unix.old

Installing new unix on the boot file system
The kernel environment includes device node files and /etc/inittab.
The new kernel may require changes to /etc/inittab or device nodes.
Do you want the kernel environment rebuilt? (y/n) y

The kernel has been successfully linked and installed.
        To activate it, reboot your system.
Setting up new kernel environment
After the system is rebooted with the new kernel,
reinvoke mkdev hd to initialize the new hard disk.
```

Reboot the computer and log back in as **root**.

```
# mkdev hd
```

```
Your root hard disk is attached to an IDE controller.
Pick one of the choices below or you may quit and
invoke mkdev hd -u for a detailed usage message.
                1) Add a hard disk to an IDE controller
                2) Add a hard disk to a SCSI controller
                3) Add a hard disk to an IDA controller (EISA)
                4) Add a hard disk to a  USB controller
Enter 1, 2, 3, 4 or enter 'q' to quit: 4

The Host Adapter parameters will be automatically configured
What is the USB Device ID for this device?
Select 0-15, or h for help, or q to quit: 0

What is the LUN of this device?
 Press <Return> to use the default: 0
Select 0-7, or h for help, or q to quit: 0

Disk already configured as disk number 1 (/dev/dsk/1s0)
During installation you may choose to overwrite all
or part of the present contents of your hard disk.
Do you wish to continue? (y/n) y

The hard disk installation program will now invoke /etc/fdisk.
Entering 'q' at the following menu will exit /etc/fdisk,
and the hard disk installation will continue.
If you wish to exit the entire installation at this menu,
press the <DEL> key.
        1. Display Partition Table
        2. Use Entire Disk for UNIX
        3. Use Rest of Disk for UNIX
        4. Create UNIX Partition
        5. Activate Partition
        6. Delete Partition
        7. Create Partition
Enter your choice or 'q' to quit: 2

Current Hard Disk Drive: /dev/rdsk/1s0
        +-------------+----------+-----------+---------+---------+---------+
        | Partition   | Status   | Type      |   Start |     End |    Size |
        +-------------+----------+-----------+---------+---------+---------+
        | 1           | Active   | UNIX      |       1 | 3720959 | 3720959 |
        +-------------+----------+-----------+---------+---------+---------+
Total disk size: 3721215 tracks (256 reserved for masterboot and diagnostics)
Press <Return> to continue Enter

        1. Display Partition Table
        2. Use Entire Disk for UNIX
        3. Use Rest of Disk for UNIX
        4. Create UNIX Partition
        5. Activate Partition
        6. Delete Partition
        7. Create Partition
Enter your choice or 'q' to quit: q
```

```
There are 117202207 blocks in the UNIX area.
Please enter the number of file systems you want this area
to be divided into, or press <Return> to get the default of 7 file system(s)
1

The layout of the filesystems and swap area is now prepared.
Do you wish to make any manual adjustments to the sizes or
names of the filesystems or swap area before they are created
on the hard disk? (y/n) y
+-------------------+------------+--------+---+-------------+------------+
| Name              | Type       | New FS | # | First Block | Last Block |
+-------------------+------------+--------+---+-------------+------------+
| d45050            | HTFS       |  yes   | 0 |           0|   117202206|
|                   | NOT USED   |  no    | 1 |           -|           -|
|                   | NOT USED   |  no    | 2 |           -|           -|
|                   | NOT USED   |  no    | 3 |           -|           -|
|                   | NOT USED   |  no    | 4 |           -|           -|
|                   | NOT USED   |  no    | 5 |           -|           -|
|                   | NOT USED   |  no    | 6 |           -|           -|
| d45057all         | WHOLE DISK |  no    | 7 |           0|   117210207|
+-------------------+------------+--------+---+-------------+------------+
117202207 1K blocks for divisions, 8001 1K blocks reserved for the system
 n[ame]       Name or rename a division.
 c[reate]     Create a new file system on this division.
 d[elete]     Delete a file system on this division.
 t[ype]       Select or change filesystem type on new filesystems.
 p[revent]    Prevent a new file system from being created on this division.
 s[tart]      Start a division on a different block.
 e[nd]        End a division on a different block.
 r[estore]    Restore the original division table.
Enter your choice or q to quit: n
 which division? (0 through 7)?0
 what do you want to call it? backups
+-------------------+------------+--------+---+-------------+------------+
| Name              | Type       | New FS | # | First Block | Last Block |
+-------------------+------------+--------+---+-------------+------------+
| backups           | HTFS       |  yes   | 0 |           0|   117202206|
|                   | NOT USED   |  no    | 1 |           -|           -|
|                   | NOT USED   |  no    | 2 |           -|           -|
|                   | NOT USED   |  no    | 3 |           -|           -|
|                   | NOT USED   |  no    | 4 |           -|           -|
|                   | NOT USED   |  no    | 5 |           -|           -|
|                   | NOT USED   |  no    | 6 |           -|           -|
| d45057all         | WHOLE DISK |  no    | 7 |           0|   117210207|
+-------------------+------------+--------+---+-------------+------------+
117202207 1K blocks for divisions, 8001 1K blocks reserved for the system
 n[ame]       Name or rename a division.
 c[reate]     Create a new file system on this division.
 d[elete]     Delete a file system on this division.
 t[ype]       Select or change filesystem type on new filesystems.
 p[revent]    Prevent a new file system from being created on this division.
 s[tart]      Start a division on a different block.
 e[nd]        End a division on a different block.
 u[ndo]       Undo the last change.
 r[estore]    Restore the original division table.
Enter your choice or q to quit: q
 i[nstall]      Install the division set-up shown
 r[eturn]       Return to the previous menu
 e[xit]         Exit without installing a division table
Please enter your choice: i
Making filesystems
Hard disk initialization procedure completed.
```

Please note that it may take a while to create a new filesystem on a large USB hard drive.

Device Node Identification

For this example, the hard drive used was only the second hard drive on the system and the first USB device instance, so that in the commands above the controller is **0** and the LUN is **0**, yielding the following useful nodes:

Description	Device Node
Raw device node - Entire disk - Used for fdisk	`/dev/rdsk/1s0`
Block Device Node - Entire disk - used in *af Resource* & *RecoverEDGE*.	`/dev/dsk/1s0`
Block Device Node - Entire disk - used for divvy command	`/dev/dsk/1s0`
Block Device Node - Partition 1 - Disk Partition used for backups (mount device)	`/dev/backups`

Creating Partitions on (additional drives / cartridges)

Initial preparation would have created an fdisk partition, divvy table and filesystem on the drive or disk cartridge connected at the time of configuration above. For each additional drive or cartridge, you must...

1 Run "**fdisk -f /dev/rdsk/1s0**" to configure the drive.

```
        1. Display Partition Table
        2. Use Entire Disk for UNIX
        3. Use Rest of Disk for UNIX
        4. Create UNIX Partition
        5. Activate Partition
        6. Delete Partition
        7. Create Partition

Enter your choice or 'q' to quit: 2

Current Hard Disk Drive: /dev/rdsk/1s0

        +-------------+----------+-----------+---------+---------+---------+
        | Partition   | Status   | Type      |   Start |     End |    Size |
        +-------------+----------+-----------+---------+---------+---------+
        | 1           | Active   | UNIX      |       1 | 2441535 | 2441535 |
        +-------------+----------+-----------+---------+---------+---------+

Total disk size: 2441600 tracks (65 reserved for masterboot and diagnostics)

Press <Return> to continue Enter

        1. Display Partition Table
        2. Use Entire Disk for UNIX
        3. Use Rest of Disk for UNIX
        4. Create UNIX Partition
        5. Activate Partition
        6. Delete Partition
        7. Create Partition

Enter your choice or 'q' to quit: q
```

2 Run "**divvy -m /dev/dsk/1s0**" to configure as 1 partition and create a new filesystem.

```
There are 39063552 blocks in the UNIX area.
Please enter the number of file systems you want this area
to be divided into, or press <Return> to get the default of 7 file system(s)
1

The layout of the filesystems and swap area is now prepared.

Do you wish to make any manual adjustments to the sizes or
names of the filesystems or swap area before they are created
on the hard disk? (y/n) n

Making filesystems
```

Your hard disk drives, cartridges and filesystems are now prepared. Use the correct nodes in *EDGEMENU* to create a new AF Resource.

Completed AF Example Resource.

```
+ BackupEDGE Resource Information ------------------------------------------+
|- General Resource Information ------------------------------------------- |
|Resource Type       Attached Filesystem                                     |
|Resource Name       [af0               ] Change as appropriate              |
|Description         [Attached Filesystem Resource]                          |
|Changer Assoc       [Standalone Device]                                     |
|Interface           [Other      ]                                           |
|                                                                            |
|- Attached Filesystem Information ---------------------------------------- |
|Mount Dir           [/usr/lib/edge/system/mnt/af0                         ] |
|Mount Device Node   [/dev/dsk/backups           ]                           |
|Mount Command       [/etc/mount %m %M                                     ] |
|Unmount Command     [/etc/umount %M                                       ] |
|Exclude Node        [/dev/dsk/1s0                                         ] |
|                                                                            |
|[Next]                              [Prev]                          [Cancel]|
+----------------------------------------------------------------------------+
```

The **`Mount Device Node`** and **`Exclude Node`** are critical. Get the **`Mount Device Node`** wrong and you can't make backups. Get the **`Exclude Node`** wrong and *Recover**EDGE*** won't know to always exclude this device from (being erased) during disaster recovery.

Remember to create a matching Attached Filesystem (af) Resource, as shown i.n "Setting Up a FileSystem Partition Resource" on page 163, and associate it with the AF.

Insert each cartridge, or plug in each drive to be used, and use the initialization command in edgemenu to prepare the drive or cartridge to accept a *Backup**EDGE*** archive.

14.13 - D2D Notes

Some release of *Backup**EDGE*** have an initialization problem. If initialization fails, mount the device manually, create an **fspo** directory on the media, unmount it, and re-initialize it. For example, the procedure might be:

```
# mount /dev/dsk/c0b1t0d0p1s0 /mnt
# mkdir /mnt/fsp0
# umount /mnt
```

Run `edgemenu - Admin - Set Default Backup Resources`. Set the default Resource to **fspo**.

Run `edgemenu - Admin - Initialize Medium`. Initialize the disk drive or cartridge.

You must initialize each removable disk drive or disk cartridge before use.

*Backup**EDGE*** does allow access to an attached storage device on a remote machine that is also controlled by *Backup**EDGE***, just like it can write to a remote tape drive. This works fine with disaster recovery. In other words, the attached storage device should be defined as a resource **only** on the machine to which the storage is physically attached. If that resource is an FSP with an AF, then it may be used for disaster recovery by that machine, and by remote machines. If it is an FSP without an AF, then it can be used for disaster recovery by remote machines only.

14.14 - RecoverEDGE Reminder

After adding a new *Resource* to *Backup**EDGE*** and creating at least one successful backup, always remember to re-create your *Recover**EDGE*** media and / or images so that they will understand how to use the *Resource*. Test them to make sure you can read from the *Resource* if necessary.

15 - MySQL / MariaDB Backups

15.1 - Configuring MySQL™ / MariaDB Backups

*Backup**EDGE*** performs MySQL[1] Hot Backups (live backups of MySQL databases[2]) by creating a special *Backup Domain* with the information and instructions necessary to cause the `mysqldump` command to send its output directly into its file input stream. The MySQL *Domain* is generally appended to the full `system` *Backup Domain* (or any other *Domain* but can also be scheduled separately.

To set up MySQL™ backups in *Backup**EDGE***, you should only have to run the installation program. It will ask you if you would like to include MySQL backups along with your normal filesystem backups. You will need to provide the following information (see example screen shots below):

- Connection Method (UNIX or TCP/IP Socket)
- Socket Path (usually autodetected) / Hostname and TCP/IP Port
- MySQL User Name
- MySQL Password

*Backup**EDGE*** will automatically detect all databases and tables supported by one MySQL server and display a count of tables and databases detected. It will then create a *Backup**EDGE*** Domain called mysql that includes this information. You may (and are encouraged to) review and edit this information, to see if the *Backup**EDGE*** autodetector has done something sane in your installation. This can be done via the *Domain Editor*.

There are a few things to keep in mind when using *Backup**EDGE*** for MySQL backups:

- By default, *Backup**EDGE*** creates one *Domain* for MySQL backups. The domain further subdivides your MySQL data into what are called `pieces`. Each `piece` will ultimately correspond to a single file on the archive (i.e., you can choose to restore one `piece` independently of the next). Further, by default, each `piece` corresponds to a single database. While you may change this default setup in the domain editor, it is important to realize that it exists. Note that each `piece` represents a call to the *mysqldump* utility.
- *Backup**EDGE*** cannot perform a level-2 verification of MySQL data, since it is assumed that the data in the MySQL server will change. This data will be level-1 verified, even if the backup job specifies level-2 verification. Other data, such as filesystem data, will be verified via level-2 as always.
- You should review the settings that *Backup**EDGE*** will use during backup by using the Domain Editor. To access this, enter *EDGEMENU*, use `Setup:Enable Advanced`, then *Schedule: Create/Edit Domain*.
- *Backup**EDGE*** can perform only *Master Backups* of MySQL data. *Differential Backups* and *Incremental Backups* are not supported and MySQL backups will ignore those settings at this time, in favor of a *Master Backup*. Binary log backups are not supported.
- A MySQL setup wizard can be run automatically during *Backup**EDGE*** installation. You may re-run the setup wizard to either configure MySQL backups or to add new databases by running EDGEMENU and selecting:
  `Setup -> Configure BackupEDGE -> Configure MariaDB/MySQL(tm) Backups`

1. MySQL or MariaDB backups are identical. This guide will only use the term MySQL to refer to both.
2. This feature is not available on OpenServer 5.

- During a disaster recovery, you can not restore MySQL backups until after you have rebooted and launched *EDGEMENU*.

NOTE: It may be necessary, especially with InnoDB™ tables, to take some corrective action before performing the restore. This is because InnoDB tables sometimes do not restart cleanly after an unclean shutdown without additional steps. If you have backed up all tables from all databases, then you can simply remove all tables and databases and restore them all from your archive. Restores might fail until you do this, complaining that the connection to the MySQL server has been lost.

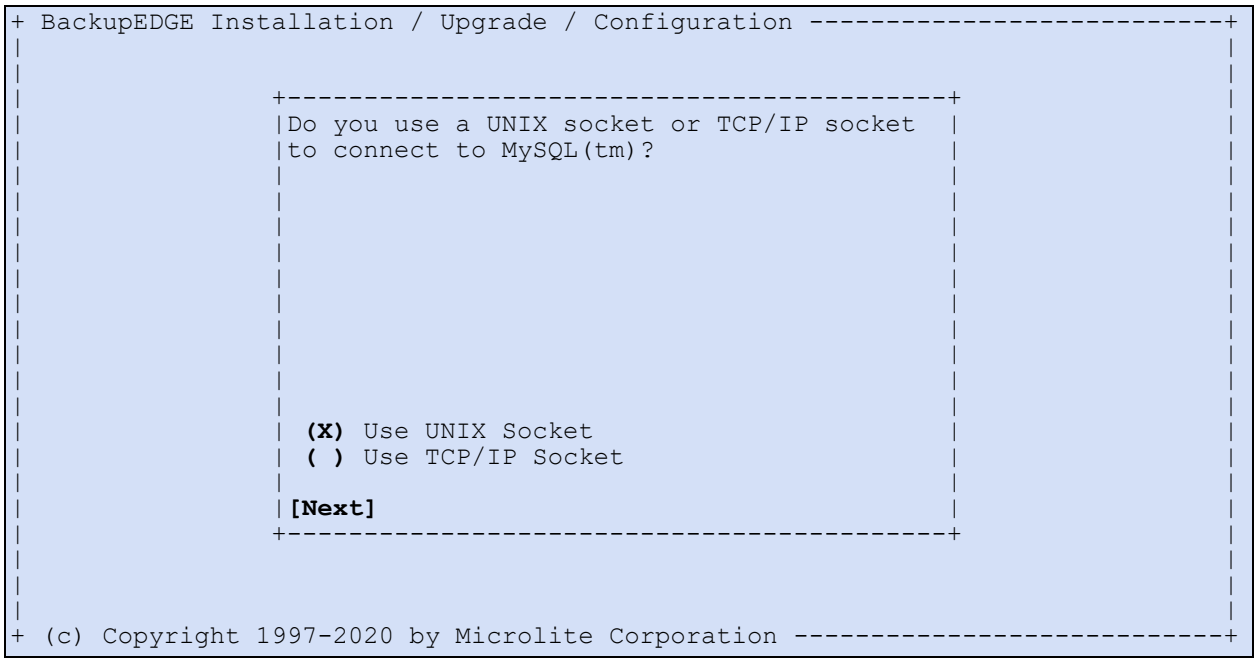
- As mentioned earlier, by default, *Backup**EDGE*** backs up each database separately. For each, if all tables are InnoDB tables, then it will wrap the entire backup in a single transaction, else it will lock all tables to ensure consistency. In the former case, exactly what consistency guarantees a transaction provides depends on how you have configured transaction isolation in the MySQL server.
- It is not currently possible to select a different database during restore; if you want to isolate the data for testing, use a different MySQL server.

MySQL Backup - Autodection of Connection

```
+ BackupEDGE Installation / Upgrade / Configuration ----------------------------+
|                                                                               |
|                                                                               |
|                 +-------------------------------------------+                 |
|                 |           MySQL(tm) Connection            |                 |
|                 |                                           |                 |
|                 |It appears that you use a UNIX socket      |                 |
|                 |/var/lib/mysql/mysql.sock to access the    |                 |
|                 |MySQL server.  Is this right?              |                 |
|                 |                                           |                 |
|                 |                                           |                 |
|                 |                                           |                 |
|                 |                                           |                 |
|                 |                                           |                 |
|                 |                                           |                 |
|                 |                                           |                 |
|                 | (X) Yes, Use This Socket                  |                 |
|                 | ( ) No, Let Me Pick                       |                 |
|                 |                                           |                 |
|                 |[Next]                               [Exit]|                 |
|                 +-------------------------------------------+                 |
|                                                                               |
|                                                                               |
|                                                                               |
+ (c) Copyright 1997-2020 by Microlite Corporation ----------------------------+
```

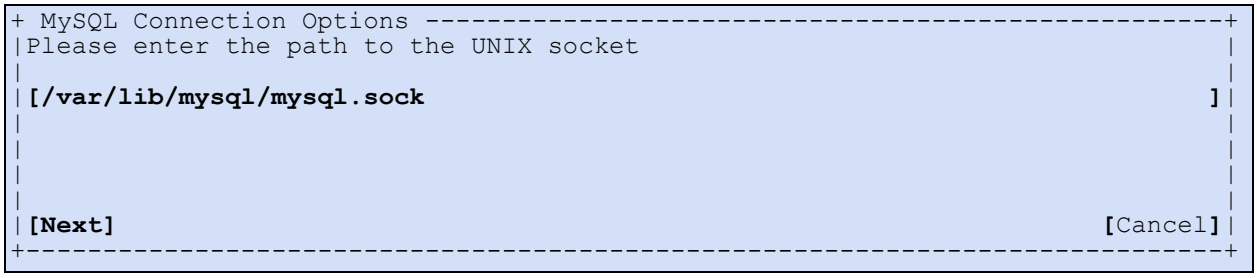
If the installer autodetects a connection to a MySQL database, it will offer to use this connection. Selecting it will continue to the `Username` and `Password` prompts below. Otherwise you'll need to choose the `Connection Method` and `Socket Path` as shown in the next two examples.

MySQL Setup - Connection Method



By default, MySQL is configured to use UNIX sockets. Change this selection only if your administrator has configured the MySQL server differently.

MySQL Setup - Socket Path



The installed will autodetect the UNIX socket path. You must generally enter a TCP/IP socket manually.

MySQL Setup - Login Name

```
+ MySQL Username and Password ------------------------------------------------+
|Please enter the MySQL user name which will be used by BackupEDGE to perform  |
|MySQL backups.                                                                |
|[root                                                                        ]|
|                                                                              |
|                                                                              |
|                                                                              |
|                                                                              |
|[Next]                                                              [Cancel]|
+------------------------------------------------------------------------------+
```

MySQL Setup - Password

```
+ MySQL Username and Password ------------------------------------------------+
|Please enter the password for the MySQL user.                                 |
|                                                                              |
|[********                                                                   ]|
|                                                                              |
|                                                                              |
|                                                                              |
|                                                                              |
|[Next]                                                              [Cancel]|
+------------------------------------------------------------------------------+
```

If *Backup**EDGE*** can successfully authenticate to the MySQL server, the number of tables and databases found will be displayed. If not, an error will occur and you will be prompted to either retry or cancel the MySQL setup.

15.2 - The BackupEDGE MySQL Domain

Here is a screen shot of the basic MySQL *Domain* as detected by *Backup**EDGE***:

MySQL Setup - Password

```
+Edit Backup Domain----------------------------------------------------------+
|Machine:            web2v.microlite.com                                     |
|Name:               [mysql                                                ]|
|Description:        [MySQL Autodetected Backup Domain                     ]|
|                                                                            |
|-Edit MySQL Backup Domain-----------------------------------------------------|
|Piece Name:         [information_schema                                   ]|
|                                                                            |
| +Piece Name------+                                                         |
| |-> information_s| [ ]  All Databases     [X]  Add DROP DATABASE          |
| |   microlite    | [ ]  Add DROP TABLE    [X]  Include --opt              |
| |   mysql        | [ ]  Lock All Tables   [X]  Include --routines         |
| +-----vv More vv-+ [X]  Lock Tables Per DB  [X]  Include --triggers        |
|                    [ ]  Single Transaction                                 |
|  Additional Args:  [--databases --extended-insert=false --net_buffer_len=409]|
|  Database Name(s): [information_schema                                   ]|
|                                                                            |
|  Config File:      [/usr/lib/edge/system/my.cnf                          ]|
|  Encrypt All:      [ ]                                                     |
|                                                                            |
|                                                                            |
|[Save]                        [Back To Select]                    [Cancel]|
+----------------------------------------------------------------------------+
```

A *Backup**EDGE*** MySQL domain breaks the database up into `pieces`. By default, a `piece` corresponds to exactly one MySQL database. While it is not required that this be true, the *Backup**EDGE*** MySQL autodetection system will create one `piece` per database.

Each `piece` can be configured, via the checkboxes, to use different arguments to the `mysqldump` command-line utility. `[Tab]`bing into the `Piece Name` window and scrolling through the `pieces` will displays the options and additional arguments for that piece. While on a specific `piece` it is possible to `[Tab]` to the options flags and select or de-select them. Further, the `Additional`

`Args` and `Database Name(s)` specify per-piece options. The `Config File` field and `Encryption` checkbox affect the entire MySQL Domain. The `Encrypt All` checkbox can only be used if the *BackupEDGE* encryption option has been licensed.

When configuring a piece, it is important to guarantee that the backup will be a consistent snapshot. If the tables included in the `piece` are in use during the backup, then failure to do this could result in an unusable backup. Generally, there are three options: `Lock All Tables`, `Lock Tables Per DB`, and `Single Transaction`. These options are mutually exclusive.

`Lock All Tables` causes `mysqldump` to obtain a global lock across all tables, regardless of the database they are in, before beginning the backup. This corresponds to the `mysqldump` command-line option `--lock-all-tables`. Note that this can have a large impact on database performance during the backup.

`Lock Tables Per DB` corresponds to the `mysqldump` command-line option `--lock-tables`. It locks tables in the current database.

`Single Transaction` is valid only for those pieces that consist entirely of tables which support ACID transactional semantics. Generally, this includes InnoDB but not MyISAM tables. If you are backing up only InnoDB tables in this piece, then `Single Transaction` will use transactions instead of locks to guarantee a consistent backup. This corresponds to the `mysqldump` option `--single-transaction`. Using this option when MyISAM tables are included in the piece will cause those tables to be backed up without any locking

The `All Databases` option, if checked, causes *BackupEDGE* will include all databases in this `piece`, regardless of the databases listed in the `Database Name(s)` field. Normally, this option should be left unchecked. In that case, *BackupEDGE* will include the `--databases` option to `mysqldump`.

As mentioned above, The `Encrypt All` checkbox can only be used if the *BackupEDGE* encryption option has been licensed.

The remaining options correspond directly to `mysqldump` command-line options; please consult the documentation for your particular version of `mysqldump`.

15.3 - Restoring MySQL Backups

How to Restore MySQL™ Backups as Part of Normal Operation Directly into MySQL

This section is for those people who:

- Want to restore one or more MySQL backups from a *BackupEDGE* archive, **and**
- Have a functioning MySQL installation

This procedure is generally straightforward. The major steps are:

1. Decide which database piece(s) from which archive(s) you wish to restore. Use *EDGEMENU* to read the archive labels to see the *date* and *Domain* names, and the listing option to see individual filenames.
2. Stop any applications that are using the database(s), or will otherwise be affected by the restore operation.
3. In rare cases, drop any tables that are to be restored. By default, the drop commands will be executed automatically as part of the restore process, so usually this step is not needed.
4. Execute the restore via *EDGEMENU*.

Recall that a `piece` is a *BackupEDGE* term for **part of a database**. By default, *BackupEDGE* creates one `piece` per MySQL database as part of the MySQL autodetection process.

When viewing an archive listing, each piece appears as one file on the archive. When you select the file(s) to restore, you are actually selecting the `piece(s)`.

The most crucial part is to decide which database `piece(s)` are to be restored. If you want to restore part of a piece, then you should skip to "How to Restore MySQL™ Backups as Part of Normal Operation Directly into a File" on page 183 below.

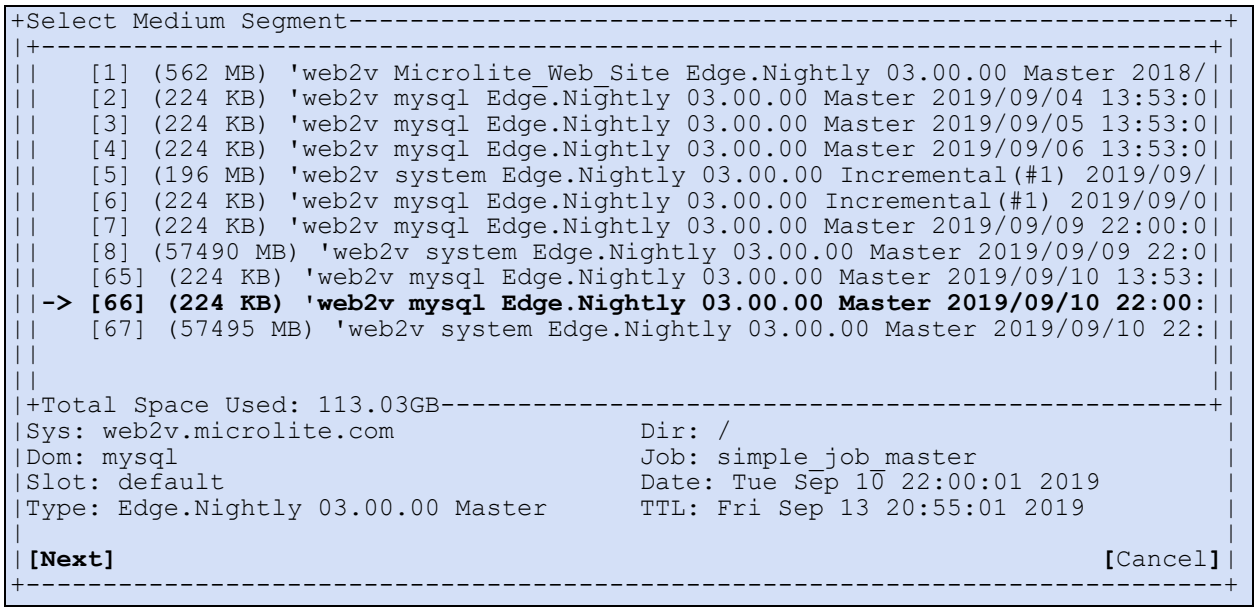
If you do want to restore one or more complete pieces, simply note the filenames. By performing a selective restore in *EDGEMENU*, you may select exactly those files. *Backup**EDGE*** will prompt for confirmation before it restores each.

For each file, the data will be sent to the MySQL server that was last used for autodetection on the current machine. This is a very important point: *Backup**EDGE*** does not automatically try to restore the data to the original MySQL server This allows a lot of flexibility to restore archives to new MySQL instances to inspect the data, without modifying the live database.

Again, *Backup**EDGE*** will try to restore the MySQL data to the MySQL server that was last used for autodetection. The settings can be found in `/usr/lib/edge/system/config/my.cnf`.

After the restore completes, you will be notified about the success or failure.

Choose `Restore -> Restore Entire Archive` and select the MySQL backup to be restored.



On the restore screen, choose ONLY `Execute Restore`. Don't change anything else.

```
+ Edgemenu for BackupEDGE ------------------------------------------------+
|+-------------------------------------------------------------------------+|
||-----------------[Restore]-----------------------------------------------||
|+-------------------------------------------------------------------------+|
|- Restore Entire Archive ------------------------------------------------|
| Restore Parameters                          Archive Label Info          |
| [Y] Destructive                Edge.Nightly 03.00.00 Master             |
| [N] Strip Absolute Path        Domain:   MariaDB-MySQL Autodetected Backup D|
| [N] Flat Restore               Sequence: On-Site Backups                |
| [N] Restore If Newer           Date:     Tue Sep 10 22:00:01 2019       |
| [N] Use Xtrct mtime            System:   web2v.microlite.com            |
|                                Medium Usage: 1                          |
|                                                                         |
| Original Dir: /                                                         |
| Restore To:  [/                                                      ]  |
| [Execute Restore]  [Modify Excludes]                  [Cancel]          |
|+-----------------------------------------------------------------------+|
||Primary Resource : web2v:url!url0                                       ||
||  Compress: Soft, HW Block:  N/A, Edge Block:   64, Partition: C        ||
||                                                                        ||
||                                                                        ||
||                                                                        ||
||Last Master Backup: Tuesday Sep 10 22:00:01 2019                        ||
|+Local Machine: web2v.microlite.com  Administering: web2v.microlite.com -----+|
+-------------------------------------------------------------------------+
```

For **each** piece in the MySQL backup, answer `[Yes]` to restore, or `[No]` to skip.

```
+ Edgemenu for BackupEDGE ------------------------------------------------+
|+-------------------------------------------------------------------------+|
|| [File] [Backup] [Restore] [Verify] [Admin] [Setup] [Schedule]           ||
|+-------------------------------------------------------------------------+|
|- Restore Entire Archive ------------------------------------------------|
| Restore Parameters                          Archive Label Info          |
| [Y] Destructi+Selection Box-----------------------------------+         |
| [N] Strip Abs|                                                |ckup Domain   |
| [N] Flat Rest|       Really restore MySQL(tm) olof.sql?       |         |
| [N] Restore I|                                                |019      |
|+ Restoring Fi|                                                |---------+|
||             |                                                |         ||
||             |                                                |         ||
||             |                                                |' to Cancel] ||
|+Files: 2   Se|                                                |---------+|
| [Execute Rest|                                                |l]       |
|+-------------|   [Yes]                                 [No]   |---------+|
||Primary Resou|                                                |         ||
||  Compress: N+-----------------------------------------------+C         ||
||                                                                        ||
||                                                                        ||
||                                                                        ||
||Last Master Backup: Tuesday Sep 10 22:00:01 2019                        ||
|+Local Machine: web2v.microlite.com  Administering: web2v.microlite.com -----+|
+-------------------------------------------------------------------------+
```

How to Restore MySQL™ Backups as Part of Normal Operation Directly into a File

This is for those people who...

- Have *Backup**EDGE*** MySQL backups that they would like to view, edit, or otherwise handle specially, before optionally sending to the MySQL server

*Backup**EDGE*** stores MySQL backups as a series of SQL commands. These commands, when executed, have the effect of restoring the data to the MySQL server.

From time to time, it may be beneficial to restore these SQL commands to a file, rather than sending them to the MySQL server. This allows you to change the database name (e.g., if you

want to restore the data into a differently named database for inspection, rather than over the original). It also allows you to inspect the state of the data, and make modifications manually.

Doing this requires use of the *EDGE* command line. You should select the archive and filenames as described in the previous section. You may use *EDGEMENU* to do this.

Once you have selected the archive and filenames, then you should go to a UNIX shell. Run the edge command line as follows:

```
# cd /
# edge xvf resource_name -zSCRIPT_MODE=ASFILE ./tmp/mysql_data/filename1
./tmp/mysql_data/filename2 …
```

where `resource_name` is the name of the resource that contains the archive. `./tmp/mysql_data/filename1` and `…2` are the filenames selected earlier. If you would like to restore these to some other directory than `/tmp/mysql_data`, change the `cd` command to reflect this. For example, `cd /usr` will restore the data to `/usr/tmp/mysql_data/filename1`.

After you have done this, the SQL commands will be located in these files. You may view, edit, delete, or send them to MySQL as you like. The `mysql` command-line utility can be used to send them to MySQL, via:

```
cat /tmp/mysql_data/filename1 |mysql
```

How to Restore MySQL™ Backups after a Disaster Recovery, or If Other Types of Restores Fail Due to a Damaged MySQL Installation

This section is for those people who:

- Have just performed a disaster recovery, and would like to recover their MySQL data from a *Backup**EDGE*** backup, **or**
- Have a non-functional MySQL installation due to serious data corruption (e.g., power-failure, etc.)

MySQL backups are ignored during a disaster recovery via *Recover**EDGE***, because the MySQL server is not running on the recovery media. The appropriate way to restore this data is to reboot normally under the hard drive, make sure that the MySQL server is operating correctly, then restore the MySQL backups via *EDGEMENU*.

The most common issue that occurs after a disaster recovery is that MySQL refuses to start. Recall that the system-level backup from which the disaster recovery restores the filesystem data does not treat MySQL data specially. As such, the files that are used by the MySQL server may be in an unreliable state. MySQL can refuse to start, or refuse to add data to existing tables, if this happens.

The solution is generally straightforward. Since all of the data will be restored from the *Backup**EDGE*** MySQL backup anyway, the goal is simply to return MySQL to a functional state. This can involve removing any of the existing MySQL data, or even removing and re-installing MySQL itself in the extreme case.

The same situation can arise if the system is shut down suddenly, such as due to a power failure. In this case, no disaster recovery has been performed, but it might still be necessary to restore MySQL data following this guide if the MySQL server does not restart cleanly. Of course, there are many methods detailed in the MySQL documentation that could recover the data in-place in this event; you might want to look into those options before resorting to restoring from your most recent *Backup**EDGE*** archive.

Either way, if you decide to restore from a *Backup**EDGE*** archive, but MySQL is not in a state to allow it, then you should consider the following.

MyISAM tables usually recover without additional work. At worst, it might be necessary to drop those tables and database(s) to be restored manually via a MySQL admin interface, or through

the MySQL command-line interface. There are other options available in the MySQL documentation for repairing MyISAM tables that might obviate the need for a restore from archive.

InnoDB tables, however, are more complicated. Broadly speaking, InnoDB tables are stored on the filesystem either (a) as two files per table, or (b) as two files per MySQL installation. The default is (b). This means that every InnoDB table in every MySQL database managed by this MySQL server shares the same two files.

If MySQL shuts down uncleanly, there are a few options in the MySQL documentation to recover them. If these methods fail, or if you desire to restore from a *Backup**EDGE*** archive for some other reason, then you must generally remove those InnoDB files which are affected. The MySQL log will often list them.

Note that in the case where only two files are used for all InnoDB tables, it is generally not possible to remove one table without removing all tables in all databases that are managed by the InnoDB engine. Consult the MySQL documentation for the proper procedure for your version of MySQL.

After the MySQL server is operating normally, you may proceed as described in the above sections. For a disaster recovery, generally you will restore all databases from the most recent archive via *EDGEMENU*.

16 - Configuring Web Services and X11 Interfaces

*Backup**EDGE*** has a unique user interface design. The interface can be rendered in one of three ways:

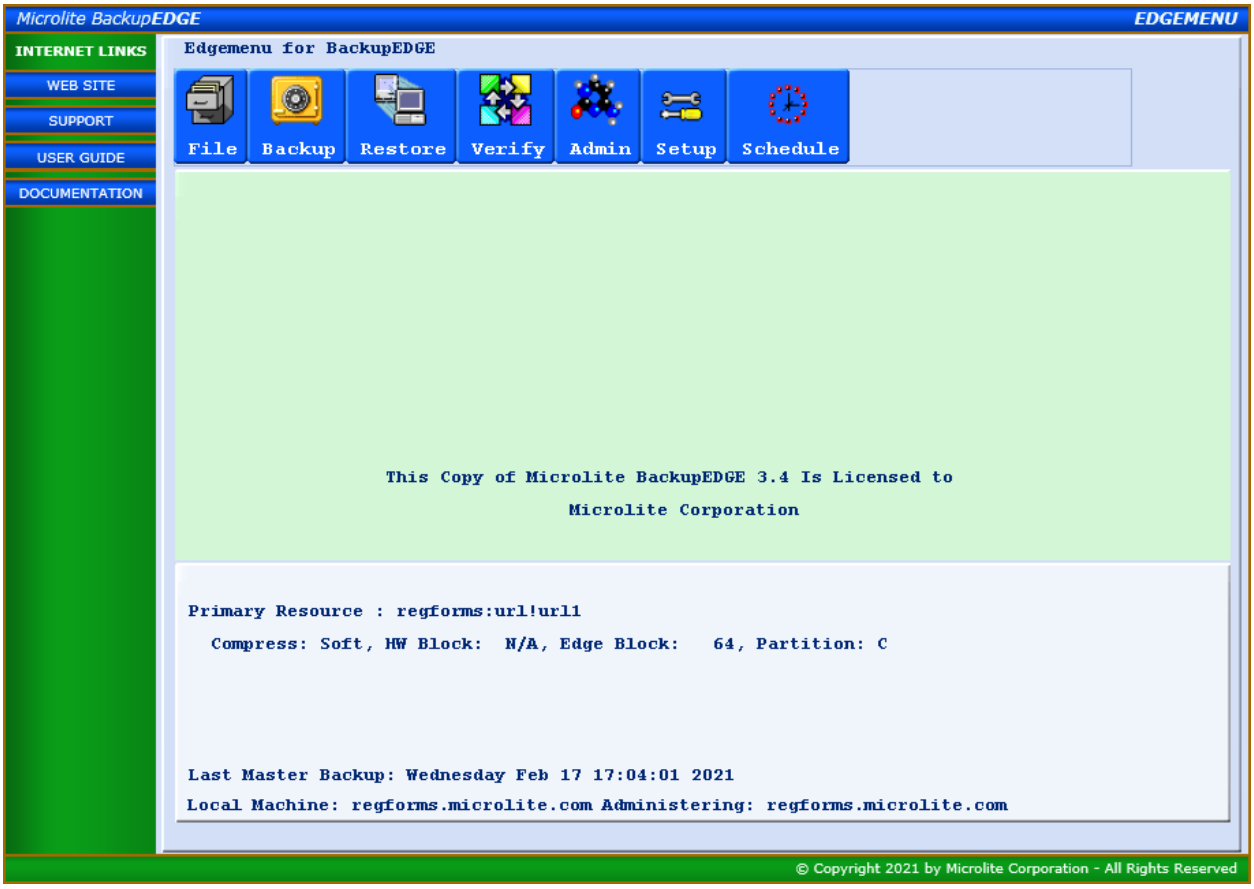
- in graphical mode as a *Web Service* from any client system supporting Sun Java 1.4.2[1] or later, such as a Windows PC.

NOTE: Many web browsers have deprecated Java plug-in support. *Backup**EDGE*** is currently known to run as a *web service* only under the *Microsoft Internet Explorer* Java plug-in.

- in graphical mode on X11 consoles or clients equipped with Sun Java 1.4.2 or later.
- in character mode on system consoles, dumb terminals or xterm clients.

The user interface runs in all three modes using the same compiled program. There are no operational differences between the interfaces, although the user has full access to features such as buttons and drop down menus when running graphically.

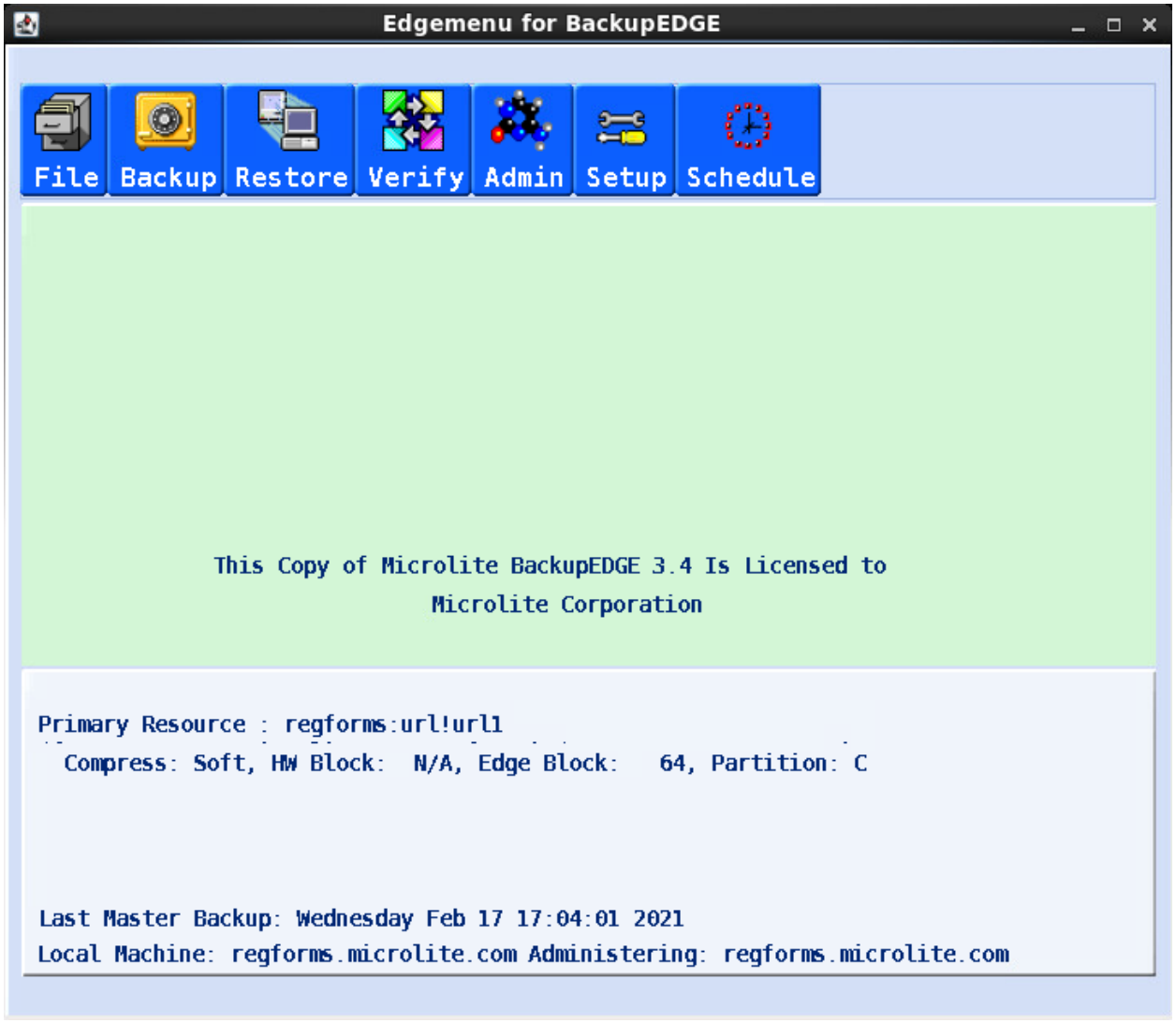
Web Services Interface Example



This is the Web Services interface example. After setup, it is accessed by browsing to port 3946 on the desired server using https.

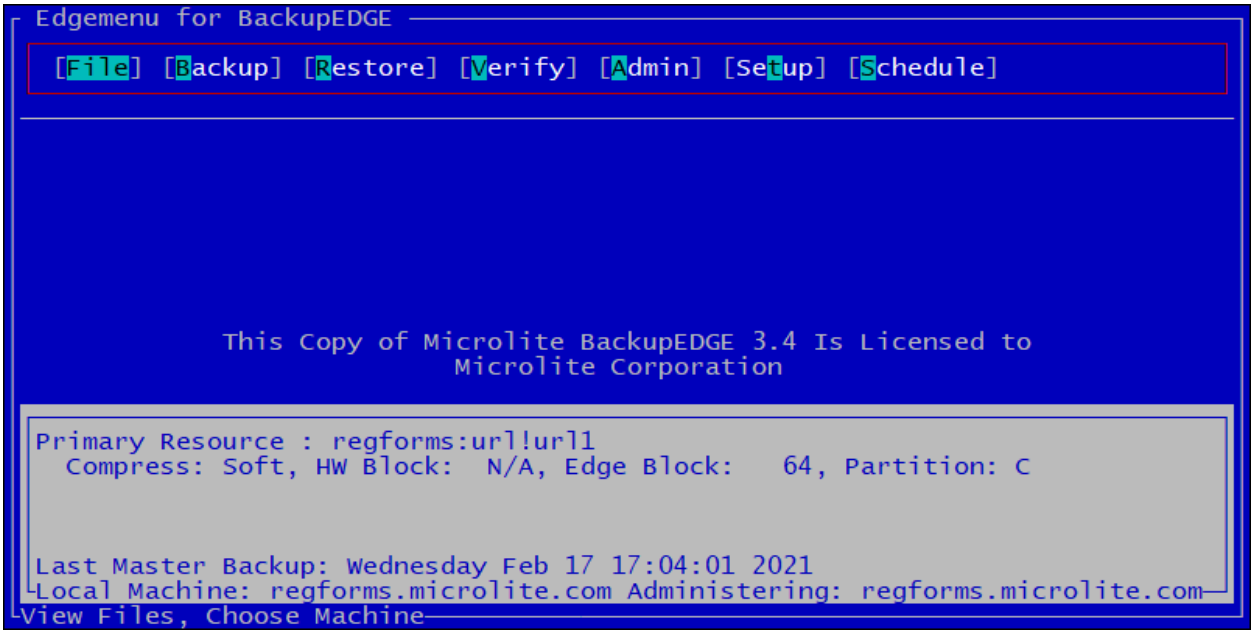
1. Sun Java 1.4.2_06 or later is recommended.

Java Interface Example



This is the native Java interface in native Window Manager of a Linux system.

Character Mode Interface Example



The character interface will scale to any window size (the window should be sized before starting *EDGEMENU*). 80x24 is the minimum size necessary for proper operation.

16.1 - X11 Interface

Theory of Operation

The *Backup**EDGE** X11 Interface* provides a graphical user interface on a user's X11 desktop.

Requirements

The X11 interface requires that the *Backup**EDGE*** server has a Java runtime environment (JRE) installed. This runtime must be version 1.4.2 or later, and must be installed before *Backup**EDGE*** so that it can be detected.

Using the X11 Interface

The *Backup**EDGE*** graphical interface for X11 is independent of *Backup**EDGE** Web Services*. Using one does not require nor preclude using the other.

Normally, during installation, a *Backup**EDGE*** icon is installed onto the desktop. Clicking this icon will start *EDGEMENU*. If Java was detected on the machine, then it will start the *EDGEMENU* graphical X11 desktop. Otherwise, a window should open containing the *EDGEMENU* character interface. Note that it can take a moment to start the X11 interface because the Java runtime must load.

If you want to configure the icon to start the character interface even if Java was detected, edit the file:

```
/usr/lib/edge/system/pconfig/defaults/java
```

Change the line:

```
JAVA_X11=YES
```

to say

```
JAVA_X11=NO
```

The icon will now always start the character interface.

16.2 - The Web Services Interface

NOTE: Beginning with release 03.01.01 build 2, a Java Commercial Code Signing Certificate is used with our Web Services Interface. Security Updates in Java 8 Update 71 or later are not compatible with our Java signed certificate by default. Please see the support note at: http://www.microlite.com/support/edgefax71.ts.html for the proper changes to support *Backup**EDGE***.

Theory of Operation

*Backup**EDGE** Web Services* provides access to the *EDGEMENU* user interface of a *Backup**EDGE*** installation from any Java-enabled web browser. By using SSL[1] to communicate with the server, *Backup**EDGE** Web Services* provides secure access to a *Backup**EDGE*** installation even via the Internet.

1. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/). Please see /usr/lib/edge/docs/LICENSE.OPENSSL for more information about the OpenSSL project and its licensing terms.

Requirements

In order to run the *BackupEDGE Web Services* interface:

- You must have a Java-enabled web browser. The JRE must be 1.4.2 or later. Earlier versions of the JRE will not work with *BackupEDGE Web Services*.
- The web browser must be able to access the *BackupEDGE* server via the network.
- Port 3946 must be open if the web service will be connected through a firewall.

It is *not* necessary for the *BackupEDGE* server to have JRE installed on it to use the *BackupEDGE Web Services* interface. Only the client web browser is required to have a Java plug-in installed.

Configuring and Starting the Web Services Daemon

BackupEDGE Web Services must be configured before they can be used. To do this, log in as `root`, go into *EDGEMENU* and select
`Setup -> Configure BackupEDGE -> Configure ->BackupEDGE Web Interface`.

Or from the command line, type:

```
edge.config -web_setup
```

Either of these will start the *BackupEDGE Web Services* configuration program. This program takes the following steps:

- An SSL key is generated. *BackupEDGE Web Services* uses this key to communicate with the web browser client securely. This can take a moment.
- You are asked for a *BackupEDGE Web Services* password. If a password is already set, you are given the option to keep it. Either way, the *BackupEDGE Web Services* password must be entered before the web browser client is allowed to access *BackupEDGE*. This password does **not** have to be the same as any user account on the system. Remember, however, that *BackupEDGE Web Services* provides access as `root` to the *EDGEMENU* user interface. While the *BackupEDGE Web Services* password does not have to be the same as your `root` password, you should be ensure that it is not easily guessed.
- You are asked if *BackupEDGE Web Services* should be started automatically on system bootup. If this is enabled, then the *BackupEDGE Web Services* daemon will be available to accept client connections after any reboot. If it is disabled, then the *BackupEDGE Web Services* daemon will have to be started manually before any clients can connect. It is generally a good idea to enable this feature.

  Note that enabling this feature does not start the *BackupEDGE Web Services* daemon at this point; it only causes it to be started during the bootup sequence.
- If the *BackupEDGE Web Services* daemon is not currently running, then you are given the option to start it immediately. This daemon allows web browser clients to use the *BackupEDGE Web Services* interface.

After these steps have been completed, *BackupEDGE Web Services* should be configured and ready for use (assuming that the daemon has been started, of course).

Access Through Firewalls

If you would like to access *BackupEDGE Web Services* from beyond a firewall, then you must allow connections to port `3946/tcp`. This port is used by the Java client to talk to the *BackupEDGE Web Services* daemon.

Stopping Web Services

To stop any currently running *BackupEDGE Web Services* daemon, issue the following command while logged in as root:

```
/usr/lib/edge/bin/edge.launch stop websrv
```

This will stop any new clients from connecting to *BackupEDGE Web Services* on this machine. Existing clients will not be disconnected.

To stop the *BackupEDGE Web Services* daemon from restart on the next system reboot, you should use

```
edge.config -web_setup
```

or `Setup -> Configure BackupEDGE -> Configure ->BackupEDGE Web Interface` from EDGEMENU.

This won't stop any currently running daemon; you must run both `edge.launch` as shown above and `edgemenu -web_setup` to stop the current daemon and disable the start-on-bootup behavior. Of course, if no daemon is running, it is not necessary to run `edge.launch`. Similarly, if *BackupEDGE Web Services* is not configured to start during bootup, then `edge.config -web_setup` may be skipped.

Launching EDGEMENU through Web Services

Open a browser and Browse to:

`https://server_name:3946`, where `server_name` is the hostname or IP address of the server to be administered. The browser will pop up a window and ask you for your *Web Services* password. If authentication succeeds, the *EDGEMENU* user interface will be displayed after a brief pause.

Running *EDGEMENU* as a *Web Service* and performing live backups of large numbers of files implies significant processing and network bandwidth usage as the filenames and backup status are transmitted through the network. This overhead can impact backup performance. It is anticipated that the primary uses of *Web Services* would be backup scheduling and management, and file and directory restores, as opposed to performing interactive live backups of large numbers of files.

16.3 - Java / Web Services Themes

The Java and *Web Services* interfaces were designed with user customization in mind. Users may create any number of theme directories and modify virtually any color or graphic shown on the screen. See “Themes (Java / Web Services)” on page 354 for more information.

The HTML code, borders and graphics used by *BackupEDGE Web Services* may also be changed as desired.

17 - Removing BackupEDGE

17.1 - OSR5 Platform Only

*Backup**EDGE*** is removed by typing `custom` from a character interface or running **Software Manager** from the *GUI* or `scoadmin`. From the full-screen interface, make sure that `BackupEDGE for SCO OpenServer 5` is highlighted, then use the `Software -> Remove Software` option.

Alternately, you may run `custom` from the command line. The following command will remove `BackupEDGE for SCO OpenServer 5` ...

```
custom -p misc:edgesco5 -r
```

17.2 - OSR6 Platform Only

*Backup**EDGE*** is removed by typing `custom` from a character interface or running **Software Manager** from the *GUI* or `scoadmin`. From the full-screen interface, make sure that `BackupEDGE for SCO OpenServer 6` is highlighted, then use the `Software -> Remove Software` option.

Alternately, you may run `custom` from the command line. The following command will remove `BackupEDGE for SCO OpenServer 6` ...

```
custom -p misc:edgesco6 -r
```

NOTE: *Backup**EDGE*** OSR6 releases prior to 02.02.00 must be removed using the command listed below for “All Other Operating Systems”.

17.3 - All Other Operating Systems

*Backup**EDGE*** has a simple, single command removal process. From a `root` prompt type the following commands...

```
cd /
/usr/lib/edge/bin/edge.remove
```

18 - Running EDGEMENU (Basics)

EDGEMENU is the name of the main menu program that provides an interface to all *Backup**EDGE***-related operations.

During installation, *Backup**EDGE*** will populate the `root` desktop of many popular operating systems with a *Backup**EDGE** Icon*. Simply click or double-click on the *Icon* (as the window system requires) to launch *EDGEMENU*. The character or Java version will launch as appropriate.

From a character login, type:

```
edgemenu
```

To launch EDGEMENU as a Web Service, launch your web browser and authenticate to the server system as described in “Launching EDGEMENU through Web Services” on page 191.

18.1 - First Time Execution

The first time you launch *EDGEMENU* after a new installation, you’ll get a pop-up menu that says:

```
No Primary Backup Resource Selected!
```

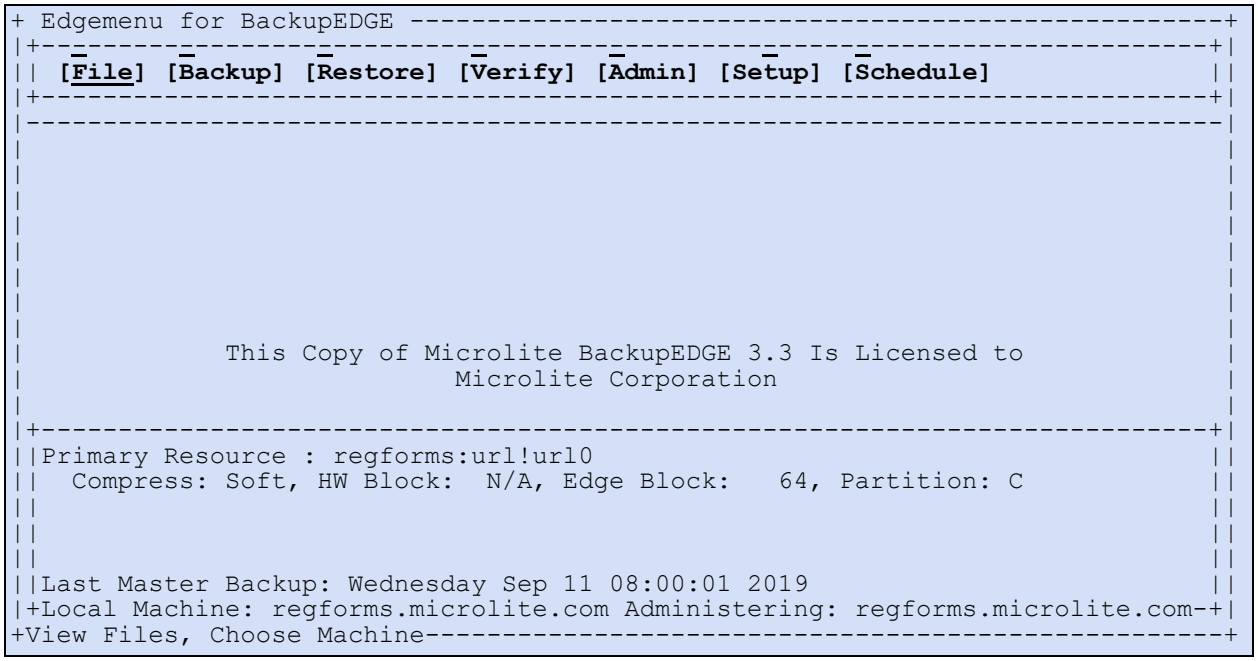
This is because *EDGEMENU* doesn’t know which backup *Device* to use when running attended backups and restores. Acknowledge the message (press `[OK]`) and you’ll get a **Fast Select** screen.

Select Primary Device

```
+ Select Primary Device ------------------------------------------------------+
|You are selecting the Destination Resource(s) to use for this Backup / Verify.|
|  This will be the Primary Resource used.                                     |
|                                                                              |
|+ Resource List -------+                                                      |
||-> optical0           | Resource :   optical0                                |
||   s3cloud0           |              HL-DT-ST BD-RE GGW-H20L YL05             |
||   tape0              | Machine :    [web2v.microlite.com                  ]|
||   url0               |                                                      |
||   sdrive0            | To select a different resource, use the Up / Down    |
||   floppy0            | arrow keys while the Next button is highlighted.  To |
||   NullDevice         | view resources on a different machine, press the TAB |
||   [NEW]              | key and type the system name in the "Machine" field, |
||                      | and press ENTER.                                     |
|+----------------------+                                                      |
|                                                                              |
|[Next]                              [Prev]                            [Cancel]|
+------------------------------------------------------------------------------+
```

Choose from the *Resource List* and press `[Next]`. or `[Tab]` up to the `Machine:` field and type a different system name to choose a *Resource* on a remote system.

18.2 - Main Menu



18.3 - Navigating EDGEMENU

`[F1]` - Field Help
`[F2]` - Exits *EDGEMENU* from almost anywhere.
`[F4]` - Completes Pathnames in *Selective Restore*.
`[F6]` - Deletes things (*Resources*, etc.).
`[F8]` - Refresh key. Redraws the display in the even it gets corrupted.
`[F10]` - Send cursor to first entry in top menu bar.
`[Up-Arrow]`/`[Down-Arrow]` - Displays drop down menus and navigates them. Scrolls through fields
`[Left-Arrow]`/`[Right-Arrow]` - Change values in scrollable fields, edit text fields, change current selection on menu bars.
`[Tab]` - Fast navigate to first field in a section
`[Enter]` - Commit a change or press the highlighted button. Start a highlighted menu operation.
`[Hot Letter]` - The highlighted letter for any menu entry may be pressed. In the screen examples in this manual, the hot letter has an Overstrike.

All *Backup**EDGE*** operations can be run from *EDGEMENU*.

18.4 - Quick - What's the fastest way to do a backup?

The quickest way to do a backup is simply to press `[B] [U] [Enter]`. This chooses the `[Backup]` drop down menu, selects the `[Unscheduled Full Backup]` option, and does an `[Execute Backup]` with all defaults intact. There are many settings on the *Unscheduled Full Backup* screen which the user may explore. They will be explained a little later in this document.

18.5 - What's the best way to do a backup?

We recommend selecting the `[Backup]`, `[Run Scheduled]` option, choosing the `Basic Schedule`, and `[Run]`ning it. This takes one extra keystroke, but it runs the same nightly backup *Scheduled Job* that you defined during installation. It also keeps *Sequence* information intact.

18.6 - Exploring EDGEMENU

Let's take a look at each option from the main menu bar.

Main Menu Bar

```
+-------------------------------------------------------------------------+
¦ [File] [Backup] [Restore] [Verify] [Admin] [Setup] [Schedule]           ¦
+-------------------------------------------------------------------------+
```

The File Menu

```
[Toggle Color/Mono]
[About edgemenu]
[Check for Updates]
[eXit]
```

Toggle Color/Mono

Some users of character color terminals and consoles prefer the visibility and speed of a mono display. This entry will toggle back and forth between black & white and color. It has no function on monochrome displays or with the Java or Web Services interfaces.

NOTE: *Backup**EDGE*** has color palette and themes that can be modified by the end user at any time. See "Themes (Java / Web Services)" on page 354 and "Color Palettes (Character Interface)" on page 354 for more information.

About edgemenu

This displays version and build date information for this version of *Backup**EDGE***, as well as current registration status and copyright notice. When calling for technical support, please have the information displayed with this button available.

Check for Updates

EDGEMENU can contact the Microlite Corporation website to determine if a newer version of *Backup**EDGE*** is available and eligible for download. Using this option instructs it to do so. You may also schedule periodic checks using the *Schedule* menu, described below.

Of course, a functioning Internet connection on the UNIX or Linux machine is required for this to work. Transport Protocol Port 80 (http) is used, so must be open outbound from your server.

eXit

This terminates *EDGEMENU*. If *EDGEMENU* was launched from an *Icon* the window will be closed. If launched from some other menu system control will be returned to the prior system. Otherwise, control is returned to the operating system prompt.

NOTE: Remember that `[F2]` can quickly exit *EDGEMENU* from almost anywhere.

The Backup Menu

```
[Unscheduled Full Backup]
[Backup Single Dir]
[Backup Multiple Files]
[Expert Backup]
[Run Scheduled]
```

Unscheduled Full Backup

This performs a full system backup, with an optional *Verify* and/or *Index* pass, and places all of its log files in the *Directory* `/usr/lib/edge/lists/menu`.

Unscheduled Full Backups performed with this menu option are ***not*** described by any *Domain* nor logged within any *Sequence*. This option is really for compatibility with older versions of *Backup**EDGE***. The preferred method of performing such a backup is to choose the *Run Scheduled* option (described on page 197) and choose either the default *Scheduled Job* or another *Scheduled Job* which better describes the actions your backup will take.

This method of creating a *Unscheduled Full Backup* is described more fully in “Unscheduled Full Backup” on page 238.

Backup Single Dir

This allows a very fast backup of a single *Directory*. The *Default Directory* is the *Working Directory* at the time *Backup**EDGE*** was launched, but it can be changed easily to any other *Directory*. Operations are logged in `/usr/lib/edge/lists/menu`.

See “Backup Single Dir” on page 238 for more information on backing up single *Directories*.

If you plan to back up the same subset of your data more than once, it is a good idea to define a *Domain*, *Sequence*, and *Scheduled Job* for this, and use “Run Scheduled” on page 243.

Backup Multiple Files

This option presents two separate lines for data entry. The first (top) line is for the entry of individual files or *Directories* to be backed up. Files and *Directories* are separated by spaces. The bottom line is to give *EDGEMENU* the full pathname of a file which contains a list of the files to be backed up. Multiple filenames containing lists of files maybe entered here. In fact, any combinations of individual files or *Directories* in the top line and pathnames of file lists in the bottom line may be combined. All filenames, *Directory* names, and lists should be typed in *Absolute Pathname* format. Operations are logged in `/usr/lib/edge/lists/menu`.

Unlike older versions of *Backup**EDGE***, the filenames you provide will not control exactly how the files are named on the archive. Instead, *EDGEMENU* will select an appropriate *Root Directory* and use relative paths to back up everything you request. This way, restore operations through *EDGEMENU* will be more likely to find the files you’re looking for later. If you *really* want the old behavior, use the “Expert Backup” option instead. It is recommended that you at least review the restore procedures before deciding, however.

See “Backup Multiple Files / Dirs” on page 239 for more information on backing up multiple files and/or *Directories*.

If you plan to back up the same subset of your data more than once, it is a good idea to define a *Domain*, *Sequence*, and *Scheduled Job* for this, and use “Run Scheduled” on page 243.

Expert Backup

Expert Backups follows very different rules than the *Backup Multiple Files* option, but that the interface is very similar. The only significant change to the interface is that before the backup begins, you may specify a different *Root Directory* for the backup.

Any of the file or *Directory* names specified will be interpreted as relative to the *Root Directory* chosen, and will be stored ***exactly that way*** on the archive. Filenames to include may be given in relative or absolute format. However, the *List File* pathnames for the second line should always be *Absolute Paths*.

It is important to understand the distinction between an Expert-mode backup and a non-Expert-mode backup. When restoring data from an Expert-mode backup, you must specify the filename exactly as they appear on the archive. Further, you must select the root directory for the restore manually. For non-Expert-mode backups, *Backup**EDGE*** expects that you will enter filenames as you would for any UNIX command. It also automatically handles the working directory unless you specifically want to change it.

The other backup options are preferable to this method, because *Backup**EDGE*** is able to predict how your data is stored on the archive, and can thus help you get it back with a minimum of hassle. With an Expert-mode backup, you must manage these details without much assistance. (For those familiar with *Backup**EDGE*** 01.01.0x and earlier, this emulates the behavior in those products.)

This is the only way to make an Expert-mode backup from within *EDGEMENU*. It is provided only for backwards compatibility, and rarely offers any advantage at all over a non-Expert-mode backup.

Operations are logged in `/usr/lib/edge/lists/menu`.

It is ***strongly*** recommended that you use “Backup Multiple Files” or create a *Scheduled Job* instead.

See “Expert Backup” on page 241 for more information on *Expert Backups*.

Run Scheduled

This option allows the user to start a *Scheduled Job* that has been previously defined in the *Scheduler*. This gives the user the ability to start well-defined tasks quickly, and is the preferred method of performing attended system backups. You may quickly select from any pre-defined *Scheduled Job* and have it start as an attended task. Operations are logged in the log *Directory* defined for that *Scheduled Job*. Notification is disabled when starting a *Scheduled Job* in this fashion.

See “Run Scheduled” on page 243 for more information on running *Scheduled Jobs*.

Run Scheduled Legacy

This is the same as *Run Scheduled*, except that the *Job* will be run in *Legacy Mode*. This clears the screen and scrolls the files in a full window instead of on a single status line. It also provides for interrupting backups. Timing tests show that *Legacy Mode* can be significantly slower than standard mode due to display overhead. In *Legacy Mode*, the user must press `[Enter]` between the backup and the *Verify* and/or *Index* phase.

See “Advanced File Restore” on page 244 for more information on running *Scheduled Jobs* in *Legacy Mode*.

Generally, *Legacy Mode* is only useful for troubleshooting purposes.

The Restore Menu

Restore attempts to restore files from your currently selected *Primary Resource*. The options in this drop-down menu will attempt to read the label and identify your media before continuing. You should have media in the *Device* before selecting any *Restore* options. These options are:

```
[Restore Entire Archive]
[Selective Restore]
[Expert Restore]
```

Restore Entire Archive

This performs a full *Restore* of all the files on your archive media. There are a variety of options available for selecting restore location (if other than the original), choosing destructive vs. non-destructive restore, etc. The archive will be identified and you'll have a chance to modify your selections before proceeding. Operations are logged in `/usr/lib/edge/lists/menu`. See "Restore Entire Archive" on page 244 for more information.

Selective Restore

With *Selective Restore* you'll have two options for restoring files: a powerful browser and a "type your filenames" screen.

The browser has a very `bash`-like feel for completing filenames and pathnames, except that the `[F4]` key is used instead of the `[Tab]` key for filename completion. Files in the *Current Directory* are shown in the `Available` window. Pressing `[Enter]` on a displayed path places it in the `Files Selected For Restore` window. Pressing `[Enter]` on a path in the `Files Selected For Restore` window deletes it from the selection. When you've got everything selected properly, `[Tab]` down and press `[Restore]`.

EDGEMENU will automatically use *FFR* or *IFR* if they are available for your media.

The non-browser interface will present you with two text lines that are very similar to the *Backup Multiple Files* option in the *Backup* drop down menu. For those familiar with older versions of *Backup**EDGE***, be sure to read this description carefully as it is not what you [probably] expect.

This option presents two separate lines for data entry. The first (top) line is for the entry of individual files or *Directories* to be restored. Files and *Directories* are separated by spaces. The bottom line is to give *EDGEMENU* the full pathname of a file which contains a list of the files to be restored. Multiple filenames containing lists of files maybe entered here. In fact, any combinations of individual files or *Directories* in the top line and pathnames of file lists in the bottom line may be combined. All filenames, *Directory* names, and lists should be typed in *Absolute Pathname* format. Operations are logged in `/usr/lib/edge/lists/menu`.

Regardless of which method you choose, or how the files are stored on the archive, using "Selective Restore" will default to restoring them to their original locations.

NOTE: *EDGEMENU* will automatically use *FFR* or *IFR* if they are available for your media.

NOTE: If you are using *Legacy Backups*, or backups that were made with "Expert Mode" backups, you must use the "Expert Restore" option to restore from them! Backups done through the *Scheduling* system of *Backup**EDGE*** **can use** "Selective Restore", however.

See "Selective Restore" on page 245 for more information.

Expert Restore

This option is typically used to restore from *Legacy Backups* and backups made with "Expert Mode". Its user interface is the same as the non-browser interface in *Selective Restore* above,

except that you must use the same *Absolute Pathname* or *Relative Pathname* format that appear on the archive.

Operations are logged in `/usr/lib/edge/lists/menu`.

For those familiar with *BackupEDGE* 01.01.0x and earlier, this is behavior should be familiar. It is strongly recommended, however, that you do ***not*** use Expert backups, and instead use "Selective Restore" when using *BackupEDGE* 01.02.00 and later. If you are restoring files from a backup made with an pre-01.02.00 version of *BackupEDGE*, the filenames you type here should be the same as you would have typed in the older version of *BackupEDGE*. In other words, they must match exactly with how the filenames appear on the archive.

While you may use this option to restore non-Expert backups, it is ***strongly*** recommended that you do not, as the names that appear on such backups are not always easy to predict. There is also no advantage to restoring files from a non-Expert backup with "Expert Mode".

The Verify Menu

All operations which open the media for reading, but which do not actually restore any files, are in this drop down menu.

```
[Verify / Index Archive]
[Verify (Only) Archive]
[List Archive Contents]
[Show Archive Label]
------------------------
[Device Status (Pri)]
[TapeAlert Status (Pri)]
[View BackupEDGE LogFile]
```

Verify / Index Archive

All normal backup operations have default settings for performing verify passes after the backup, and also for creating index databases for *FFR* and *IFR*. You may use this option to verify and/or index the media at a later time. Prior to beginning, the media label will be read, and you may set verify level and change the relative *Root Directory* for bit-level verifies. By default, however, *BackupEDGE* will use the correct *Root Directory* to verify the archive.

For users of older (pre-01.02.00) versions of *BackupEDGE*, this is different behavior. In those versions, you were responsible for selecting the right *Root Directory*.

Verify (Only) Archive

This shows the same fields and options as *Verify / Index Archive*, differing only in the choice of default setting (indexing is turned off by default).

List Archive Contents

This starts a listing without checking the media label first. There is no need to set the *Working Directory* for a listing.

Show Archive Label

This option will attempt to read and display the *Backup**EDGE*** label from the media. Here is an example of the human-readable version of an archive label...

```
Type        : Edge.Nightly 03.00.00 Master
Date        : Wed Sep 11 08:00:01 2019
Resource    : regforms:url!url0
Device Type : URL Resource
Retention   : Mon Sep 16 06:55:01 2019
Job Name    : regforms.microlite.com:simple job master
Job Desc    : (Master) Basic Schedule
Seq. Name   : regforms.microlite.com:onsite
Seq. Desc   : On-Site Backups
Domain Name : regforms.microlite.com:system
Domain Desc : Entire System
Block Factor: 64
Tape Block  : 4096
Volume Size : 1048544
Slot Name   : default
Seg Number  : 1
Media Usage : 1 (ID: 00dfaad36162652b)
Archive ID  : 10722379593bcd91
Instance ID : 1df4baa9607935cd
Job ID      : 4bc69f943b11cfc9
System Name : regforms.microlite.com
Directory   : /
Log Version : 8
```

The label records what type of backup, if any, is on this medium. It also records when the backup was made.

NOTE: The `ID:` listed in the `Media Usage` line is the *Backup**EDGE*** medium identifier. It may be ignored.

Device Status (Pri)

Performs a status check on the current *Primary Resource*. This directly queries the *Device* and prints information on make and model, media presences, write protect status, *Tape Block Size*, compression settings, and more.

TapeAlert Status (Pri)

This perms a *TapeAlert* query on the current primary *Resource*. If there are queued messages they will be displayed and cleared from the *Device*. You will also be notified if (a) the *Resource* has no messages queued or (b) the *Resource* does not support *TapeAlert*.

Remember that a *TapeAlert* message is generated by the tape drive, not by *Backup**EDGE***. *Backup**EDGE*** simply reports whatever messages the drive currently has pending.

View BackupEDGE LogFile

Each *Scheduled Job* creates a brief (usually one line per backup, one line per verify) entry in the log file. This selection allows you to view the log file to see a short history of your recent backups.

The Admin Menu

The *Admin* drop down menu contains a variety of useful administrative tools and functions.

```
[Define Resources]
[Set Default Backup Resources]
[Initialize Medium]
[Delete Archives]
[Changer Control]
[Eject Medium]
```

Define Resources

This is the Add/Edit/Delete *Resource* menu. It allows you to create new *Resources*, change the settings of a current *Resource*, or to delete *Resources* that are no longer used.

You select the *Resource* to be changed using the same selection screen described in “Schedule Job Wizard - Select Primary Resource” on page 65 using **Fast Select**. While the arrow is pointing at a *Resource*, you may press `[F6]` to delete it. Press `[Edit]` to enter the same *Resource* screens that were described starting on page 61. Press `[Edit]` while **FastSelect** is pointing at `[New]` to create a new *Resource*.

When you are finished editing a *Resource*, press `[Next]` to save the information and return to the selector. Press `[Done]` from the selector to return to *EDGEMENU*.

If you add a new storage *Device* after installing *Backup**EDGE***, we recommend you place media in it, then use `Admin -> Autodetect New Devices` to detect the *Device* and set up the *Resource*.

If you think you’ve made changes to a *Resource* that render the associated *Device* inoperable, delete the *Resource*, insert some media, then use `Admin -> Autodetect New Devices` to re-create it. Be sure that the name of the *Resource* is the same after it is autodetected, so any *Scheduled Jobs* that use it function properly.

If you want to use data files with *EDGEMENU*, use *Define Resources* to create entries for them using type `Other Device`. Be sure the file exists before you attempt to write to it with *Backup**EDGE***. Here is an example of a **file** *Resource*.

Sample File Resource

```
+ BackupEDGE Resource Information ------------------------------------------+
|- General Resource Information ---------------------------------------------|
|Resource Type       Other Device                                           |
|Resource Name       [file0             ] Change as appropriate             |
|Description         [Test Data File          ]                             |
|Changer Assoc       [Standalone Device]                                    |
|                                                                           |
|- Other Device Information -------------------------------------------------|
|Data Node           [/tmp/archive0.edge          ] [Y] Device Can Seek?    |
|                                                                           |
|- Default Backup Properties ------------------------------------------------|
|Volume Size         [0            ] [S] Compression Level  [5]             |
|Edge Block Size     [64           ] [Y] Double Buffering                   |
|[Next]                              [Prev]                          [Cancel]|
+---------------------------------------------------------------------------+
```

Set Default Backup Resources

You may quickly change the *Resource* that *EDGEMENU* uses at any time. This option will present you with the same selection screen you saw the first time you ran *EDGEMENU*. See “Select Primary Device” on page 193 for more information.

Initialize Medium

URL, S3CLOUD and FSP Resources

For these *Resources* this option tests the connection and writes a control file to the proper directory on the remote *Resource*. If run on an already initialized *URL*, S3CLOUD or *FSP Resource*, it will update the control file based on the currently available archives. It will not erase any of the archives. Use the *Delete Archives* menu option to delete archives from *URL*, S3CLOUD and *FSP Resources*.

SharpDriveResources

For *SharpDrive Resources* two possibilities exist:

Non-Destructive Initialization checks the filesystem state, examines and updates the control file based on the currently available archives. It will not erase any of the archives.

Destructive Initialization prompts for a media label, erases and creates a new filesystem, and adds a blank control file. All data on the SharpDrive, including those created by other operating systems or products, or already initialized *SharpDrive*or *FSP Resource*s, will be completely erased.

Tape Resources

Before using a new blank tape, you may use *Initialize Medium*. This writes a single block of data on the front of the medium. While not absolutely required, this ensures that (a) the *Device* is working, and (b) the tape has been written on using exactly the same *Tape Block Size* that will be used during backups, if applicable. This facilitates faster startups of backups, and allows *Backup**EDGE*** to track media usage better. In fact, we recommend that you *Initialize* the tape, then perform a *Show Archive Label* from the *Verify* drop down menu, the first time you use a new piece of media.

You may modify the initial usage count for the medium if desired. If the medium was accidentally overwritten by something other than *Backup**EDGE***, you may wish to start this number higher. By default, *Backup**EDGE*** treats this medium as blank and previously unused.

For write-once media such as CD-R, DVD-R, DVD+R and WORM tape, **do not use this option**. Under normal conditions, *Backup**EDGE*** will produce an error message if you attempt to do so.

Re-Writable optical media do not need initialization. This is handled automatically by *Backup**EDGE*** if required.

Delete Archives

If your *Primary Resource* is associated with a *SharpDrive*, *URL*, *S3Cloud* or *FSP Resource*, this option will present a list of archives on the *Resource*, allow you to view the archive summary information and optionally delete unwanted archives.

```
+Select Archive(s) to Delete from s3cloud0-------------------------------------+
|+-------------------------------------------------------------------------------+|
||   *[1] (4583 MB) 'regforms system Edge.Nightly 03.00.00 Master 2019/09/07 0||
||   *[6] (4583 MB) 'regforms system Edge.Nightly 03.00.00 Master 2019/09/08 0||
||-> *[11] (4584 MB) 'regforms system Edge.Nightly 03.00.00 Master 2019/09/09 ||
||    [16] (4581 MB) 'regforms system Edge.Nightly 03.00.00 Master 2019/09/10 ||
||    [21] (4586 MB) 'regforms system Edge.Nightly 03.00.00 Master 2019/09/10 ||
||    [26] (4594 MB) 'regforms system Edge.Nightly 03.00.00 Master 2019/09/11 ||
||                                                                             ||
||                                                                             ||
||                                                                             ||
||                                                                             ||
||                                                                             ||
||                                                                             ||
||                                                                             ||
|+Total Space Used: 26.86GB-----------------------------------------------------+|
|Sys: regforms.microlite.com            Dir: /                                  |
|Dom: system                            Job: simple_job_master                  |
|Slot: default                          Date: Mon Sep  9 08:00:01 2019          |
|Type: Edge.Nightly 03.00.00 Master     TTL: Sat Sep 14 06:55:01 2019           |
|                                                                               |
|[Delete]                                                          [Cancel]|
+-------------------------------------------------------------------------------+
```

It is possible to delete multiple archives by pressing the `[Space Bar]` at each archive requiring deletion. An asterisk (*) will appear next to the archive. When all archives to be removed have been selected, choose `[Delete]`.

Changer Control

If your *Primary Resource* is associated with an *Autochanger*, this menu will allow you to manually move media between *Elements*. When you select *Changer Control*, your cursor will be in a window listing all current *Full Elements* (those currently containing media). Choose the media you wish to move and press `[Enter]`. A list of all *Empty Elements* will be displayed. Choose the correct *Element* and press `[Enter]`. A menu of possible options will appear. Press `[Move]` to move the media.

When finished, press `[Done]` to return to *EDGEMENU*, or press `[Tab]` to return to the *Full Elements* window and make another selection.

See “Autochanger Media Manipulation” on page 250 for more information and a visual example of the use of *Changer Control*.

Eject Medium

Issues an eject command to the selected *Resource*. If the *Device* is embedded within an *Autochanger*, this will unload the medium back into the magazine **without** ejecting the magazine itself.

The Setup Menu

The *Setup* drop down menu provides setup and configuration options for *BackupEDGE*.

```
[Activate BackupEDGE]
[Make RecoverEDGE Media]
[Enable Advanced]
-------------------------
[Configure BackupEDGE]
```

or if encryption is enabled...

```
[Activate BackupEDGE]
[Make RecoverEDGE Media]
[Enable Advanced]
-------------------------
[Edit Encryption List]
[Decryption Key Backup
[Load Decryption Keys]
[Delete Plaintext Keys]
-------------------------
[Configure BackupEDGE]
```

Unless you have (or plan to get) a serial number for the Encryption feature, then you should not use enable encryption while *BackupEDGE* is operating in demo mode. When *BackupEDGE* is activated permanently, *encryption will be disabled unless you also provide a separate serial number for Encryption along with the appropriate activation code*. See “Encryption” on page 259.

Activate BackupEDGE

As mentioned previously, new *BackupEDGE* installations are activated automatically for 60 days. During this time, you MUST *Register* and *Activate* the program for it to continue to function.

NOTE: *BackupEDGE* serial numbers for release 02.0x and earlier are not valid for release 03.00.00 and later. You must purchase a new retail license to obtain a serial number compatible with this release of *BackupEDGE*.

Registration and *Permanent Activation* may be performed at any time after the installation from this menu.

The first time you run *Activate BackupEDGE*, all fields are available for data input. After you've sent in an activation form and received a *Permanent Activation Code*, run *Activate BackupEDGE* again and you'll be placed directly into the *Activation Code* field. Type the code and press `[F2]` or `[Ctrl-E]` and your product will be permanently activated.

See “Product Registration and Activation” on page 272 for more information.

NOTE: It is possible to remove the registration / activation options from *EDGEMENU* after activation. To do so you must edit a variable in the master configuration file `/usr/lib/edge/config/master.cfg`.

```
HIDE_REG={YES|NO}
```

If set to `YES`, *EDGEMENU* will hide the registration / activation options. This is useful to keep casual users from accidentally changing the registration information.

Make RecoverEDGE Media

If your version of *BackupEDGE* comes with our *RecoverEDGE Disaster Recovery* component, this selection will take you to the *RecoverEDGE Boot Media* and *Boot Image* creation menu. See “Disaster Recovery - Preparation” on page 279 for more information.

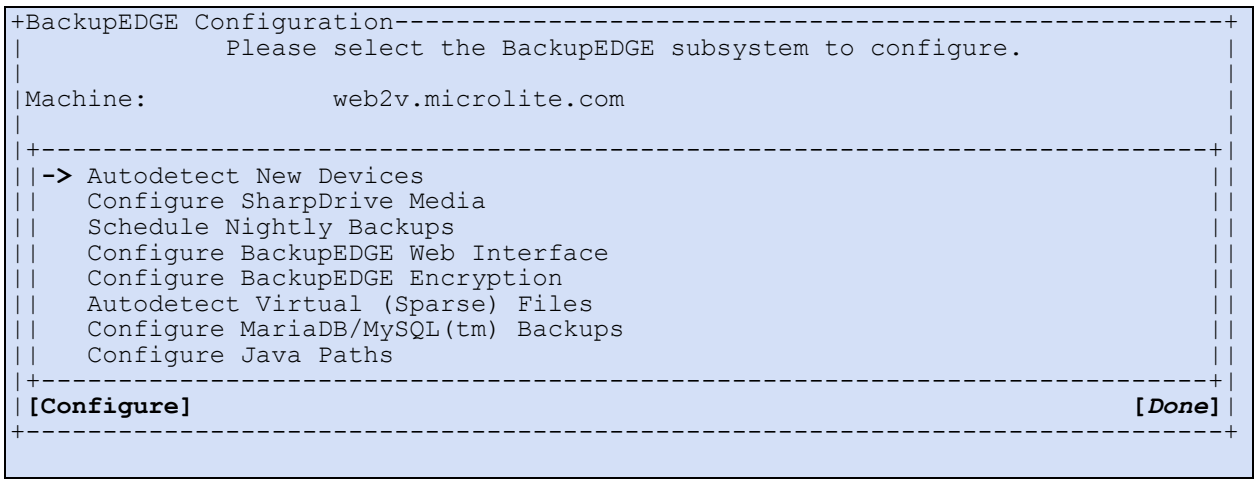
Enable Advanced

By default, *BackupEDGE* uses a simplified version of its scheduling system, since that is sufficient for many users. If you wish to enable all the features of the scheduler, then select this option. New options under the *Schedule* menu will appear.

When *Advanced Scheduling* is enabled, this menu option will be replaced with `Disable Advanced`, which will disable all *Advanced Schedules* and remove the option to edit them. Any configuration will be saved, so if *Advanced Scheduling* is re-enabled, they can be edited normally.

The Setup - Configure BackupEDGE Menu

The *Setup* drop down menu provides a `Configure BackupEDGE` sub-menu.



Autodetect New Devices

If you add a new storage *Device* to your system, or have deleted a *Resource* and wish to re-create it, use this selection. It will run the same part of the Installation Manager that detected *Resources* previously. See “Device Autodetection” on page 59 for a refresher course.

Format SharpDrive Media

Prepares USB and SATA flash drives, disk drives and cartridges for use with SharpDrive backups. See “Configuring SharpDrive Backups” on page 80 for a refresher course.

Not available under OpenServer 5.

Schedule Nightly Backups

This option runs the basic *Scheduler*, just like the `EDGEMENU -> Schedule -> Basic Schedule` menu option. See “Scheduling - Basic” on page 210.

Configure BackupEDGE Web Interface

As described in “Configuring and Starting the Web Services Daemon” on page 190, sets up and administers the *Web Services* interface.

Configure BackupEDGE Encryption.

Starts the Encryption setup wizard. See “Encryption” on page 259.

Autodetect Virtual (Sparse Files)

Allows the administrator to re-scan the system for sparse files and add them to the list for special sparse file handling during backups (`/etc/edge.virtual`).

Configure MariaDB/MySQL Backups

Starts the MySQL setup wizard. See “MySQL / MariaDB Backups” on page 177.

Configure Java Paths

Allows entry/change of the directory with the Java runtime system should Java be changed after installation or if the installed fails to find it. This is for the X11 interface only and does not affect Web Services.

The Schedule Menu

This menu allows you to create and edit *Schedules*, *Domains* and *Sequences*, as well as allowing interaction with running *Scheduled Jobs* and editing *Notifiers*. If you have not already done so, is strongly recommended that you read "Anatomy of a BackupEDGE Backup" on page 40 before continuing to get an overview of the concepts involved here.

```
[[Basic Schedule]
[Create/Edit Domain]
[Create/Edit Sequence]
[Advanced Schedule]
[Browse Running Jobs]
[Acknowledge All]
[Edit Notifiers]
[Update Checking]
```

NOTE: Initially, this menu will be missing the **boldface** entries. To see the full menu, you enable the *Advanced Scheduler* using `Enable Advanced` in the *Setup* dropdown menu. After you have done this, all of these options will be available. If you do not need *Advanced Scheduling*, it is recommended that you do not enable it. It can be enabled later at any time.

Basic Schedule

If a default *Scheduled Job* was created during initial installation, this option will place you directly into the editing screen previously shown in "Schedule Job Wizard - Edit Backup Schedule" on page 66. If you did not create a default *Scheduled Job*, or if you for any reason deleted the default *Scheduled Job* from the *Advanced Schedule* menu, this option will create a new default *Scheduled Job* using the wizard, as shown starting at "Schedule Job Wizard - Select Primary Resource" on page 65. Typically the *Scheduled Job* exists.

This is the primary way to make changes in the default *Scheduled Job*, which is the most-used *Scheduled Job* in *Backup**EDGE***. It is used to perform *Master Backups* of your entire system on one or more days of the week at a specified time.

See "Scheduling - Basic" on page 210 for additional information on the basic and advanced scheduling capabilities of *Backup**EDGE***.

Create/Edit Domain

This is where you create a new *Domain* or edit and existing one. As mentioned previously, a *Domain* is a "thing to archive". Selecting this displays a **FastSelect** screen allowing you to select an existing *Domain* to edit, `[New]` create a new *Domain* manually, or `[New from Wizard]` to create a new *Domain* with the help of a wizard.

See "Creating Backup Domains" on page 231 for more information on creating and editing *Domains*.

Create/Edit Sequence

This is where you create new *Sequences* which, as mentioned elsewhere, are "organizational units for backups". Choosing this places you in a **FastSelect** screen allowing you to edit an existing *Sequence*, or create a new *Sequence* either manually (`[New]`) or with the help of a wizard (`[New from Wizard]`).

See "The Default Backup Sequence" on page 233 for more information on creating and editing *Sequences*.

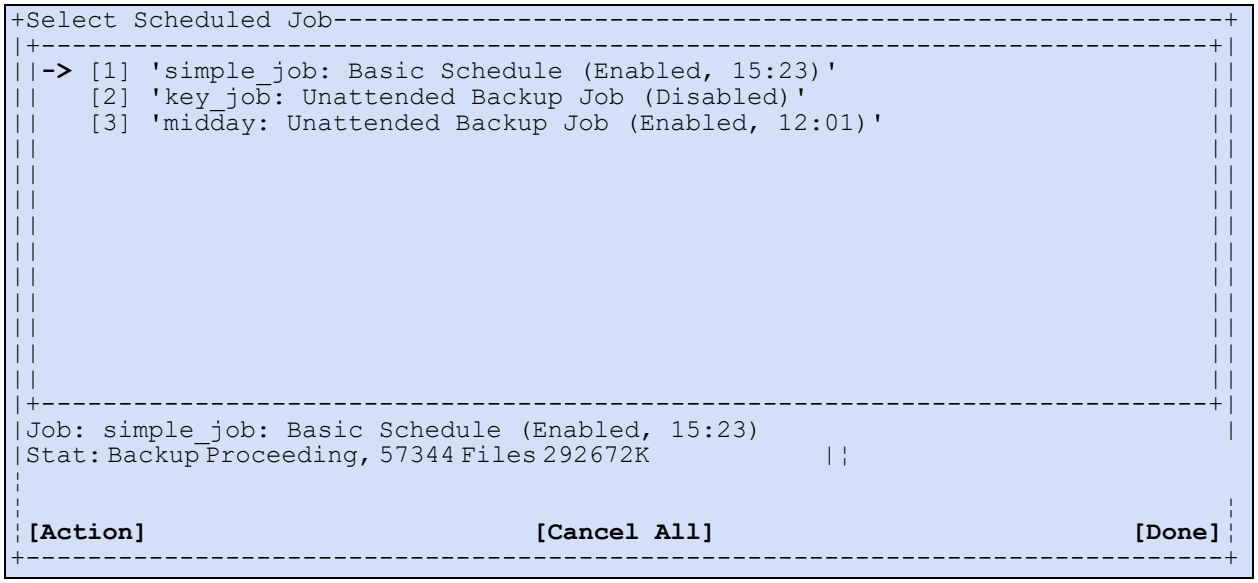
Advanced Schedule

This will provide a **FastSelect** screen allowing you to...

- Modify the default *Scheduled Job* in advanced mode.
- Modify any other *Scheduled Job*.
- Create a new *Scheduled Job* in menu mode.
- Create a new *Scheduled Job* in Wizard mode.
- Delete a *Scheduled Job*.

See “Scheduling - Advanced” on page 220 for more information on creating and editing *Advanced Scheduled Jobs*.

Browse Running Jobs



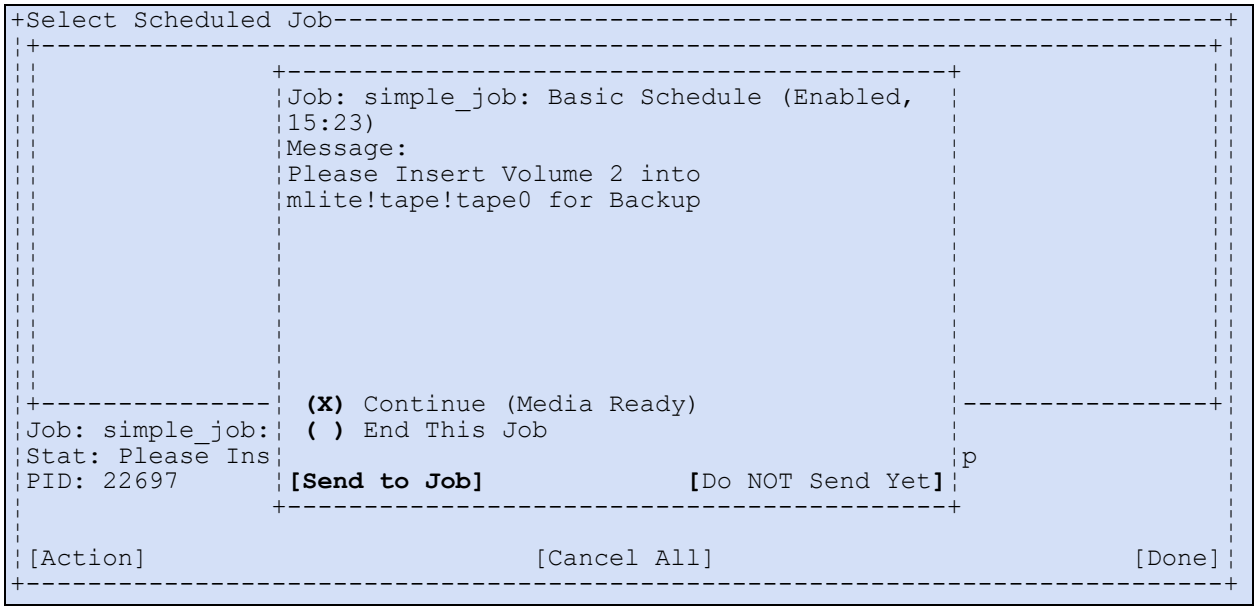
This will display each scheduled job and its current status. Use the **Fast Select** arrow keys to point the arrow at the top to a *Scheduled Job*. Its status will display below.

Selecting `[Cancel All]` will end all jobs currently running or awaiting input from within the *Backup**EDGE*** scheduler.

Selecting `[Action]` for any single running job will offer to cancel the job.

If the job awaiting user intervention, for instance it is waiting for a new media volume to be inserted, selecting `[Action]` will offer to continue (after inserting new media or taking the action

indicated by the prompt), or immediately end the job. It is also possible to select `Do Not Send Yet` and come back to this prompt at a later time.



Acknowledge All

Acknowledge All will scan for *Scheduled Jobs* requiring action, identify them and provide you with the appropriate information. It also allows you to signal the *Scheduled Job* to continue, if desired, using the same interface described above.

Edit Notifiers

This powerful feature of *Backup**EDGE*** provides user control over printed and emailed output. Each email name, alias, or printer name you place in a *Scheduled Job* is actually a *Backup**EDGE** Notifier*. The *Notifier* can be modified to notify multiple email addresses (or printers), or filter or modify the output.

See “Working with Notifiers” on page 235 for more information on creating and editing *Notifiers*.

Update Checking

You may configure *Backup**EDGE*** to check periodically to see if a newer version is available from the Microlite Corporation website and eligible for download. This option allows you to enable or disable such checks, as well as control how often they occur. You may also use the *Check for Updates* option under the *File* menu to check at any time.

Of course, the UNIX or Linux machine must have a functioning Internet connection for this option to work. Transport Protocol Port 80 (http) is used, so must be open outbound from your server.

19 - Scheduling - Basic

NOTE: This section has changed for *Backup**EDGE** 3.x*. You should review this section completely if you are used to the prior scheduling system.

The “backup” part of any backup / restore / disaster recovery product is the most often used feature. You may perform hundreds or even thousands of backups before you ever have to restore a file, or perform a system recovery. Usually, most of the backups are *Scheduled* (unattended) backups.

If you have not already done so, please review “Anatomy of a BackupEDGE Backup” on page 40 *before* reading further.

*Backup**EDGE*** has two scheduling modes. The *Basic Schedule* mode very quickly creates a *Scheduled Job* for a simple rotation of full system backups.

The *Basic Scheduler* in *Backup**EDGE** 3.x* allows...

- *Master*, *Incremental*, *Differential* or *No Backups* to be performed on any day of the week.
- *Retention Times* to be set for every archive in the *Basic Schedule* (in the `Notify / Advanced` screen).
- *Disk-to-Anything-To-Anything* backups to be enabled (in the `Notify / Advanced` screen).
  - A *Retention Time* can also be set for the “Copy to:” *Resource*.
- Defaults to be restored via a `[Reset Dates]` button. Most helpful in advanced scheduling.
- Combining *Backup Retention Times*, *Resource Quotas* and *Lazy Reclamation* to get the most out of *S3CLOUD*, *URL*, *FSP* and *Tape Resources*.

Entry of *Media Lists* (slot names or barcode IDs) for tape libraries. This has been moved to a sub-menu.

Lazy Reclamation. When an archive has expired (it is past its *Retention Time*) it will simply stay on the *Resource* until its space needs to be re-used, then be deleted automatically. This allows for a maximum number of available archive copies in the event of a data disaster.

The *Advanced Scheduler* adds powerful additional capabilities (see “Scheduling - Advanced” on page 220):

- *Triplets Scheduling*. Change / define the frequency of the *Scheduled Job* using *Triplets*. This goes far, far beyond the default 7 day selections available in the *Basic Schedule*.
- Add, delete, and alter priority of different *Triplet* entries within a single *Schedule*.
- Setting *Custom Retention Times* per line of the *Schedule*.[1]
- Selecting the *Sequence* used to track the *Scheduled Job*.
- Add additional tracking *Sequences*.
- Create and edit as many *Backup Domains* as desired.
- Add more than one *Backup Domain* to a *Scheduled Job*.
- Created an unlimited number of new *Scheduled Jobs*.
- Add, delete, and alter priority of different *Triplet* entries within a single *Schedule*.

1. Requires *Backup**EDGE*** 03.00.02 or later.

19.1 - Master / Differential / Incremental Backups

Most clients run a full system backup every night, which we define as a Master Backup of the default Domain. However, more granularity is available. If you will be using only Master Backups, please skip to "Basic Schedules" on page 212.

Otherwise, lets define the possible backup types.

A *Master Backup* is a full backup of all data in a *Domain*.

A *Differential Backup* follows the same *Domain* rules, but backs up only that data (files or *Directories*) that have been created or modified since the last successful *Master Backup* in the *Sequence* to which both backups belong.

An *Incremental Backup* follows the same *Domain* rules, but backs up only those files or *Directories* that have been created or modified since the last successful *Differential Backup* **or** the last successful *Incremental Backup*, whichever is newer.

A *Master Backup* has no dependencies on other backups; each one can restore all the data for a *Domain* to the point in time when that backup was made.

A *Differential Backup* is dependent on the *Master Backup* it is based on. That is, it takes the *Differential Backup* **plus** the *Master Backup* on which it is based to restore all the data in a *Domain* to the state it was in when that *Differential Backup* was made.

When a new *Master Backup* is made for a *Sequence*, any previous *Differential Backup*s in that *Sequence* are no longer needed (unless you want to restore the *Domain's* data to a point prior to the last backup, of course). It will not impact the contents of any future *Incremental Backup* (see below) for the *Sequence*.

You cannot perform a *Differential Backup* which will overwrite the *Master Backup* upon which it would be based. If *Backup**EDGE*** detects this, It will either **Fail** to do the backup, or **Promote** the backup to be a *Master Backup*, depending on the setting of the `Promote A` flag in the *Advanced Settings* window of the *Scheduled Job*.

The *Default* behavior is **Fail**. See page 216 for more information on setting the `Promote A` flag and its consequences.

If a *Master Backup* has never been performed in a *Sequence*, there is no reference backup for the *Differential Backup* to use. If *Backup**EDGE*** detects this, It will either **Fail** to do the backup, or **Promote** the backup to be a *Master Backup*, depending on the setting of the `Promote B` flag in the *Advanced Settings* window of the *Scheduled Job*.

The *Default* behavior is **Promote**. See page 216 for more information on setting the `Promote B` flag and its consequences.

An *Incremental Backup* is a backup of all data that has changed since the last *Incremental Backup* (or *Differential Backup*, if it is newer than the last *Incremental Backup*). To restore the data in a *Domain* to the state it was in when an *Incremental Backup* was made, it is necessary to have that *Incremental Backup* plus any previous *Incremental Backups*, plus the *Differential Backup* on which the earliest *Incremental Backup* is based, plus the *Master Backup* on which the *Differential Backup* is based. As you can see, *Incremental Backups* must be used judiciously; if one archive is damaged, all backups based on it directly or indirectly are useless.

Whenever a new *Differential Backup* or *Master Backup* is performed in a *Sequence*, any *Incremental Backups* are no longer current and may be overwritten without data loss. They will not have any further impact on future *Incremental Backups* performed for that *Sequence*. Of course, if you wish to recover the data to a time that is earlier than the most recent backup, the *Incrementals* (and other backups on which they are based) should be retained.

You cannot perform *Incremental Backups* which will overwrite the *Master Backup* or the *Differential Backup* upon which they are based. If *Backup**EDGE*** detects this, it will either **Fail**

to do the backup, or **Promote** the backup to be a *Master Backup* or a *Differential Backup*, depending on the setting of the `Promote A` flag in the *Advanced Settings* window of the *Scheduled Job*.

The *Default* behavior is **Fail**. See page 216 for more information on setting this flag and its consequences.

If a *Differential Backup* has never been performed for a *Sequence*, then there is no reference backup for the *Incremental Backup* to use. If *Backup**EDGE*** detects this, it will either **Fail** to do the backup, or **Promote** this backup to be a *Differential Backup*, depending on the setting of the `Promote B` flag in the *Advanced Settings* window of the *Scheduled Job*. If there is neither a *Differential* or *Master Backup*, *Backup**EDGE*** will promote this backup to be a *Master Backup* based on the setting on `Promote B`.

The *Default* behavior is **Promote**. See page 216 for more information on setting the `Promote B` flag and its consequences.

There can be multiple current *Incremental Backups* per *Sequence*. They are labeled `Incremental 1`, `Incremental 2`, `Incremental 3`, etc. Overwriting an older *Incremental Backup* sets the *Incremental* counter to the level of the older backup and invalidates all higher numbered *Incrementals*. This is because higher-numbered *Incrementals* are (generally) useless if an earlier one has been erased!

For any given backup, the label contains information about any previous backup(s) on which it is based.

Having three levels of backup available for each *Sequence*, combined with multiple promotion strategies, makes it very easy for *Backup**EDGE*** to control large environments, even those where on-line storage far exceeds the capabilities of your archiving *Device*. However, *we definitely recommend matching your archiving device to your system* such that only one, or at most two, backup levels are required. If you find *Incremental Backups* in your backup strategy, it may be wise to re-evaluate it.

Both *Differential* and *Incremental Backups* select files to be archived by the time at which they were last modified. However, UNIX provides two methods for deciding when a file has been altered. *Backup**EDGE*** can use either method. Please read “Level 1 and 2 Differential/Incremental Backups” on page 361 for information about the differences, and how to choose between them.

19.2 - Basic Schedules

Let’s examine the *Basic Schedule* we created during system installation a little more thoroughly. From *EDGEMENU* we would select `Admin -> Basic Schedule`.

If a default *Scheduled Job* was created during initial installation, this option will place you directly into the editing screen shown below. If you did not create a default *Schedule*, or if you for any reason deleted the default *Schedule* using the *Advanced Schedule* menu, this option will create a new *Basic Schedule* using the wizard, as shown starting at “Schedule Job Wizard - Select Primary Resource” on page 65.

NOTE: Using the `[Tab]` key to navigate on this screen is helpful.

Basic Schedule

```
+ Edit Backup Schedule ------------------------------------------------------+
| Schedule Name:     simple_job                                               |
|          Time:     [23:00 ] (14:58:46)  Enabled: [X]                        |
| Sequence:                   web2v.microlite.com:esequence/onsite            |
| Backup Domain:              system                                         |
| Primary Resource:  [Change] web2v.microlite.com:optical!optical0           |
|                                                                            |
| +-------------------------------------------------+     September 2019      |
| | Every Sunday of the week                (None) |  Su Mo Tu We Th Fr Sa    |
| | Every Monday of the week               Master |   1 M  M  M  M  M   7    |
| | Every Tuesday of the week              Master |   8 M  M  M  M  M  14    |
| | Every Wednesday of the week            Master |  15 M  M  M  M  M  21    |
| | Every Thursday of the week             Master |  22 M  M  M  M  M  28    |
| | Every Friday of the week               Master |  29 M                    |
| | Every Saturday of the week              (None) |                         |
| +-------------------------------------------------+                         |
|                                                                            |
| Notify / Advanced: [Change]  [Reset Dates]                                 |
| Mail Summary To:   root                    Print Summary To:   NONE        |
| Mail Failures To:  NONE                    Print Failures To:  NONE        |
|[Save]                                                          [Cancel]|
+----------------------------------------------------------------------------+
```

Schedule Name:
The *Schedule Name* for the *Basic Schedule* is always called `simple_job`. It cannot be changed.

Time:
This is the time of day that the *Scheduled Job* will be run. You must type the time in 24 hour time format, hour, colon (`:`) minute after the hour, as shown above. In the example, this *Scheduled Job* will be run at one hour before midnight. If you type an invalid time, you'll be warned when you press `[Save]` or `[Next]`.

Enabled:
If this field contains an **x**, the job will be run automatically at the time indicated on the selected days once it has been saved with the `[Next]` button. If you remove the **x** (press `[Space]` with the cursor in the field), the *Scheduled Job* will be saved normally, but won't actually be run automatically. This is useful for temporarily suspending a *Scheduled Job*, and also for creating special *Scheduled Jobs* which will be run only from *EDGEMENU* in attended mode.

Sequence:
This cannot be changed in the *Basic Schedule*. When creating your own *Advanced Scheduled Jobs*, you may define a custom *Sequence*, or use the default *Sequence* (`onsite`) to log your backups. Recall from "Anatomy of a BackupEDGE Backup" on page 40 that a *Sequence* keeps related backups of the same data together.

In the *Basic Schedule*, the *Sequence* will be `onsite`, which is used for on-site backups to protect all data on your system.

Backup Domain:
Domain(s) cannot be changed directly within any *Backup Schedule*. They are selectable within the *Advanced Schedule*.

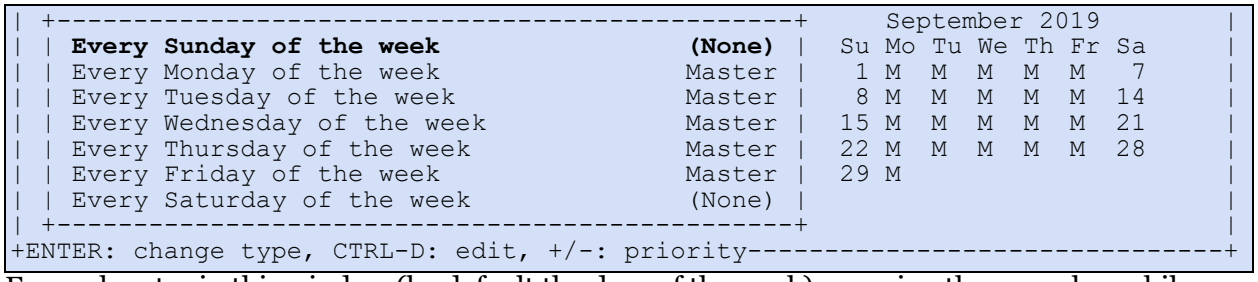
Primary Resource:
This field indicates the *Resource* which will be used to store this archive.

Pressing change on the *Primary Resource* field brings up a **Fast Select** screen allowing you to quickly select the proper *Primary Resource*, or create a new one. You may select a *Resource* on

this machine or on a remote machine, assuming *Backup**EDGE*** has been installed and configured on that machine.

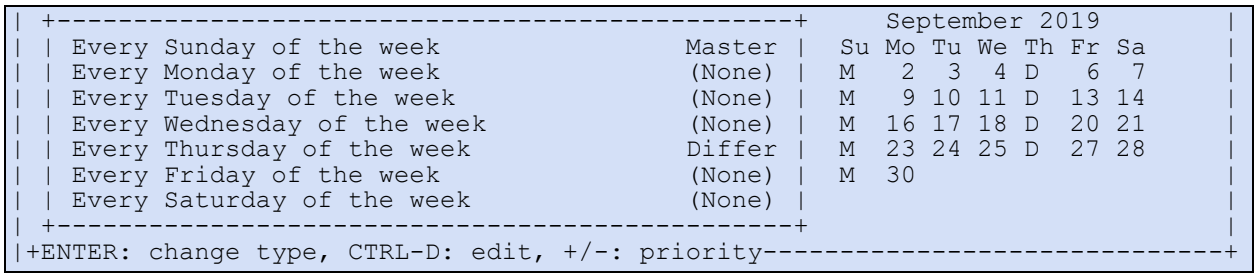
NOTE: If you have an autochanger and wish to have this *Scheduled Job* use it to load tapes automatically, you should select the *Resource* for the tape drive. You will then be asked if you wish to use the associated autochanger. If you answer *Yes* to this question, you will be given the option of filling in a media list to be loaded on each day the *Scheduled Job* runs (see below).

Frequency Window



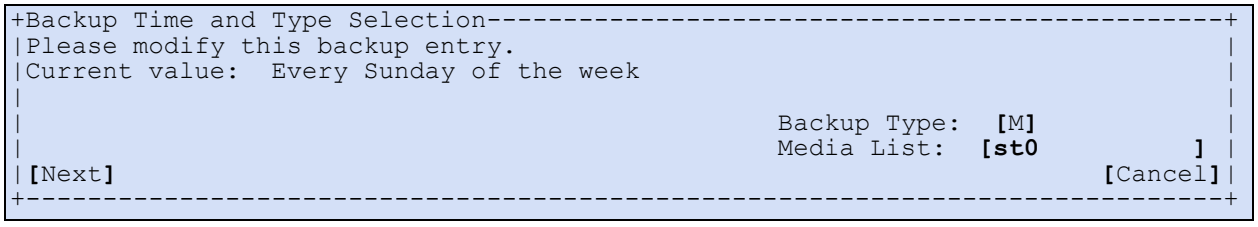
For each entry in this window (by default the days of the week), pressing the space bar while highlighted will toggle that days entry among `(None)`, `Master`, `Differ`ential, and `Increm`ental.

If a backup is selected for a particular date, the date is replaced with an `M`, `D`, or `I`, respectively on the calendar to the right. If no backup is scheduled for a particular date, the date itself appears on the calendar. Contrast the *Schedule* above to one where the only backs selected are a *Master Backup* on Sundays and a *Differential Backup* on Thursdays.



MediaList

This is for *Autochangers*. If the *Primary Resource* is associated with an *Autochanger*, you may select which media will be inserted for the *Scheduled Job* each night. Media may be selected by *Storage Element* (`st0`, `st1`, etc.) or by *Physical Volume Tag* (barcode) if the *Autochanger* is so equipped. To specify barcodes, use the prefix `bc` followed by the barcode itself, such as `bcmonday`. Barcodes and *Storage Elements* may be intermixed if desired, although doing so can be confusing. Highlight a particular day and press `[Ctrl-D]`.



More than one piece of media may be used each night. For instance, you may type `st0,st5` in the Monday *MediaList*. This means that on Monday, `st0` will be inserted before the backup commences. If the media should fill, it will be returned to `st0` and the media from `st5` will be inserted. When the backup completes, `st0` will be re-inserted and the verify will begin.

NOTE: You may run a *Scheduled Job* that contains a *MediaList / Slot Name* from *EDGEMENU* using `Backup -> Run Scheduled`. You will be given the chance to enter a new *MediaList* manually.

Reset Dates
Pressing the `[Reset Dates]` button resets the *Schedule* to the default, which is Monday through Friday *Master Backups*. This is most useful if you are using the *Advanced Scheduler*, make too many changes to track properly, and wish to start over.

Notify / Advanced
Pressing the `[Change]` button for this field brings up a new window used to change advanced backup options, and to add or edit *Notifiers*. Let's take a closer look.

Basic Schedule - Notify / Advanced

```
+ Edit Backup Advanced Properties ------------------------------------------+
|                    Backup Schedule Advanced Properties                     |
|                                                                            |
| Schedule Name:     simple_job                                              |
|                                                                            |
| Verify Type:       [B]                 Checksumming:  [X]                  |
| Attempt Index:     [X]                                                     |
| Attempt Bootable:  [ ]                                                     |
| Promote A:         [ ]                 Retention:     [1 Weeks]            |
| Promote B:         [X]                 Copy to:       [NONE]               |
| Eject/Vol Switch:  [ ]                 Copy Retention:[Forever]            |
| Eject/Verify:      [ ]                 Copy Sequence: [ ]                  |
|                                                                            |
| Mail Summary To:   [tom                                                   ]|
| Print Summary To:  [                                                      ]|
| Mail Failures To:  [                                                      ]|
| Print Failures To: [                                                      ]|
|                                                                            |
|[Next]                                                          [Cancel]    |
+----------------------------------------------------------------------------+
```

19.3 - Advanced Properties

Verify Type:
Options are [**B**] (*Level 2 Verify*, or *Bit-Level Verify*), [**1**] (*Level 1 Verify*) and [**N**] (*No Verify*). A *Level 2 Verify* starts after a backup, reading each file from the archive and comparing it against the same file on the hard drive to ensure data integrity. *Level 1 Verify* reads the tape only and compares file checksums for a faster check. The default, **[B]**it-Level, is the default and **highly recommended setting**.

NOTE: Just because a backup completes without error ***does not mean the data was transferred properly to the medium***. It is ***essential*** to use Bit-Level Verification to read back the archive and compare it to the original data. While *Backup**EDGE*** will report all write errors it encounters, many archive *Devices* cannot detect them. Do not assume that your archive *Device* is able to detect write errors reliably!

Attempt Index
If this box contains an [**X**], an index will be created to allow *Fast File Restore* or *Instant File Restore*, depending on the media type. For this to occur, the *Resource* must have a *Locate Threshold* other than -1 in the *Resource Manager* (`Admin -> Define Resources`).

Starting with *Backup**EDGE 2.1***, multi-volume archives may be indexed.

Attempt Bootable:
This option tells *Backup**EDGE*** to place a *Boot Image* on the front of each backup, allowing the

tape, *CD-R/RW* or *DVD* to be booted directly into the *Recover**EDGE*** menu in the event of a data disaster. Currently, only *Linux*, *OSR5, OSR6*, and *UW7* support *Bootable Backups*.

NOTE: There are specific tasks that must be completed in order to make backups bootable. If this flag is checked and the tasks are not complete, backups ***will not*** be performed. Tasks include making *Recover**EDGE** Boot Images* and setting *Tape Block Sizes* for the backup *Resource*. See “Making Bootable SharpDrive / Optical Drive Backups” on page 289 for more information.

Promote A:
If checked, *Backup**EDGE*** will promote a *Scheduled Job* from a *Differential* or *Incremental* to a *Master* or *Differential* as needed when a *Scheduled Job* is about to overwrite the *Master* or *Differential* on which it would be based. If not checked, the *Scheduled Job* will **fail** under these circumstances. For example, if this Scheduled Job tries to make a *Master Backup* on Monday and a *Differential Backup* on Tuesday but you forget to change media, the Tuesday backup will become a *Master Backup* if this is checked. The backup will **fail** on Tuesday otherwise.

Note that the case of an *Incremental* overwriting an earlier *Incremental* is not covered by this flag; the new *Incremental* will simply use the old *Incremental*'s time stamp, and the old *Incremental* (and any ones produced afterwards) will be forgotten. The default is unchecked.

Promote B:
If checked, *Backup**EDGE*** will promote a job from a *Differential* or *Incremental Backup* to a *Master* or *Differential* if the higher-level backup does not exist when the operation starts. For example, if you set up *Incremental Backups* Monday - Friday but don't bother to do a *Master* or *Differential*, the first backup to run will be promoted to a *Master* if this option is checked. The second backup would be promoted to a *Differential*. Otherwise, the *Incrementals* would fail and you'd have to do a *Master* and *Differential* yourself. The default is checked.

WARNING: In the preceding example, only one *Master Backup* and *Differential Backup* would **ever** be performed.

Eject / Vol Switch:
If checked, when this job is run unattended, the outgoing media will be ejected before the user is prompted to load the next volume of a multi-volume backup (or reload the first volume for verify). If not checked, the medium will not be automatically ejected during volume switches.

Eject / Verify:
If checked, the medium will be ejected after verification, even if it fails. If unchecked, completing a verify will not eject the medium. This setting only applies to *Scheduled Jobs* which are run unattended (not through *EDGEMENU*).

Checksumming:
When this option is checked, *Backup**EDGE*** will include a checksum of the data of each file that it writes in the archive. This enables it to detect if the archive has changed since it was written. For example, with *Checksumming* enabled, *Backup**EDGE*** can detect and warn you if the archive has been damaged while it is restoring data from that archive. If this option is unchecked, only the header information (filename, permissions, etc.) are checksummed. Normally, this option should be enabled. The only time you may wish to disable it is in a case where you are attempting to create an archive designed to be restored by a legacy program such as *tar* or *pax*.

Retention:
This is the minimum time a backup is allowed to exist before it may be overwritten. The default is 1 Week (7 days). With this time set, and archive created on, for instance, Monday evening at 11:00pm won’t be erased or over-written until on or after the following Monday at the same time. An archive past its *Retention Time* is said to have *Expired*.

Retention: may be set to `0 Days` (may be overwritten immediately), any real number of days, weeks, or years, or `Indefinitely` (will never be overwritten by a *Scheduled Job*). `Indefinitely` displays as `Forever` in the `Retention:` field.

The following tables describes the operation of each *Backup**EDGE*** resource and media type and what happens when a backup starts, depending on the *Retention Time* and state of the `Multiple Archives` flag in the *Resource Manager*.

Medium Type	Multiple Archive Flag Set to YES	Multiple Archive Flag Set to NO
Tape	Backup will append to the tape starting after the last *expired* archive. If all archives have expired, Backup will start at beginning of tape	Backup will always start at *beginning of tape*. Backup will **FAIL** if tape contains an unexpired archive.
BD-RE DVD-RAM	Backup will intersperse new archives with old archives, lazily reclaiming space as available.	Backup will always blank and start at beginning of medium. Archive will **FAIL** if a current unexpired backup exists on the medium.
DVD-RW DVD+RW	**Not Supported**. Currently behaves as if flag is set to **NO**.	Backup will always blank and start at beginning of medium. Archive will **FAIL** if a current unexpired backup exists on the medium.
DVD-R DVD+R DVD+R DL	**Not Supported**. Currently behaves as if flag is set to **NO**.	Backup will **FAIL** if another archive (or any other data) already exists on the medium.

Here is the behavior for *SharpDrive Resources* when a backup starts.

Resource Type	Archive Behavior
SharpDrive	The process will attempt to create a new archive. If starting a new segment would cause the quota to be reached, the oldest expired archive will be erased in its entirety (all segments). If starting a new segment would exceed the quota and no more expired archives exist, the *Scheduler* will prompt for a new volume.

Backups to any medium listed above will prompt for new media if they can not reclaim any more space and won't fail at startup as listed above.

Here is the behavior for *URL*, *FSP*, and *FSP Resources* when a backup starts.

Resource Type	Archive Behavior
URL / S3CLOUD / FSP	The process will attempt to create a new archive. If starting a new segment would cause the quota to be reached, the oldest expired archive will be erased in its entirety (all segments). If starting a new segment would exceed the quota and no more expired archives exist, the backup will **FAIL**.

Copy To:
The `Copy To:` field enables disk-to-anything-to-anything backups. When this field is changed from its default of `[None]` to any defined *Resource*, a pop-up list appears. You may select a *Resource* on the local system or that of one on another `Machine:`. After the *Backup* and *Verify* are complete for the current *Scheduled Job* (including all *Domains* that may be part of the *Job*, each of the archives that were created will be copied directly from the *Primary Resource* to the *Copy_To Resource*. The report will be extended to include all of the copied archives.

During the *Copy_To* function, archives will generally follow the definitions in the *Copy_To Resource*. For instance, if the archive is being copied from `tape0` to a `url0`, and `url0` has software compression enabled. the copied archive will be automatically be re-compressed at the

compression level set in the `url0` *Resource* definition, while re-segmenting the archive as necessary.

Compression levels do not change when copying Encrypted archives.

The *Copy_To Resource* cannot prompt for a second volume. When using physical media devices the archive must fit entirely on the first volume.

Copy Retention:
This sets the Retention Time of the archive copy sent to the *Resource* defined in the `Copy To:` field. The default is `[Forever]` which means the archive will never be overwritten or erased by a *Scheduled Job*. Be sure to set a different *Retention Time* if you wish this archive to be periodically over-written or deleted.

Copy Sequence:
If checked, then *Backup**EDGE*** will record the copy in the same *Sequence* used for the original backup.

This allows multiple identical copies of a single archive to be created. If this option is unchecked (the default), then the copy will be created but the *Sequence* will not be told that it exists.

Which behavior is appropriate depends on what the user is trying to do.

As one example, the user might be performing a copy in order to take a copy off-site. Since the backup isn't readily available for use for day-to-day operations, it is probably not a good idea to tell *Backup**EDGE*** about it. If *Backup**EDGE*** did realize that the copy exists, then it might reclaim onsite copies once their retention time expires. This would make restores difficult without collecting the off-site copy! In this instance it is better to have *Backup**EDGE*** forget about the off-site copy, so that it relies only on the on-site one.

In another example, one might argue that the copy should be recorded in a different *Sequence*, such as the *offsite Sequence*. *Backup**EDGE*** currently does not support this feature for copies, only for *Scheduled Jobs*.

In a third example, the user might be performing *Master* and *Differential Backups* to a fast device in order to reduce the backup window, but then perform a copy to a slower device. In this case, the faster device is being used as a cache; the user doesn't necessarily want to have enough space to hold all backups from every nightly backup on it. It is probably better to tell *Backup**EDGE*** about the copy, so that it is free to reclaim the space on the faster resource. Otherwise, *Backup**EDGE*** might not be willing to reclaim a *Master Backup* in favor of a *Differential*, or would insist on promoting the *Differential* to a *Master* in the process.

Note that it is also very likely that the copy should be given a different retention time than the original. The cached copy would likely have a short (or zero) retention, while the copy would have whatever retention the user wants. This enables edge to reclaim space on the faster resource.

19.4 - Notification Options

Mail Summary To:
Any number of mail addresses, aliases and *Notifiers* may be entered here. Each will be sent notification of the pass or fail status of every backup performed through this job. The default is simple text mail. However, more complicated options, including HTML (MIME encapsulated) mail, alpha-numeric pager, and numeric pager, are available for each entry by using the *Edit Notifiers* section of *EDGEMENU*.

Print Summary To:
Any number of printers and *Notifiers* may be entered here. Each will be sent notification of the pass or fail status of every backup performed through this job. The default is simple text with no carriage returns or form feeds. However, more complicated options, including filtering the text or

adding carriage returns and/or form feeds, are available for each entry by using the *Edit Notifiers* section of *EDGEMENU*.

Notifiers provide significantly more control over notification than was present in *Backup**EDGE*** versions prior to 01.02.00. For more information on how to configure them, please consult "Working with Notifiers" on page 235.

NOTE: This entry should be the name of a printer, ***not the spooler command***. Use "**Edit Notifiers"** from the **Schedule** menu to modify the spooler command, which defaults to "`|lp -s -d [printer_name]`" or "`|/usr/bin/lpr -P[printer_name]`" as appropriate. For most installations, this is correct.

Mail Failures To:
This field works exactly like the **Mail Summary To:** field, except that addresses, aliases and *Notifiers* will only be sent messages in the event of a failure or warning.

NOTE: Entries in this field are sent in addition to the normal failure message sent to those listed in the **Mail Summary To:** field. Typically, it is used to send an email or page to an **additional** party, such as a consultant or supervisor, who only needs to be notified in the event of a problem. Listing the same *Notifier* in both fields will result in duplicate messages on failure.

Print Failures To:
This field works exactly like the **Print Summary To:** field, except that printers and *Notifiers* will only be sent messages in the event of a failure or warning.

NOTE: Entries in this field are sent in addition to normal failure message sent by the **Print Summary To:** field. Typically, it is used to send report to an **additional** party, such as a consultant or supervisor, who only needs to be notified in the event of a problem.

20 - Scheduling - Advanced

The *Advanced Scheduler* allows the user to get the most out of *BackupEDGE Scheduling*, by providing:

- *Triplets Scheduling*. Change / define the frequency of the *Scheduled Job* using *Triplets*. This goes far, far beyond the default 7 day selections available in the *Basic Schedule*.
- Add, delete, and alter priority of different *Triplet* entries within a single *Schedule*.
- Setting *Custom Retention Times* per line of the *Schedule*.[1]
- Selecting the *Sequence* used to track the *Scheduled Job*.
- Add additional tracking *Sequences*.
- Create and edit as many *Backup Domains* as desired.
- Add more than one *Backup Domain* to a *Scheduled Job*.
- Created an unlimited number of new *Scheduled Jobs*.
- Add, delete, and alter priority of different *Triplet* entries within a single *Schedule*.

To get the most out of *BackupEDGE Advanced Scheduling*, a good understanding of *Domains*, *Sequences* and *Notifiers* is required. If you have not already done so, please read "Anatomy of a BackupEDGE Backup" on page 40 carefully *before* proceeding.

After you have familiarized yourself with that section and this one, you may be interested in "Scheduled Jobs in More Detail" on page 342 for a detailed look at *Scheduled Jobs*.

NOTE: The *Advanced Scheduler* entries in the Schedule dropdown are **disabled** by default. To see the full menu, you enable the *Advanced Scheduler* using `Enable Advanced` in the *Setup* dropdown menu. After you have done this, all of these options will be available. If you do not need *Advanced Scheduling*, it is recommended that you do not enable it. It can be enabled later at any time.

20.1 - Triplets Scheduling

Theory

A *triplet* is read as follows: **Frequency**, **Day Variable** of the **Time Frame**. An example of this would be **1st Friday** of **March**, or **Last Day** of **Year**. When creating a *triplet* you will be able to choose from the options "*week*", "*month*", "*year*" or a *specific month*. After choosing this you will then be able to specify the *day(s)*, such as "**Monday**" or "**Weekday**". Then depending on the previous choices you will see *Frequency Options* such as **every**, **last**, **first**, **10th**. These options are stackable and will permit you the ability to control the granularity of your backups down to the day of the year.

Let's look at the *Basic Schedule* in *Advanced Schedule* mode. Make sure Advanced Scheduling has been enabled. From *EDGEMENU* select `Schedule -> Advanced Schedule`.

You may **FastSelect** any current *Scheduled Job*, or create a new *Scheduled Job*, with or without using the *Wizard*. You may also **Delete** a *Scheduled Job* by pointing to it and pressing `[F6]` or `[CTRL-X]`.

1. Requires *BackupEDGE* 03.00.02 or later.

Advanced Schedule FastSelect

```
+Scheduled Job Selection-------------------------------------------------------+
|                    Please Select The Scheduled Job To Use                     |
|                                                                               |
|Machine:            web2v.microlite.com                                        |
|Press F6 Or CTRL-X To Delete                                                   |
|+------------------------------------------------------------------------------+|
||   [New From Wizard]                                                          ||
||   [New]                                                                      ||
||   key_job: Unattended Backup Job (Disabled)                                  ||
||-> simple_job: Basic Schedule (Enabled, 23:00)                               ||
|[Edit]                              [Prev]                            [Cancel]|
+-------------------------------------------------------------------------------+
```

Each *Scheduled Job* is displayed with its name (the default *Scheduled Job* is called `simple_job`), description (the default is `Basic Schedule`), and its current status (`Enabled` to run at `23:00`, although the list of which days is not shown here). When you've created your own *Advanced Schedules* they will also appear here.

NOTE: Never modify the `key_job` *Schedule*. It is for backing up encryption keys and is handled by the encryption setup menus.

Basic Schedule in Advanced Mode

The Basic Schedule (Viewed in the Advanced Scheduler)

```
+ Edit Backup Schedule ---------------------------------------------------------+
| Schedule Name:     [simple_job   ]                                            |
|          Time:     [23:00 ] (17:05:41)  Enabled: [X]                          |
| Sequence:          [Change] web2v.microlite.com:esequence/onsite              |
| Backup Domain:     [Change] system mysql                                      |
| Primary Resource:  [Change] web2v.microlite.com:optical!optical0              |
|                                                                               |
| +-----------------------------------------------+     September 2019         |
| | Every Sunday of the week                (None) |  Su Mo Tu We Th Fr Sa     |
| | Every Monday of the week               Master |   1 M  M  M  M  M   7     |
| | Every Tuesday of the week              Master |   8 M  M  M  M  M  14     |
| | Every Wednesday of the week            Master |  15 M  M  M  M  M  21     |
| | Every Thursday of the week             Master |  22 M  M  M  M  M  28     |
| | Every Friday of the week               Master |  29 M                     |
| | Every Saturday of the week              (None) |                           |
| +-----------------------------------------------+                           |
|                                                                               |
| Notify / Advanced: [Change]  [Reset Dates]                                    |
| Mail Summary To:   root                  Print Summary To:   NONE             |
| Mail Failures To:  NONE                  Print Failures To:  NONE             |
|[Save]                                                            [Cancel]|
+-------------------------------------------------------------------------------+
```

Note that it is now possible to change the *Sequence* and add or remove *Domains*. Our concentration will be on the center section of the screen, called the *Frequency Window*.

This is where all of the *Backup**EDGE*** scheduling magic occurs. Consider the default *Basic Schedule*.

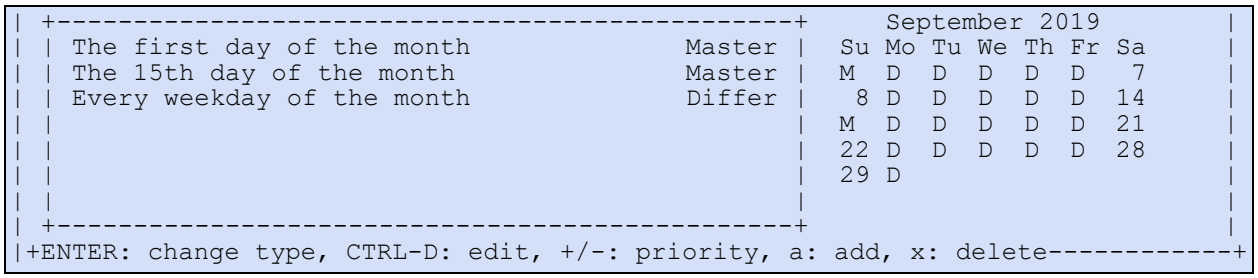
```
| +-----------------------------------------------+     September 2019         |
| | Every Sunday of the week                (None) |  Su Mo Tu We Th Fr Sa     |
| | Every Monday of the week               Master |   1 M  M  M  M  M   7     |
| | Every Tuesday of the week              Master |   8 M  M  M  M  M  14     |
| | Every Wednesday of the week            Master |  15 M  M  M  M  M  21     |
| | Every Thursday of the week             Master |  22 M  M  M  M  M  28     |
| | Every Friday of the week               Master |  29 M                     |
| | Every Saturday of the week              (None) |                           |
| +-----------------------------------------------+                           |
+ENTER: change type, CTRL-D: edit, +/-: priority, a: add, x: delete------------+
```

Each line in the *Frequency Window* represents one day of the week, and there are only two available options for each day:

- Choose the backup type, i.e. *Master*, *Differential*, *Incremental*, or *(None)*.
- Choose the *Media List* if a changer is involved (by pressing Ctrl-D while the proper line is selected.

Each line represents the simplest form of *Triplet*, i.e. *Every Sunday* of the *Week* has a **Frequency** (*Every*), **Day Variable** (*Sunday*), and **Time Frame**, (*Week*).

Now, let's look at another possible schedule created in the *Advanced Scheduler*



This *Schedule* will **ALWAYS** perform a *Master Backup* on the **first day** of the **month**, even if it falls on a weekend. It will **ALWAYS** perform a *Master Backup* on the **15th day** of the **month**, even if it falls on a weekend. It will ONLY perform a *Differential Backup* on a **weekday** of the **month** which is **not** the **1st** or **15th day** of the **month**.

NOTE: In the screen shot above, the priority of the entries is to-to-bottom. For instance, if the `Every weekday of the week Differ` *Differential Backup* were on the top instead of the bottom, it would have priority and the *Master Backups* scheduled for the **1st** and **15th** would be ignored unless, in this instance, they occurred on a weekend day.

Triplets Scheduling provides the key to some very useful scheduling variation.

Reviewing from a few pages ago, a *triplet* is read as follows **Frequency**, **Day Variable** of the **Time Frame**, for example **1st Friday** of **March**, or **Last Day** of **Year**.

When creating a *triplet* you first need to choose from the **Time Frame** options, which consist of "*week*", "*month*", "*year*" or a *specific month*.

After choosing this you can specify the **Day Variable**, such as "**Monday**" or "**Weekday**".

Then **depending** on the previous choices you will see **Frequency** options such as **every**, **last**, **first**, **10th**. These options are stackable and will permit you the ability to control the granularity of your backups down to the day of the year.

For example, if **Time Frame** is set to *week*, then **Frequency** is automatically set to *every* and **Day Variable** can be one of the following:

```
every day of the week
every weekday of the week
every Sunday of the week
every Monday of the week
every Tuesday of the week
every Wednesday of the week
every Thursday of the week
every Friday of the week
every Saturday of the week
every Sat. or Sun. of the week
```

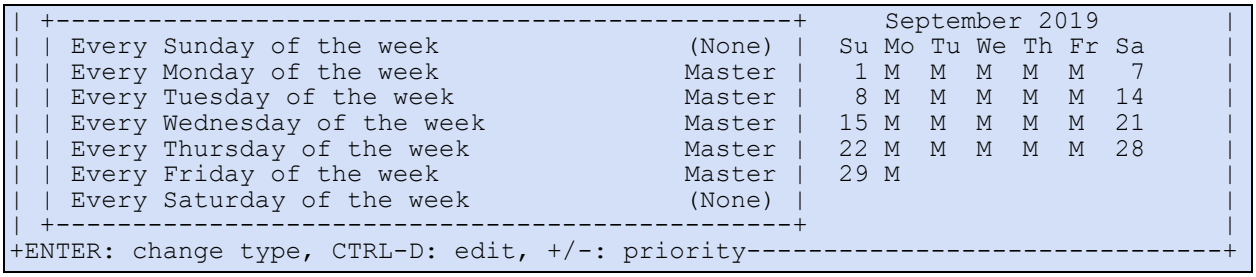
If **Time Frame** is set to *month* (or a specific month, i.e. *January*, *February*, *March*, etc.), then the **Day Variable** options remain the same while the **Frequency** can be:

```
every
last
first
second
third
4th
5th
...
31st
```

If **Time Frame** is set to *year*, then the **Day Variable** options remain the same while the **Frequency** can be *every*, *last*, *first*, or any *day* of the *year*.

Each of the **Frequency**, **Day Variable** and **Time Frame** variables recognizes its interdependency with the other two, so that only valid combinations may be set. For instance, if **Time Frame** is set to *month* and **Day Variable** is set to *Sunday*, only *every*, *last*, and *first* through *fifth* **Frequencies** can be selected.

Frequency Window Navigation



While the cursor is in the schedule screen, the following navigation keys work...

`[F1]` - Field Help
`[F2]` - Exits *EDGEMENU* from almost anywhere.
`[Up-Arrow]`/`[Down-Arrow]` - Scrolls among fields.
`[Left-Arrow]`/`[Right-Arrow]` - Scrolls among fields or through text fields.
`[Tab]` - Fast navigate to first field in a section
`[Enter]` - Commit a change or start a highlighted menu operation.
`[F8]` - Refresh key. Redraws the display in the even it gets corrupted.

While in the *Frequency Window*...

`[F6]` - Deletes *Triplet* lines.
`[X]` - Deletes *Triplet* lines.
`[A]` - Adds *Triplet* lines.
`[Ctrl-D]` - Edits *Triplet* lines.
`[+]` - (Plus Sign) Increases the priority of a *Triplet* line.
`[-]` - (Minus Sign) Decreases the priority of a *Triplet* line.
`[Space]` - (Space Bar) Toggles the *Backup Type* of a *Triplet* line among `Master`, `Differ`, `Increm` and `(None)`.

Backup Time and Type Selection (Triplet Editing Window).

```
+Backup Time and Type Selection-------------------------------------------------+
|Please modify this backup entry.                                               |
|Current value:  Every Sunday of the week                                       |
|+----------+ +----------------+ +-------------+                                |
||-> every  | |   day          | |-> week      |  Backup Type:  [M]             |
||          | |   weekday      | |   month     |                                |
||          | |-> Sunday       | |   year      |  Min. Retention: [(Default)]   |
||          | |   Monday       | |   January   |                                |
||          | |   Tuesday      | |   February  |                                |
||          | |   Wednesday    | |   March     |                                |
||          | |   Thursday     | |   April     |                                |
||          | |   Friday       | |   May       |                                |
||          | |   Saturday     | |   June      |                                |
||          | |   Sat. or Sun. | |   July      |                                |
||          | |                | |   August    |                                |
||          | |                | |   September |                                |
||          | |                | |   October   |                                |
||          | |                | |   November  |                                |
|+----------+ +----------------+ +--vv More vv-+                                |
|[Next]                                                          [Cancel]       |
+-------------------------------------------------------------------------------+
```

When you first enter the window it will look similar to the one above. Use the `[Left-Arrow]`/`[Right-Arrow]` to switch sections left to right, and the `[Up-Arrow]`/`[Down-Arrow]` to change entries within the section. For instance, move to the **Time Frame** section and select month and the screen will chance to:

```
+Backup Time and Type Selection-------------------------------------------------+
|Please modify this backup entry.                                               |
|Current value:  Every Sunday of the month                                      |
|+----------+ +----------------+ +-------------+                                |
||-> every  | |   day          | |   week      |  Backup Type:  [M]             |
||   last   | |   weekday      | |-> month     |                                |
||   first  | |-> Sunday       | |   year      |  Min. Retention: [(Default)]   |
||   second | |   Monday       | |   January   |                                |
||   third  | |   Tuesday      | |   February  |                                |
||   4th    | |   Wednesday    | |   March     |                                |
||   5th    | |   Thursday     | |   April     |                                |
||          | |   Friday       | |   May       |                                |
||          | |   Saturday     | |   June      |                                |
||          | |   Sat. or Sun. | |   July      |                                |
||          | |                | |   August    |                                |
||          | |                | |   September |                                |
||          | |                | |   October   |                                |
||          | |                | |   November  |                                |
|+----------+ +----------------+ +--vv More vv-+                                |
|[Next]                                                          [Cancel]       |
+-------------------------------------------------------------------------------+
```

If you want to change the *Retention Time* for an individual *Triplet*, click on the `Min. Retention` field. See “Per-Triplet Retention Times” on page 226 for more information.

Change the **Day Variable** from *Sunday* to *day*, and your options become:

```
+Backup Time and Type Selection-------------------------------------------------+
|Please modify this backup entry.                                               |
|Current value:  Every day of the month                                         |
|+----------+ +----------------+ +-------------+                                |
||-> every   | |-> day          | |   week      |  Backup Type:   [M]            |
||   last    | |   weekday      | |-> month     |                                |
||   first   | |   Sunday       | |   year      |  Min. Retention: [(Default)]   |
||   second  | |   Monday       | |   January   |                                |
||   third   | |   Tuesday      | |   February  |                                |
||   4th     | |   Wednesday    | |   March     |                                |
||   5th     | |   Thursday     | |   April     |                                |
||   6th     | |   Friday       | |   May       |                                |
||   7th     | |   Saturday     | |   June      |                                |
||   8th     | |   Sat. or Sun. | |   July      |                                |
||   9th     | |                | |   August    |                                |
||   10th    | |                | |   September |                                |
||   11th    | |                | |   October   |                                |
||   12th    | |                | |   November  |                                |
|vv More vv-+ +----------------+ +--vv More vv-+                                |
|[Next]                                                          [Cancel]|
+-------------------------------------------------------------------------------+
```

where the **Frequency** add more possibilities as the other two variables change, and the `Current Value` displays the entry that will be made if you `[Tab]` down to `[Next]` to save it.

Media List

For Autochangers, the *Triplet Editing Window* displays one other option; the `Media List`.

```
+Backup Time and Type Selection-------------------------------------------------+
|Please modify this backup entry.                                               |
|Current value:  Every Monday of the week                                       |
|+----------+ +----------------+ +-------------+                                |
||-> every   | |   day          | |-> week      |  Backup Type:   [M]            |
||           | |   weekday      | |   month     |  Media List:  [st0          ]  |
||           | |   Sunday       | |   year      |  Min. Retention: [(Default)]   |
||           | |-> Monday       | |   January   |                                |
||           | |   Tuesday      | |   February  |                                |
||           | |   Wednesday    | |   March     |                                |
||           | |   Thursday     | |   April     |                                |
||           | |   Friday       | |   May       |                                |
||           | |   Saturday     | |   June      |                                |
||           | |   Sat. or Sun. | |   July      |                                |
||           | |                | |   August    |                                |
||           | |                | |   September |                                |
||           | |                | |   October   |                                |
||           | |                | |   November  |                                |
|vv More vv-+ +----------------+ +--vv More vv-+                                |
|[Next]                                                          [Cancel]|
+-------------------------------------------------------------------------------+
```

The slot name or barcode name must be entered in each individual *Triplet* entry to select the tape cartridge that will be used for that day's backup.

If you wish to use different cartridge on a large library, it is easy to create a schedule that has

many *Triplet* lines, each of which can have a cartridge entry. For instance...

```
first Monday of the month
first Tuesday of the month
first Wednesday of the month
first Thursday of the month
first Friday of the month
second Monday of the month
second Tuesday of the month
second Wednesday of the month
second Thursday of the month
second Friday of the month
...
```

There is no limit to the number of *Triplet* entries that the window can contain.

Quarterly Backup Schedule Example

```
last day of March
last day of June
last day of September
last day of December
```

When creating new schedules, remember to set the *Retention Time* of all backups in the *Schedule* to whatever is appropriate.

Reset Dates
Pressing the `[Reset Dates]` button resets the *Schedule* to the default, which is Monday through Friday *Master Backups*. This is most useful if you are using the *Advanced Scheduler*, make too many changes to track properly, and wish to start over.

Notify / Advanced
Pressing the `[Change]` button for this field brings up a new window used to change advanced backup options, and to add or edit *Notifiers*. Let's take a closer look.

Per-Triplet Retention Times[1]

As noted, each *Scheduled Job* has a default `Retention Time` of `1 Week`. This can be changed in the `Notify/Advanced` screen of the *Schedule*, in either *Basic Schedule* or *Advanced Schedule* mode.

In the *Advanced Scheduler*, it is possible to change the *Retention Time* on a per-Triplet line basis. This creates great scheduling flexibility. Some possible uses are:

- Master backups a few times per month with longer retention times.
- Master backups with longer retention times than differential backups.
- End-of-month backups that do not expire.

Whenever the *Retention Time* of a *Triplet* is different from the *Default* time in a *Scheduled Job*, an asterisk (*) will appear in front of the *Triplet* line.

For instance, in the *Scheduled Job* we modified earlier, we may have wanted to change the *Retention Time* of `The first day of the month` backup to **1 Year**, and of

1. Requires 03.00.02 build 1 or later.

`The 15th day of the month` backup to **2 Months**, while allowing all other backups to expire in one week. The schedule would look like this:

```
| +-----------------------------------------------+     September 2019        |
| |*The first day of the month             Master |  Su Mo Tu We Th Fr Sa     |
| |*The 15th day of the month              Master |  M  D  D  D  D  D   7     |
| | Every weekday of the month             Differ |   8 D  D  D  D  D  14     |
| |                                               |  M  D  D  D  D  D  21     |
| |                                               |  22 D  D  D  D  D  28     |
| |                                               |  29 D                     |
| |                                               |                           |
| +-----------------------------------------------+                           |
|+ENTER: change type, CTRL-D: edit, +/-: priority, a: add, x: delete-----------+
```

Pressing `Ctrl-D` on these lines would show that we made the following changes:

```
+Backup Time and Type Selection-------------------------------------------------+
|Please modify this backup entry.                                               |
|Current value:  On the first day of the month                                  |
|+----------+ +----------------+ +-------------+                                |
||   every  | |-> day          | |   week      |  Backup Type:  [M]             |
||   last   | |   weekday      | |-> month     |                                |
||-> first  | |   Sunday       | |   year      |  Min. Retention: [1 Years]     |
||   second | |   Monday       | |   January   |                                |
||   third  | |   Tuesday      | |   February  |                                |
||   4th    | |   Wednesday    | |   March     |                                |
||   5th    | |   Thursday     | |   April     |                                |
||          | |   Friday       | |   May       |                                |
||          | |   Saturday     | |   June      |                                |
||          | |   Sat. or Sun. | |   July      |                                |
||          | |                | |   August    |                                |
||          | |                | |   September |                                |
||          | |                | |   October   |                                |
||          | |                | |   November  |                                |
|+----------+ +----------------+ +--vv More vv-+                                |
|[Next]                                                          [Cancel]|
+-------------------------------------------------------------------------------+
```

```
+Backup Time and Type Selection-------------------------------------------------+
|Please modify this backup entry.                                               |
|Current value:  On the 15th day of the month                                   |
||^^ More ^^-+ +----------------+ +-------------+                               |
||   second | |-> day          | |   week      |  Backup Type:  [M]             |
||   third  | |   weekday      | |-> month     |                                |
||   4th    | |   Sunday       | |   year      |  Min. Retention: [8 Weeks]     |
||   5th    | |   Monday       | |   January   |                                |
||   6th    | |   Tuesday      | |   February  |                                |
||   7th    | |   Wednesday    | |   March     |                                |
||   8th    | |   Thursday     | |   April     |                                |
||   9th    | |   Friday       | |   May       |                                |
||   10th   | |   Saturday     | |   June      |                                |
||   11th   | |   Sat. or Sun. | |   July      |                                |
||   12th   | |                | |   August    |                                |
||   13th   | |                | |   September |                                |
||   14th   | |                | |   October   |                                |
||-> 15th   | |                | |   November  |                                |
|vv More vv-+ +----------------+ +--vv More vv-+                                |
||[Next]                                                          [Cancel]|
+-------------------------------------------------------------------------------+
```

You could even go a step further and add another *Triplet* such as `The last day of the year` with an expiration of, say, **7 Years**, and make it the top priority *Triplet*. In this event, *December 31* would always get a *Master Backup* that wouldn't expire for a long time.

See Expiration Time / Delete Expired

It is always possible to see the expiration time of a backup, and to manually delete it. Any of the EDGEMENU screens which display archive lists, such as `Verify->Show Archive Label` or

Admin->Delete Archives will show the archive list along with the archive expiration time (shown as TTL or Time To Live).

```
+Select Archive(s) to Delete from url0-----------------------------------------+
|+-------------------------------------------------------------------------------+|
||     [1] (562 MB) 'web2v Microlite_Web_Site Edge.Nightly 03.00.00 Master 2018||
||->  [2] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Master 2019/09/05 13:53:||
||     [3] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Master 2019/09/06 13:53:||
||     [4] (196 MB) 'web2v system Edge.Nightly 03.00.00 Incremental(#1) 2019/09||
||     [5] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Incremental(#1) 2019/09/||
||     [6] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Master 2019/09/09 22:00:||
||     [7] (57490 MB) 'web2v system Edge.Nightly 03.00.00 Master 2019/09/09 22:||
||     [64] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Master 2019/09/10 13:53||
||     [65] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Master 2019/09/10 22:00||
||     [66] (57495 MB) 'web2v system Edge.Nightly 03.00.00 Master 2019/09/10 22||
||     [123] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Master 2019/09/11 13:5||
||                                                                             ||
||                                                                             ||
|+Total Space Used: 113.03GB-----------------------------------------------------+|
|Sys: web2v.microlite.com                Dir: /                                 |
|Dom: mysql                              Job: mysql_master                      |
|Slot: default                           Date: Thu Sep  5 13:53:01 2019         |
|Type: Edge.Nightly 03.00.00 Master      TTL: Thu Sep 12 12:48:01 2019          |
|                                                                               |
|[Delete]                                                          [Cancel]|
+-------------------------------------------------------------------------------+
```

The screen example above is from `Delete Archives`. Note that the highlighted entry above is set expire approximately one week after it was created.

20.2 - Creating an Advanced Schedule

Before creating an *Advanced Schedule*, it is strongly recommended that you become familiar with the concepts discussed in “Anatomy of a BackupEDGE Backup” on page 40 if you are not already. Also remember to review “Master / Differential / Incremental Backups” on page 211.

Unlike the *Basic Schedule*, *Advanced Schedules* give you more control over what will be archived, and how it will be archived.

In addition to modifying the *Basic Schedule* in ways defined in the section up to this point, you may also:

- Select the *Sequence* used to track the *Scheduled Job*.
- Add additional tracking *Sequences*.
- Create and edit as many *Backup Domains* as desired.
- Add more than one *Backup Domain* to a *Scheduled Job*.
- Created an unlimited number of new *Scheduled Jobs*.

Advanced Schedule FastSelect

```
+Scheduled Job Selection-------------------------------------------------------+
|                    Please Select The Scheduled Job To Use                     |
|                                                                               |
|Machine:            web2v.microlite.com                                        |
|Press F6 Or CTRL-X To Delete                                                   |
|+------------------------------------------------------------------------------+|
||   [New From Wizard]                                                          ||
||   [New]                                                                      ||
||   key_job: Unattended Backup Job (Disabled)                                  ||
||   midday: Unattended Backup Job (Enabled, 12:01)                             ||
||-> simple_job: Basic Schedule (Enabled, 13:13)                               ||
||   special: Unattended Backup Job (Enabled, 14:35)
|||[Edit]                              [Prev]                          [Cancel]|
+-------------------------------------------------------------------------------+
```

You may **FastSelect** any current *Scheduled Job*, or create a new *Scheduled Job*, with or without using the *Wizard*. You may also **Delete** a *Scheduled Job* by pointing to it and pressing `[F6]` or `[CTRL-X]`.

Each *Scheduled Job* is displayed with its name (`simple_job`), description (`Basic Schedule`), and its current status (`Enabled` to run at `23:00`, although the list of which days is not given).

You may use the *Advanced Schedule* option to create or edit the *Basic Schedule* as well as other *Scheduled Jobs*. The *Basic Schedule* is listed as:

```
Basic Schedule (mlite:simple_job)
```

Fast Selecting the *Basic Schedule* in the *Advanced Schedule* menu opens up the `Enable?` field for more options. You'll see that all of the **X** fields have been changed to **M** for *Master Backup*, just as they are for *Advanced Schedules*.

The Basic Schedule (Viewed in the Advanced Scheduler)

```
+ Edit Backup Schedule ---------------------------------------------------------+
| Schedule Name:     [simple_job   ]                                            |
|          Time:     [23:00 ] (17:05:41)  Enabled: [X]                          |
| Sequence:          [Change] web2v.microlite.com:esequence/onsite              |
| Backup Domain:     [Change] system mysql                                      |
| Primary Resource:  [Change] web2v.microlite.com:optical!optical0              |
|                                                                               |
| +-----------------------------------------------+     September 2019         |
| | Every Sunday of the week                (None) |  Su Mo Tu We Th Fr Sa     |
| | Every Monday of the week               Master |   1 M  M  M  M  M   7     |
| | Every Tuesday of the week              Master |   8 M  M  M  M  M  14     |
| | Every Wednesday of the week            Master |  15 M  M  M  M  M  21     |
| | Every Thursday of the week             Master |  22 M  M  M  M  M  28     |
| | Every Friday of the week               Master |  29 M                     |
| | Every Saturday of the week              (None) |                          |
| +-----------------------------------------------+                           |
|                                                                               |
| Notify / Advanced: [Change]  [Reset Dates]                                    |
| Mail Summary To:   root                    Print Summary To:   NONE           |
| Mail Failures To:  NONE                    Print Failures To:  NONE           |
|[Save]                                                              [Cancel]|
+-------------------------------------------------------------------------------+
```

Schedule Name:
The *Schedule Name* for the *Basic Schedule* is always called `simple_job`. The field is now open for editing. Change this only when creating a new *Schedule*.

Time:
Same as in the Basic Schedule. This is the time of day that the *Scheduled Job* will be run. You must type the time in 24 hour time format, hour, colon (`:`) minute after the hour, as shown above. In the example, this *Scheduled Job* will be run at one hour before midnight. If you type an invalid time, you'll be warned when you press `[Save]` or `[Next]`.

Enabled:
Same as in the Basic Schedule. If this field contains an **x**, the job will be run automatically at the time indicated on the selected days once it has been saved with the `[Next]` button. If you remove the **x** (press `[Space]` with the cursor in the field), the *Scheduled Job* will be saved normally, but won't actually be run automatically. This is useful for temporarily suspending a *Scheduled Job*, and also for creating special *Scheduled Jobs* which will be run only from *EDGEMENU* in attended mode.

Sequence:
The field is now open for editing. When creating your own *Advanced Scheduled Jobs*, you may define a custom *Sequence*, or use the default *Sequence* (`onsite`) or alternate Sequence (`offsite`) to log your backups. Recall from "Anatomy of a BackupEDGE Backup" on page 40 that a *Sequence* keeps related backups of the same data together.

Backup Domain:
The field is now open for editing. *Domain(s)* can be added or deleted by selecting `[Change]` here.

```
+Backup domain selection-------------------------------------------------------+
|            Select the domain(s) to include in this scheduled job.            |
|                                                                              |
|Machine:            web2v.microlite.com                                       |
|                                                                              |
|-Backup Domains NOT Included In Job---------------------------------------|
||-> Decryption Keys (web2v:key_domain)                                       ||
||                                                                           ||
||                                                                           ||
|-Backup Domains Included In Job-------------------------------------------|
||-> Entire System (web2v:system)                                           ||
||   MySQL Autodetected Backup Domain (web2v:mysql)                          ||
||                                                                           ||
|[Next]                                                          [Cancel]|
+------------------------------------------------------------------------------+
```

This displays **All** the *Domains* that have been system defined or user defined. If the *Domain* is included in the currently defined Scheduled Job, it will show in the bottom window. If not included, it will show in the top window.

To include a *Domain* in the *Scheduled Job*, Press `[Tab]` to place the arrow cursor in the top window, point to the *Domain* to be added, and press `[Enter]` to move it to the bottom window.

To remove a *Domain* from the *Scheduled Job*, Press `[Tab]` to place the cursor in the bottom window, point to the *Domain* to be added, and press `[Enter]` to move it to the top window.

NOTE: Entries included in the `Backup Domains Included In Job` are archived in the order shown. To change the order, it is easiest to remove them all, the add them back in the order desired.

The `Decryption Keys` domain should never be added to a *Scheduled Job*.

As many *Domains* as are defined can be added to a *Scheduled Job*. One of the many uses for this feature is that it is possible to excluded data or application filesystems or directories from the default *Domain*, then create new *Domains* to archive them separately. This makes it very easy to do targeted archives for the separate filesystems or directories with one *Scheduled Job* while combining them for complete system backups at a different time. If you choose this method:

- **Never** exclude the *boot* filesystem from being archived along with the *root* filesystem.
- Remember that all restores of the separate *Domains* will be separate tasks, i.e. they won't come back automatically with a full restore of the primary *Domain* or a disaster recovery. You'll have to select them separately.

Primary Resource:
As in the *Basic Schedule*, this field indicates the *Resource* which will be used to store this archive.

Frequency Window

The default is the same 7 day *Triplet* list as defined in the *Basic Schedule*. See "Triplets Scheduling" on page 220 for ways to customize these entries.

Reset Dates

Pressing the `[Reset Dates]` button resets the *Schedule* to the default, which is Monday through Friday *Master Backups*. This is most useful if you are using the *Advanced Scheduler*, make too many changes to track properly, and wish to start over.

Notify / Advanced

Pressing the `[Change]` button for this field brings up a new window used to change advanced backup options, and to add or edit *Notifiers*. Let's take a closer look.

20.3 - Creating Backup Domains

This is the default *Domain* installed by *Backup**EDGE***. (It may vary slightly depending on the operating system.) It can be seen by using the **Create / Edit Domain** option from the **Schedule** menu in *EDGEMENU*.

Default Domain

```
+Edit Backup Domain-------------------------------------------------------------+
|Machine:            web2v.microlite.com                                        |
|Name:               [system                                                  ]|
|Description:        [Entire System                                           ]|
|                                                                               |
|-Edit Filesystem Backup Domain---------------------------------------------- |
|Include:            [/                                                       ]|
|Exclude:            [/proc                                                   ]|
|Exclude Netmounts:  [N]                                                       |
|Exclude Readmounts: [N]                                                       |
|Exclude Allmounts:  [N]                                                       |
|Incl. Filelist:     [                                                        ]|
|Excl. Filelist:     [/etc/edge.exclude                                       ]|
|Encryption List     [                                                        ]|
|                    [Advanced Properties]                                     |
|[Save]                        [Back To Select]                      [Cancel]|
+-------------------------------------------------------------------------------+
```

`Advanced Properties`

```
+Edit Advanced Domain Properties------------------------------------------------+
|Machine:            web2v.microlite.com                                        |
|Virtual Filelist:   [/etc/edge.virtual                                       ]|
|Start/Stop Script:  [/usr/lib/edge/bin/edge.bscript                          ]|
|Raw Dev Filelist:   [/etc/edge.raw                                           ]|
|Raw Script:         [/usr/lib/edge/bin/edge.rawscript                        ]|
|No-check Filelist:  [/etc/edge.nocheck                                       ]|
|Config Script:      [                                                        ]|
|Follow Symlinks     [N]                                                       |
|Read Locking        [U]                                                       |
|Preserve Atime      [N]                                                       |
|Diff/Incr Level     [2]                                                       |
|[Save]                                                          [Cancel]     |
+-------------------------------------------------------------------------------+
```

Let's translate that into English.

When we tell *Backup**EDGE*** to back up the *Domain* called `system`, it means:

This *Domain* includes all files starting with (`/`), except the specifically Excluded `/proc` *Directory*.

The three entries `Exclude Netmounts`, `Exclude Readmounts`, and `Exclude Allmounts` all default to `N` for **No**. These, respectively, exclude network mounted filesystem, filesystems flagged as read-only, and all mounted filesystems. Leave these set at the default unless you have tested

their behavior and it is consistent with your wishes. It is better to specifically exclude files and directories you do not want included in a *Domain*.

There is no additional list of files to include, since `Incl. Filelist` is blank. If it were not, the files given would be assumed to each contain a list of filenames, one per line, to be included in this *Domain*.

Similarly, `Excl. Filelist` provides files that contain a list of files to be excluded. In this example, if there are any files listed in the file `/etc/edge.exclude`, they will also be excluded from the data described by this *Domain*. By default, `/etc/edge.exclude` contains a number of files and directories which are operating system specific an do not need to be part of system backups. The user may add to these or create their own files.

Each of `Include`, `Exclude`, `Incl. Filelist`, and `Excl. Filelist` could contain multiple entries, separated by spaces. (If it is desired to specify a file to include or exclude that contains a space in the filename, it must be stored in a *filelist*. The *filelists* themselves must be stored in filenames without spaces.)

`Encryption List`: This allows you to specify a file that contains a list of files to be encrypted in this *Domain*. This is discussed in detail in the *Backup**EDGE*** Encryption section of this guide. ***If you do not have Encryption enabled and licensed, then this line must be blank if it appears. Normally, it will not be displayed in this case.***

NOTE: The Encryption List may only be used if the Encryption feature of *Backup**EDGE*** is enabled. To enable this, you must have a serial number for Encryption along with an activation code for it. Encryption is also enabled while *Backup**EDGE*** is operating as a demo.

In the *Advanced Properties* submenu:

The `Virtual Filelist` optionally defines a filename whose contents are pathnames that are to be treated as *Virtual Files*. In this example, if there are any files listed in the file `/etc/edge.virtual`, treat them as *Virtual*, or *Sparse*, files.

`Start/Stop Script`: Run `/usr/lib/edge/bin/edge.bscript` before and after a backup / verify operation to prepare the data for archive or return it to normal operation. This is discussed in more detail in “Running Scripts to Prepare for Backup” on page 342.

If there are any *Device Nodes* listed in `/etc/edge.raw`, treat them specially during the backup, and run `/usr/lib/edge/bin/edge.rawscript` before and after each one.

If there are any files listed in `/etc/edge.nocheck`, don’t check them during bit level verification.

`Follow Symlinks`: Do `Not` follow *Symbolic Links*; just back up the symlink entry itself (of course, any link targets will probably be included anyway because this domain includes all files). In other words, if this option is checked, this *Domain* treats *Symbolic Links* as if they were not links. *During* a restore of this *Domain*, the data would be restored but not the *Symbolic Link*. If this option is not checked, then any *Symbolic Links* will be stored as links. Of course, the data they point to may also be included if the Include List or Incl. Filelist

Normally, this option should be un-checked. If you wish to protect the data pointed to by *Symbolic Links*, be sure that those file(s) are selected by the Include specification. For example, the Include of / will include all files.

`Read Locking`: Do `Not` attempt to obtain a lock on each file before backing it up. If another process has a file locked, *Backup**EDGE*** will try to avoid the lock *if possible* during a backup. Other options are Unenforced Locking and Enforced Locking, both of which obey locks held by other programs, and will place an Unenforced or Enforced lock on each file while it is being archived.

`Preserve Atime`: Do `Not` attempt to preserve the access time of each file during a backup. Use the `ctime` (`2`) of a file when comparing for *Differential* and *Incremental Backups*. Usually, the

default option is desirable for most data. For more information, please consult “Level 1 and 2 Differential/Incremental Backups” on page 361.

As you can see, it is easy to design very powerful backup *Domains* using this screen. Let’s create another *Domain*, for the popular database program filePro.

Example filePro Domain

```
+Edit Backup Domain-------------------------------------------------------------+
|Machine:            web2v.microlite.com                                        |
|Name:               [filePro                                                  ]|
|Description:        [All filePro Programs and Databases                       ]
|                                                                               |
|-Edit Filesystem Backup Domain---------------------------------------------------|
|Include:            [/u/appl /etc/default/fppath /usr/bin/P /usr/bin/p        ]
|Exclude:            [                                                         ]|
|Exclude Netmounts:  [N]                                                        |
|Exclude Readmounts: [N]                                                        |
|Exclude Allmounts:  [N]                                                        |
|Incl. Filelist:     [                                                         ]|
|Excl. Filelist:     [/etc/edge.exclude                                        ]|
|Encryption List     [                                                         ]|
|                    [Advanced Properties]                                      |
|[Save]                          [Back To Select]                      [Cancel]|
+-------------------------------------------------------------------------------+
```

Advanced Properties

```
+Edit Advanced Domain Properties-----------------------------------------------+
|Machine:            web2v.microlite.com                                        |
|Virtual Filelist:   [                                                         ]|
|Start/Stop Script:  [/u/appl/fp/fpclean                                       ]|
|Raw Dev Filelist:   [                                                         ]|
|Raw Script:         [                                                         ]|
|No-check Filelist:  [                                                         ]|
|Config Script:      [                                                         ]|
|Follow Symlinks     [N]                                                        |
|Read Locking        [U]                                                        |
|Preserve Atime      [N]                                                        |
|Diff/Incr Level     [2]                                                        |
|[Save]                                                              [Cancel]|
+-------------------------------------------------------------------------------+
```

This *Domain* would back up all *filePro* databases and system files each night. Before starting, it would run the `fpclean` program, which might be set up to remove lock files, trim or re-create indexes, etc.

With a little creativity, databases, accounting systems, POS systems, etc. could be defined as *Domains* and backed up easily using *Backup**EDGE***.

The terminology used here is defined in “Domains” on page 42.

Please remember that a *Domain* describes only *what* is to be archived and *what steps must be taken* to prepare it for archiving. It is independent of the type (*Master*, *Differential*, or *Incremental*) of backup to be performed, and the number of such backups.

NOTE: *Backup**EDGE** 3.x* has special support for MySQL Hot Backups and can create a specialized backup Domain. See “MySQL / MariaDB Backups” on page 177 for MySQL information.

20.4 - The Default Backup Sequence

As mentioned in “Anatomy of a BackupEDGE Backup” on page 40, a *Sequence* is a group of backups of the same *Domain*. If you have not done so, please refer to that section for an overview of what a *Sequence* is. If you do not intend to use *Differential* and / or *Incremental Backups*, this section may be ignored.

There are two Sequences pre-defined in *BackupEDGE*; `onsite` and `offsite`, and more can be defined.

Let's take a look at the default *Sequence* (called `onsite`).

Default Sequence

```
+-------------------------------------------------------------------------------+
|                            Edit Backup Sequence                               |
|                                                                               |
|Machine:            web2v.microlite.com                                        |
|Name:               [onsite                                                   ]|
|Description:        [On-Site Backups                                          ]|
|                                                                               |
|[Save]                          [Back To Select]                      [Cancel]|
+-------------------------------------------------------------------------------+
```

This *Sequence* will be the only one ever used on many systems. The default backup *Schedule* tracks all *Master*, *Differential* and / or *Incremental Backups* through this *Sequence*.

Another Sequence, called `offsite`, is also pre-defined and may be used to separate backups that are designed for off-site backups. Using this would ensure that a *Master Backup* tracked through the `offsite` *Sequence* would not change the information used for *Differential* and *Incremental Backups* tracked via `onsite`.

The terminology used here is defined in "Sequences" on page 44.

21 - Scheduling - Other

21.1 - Working with Notifiers

As previously mentioned, *BackupEDGE Notifiers* provide control over printed and mailed output. Each email name, alias, or printer name you place in a *Scheduled Job* can be modified by editing its associated *Notifier*. The *Notifier* can produce multiple copies of each message, or filter or modify the message in other ways. It specifies the message format to be used, such as plain text or numeric pager.

By default, names entered into an email list are simply mailed a plain text summary. Names entered into a printer list should be the simply the name of a printer, and are sent plain text output in *UNIX* format (Line Feeds only). However, *BackupEDGE* really creates a *Notifier* for each email address and printer name. You don't have to edit this *Notifier* (or even care that it exists) if you want the default behavior, but by modifying it you can get much more sophisticated backup notifications.

Let's take a look at an email *Notifier*.

Email Text Notifier

```
+-------------------------------------------------------------------------------+
|                          Edit BackupEDGE Notifier                             |
|Machine:             mlite.microlite.com                                       |
|Notifier Name:       [root                                                    ]|
|Description:         [this is root                                            ]|
|Notifier Type:       [E-Mail             ]                                     |
|Message Format:      [Text               ]                                     |
|Command:             [|mail -s %S %n                                          ]|
|Recipient(s):        [root                                                    ]|
|Append CR:           [ ]                                                       |
|Include FF:          [ ]                                                       |
|                                                                               |
|[Save]                            [Back To Select]                    [Done]   |
+-------------------------------------------------------------------------------+
```

This will send a basic text message to `root` on the local system whenever a backup is performed. *BackupEDGE* can do better than that.

Email HTML Notifier

```
+-------------------------------------------------------------------------------+
|                          Edit BackupEDGE Notifier                             |
|Machine:             show1.microlite.com                                       |
|Notifier Name:       [tom                                                     ]|
|Description:         [Toms HTML Backup Messages                               ]|
|Notifier Type:       [E-Mail             ]                                     |
|Message Format:      [HTML (MIME)        ]                                     |
|Command:             [|/bin/mail -s %S %n                                     ]|
|Recipient(s):        [tom.podnar@microlite.com tom@gmail.com                  ]|
|Append CR:           [ ]                                                       |
|Include FF:          [ ]                                                       |
|                                                                               |
|[Save]                            [Back To Select]                    [Done]   |
+-------------------------------------------------------------------------------+
```

Using this *Notifier*, if you type `tom` in the `Mail Summary To:` (or `Mail Failures To:`) field in a *Schedule*, it means the following...

- Format the email in *HTML* (MIME encapsulated) format, using color, text and graphics.
- Send the mail to both of the indicated recipients.

Similarly, the following would be a valid *Notifier*:

Email Pager Notifier

```
+-------------------------------------------------------------------------------+
|                          Edit BackupEDGE Notifier                             |
|Machine:              show1.microlite.com                                      |
|Notifier Name:        [emergency                                             ] |
|Description:          [Toms Emergency Backup Notifier                        ] |
|Notifier Type:        [E-Mail             ]                                    |
|Message Format:       [Alpha-Numeric      ]                                    |
|Command:              [|/bin/mail -s %S %n                                   ] |
|Recipient(s):         [7243750000@mobile.att.net                             ] |
|Append CR:            [ ]                                                      |
|Include FF:           [ ]                                                      |
|                                                                               |
|[Save]                           [Back To Select]                      [Done]  |
+-------------------------------------------------------------------------------+
```

This will send a message formatted with a maximum of 128 characters to an Alpha Pager, email equipped cell phone, PDA, etc.

Options for email format are `Text`, `HTML`, `Alpha-Numeric` and `Numeric`. `Numeric` sends a useful status message in 10 numbers for those with numeric-only pagers. You press `[Right-Arrow]` or `[Left-Arrow]` while in the `Message Format:` field to change formats.

Numeric Pagers

Numeric pager messages may be interpreted as follows:

`xxx - abc - hhmm`

`xxx - site code -` This may be set in `/usr/lib/edge/config/master.cfg` as a system-wide default. In case you are managing multiple *BackupEDGE* installations, this will allow you to tell which one sent the message. To change this value for a particular site, please consult the section “Configuration Variables Explained” on page 358.

`a - result code -` `7` indicates that the operation ***P***assed. `3` indicates a ***F***ailure. `9` means that the operation passed, but with e***X***ceptions. Note that on many telephones, the letters *P*, *F*, and *X* are printed on the `7`, `3`, and `9` keys, respectively.

`b - TapeAlert -` This indicates the number of *TapeAlert* messages discovered during the operation. If this is nonzero, you should consult the backup summary found in `/usr/lib/edge/config/`***`<the job name>`***`/edge.summary`.

`c - cleaning flag -` `3` indicates that *BackupEDGE* believes that the drive should be cleaned. `7` indicates that *BackupEDGE* does not believe this. Note that if your drive does not support *TapeAlert* (or does not issue *TapeAlert* cleaning messages), *BackupEDGE* will not be able to tell that the tape drive requires cleaning. This does not negate the fact that it must be cleaned regularly. (Cleaning a drive is generally accomplished by inserting a special Cleaning Cartridge.)

`hhmm - start time -` Indicates the start time of the job with a 24-hour clock.

Printer Notifier

```
+-------------------------------------------------------------------------------+
|                          Edit BackupEDGE Notifier                             |
|Machine:              mlite.microlite.com                                      |
|Notifier Name:        [optra1                                                ] |
|Description:          [BackupEDGE Notifier                                   ] |
|Notifier Type:        [Printer           ]                                     |
|Message Format:       [Text              ]                                     |
|Command:              [|/usr/bin/lp -d %n                                    ] |
|Recipient(s):         [optra2                                                ] |
|Append CR:            [ ]                                                      |
|Include FF:           [ ]                                                      |
|                                                                               |
|[Save]                          [Back To Select]                       [Done]|
+-------------------------------------------------------------------------------+
```

This is the a default print *Notifier*. You may add carriages returns and form feeds if your printer requires them by using `[Space]` to place an **X** in the appropriate field.

Since printers and email share the same *Notifier* formats, if you had a printer that directly accepted HTML you could choose that as the **Message Format:** type.

Since the **Command:** can be anything the user desires, there are an unlimited number of possibilities for creating the notification methods within *Backup**EDGE*** to best suit your needs.

21.2 - Checking for Updates to BackupEDGE

The *Update Checking* option from the *Schedule* menu allows you to schedule periodic checks of the Microlite Website for updated versions of *Backup**EDGE***. These checks can be performed automatically as often as weekly, if you desire. By default, no checking is performed. You may also check manually using the *Check for Updates* option of the *File* menu.

If you enable periodic checking, you will be given the option to choose the frequency in weeks of the checks, and whether or not to download newer versions automatically. Newer versions will never be installed automatically, but if you have a slower Internet connection, it might be advantageous for *Backup**EDGE*** download the newer version in the background.

During the update check, *Backup**EDGE*** fetches only pre-existing URLs; it does not send form data of any kind. Transport Protocol Port 80 (http) is used, so must be open outbound from your server.

If a new version is detected, backup summaries will include a line notifying you of this fact. If the check for updates cannot be performed for a prolonged period of time, this is also noted in the backup summaries.

To actually install a newer version, use the *Check for Updates* option in the *File* menu of *EDGEMENU*. You will be shown the Change Log of the new version, and allowed to cancel the installation if desired.

22 - EDGEMENU (Advanced)

22.1 - Making Unscheduled Backups from EDGEMENU

Unscheduled Full Backup

This performs a full *Unscheduled Full Backup*, with an optional *Verify* and/or *Index* pass, and places all of its log files in the *Directory* `/usr/lib/edge/lists/menu`. These files are called `backup_unschedfull.txt`, `verify_unschedfull.txt`, and `changedfiles_unschedfull.txt`.

Users may change any of the displayed options by using the arrow keys to position the cursor and pressing `[Space]` to change the default for that field. Pressing `[F1]` while on a field brings up context sensitive help to explain the options or rules for using that feature. Pressing `[Modify Excludes]` brings up an advanced menu for identifying files, *Directories* and filesystems to be excluded from the backup.

Press `[Execute Backup]` to begin, or press `[Tab]` or `[F10]` to return to the top menu bar and select another option.

```
+ Edgemenu for BackupEDGE ------------------------------------------------------+
¦+-------+--------+---------+---------+---------+-------+----------------------+¦
¦¦ [File] [Backup] [Restore] [Verify] [Admin] [Setup] [Schedule]                ¦¦
¦+-------------------------------------------------------------------------------+¦
|- Unscheduled Full Backup ------------------------------------------------------|
| [2] Verify Type (Bit-Level)                          Record Locking           |
| [X] Index During Verify                              ( ) Don't Lock Files     |
| [0 Days] Backup Retention Time                       (X) Unenforced Read      |
| [X] Data-Level Checksum                              ( ) Enforced Read        |
| [X] Include Raw Devices                                                       |
|                                        Notice: This backup will not affect    |
| [ ] Use /etc/edge.encrypt              Scheduled Jobs.  It is recommended     |
| [default           ] Slot Name         that you use Backup:Run Scheduled      |
|                                        instead.                               |
|                                                                               |
| [Execute Backup]  [Modify Excludes]                      [Cancel]             |
|+------------------------------------------------------------------------------+|
||Primary Resource : web2v:url!url0                                             ||
||  Compress: None, HW Block:  N/A, Edge Block:   64, Partition: C              ||
||                                                                              ||
||                                                                              ||
||                                                                              ||
||Last Master Backup: Tuesday Sep 10 22:00:01 2019                              ||
|+Local Machine: web2v.microlite.com  Administering: web2v.microlite.com -------+|
+-------------------------------------------------------------------------------+
```

As mentioned previously, the preferred method for doing this in *Backup**EDGE*** is to use the *Run Scheduled* option, not the *Unscheduled Full Backup* option. The former allows finer grained control over the backup, and keeps the *Sequence* for *Differential Backups* and *Incremental Backups* intact. It also stores the logs in the right spot for the appropriate *Scheduled Job*. Selecting *Unscheduled Full Backup* won't do this.

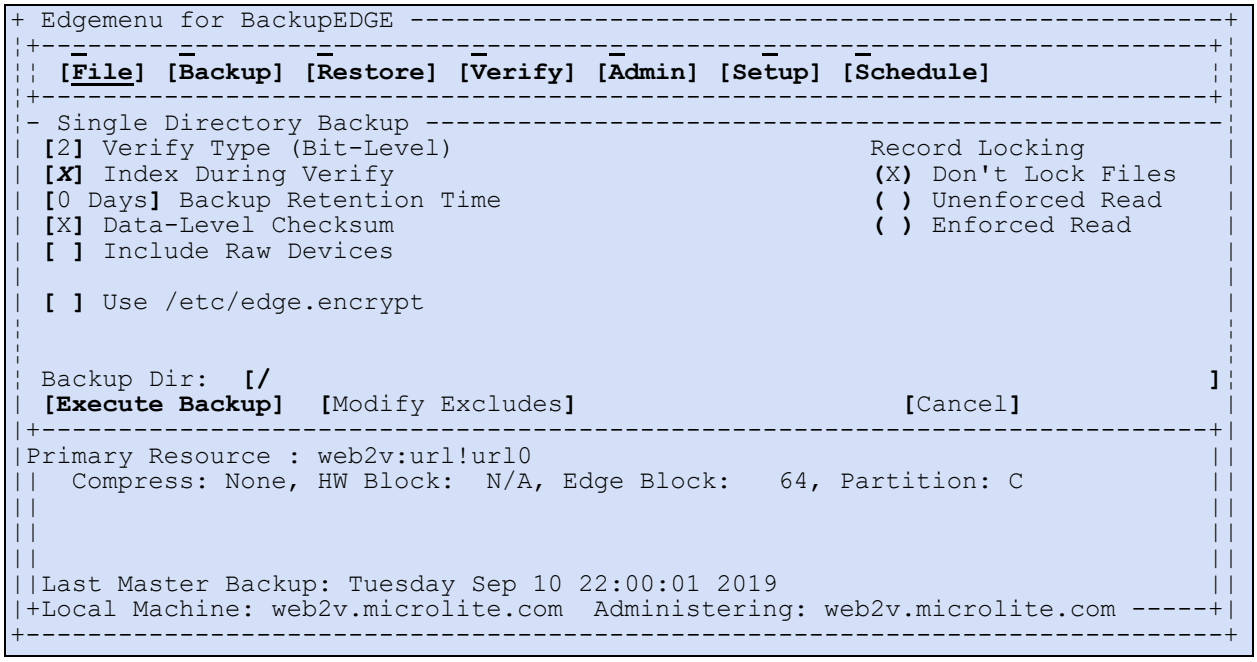
However, if you are performing *Differential* or *Incremental Backups* with *Scheduled Jobs*, using *Unscheduled Full Backup* allows you to put in an "extra" backup without affecting any *Sequence* (and thus any *Differential* or *Incremental Backup*). Which you prefer depends on what you are trying to accomplish.

See "Backup Parameters" on page 241 for information about each option.

Backup Single Dir

This allows a very fast backup of a single *Directory* (and all of its subdirectories). The *Default Directory* is the *Working Directory* at the time *EDGEMENU* was launched, but it can be changed

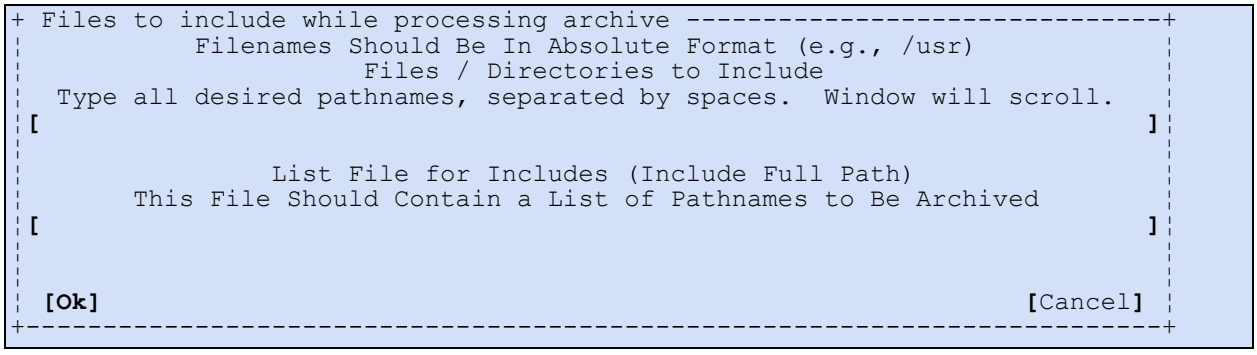
to any other *Directory*. Operations are logged in `/usr/lib/edge/lists/menu`. These files are called `backup_single.log`, `verify_single.log`, and `changedfiles_single.log`.



Simply change `Backup Dir:` to the *Directory* you wish to archive (use the *Absolute Pathname* of the *Directory* with no trailing slash), select any options or excludes, and press `[Execute Backup]`.

See “Backup Parameters” on page 241 for information about each option.

Backup Multiple Files / Dirs



This option presents two separate lines for data entry. The first (top) line is for the entry of individual files or *Directories* to be backed up. Files and *Directories* are separated by spaces. If you wish to back up a file or directory that contains a space in its name, precede the space with a backslash character ‘\’. If a name actually contains a backslash character, represent it with two back slashes: ‘\\’. Otherwise, *EDGEMENU* will treat it as two filenames!

The second line is to give *EDGEMENU* the full pathname of a file which contains a list of the files to be backed up. Multiple filenames containing lists of files may be entered here. In fact, any combinations of individual files or Directories in the top line and pathnames of file lists in the bottom line may be combined. Filenames given **in a list file** should **not** use back slashes ‘\’ to escape spaces.

All filenames, *Directory* names, and lists should be typed in Absolute Pathname format. This is not the behavior that users of older versions of *Backup**EDGE*** might expect.

```
+ Files to include while processing archive ------------------------------+
|           Filenames Should Be In Absolute Format (e.g., /usr)            |
|                        Files / Directories to Include                    |
|  Type all desired pathnames, separated by spaces.  Window will scroll.   |
|[/usr /home /u/acct/george                                               ]|
|                                                                          |
|               List File for Includes (Include Full Path)                 |
|       This File Should Contain a List of Pathnames to Be Archived        |
|[                                                                        ]|
|                                                                          |
|                                                                          |
| [Ok]                                                        [Cancel]     |
+--------------------------------------------------------------------------+
```

The above example would select the listed three *Directories* for archiving.

```
+ Edgemenu for BackupEDGE ------------------------------------------------+
|+-------------------------------------------------------------------------+|
|| [File] [Backup] [Restore] [Verify] [Admin] [Setup] [Schedule]           ||
|+-------------------------------------------------------------------------+|
|- Backup Multiple Files / Dirs ---------------------------------------------|
| [2] Verify Type (Bit-Level)                    Record Locking            |
| [X] Index During Verify                        (X) Don't Lock Files      |
| [0 Days] Backup Retention Time                 ( ) Unenforced Read       |
| [X] Data-Level Checksum                        ( ) Enforced Read         |
| [ ] Include Raw Devices                                                  |
|                                                                          |
| [ ] Use /etc/edge.encrypt                                                |
|                                                                          |
|                                                                          |
| Backup Dir:  [/                                                        ] |
| [Execute Backup]  [Modify Excludes]                  [Cancel]            |
|+-------------------------------------------------------------------------+|
|Primary Resource : web2v:url!url0                                         ||
||  Compress: None, HW Block:  N/A, Edge Block:   64, Partition: C          ||
||                                                                          ||
||                                                                          ||
||                                                                          ||
||Last Master Backup: Tuesday Sep 10 22:00:01 2019                         ||
|+Local Machine: web2v.microlite.com  Administering: web2v.microlite.com -----+|
+-------------------------------------------------------------------------+
```

The execute options are similar to those in *Master Backup*, except that you may use the `[Modify Includes]` button to return to the `Files to include` screen.

If you are not concerned with the inner workings of *Backup**EDGE***, then you only need to know that during a restore operation with *Selective Restore* or *Restore Entire Archive*, everything will be restored (by default) to wherever it was found originally. If you enter specific files to restore, you should enter them in absolute format just as when you back them up.

For those who are familiar with older versions of *Backup**EDGE***, read on to see more about the differences in *Backup**EDGE*** 01.02.00 and later.

EDGEMENU will choose the *Root Directory* for this backup appropriately based on which file(s) you want to back up. For example, if you choose to back up `/usr/lib` and `/usr/bin`, *EDGEMENU* may choose to make the *Root Directory* `/usr`, and back up `./lib` and `./bin`. This allows for more flexibility during a restore. Also note that during a restore operation (except *Expert Restore*), *EDGEMENU* will mask these decisions so that you can ask for `/usr/bin/vi` without worrying about how it was stored in the archive. This eliminates a very common cause of confusion during a restore. Further, you will be given the option to restore it to its original location or to move it elsewhere.

Operations are logged in `/usr/lib/edge/lists/menu`. The logs are stored in files are called `backup_dirs.log`, `verify_dirs.log`, and `changedfiles_dirs.log`.

See “Backup Parameters” on page 241 for information about each option.

Expert Backup

Expert Backup looks very similar to the *Backup Multiple Files* option, but in fact is ***very*** different. There are no reasons why this option would be used, except for troubleshooting purposes.

When specifying files with *Expert Backup*, you are actually controlling how they will be named in the archive. If you use *Relative Pathnames*, the archive will use *Relative Pathname*s for those files. If you use *Absolute Pathnames*, so will the archive. If you mix and match *Relative Pathnames* and *Absolute Pathnames*, the archive will reflect this also.

You will also be given the opportunity to select the *Root Directory* for the backup. Any relative file or *Directory* names to be included on the first line will be relative to that *Directory*. Filenames given on the second line should be specified as *Absolute Pathnames*, although the files listed in those files will be treated exactly as if you had typed them in on the top line manually.

The *Backup Multiple Files* option is preferable to this method.

Operations are logged in `/usr/lib/edge/lists/menu`. These logs are stored in files named `backup_expert.log`, `verify_expert.log`, and `changedfiles_expert.log`.

Backup Parameters

Many of the *Backup Parameters* for *Unscheduled Full Backup, Backup Single Dir, Backup Multiple Files* and *Expert Backup* may be modified. The defaults tend to backup all selected files exactly as expected. *Backup Parameters* may change these actions in the following ways...

Verify Type

The default *Verify Type* is [**2**], which is *Level 2 Verify*, or *Bit-Level Verify*. After the backup, a read pass is made through the media and each file is compared against the actual file on the hard drive. This is the most accurate verify type.

You may also select [**1**] which is a *Level 1 Verify*, or *Checksum Verify*. This read pass through the tape simply checksums the file headers and guarantees that the media itself is readable. It is faster, but not as accurate, as a *Level 2 Verify*.

You may select [**0**] or *No Verify* to omit a verify pass.

A *Level 2 Verify* is ***highly recommended*** for all backups.

Index During Verify

This option creates the *Index* used during *IFR* or *FFR* restores. The default is to create the *Index*. If no index is created, the archive will be restored at normal speed, and there will not be an option to browse the filenames present on the archive before a restore.

An archive may be indexed later if desired.

Backup Retention Time

The amount of time before *Backup**EDGE*** will erase or overwrite this backup. The default is `0 Days`, meaning it can be overwritten immediately.

Data-Level Checksum

This option enables a checksum of all file data on an archive. Normally, it should be checked.

Data-Level Checksums add an extra degree of protection against faulty media. If the data on the media changes after it is verified (perhaps due to physical damage), this option provides a way for *BackupEDGE* to detect this.

Include Raw Devices

If you have identified *Raw Filesystem Partitions* to be archived in their entirety by placing the *Device Node* pathnames in `/etc/edge.raw`, this flag (on by default) will tell *EDGEMENU* to archive the data within these nodes at the end of the archive using a special procedure.

If you are performing a backup that includes *Raw Filesystem Partitions*, it is ***strongly*** suggested that you use a *Scheduled Job* (even if it is run from *EDGEMENU* in attended mode) to do so.

Make Media Bootable

On systems with *RecoverEDGE Bootable Tape Disaster Recovery* available, this flag when checked will allow *EDGEMENU* to embed the *RecoverEDGE* bootable image at the start of the backup. It is also used to embed the image at the front of *Optical* and *SharpDrive Bootable Backups*.

There are specific advance procedures for making *Bootable Backups*. See “Making Bootable SharpDrive / Optical Drive Backups” on page 289 and “Making Bootable Tape Backups” on page 290 for more information.

Use /etc/edge.encrypt

If Encryption is enabled and configured, you may encrypt the archive by setting this flag. See “Encryption” on page 259.

Record Locking

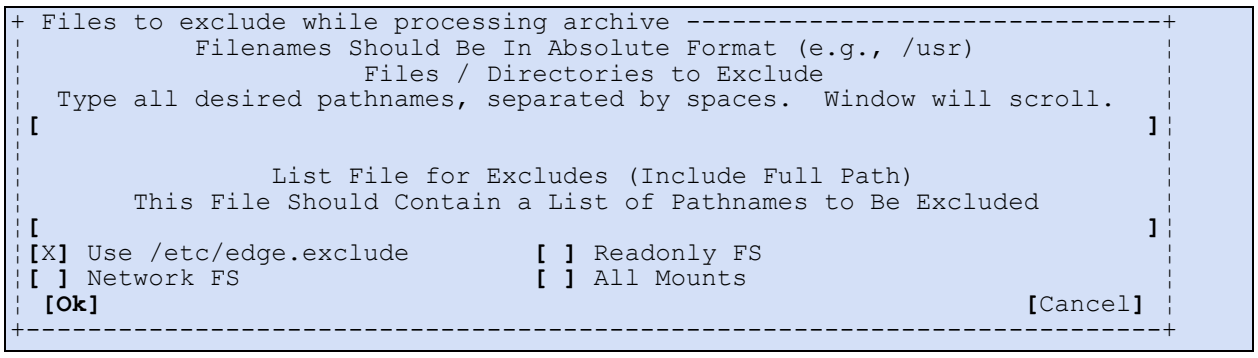
The three possible options are `Don't Lock Files`, `Unenforced Read`, and `Enforced Read`, and deal with the way *EDGEMENU* handles files in use or locked by another program.

Don't Lock Files makes no attempt to lock files, and waits if files are locked by another program. This is the default locking option for attended backups.

Unenforced Read places an advisory lock on each file while archiving it. It can archive files locked in this fashion by other programs, and files can be changed by applications while *EDGEMENU* uses this lock type.

Enforced Read placed a hard lock on files to be archived. This is not usually recommended, and may cause deadlocks during a backup.

Modify Excludes



This provides a high degree of flexibility in excluding specific files and *Directories* from being archived. Again, the first line is used to specify individual files and *Directories* to be excluded,

while the second line can be used to feed in an entire list. Further, you may check off boxes telling *EDGEMENU* to exclude the files listed in `/etc/edge.exclude`, plus exclude any files from *Read Only Filesystems*, *Network Filesystems*, or *All Mounted Filesystems*.

Modify Includes

On menus where the include files popup appears, this will return you to that menu to add additional files or *Directories*.

Run Scheduled

This option allows the user to start a *Scheduled Job* that has been previously defined. This gives the user the ability to start well defined tasks quickly, and is the most preferable method of performing system backups. You may select from any pre-defined *Scheduled Job* and have it start as an attended task. Operations are logged in the log *Directory* defined for that *Scheduled Job*. Notification is disabled when starting a *Scheduled Job* in this fashion. Instead, messages are

```
+Select Scheduled Job-------------------------------------------------------+
|                   Please select the Scheduled Job to run.                  |
|                                                                            |
|Machine:            web2v.microlite.com                                     |
|                                                                            |
|+--------------------------------------------------------------------------+|
||-> simple_job: Basic Schedule (Enabled, 23:00)                            ||
||   key_job: Unattended Backup Job (Disabled)                              ||
||   midday: Unattended Backup Job (Enabled, 12:01)                         ||
||   special: Unattended Backup Job (Enabled, 14:35)                        ||
|+--------------------------------------------------------------------------+|
|                                                                            |
|[Run]                                                          [Cancel]     |
+----------------------------------------------------------------------------+
```

displayed through *EDGEMENU*.

The default backup level for a backup run through this option is *Master Backup*. If other backup levels are available you will have a chance to select them.

For instance, if at least one valid *Master Backup* already exists for the *Sequence* to which this *Scheduled Job* contributes backups, you will be asked whether you wish to perform a *Master Backup* or a *Differential Backup*. If at least one *Master Backup* and *Differential Backup* exist, you will be asked whether you wish to perform a *Master Backup*, *Differential Backup*, or *Incremental Backup*.

If you are unfamiliar with *Sequences*, please consult “Anatomy of a BackupEDGE Backup” on page 40.

22.2 - Advanced File Restore

Restore Entire Archive

```
+Select Medium Segment-------------------------------------------------------+
|+-----------------------------------------------------------------------------+|
||   [1] (562 MB) 'web2v Microlite_Web_Site Edge.Nightly 03.00.00 Master 2018/||
||   [2] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Master 2019/09/05 13:53:0||
||   [3] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Master 2019/09/06 13:53:0||
||   [4] (196 MB) 'web2v system Edge.Nightly 03.00.00 Incremental(#1) 2019/09/||
||   [5] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Incremental(#1) 2019/09/0||
||   [6] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Master 2019/09/09 22:00:0||
||   [7] (57490 MB) 'web2v system Edge.Nightly 03.00.00 Master 2019/09/09 22:0||
||   [64] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Master 2019/09/10 13:53:||
||   [65] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Master 2019/09/10 22:00:||
||-> [66] (57495 MB) 'web2v system Edge.Nightly 03.00.00 Master 2019/09/10 22:||
||   [123] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Master 2019/09/11 13:53||
||                                                                             ||
||                                                                             ||
|+Total Space Used: 113.03GB---------------------------------------------------+|
|Sys: web2v.microlite.com               Dir: /                                  |
|Dom: system                            Job: simple_job_master                  |
|Slot: default                          Date: Tue Sep 10 22:00:01 2019          |
|Type: Edge.Nightly 03.00.00 Master     TTL: Fri Sep 13 20:55:01 2019           |
|                                                                               |
|[Next]                                                              [Cancel]|
+-------------------------------------------------------------------------------+
```

When choosing this option, the `Primary Resource` shown on the screen will be examined. If the medium has more than one archive, a list will be displayed and you'll get to choose one (the most recent of each *Domain* type will be at the bottom of the list). If there is only one archive, it will be selected and you'll be placed directly into the main restore menu.

```
+ Edgemenu for BackupEDGE ----------------------------------------------------+
|+-----------------------------------------------------------------------------+|
||-----------------[Restore]-------------------------------------------------||
|+-----------------------------------------------------------------------------+|
|- Restore Entire Archive -----------------------------------------------------|
| Restore Parameters                          Archive Label Info              |
| [Y] Destructive                 Edge.Nightly 03.00.00 Master                |
| [N] Strip Absolute Path         Domain:   Entire System                     |
| [N] Flat Restore                Sequence: On-Site Backups                   |
| [N] Restore If Newer            Date:     Tue Sep 10 22:00:01 2019          |
| [N] Use Xtrct mtime             System:   web2v.microlite.com               |
|                                 Medium Usage: 1                             |
|                                                                             |
| Original Dir: /                                                             |
| Restore To:  [/                                                          ]  |
| [Execute Restore]  [Modify Excludes]                    [Cancel]            |
|+-----------------------------------------------------------------------------+|
||Primary Resource : web2v:url!url0                                            ||
||  Compress: Soft, HW Block:  N/A, Edge Block:   64, Partition: C             ||
||                                                                             ||
||                                                                             ||
||                                                                             ||
||Last Master Backup: Tuesday Sep 10 22:00:01 2019                            ||
|+Local Machine: web2v.microlite.com  Administering: web2v.microlite.com -----+|
+-------------------------------------------------------------------------------+
```

This allows you to restore all the files on an archive. Before beginning the restore, *Backup**EDGE*** will read the label from the *Primary Resource* and display it in the above window. You may choose to modify the *Base Directory* of the restore from the original and create a list of files to exclude from the restore, as well as choose whether the restore is to be destructive or non-destructive.

The *Restore Parameters* shown above are available here, but are discussed more fully in "Restore Parameters" on page 248, as for most people a *Restore Entire Archive* means just that: "Restore

everything to wherever it was before." If the archive was made on a different system, the files will be restored locally.

Press [Execute Restore] to begin, or press [Tab] or [F10] to return to the top menu bar and select another option.

Selective Restore

There must be media in the the *Primary Resource* before choosing *Selective Restore*.

EDGEMENU will open the *Primary Resource* and read the media label. If more than one archive is available you'll get a chance to choose the one desired. If no media is in the *Primary Resource*, or if media insertion cannot be detected due to the *Resource Type* or *Interface*, *EDGEMENU* will prompt you to make sure media is inserted.

If a database exists for the archive, you'll be given two options for restoring files: a filename browser and a "type your filenames" screen.

```
+-----------------------------------------+
|A database has been found for this archive.|
|Would you like to browse it to select    |
|files, or just type the files to restore?|
|                                         |
|  (X) Browse the Database                |
|  ( ) Type Filenames                     |
|                                         |
|[Select]                  [Cancel Restore]|
+-----------------------------------------+
```

If you wish to use the browser, use **FastSelect** to choose Browse The Database.

Browser Interface - Blank

```
+ BackupEDGE Database Search ------------------------------------------------+
|Use F4 to Expand Matches, TAB to Navigate, Up/Down/Enter to Select          |
|Filespec:  [/                                                             ] |
|                                                                            |
|------------------------------------------------------------               |
|-> .Xauthority                                          [Add All Available] |
|   .Xd                                                  [Clear Selected]    |
|   .Xdefaults-mlite                                                         |
|   .Xdefaults-mlite-                                                        |
|   .Xdefaults-mliteifs-                                                     |
|   .bash_history                                                            |
|   .desked_pref                                                             |
|   .faxrc                                                                   |
|   .l123set                                        vv More vv               |
|- Files Selected for Restore ------------------------------------------------|
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|[Restore]                                                        [Cancel]   |
+----------------------------------------------------------------------------+
```

The browser has a very bash-like feel for completing filenames and pathnames, except that the [F4] key is used instead of the [Tab] key for completion matching.

Files in the *Current Directory* are shown in the Available window. As you type in a path on the Filespec: line, you'll see matches in the Available window updated automatically every time you press the / key, or anytime you press the [F4] key. Pressing [Enter] on a displayed path places it in the Files Selected For Restore window.

Use the up and down arrow keys to scroll through files listed in the Available window, pressing [Enter] to select them for restore.

Use the [Add All Available] button to select all files in the Available window.

Use the [Clear Selected] button to clear all files currently selected for restore.

Pressing [Enter] on a path in the Files Selected For Restore window deletes it from the selection.

Here is an example with some files and *Directories* selected for restore.

Browser Interface - Ready To Restore

```
+ BackupEDGE Database Search ---------------------------------------------------+
¦Use F4 to Expand Matches, TAB to Navigate, Up/Down/Enter to Select             ¦
¦Filespec:  [/usr/bin/p                                                       ]  ¦
¦                                                                              ¦
¦-/usr/bin----------------------------------------------------                 ¦
¦-> p                                                    ¦[Add All Available]  ¦
¦   pack                                                 ¦[Clear Selected]     ¦
¦   page                                                 ¦                     ¦
¦   paste                                                ¦                     ¦
¦   patch                                                ¦                     ¦
¦   pax                                                  ¦                     ¦
¦   pcat                                                 ¦                     ¦
¦   pcpio                                                ¦                     ¦
¦   pg                                         vv More vv ¦                     ¦
¦- Files Selected for Restore --------------------------------------------------¦
¦/etc/default/fppath                                                           ¦
¦/u/appl                                                                       ¦
¦/usr/bin/P                                                                    ¦
¦/usr/bin/p                                                                    ¦
¦                                                                              ¦
¦                                                                              ¦
¦[Restore]                                                          [Cancel]   ¦
+------------------------------------------------------------------------------+
```

When you've got everything selected properly, [Tab] down and press [Restore].

Browser Interface - Confirmation

```
+ Edgemenu for BackupEDGE ------------------------------------------------------+
¦+-------------------------------------------------------------------------------+¦
¦¦ [File] [Backup] [Restore] [Verify] [Admin] [Setup] [Schedule]                ¦¦
¦+-------------------------------------------------------------------------------+¦
¦- Restore Files Selectively ---------------------------------------------------¦
¦ Restore Parameters                          Archive Label Info                 ¦
¦ [Y] Destructive                 Edge.Nightly 03.00.00 Master                   ¦
¦ [N] Strip Absolute Path         Domain:   Entire System                        ¦
¦ [N] Flat Restore                Sequence: On-Site Backups                      ¦
¦ [N] Restore If Newer            Date:     Tue Sep 10 22:00:01 2019             ¦
¦ [N] Use Xtrct mtime             System:   web2v.microlite.com                  ¦
¦                                 Medium Usage: 1                              ¦
¦                                                                              ¦
¦ Original Dir: /                                                              ¦
¦ Restore To:  [/                                                           ]  ¦
¦ [Execute Restore]  [Modify Excludes]                    [Cancel]             ¦
¦+-------------------------------------------------------------------------------+¦
¦¦Primary Resource : web2v:url!url0                                            ¦¦
¦¦  Compress: Soft, HW Block:  N/A, Edge Block:   64, Partition: C             ¦¦
¦¦                                                                             ¦¦
¦¦                                                                             ¦¦
¦¦                                                                             ¦¦
¦¦Last Master Backup: Tuesday Sep 10 22:00:01 2019                             ¦¦
¦+Local Machine: web2v.microlite.com  Administering: web2v.microlite.com -----+¦
+------------------------------------------------------------------------------+
```

Before beginning the restore, *EDGEMENU* confirms the *Archive Label* and displays it in the above window. You may also choose to modify any of the *Restore Parameters* shown above. These are discussed more fully in "Restore Parameters" on page 248.

Press `[Execute Restore]` to begin, or press `[Tab]` or `[F10]` to return to the top menu bar and select another option.

EDGEMENU will automatically use *FFR* or *IFR* if they are available for your media.

You may not use this restore method for *Expert Mode* backups, or for backups that were made with versions of *Backup**EDGE*** prior to 01.02.00.

Type Pathnames Interface - Blank

```
+ Files to include while processing archive ------------------------------+
|           Filenames Should Be In Absolute Format (e.g., /usr)            |
|                       Files / Directories to Include                     |
|  Type all desired pathnames, separated by spaces.  Window will scroll.   |
|[                                                                        ]|
|                                                                          |
|               List File for Includes (Include Full Path)                 |
|       This File Should Contain a List of Pathnames to Be Restored        |
|[                                                                        ]|
|                                                                          |
|                                                                          |
| [Ok]                                                      [Cancel]       |
+--------------------------------------------------------------------------+
```

The non-browser interface will present you with two text lines that are very similar to the *Backup Multiple Files* option in the *Backup* drop down menu.

The first (top) line is for the entry of individual files or *Directories* to be restored. Files and *Directories* are separated by spaces. If you wish to specify a filename that contains a space, precede the space with a backslash '\'. Otherwise, EDGEMENU will treat it as two separate filenames! If a filename contains a backslash, represent it with two back slashes: '\\'.

The second line is to give *EDGEMENU* the full pathname of a file which contains a list of the files to be restored. Multiple filenames containing lists of files maybe entered here. In fact, any combinations of individual files or *Directories* in the top line and pathnames of file lists in the bottom line may be combined. Filenames given **in a list file** should **not** use back slashes '\' to escape spaces.

Type Pathnames Interface - Ready To Restore

```
+ Files to include while processing archive ------------------------------+
|           Filenames Should Be In Absolute Format (e.g., /usr)            |
|                       Files / Directories to Include                     |
|  Type all desired pathnames, separated by spaces.  Window will scroll.   |
|[/etc/default/fppath /u/appl /usr/bin/P /usr/bin/Q                       ]|
|                                                                          |
|               List File for Includes (Include Full Path)                 |
|       This File Should Contain a List of Pathnames to Be Restored        |
|[                                                                        ]|
|                                                                          |
|                                                                          |
| [Ok]                                                      [Cancel]       |
+--------------------------------------------------------------------------+
```

All filenames, *Directory* names, and lists should be typed in *Absolute Pathname* format. For those familiar with *Backup**EDGE*** 01.01.0x and earlier, this behavior has changed.

Restore Files Selectively - Confirmation

```
+ Edgemenu for BackupEDGE ------------------------------------------------------+
¦+-------------------------------------------------------------------------------+¦
¦¦ [File] [Backup] [Restore] [Verify] [Admin] [Setup] [Schedule]                ¦¦
¦+-------------------------------------------------------------------------------+¦
¦- Restore Files Selectively ---------------------------------------------------¦
| Restore Parameters                          Archive Label Info                |
| [Y] Destructive                 Edge.Nightly 03.00.00 Master                  |
| [N] Strip Absolute Path         Domain:   Entire System                       |
| [N] Flat Restore                Sequence: On-Site Backups                     |
| [N] Restore If Newer            Date:     Tue Sep 10 22:00:01 2019            |
| [N] Use Xtrct mtime             System:   web2v.microlite.com                 |
|                                 Medium Usage: 1                               |
|                                                                               |
| Original Dir: /                                                               |
| Restore To:  [/                                                             ] |
| [Execute Restore]  [Modify Excludes]                      [Cancel]            |
|+-----------------------------------------------------------------------------+|
||Primary Resource : web2v:url!url0                                            ||
||  Compress: Soft, HW Block:  N/A, Edge Block:   64, Partition: C             ||
||                                                                             ||
||                                                                             ||
||                                                                             ||
||Last Master Backup: Tuesday Sep 10 22:00:01 2019                             ||
|+Local Machine: web2v.microlite.com  Administering: web2v.microlite.com -----+|
+-------------------------------------------------------------------------------+
```

Before beginning the restore, *EDGEMENU* confirms the *Archive Label* and displays it in the above window. You may also choose to modify any of the *Restore Parameters* shown above. These are discussed more fully in “Restore Parameters” on page 248.

Press `[Execute Restore]` to begin, or press `[Tab]` or `[F10]` to return to the top menu bar and select another option.

EDGEMENU will automatically use *FFR* or *IFR* if they are available for your media.

You may not use this restore method for *Expert Mode* backups, or for backups that were made with versions of *Backup**EDGE*** prior to 01.02.00.

Expert Restore

If you have backups from older versions of *Backup**EDGE*** (01.01.0x and earlier), backups done in *Expert Mode*, or backups made by non-*Backup**EDGE*** applications such as *tar*, you must restore them using *Expert Mode*. In this mode, you must specify the file(s) to restore **exactly** as they appear on tape. This was the default mode for versions of *Backup**EDGE*** prior to 01.02.00. You may use *Expert Restore* for non-Expert tapes (such as are made by `Backup -> Backup Multiple Files`), but there is very little reason to do so.

This option is typically used to restore from *Legacy Backups*. Its user interface is the same as the non-browser interface in *Selective Restore* above, except that **you must use the same absolute or relative pathname format that appears on the archive during a listing!**

Operations are logged in `/usr/lib/edge/lists/menu`.

It is recommended that you use *Selective Restore* whenever it is an option.

Restore Parameters

Many of the *Restore Parameters* for *Restore Entire Archive*, *Selective Restore* and *Expert Restore* may be modified. The defaults tend to restore all selected files exactly as they were. *Restore Parameters* may change these actions in the following ways...

Destructive

The default is [**Y**]es, perform a *Destructive Restore*. All files restored will over-write any files encountered with the same pathname. If [**N**]o is selected, any files which currently exist on the hard drives will not be overwritten.

Strip Absolute Path

This option is slightly mis-named. The default is [**N**]o. If this flag is set to [**Y**]es, the first character of each pathname encountered is removed before the restore is attempted. This flag was designed to allow files with *Absolute Pathnames* to be restored relative to the current *Working Directory*. In actual practice this flag is superseded by *EDGEMENU* and its ability to place restored files regardless of the way the pathnames are stored on the archive. It should only be used with *Expert Restore* to restore *Legacy Backups* or backups made with *tar* or other *tar* compliant archiving programs that actually have *Absolute Paths* on the archive.

Flat Restore

The *Flat Restore*, or *Flat File Restore* option, allows an entire pathname to be removed during a restore. This can be used to restore files with one pathname into a totally unrelated *Directory*. For instance, suppose you wanted the following three files to be restored, but instead of going back into the `/u/acct/tom` *Directory*, you wanted them restored to the `/tmp` *Directory*...

```
/u/acct/tom/backupedge_chapter1.fm
/u/acct/tom/backupedge_chapter2.fm
/u/acct/tom/backupedge_chapter3.fm
```

If you select these three files during *Selective Restore*, then change the `Restore To:` *Directory* from `/` to `/tmp`, the default behavior would be to restore the files as...

```
/tmp/u/acct/tom/backupedge_chapter1.fm
/tmp/u/acct/tom/backupedge_chapter2.fm
/tmp/u/acct/tom/backupedge_chapter3.fm
```

But if you changed the `Restore To:` *Directory* to `/tmp` and set `Flat Restore` to [**Y**]es, the files would be restored as:

```
/tmp/backupedge_chapter1.fm
/tmp/backupedge_chapter2.fm
/tmp/backupedge_chapter3.fm
```

However, if the `Restore To:` *Directory* were initially `/u/acct/tom` instead of `/` (as might happen if the archive was not a complete system backup, but instead just a backup of the `/u/acct/tom` *Directory*), you would not need `Flat Restore` to move these to `/tmp`. If you set it, it would have no noticeable effect, as files were stored relative to `/u/acct/tom` anyway.

Restore if Newer

If this flag is set to [**Y**]es and *EDGEMENU* encounters a file during a restore that already exists, it will be replaced only if the archived file is newer than the existing file. This is most useful for restoring multiple level backups.

Use Xtrct mtime

When using `Restore If Newer`, this will switch the date comparison used to the system `mtime` instead of the `atime`.

Modify Excludes

```
+ Files to exclude while processing archive ------------------------------+
|           Filenames Should Be In Absolute Format (e.g., /usr)            |
|                      Files / Directories to Exclude                      |
|  Type all desired pathnames, separated by spaces.  Window will scroll.   |
|[                                                                        ]|
|                                                                          |
|                List File for Excludes (Include Full Path)                |
|       This File Should Contain a List of Pathnames to Be Excluded        |
|[                                                                        ]|
|[X] Use /etc/edge.exclude        [ ] Readonly FS                          |
|[ ] Network FS                   [ ] All Mounts                           |
| [Ok]                                                        [Cancel]     |
+--------------------------------------------------------------------------+
```

This provides a high degree of flexibility in excluding specific files and *Directories* from being restored. Again, the first line is used to specify individual individual files and *Directories* to be excluded, while the second line can be used to feed in an entire list. Further, you may check off boxes telling *EDGEMENU* to exclude the files listed in `/etc/edge.exclude`, plus exclude any files from *Read Only Filesystems*, *Network Filesystems*, or *Any Mounted Filesystems*.

Modify Includes

On menus where the include files popup appears, this will return you to that menu to add additional files or *Directories*. Refer to the particular type of restore for how to interpret these.

22.3 - Restoring from Multiple Archive Backups

Whenever a restore is selected from an *s3cloud*, *FSP* or a *URL Resource*, or from a writable medium (tape, optical, SharpDrive) containing more than one archive, a list of all of the available archives on the *Resource* is displayed.

```
+Select Medium Segment---------------------------------------------------------+
|+-------------------------------------------------------------------------------+|
||-> [1] (562 MB) 'web2v Microlite_Web_Site Edge.Nightly 03.00.00 Master 2018/||
||   [2] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Master 2019/09/05 13:53:0||
||   [3] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Master 2019/09/06 13:53:0||
||   [4] (196 MB) 'web2v system Edge.Nightly 03.00.00 Incremental(#1) 2019/09/||
||   [5] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Incremental(#1) 2019/09/0||
||   [6] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Master 2019/09/09 22:00:0||
||   [7] (57490 MB) 'web2v system Edge.Nightly 03.00.00 Master 2019/09/09 22:0||
||   [64] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Master 2019/09/10 13:53:||
||   [65] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Master 2019/09/10 22:00:||
||   [66] (57495 MB) 'web2v system Edge.Nightly 03.00.00 Master 2019/09/10 22:||
||   [123] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Master 2019/09/11 13:53||
||                                                                             ||
||                                                                             ||
|+Total Space Used: 113.03GB-----------------------------------------------------+|
|Sys: web2v.microlite.com              Dir: /home                              |
|Dom: Microlite_Web_Site               Job: WebSiteBackups_master              |
|Slot: default                         Date: Mon Dec 31 13:51:01 2018          |
|Type: Edge.Nightly 03.00.00 Master    TTL: (Delete Manually)                  |
|                                                                              |
|[Next]                                                          [Cancel]      |
+------------------------------------------------------------------------------+
```

Choose one archive to continue (the most recent will be at the bottom of the list).

22.4 - Autochanger Media Manipulation

From *EDGEMENU*, you may move media around within any *Element* supported by an autochanger.

There are four types of *Elements* within an autochanger...

- `dt element`. These are the "*Data Transfer*" elements, a fancy name for *Tape Devices*.
- `st element`. These are the *Storage Elements*, or *Cartridge Slots*.
- `ie element`. These are the *Import/Export Elements* in larger libraries, and are used for inserting and removing tapes from the library without having to open the door.
- `mt element`. This is the *Medium Transport Element*, or robotic arm, used to move tapes around in really large libraries. Although supported by *Backup**EDGE***, in practice you can move tapes between any of the other elements without having to transfer them through an *mt* element.

Elements are numbered from `0`. For instance, the first *Tape Device* would be `st0`, the second, `st1`, etc.

From *EDGEMENU*, select `Admin -> Changer Control`. This will allow manipulation of the autochanger associated with your current *Primary Resource*.

Autochanger Control Menu - Full Element Select

```
+ Autochanger Control Screen ------------------------------------------------+
| Machine     :  web2v                                                       |
| Resource    :  changer0                                                    |
| Description:  DELL PV-124T 0070                                            |
|                                                                            |
| Elements Detected:                                                         |
|                                                                            |
|  Import/Export (ie)    : 0                                                 |
|  Data Transfer (dt)    : 1                                                 |
|  Media Transport (mt) : 1              Move media from :  None selected    |
|  Storage (st)          : 16            Move media to   :  None selected    |
|                                                                            |
|+ Full Elements --------------------+                                       |
||-> st0:barcode:000601L3             |                                      |
||   st1:barcode:000602L3             |                                      |
||   st2:barcode:000603L3             |                                      |
||   st3:barcode:000604L3             |                                      |
||   st4:barcode:000605L3             |                                      |
||   st5:barcode:000606L3             |                                      |
||   st6:barcode:000607L3             |                                      |
|+-------------------------vv More vv-+                                       |
|                                                                            |
|        [Eject]  [Change Device]  [Rescan Device]  [Done]                   |
+----------------------------------------------------------------------------+
```

When *Autochanger Control Screen* appears, *Backup**EDGE*** has polled the device for all *Element* types and their contents. Any *Element* with a tape is displayed in the `Full Elements` window as shown above. **FastSelect** a *Storage Element* and an `Empty Elements` window will appear.

Autochanger Control Menu - Empty Element Select

```
+ Autochanger Control Screen ---------------------------------------------------+
| Machine    :  web2v                                                           |
| Resource   :  changer0                                                        |
| Description:  DELL PV-124T 0070                                               |
|                                                                               |
| Elements Detected:                                                            |
|                                                                               |
|  Import/Export (ie)   : 0                                                     |
|  Data Transfer (dt)   : 1                                                     |
|  Media Transport (mt) : 1              Move media from :  st0                 |
|  Storage (st)         : 16             Move media to   :  None selected       |
|                                                                               |
|+ Full Elements --------------------+    + Empty Elements --------------------+|
||   st0:barcode:000601L3            |    |-> dt0                              ||
||   st1:barcode:000602L3            |    |   MT0                              ||
||   st2:barcode:000603L3            |    |                                    ||
||   st3:barcode:000604L3            |    |                                    ||
||   st4:barcode:000605L3            |    |                                    ||
||   st5:barcode:000606L3            |    |                                    ||
||   st6:barcode:000607L3            |    |                                    ||
|+------------------------vv More vv-+    +------------------------------------+|
|                                                                               |
|        [Eject]  [Change Device]  [Rescan Device]  [Done]                      |
+-------------------------------------------------------------------------------+
```

FastSelect a destination *Element*. When you've done this, the bottom line will get a `[Move]` entry.

```
|[Move]  [Eject]  [Change Device]  [Rescan Device]  [Done]                      |
```

Select `[Move]` to move the tape. When the operation is complete, the `Full Elements` window will update. Any full `dt` *Elements* will display the source *Element* of the current tape

Autochanger Control Screen - After Move

```
+ Autochanger Control Screen ---------------------------------------------------+
| Machine    :  web2v                                                           |
| Resource   :  changer0                                                        |
| Description:  DELL PV-124T 0070                                               |
|                                                                               |
| Elements Detected:                                                            |
|                                                                               |
|  Import/Export (ie)   : 0                                                     |
|  Data Transfer (dt)   : 1                                                     |
|  Media Transport (mt) : 1              Move media from :  None selected       |
|  Storage (st)         : 16             Move media to   :  None selected       |
|                                                                               |
|+ Full Elements --------------------+                                         |
||   dt0:medium from:st0             |                                         |
||   st1:barcode:000602L3            |                                         |
||   st2:barcode:000603L3            |                                         |
||   st3:barcode:000604L3            |                                         |
||   st4:barcode:000605L3            |                                         |
||   st5:barcode:000606L3            |                                         |
||   st6:barcode:000607L3            |                                         |
|+------------------------vv More vv-+                                         |
|                                                                               |
|        [Eject]  [Change Device]  [Rescan Device]  [Done]                      |
+-------------------------------------------------------------------------------+
```

Select `[Done]` when you are finished moving media. (This is the default cursor position after a successful `[Move]`.)

Other options available from this screen are:

`[Eject]`
This will eject the entire *Medium Cartridge* in devices that are so equipped (on the Dell 124T shown both of the eight tape cartridges will be ejected).

`[Change Device]`
This will provide a **FastSelect** screen to yet you manipulate a different autochanger.

`[Rescan Device]`
This will throw out all cached data and check all Elements again. It is most useful if someone has manually manipulated the elements since you first started the *Changer Control Screen*.

22.5 - Deleting Backups

When using URL, S3CLOUD and FTP backups, space is automatically recovered by *Backup**EDGE***. That is, archives are erased if:

- there are expired archives
- it is necessary to delete one or more archives to get under the *Resource Quota*.

It is sometimes necessary to remove backups from the medium manually. For instance, if you have set one ore more archives *Retention Time* to `Forever`, and you no longer need the archive.

Using `edgemenu:Admin->Delete Archives` lets you view the archives on the current medium, and optionally delete one. The segment list will be the same as the one in the previous section, but a `[Delete]` option will be available. Point to the archive to be removed and press `[Delete]`.

Note that it does not work for all media types. Note that below the list of archives, the total amount of space used on the medium is displayed.

Deleting Multiple Backups at Once

On the `edgemenu:Admin->Delete Archives` screen, it is possible to delete multiple archives at one. Simply press the space bar while pointing to each archive to be deleted. When `[Delete]` is pressed, all of the selected archives will be erased.

```
+Select Archive(s) to Delete from url0----------------------------------------+
|+-------------------------------------------------------------------------+|
||   *[1] (562 MB) 'web2v Microlite_Web_Site Edge.Nightly 03.00.00 Master 2018||
||   *[2] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Master 2019/09/05 13:53:||
||-> *[3] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Master 2019/09/06 13:53:||
||    [4] (196 MB) 'web2v system Edge.Nightly 03.00.00 Incremental(#1) 2019/09||
||    [5] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Incremental(#1) 2019/09/||
||    [6] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Master 2019/09/09 22:00:||
||    [7] (57490 MB) 'web2v system Edge.Nightly 03.00.00 Master 2019/09/09 22:||
||    [64] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Master 2019/09/10 13:53||
||    [65] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Master 2019/09/10 22:00||
||    [66] (57495 MB) 'web2v system Edge.Nightly 03.00.00 Master 2019/09/10 22||
||    [123] (224 KB) 'web2v mysql Edge.Nightly 03.00.00 Master 2019/09/11 13:5||
||                                                                           ||
||                                                                           ||
|+Total Space Used: 113.03GB---------------------------------------------------+|
|Sys: web2v.microlite.com               Dir: /                               |
|Dom: mysql                             Job: mysql_master                    |
|Slot: default                          Date: Fri Sep  6 13:53:01 2019       |
|Type: Edge.Nightly 03.00.00 Master     TTL: Fri Sep 13 12:48:01 2019        |
|                                                                            |
|[Delete]                                                          [Cancel]|
+----------------------------------------------------------------------------+
```

What is the different between 'Delete Archives' and 'Initialize Medium'?

Delete Archives is lets you manage individual archives on a medium. Some media types allow you do this, while others do not. Trying to use the *Delete Archives* option will produce an error.

Initialize Medium does not deal with individual archives. Instead, it is used to initialize an entire medium for use with *Backup**EDGE***. For some media types this requires erasing everything on

the medium. For other media types (URL / FSP / S3CLOUD), this is always done non-destructively. In these instances...

If the *URL* / *FSP* / *S3CLOUD Resource* has no data, `Initialize Medium` will place a control file in the specified folder / directory.

If the *URL* / *FSP* / *S3CLOUD Resource* contains data, `Initialize Medium` will scan all of the archives, recalculate amount of space used, and update the control file.

23 - Software Compression and Performance

When dealing with non-tape backups, including those to *optical*, *URL*, *S3CLOUD* and *FSP Resources*, software compression settings can dramatically affect the space needed and the time taken for a backup. While it is not easy to demonstrate all of the possible permutations, we can demonstrate the benefits of tuning *Backup**EDGE*** to your environment.

Let's look at the FTP three backups, which were performed on the Microlite LAN from an Linux Virtual Machine to a Synology NAS...

```
->  [1] (17724 MB) 'pc19 system Edge.Nightly 03.00.00 Master 2019/09/10 12:32
    [19] (7633 MB) 'pc19 system Edge.Nightly 03.00.00 Master 2019/09/10 12:52
    [27] (7174 MB) 'pc19 system Edge.Nightly 03.00.00 Master 2019/09/10 13:07
```

These are three successive *Master Backups*, with the first being at compression level 1, the second at compression level 5 (our default) and the third with no compression. What we're looking at is the amount of time the backup + verify takes verses the actual space used.

Here are the backup and verify statistics.

Backup	Compression Level 1	Compression Level 5	Compression Off
Files Encountered	192059	192059	192059
Total Data	17.14GB	17.14GB	17.14GB
Total Written	7.43GB	6.98GB	17.26GB
Elapsed Time	00:06:20	00:10:03	00:06:40
Data Transfer Speed	73.537 GB/hr 1255.179 MB/min 21935851 bytes/sec	42.760 GB/hr 729.855 MB/min 12755149 bytes/sec	170.768 GB/hr 2914.513 MB/min 20934823 bytes/sec
Relative Speed	169.547 GB/hr 2893.754 MB/min 50572027 bytes/sec	104.940 GB/hr 1791.070 MB/min 31301225 bytes/sec	
Software Compression	59%	62%	
Verify	**Compression Level 1**	**Compression Level 5**	**Compression Off**
Data Read	7.45GB	7.00GB	17.30GB
Elapsed Time	00:03:43	00:03:31	00:05:46
Data Transfer Speed	127.644 GB/hr 2178.694 MB/min 38075440 bytes/sec	120.123 GB/hr 2050.104 MB/min 35828177 bytes/sec	183.202 GB/hr 3126.782 MB/min 54644401 bytes/sec
Files Encountered	192059	192059	192059
Net Backup/Verify/Index Time	00:10:03	00:13:33	00:12:26

The relevant parts of the statistics can be interpreted in the following manner...

- With compression Off, the backup/verify took a total of 12 minutes 26 seconds and consumed 17.26GB of disk space.
- With default (level 5) compression, the backup/verify took about a minute longer, at 13 minutes and 33 seconds. BUT, it used only 6.98GB of disk space, or 40.72% of the space of the uncompressed backup.
- With compression level 1, the backup/verify was very fast, taking only 10 minutes and 03 seconds, but consumed 0.45GB more disk space (7.43GB) than the backup with level 5 compression. This is still only 43.3% of the space of the uncompressed backup.

When protecting servers by sending data over high speed links over a local LAN, a lower compression ratio will generally provide higher speeds at quite useful compression levels. However when going over a lower speed link, higher compression levels may provide better results as they reduce the actual amount of data that has to be transmitted over the more limited bandwidth of the slower link.

There are 9 possible settings for *Backup**EDGE*** compression. While the default of 5 provides excellent average results, tuning it can provide significant benefits in performance at the expense of some amount of space.

To tune compression, simply call up the appropriate storage Resource under EDGEMENU -> Admin -> Define Resources and change Level to a number from 1 to 9. Compression must be set to [S]oftware for this field to appear. Do a backup after changing the level and note the combined (backup + verify) time. Use the time verses space setting that makes the most sense in your environment.

24 - Network Backups - BackupEDGE to BackupEDGE

Two or more copies of *BackupEDGE* can communicate seamlessly on properly configured systems. Any system can make backups or manipulate *Devices* on any other system equipped with the same version of *BackupEDGE*.

This section does not apply to URL backups, since those are backups from a machine with *BackupEDGE* installed to an FTP server. It is not a backup between two *BackupEDGE* installations, even if *BackupEDGE* happens to be installed on the machine running the FTP server too. In particular, using the *Secure Shell* for the network transport does not affect FTP backups in any way; use the Secure FTP protocol in the *Resource Manager* instead.

During initial installation, if the *Secure Shell* was detected, you were asked whether you wished to use the *Secure Shell* or the *Remote Shell* as the communications transport for *Network Backups*.

Remember, for *Network Backups* to work, the following must be true...

- A system somewhere on the network must exist that has a storage *Device* and the same release of *BackupEDGE* installed. Let's call this system `tapehost`.
- The system to be backed up must also have a copy of *BackupEDGE* installed. Let's call this system `myhost`.
- Remote communications with `root` peer (sometimes called *Trusted Host*) permissions must be set up such that `myhost` can execute commands on `tapehost`. For instance...

```
rcmd tapehost ls
rsh tapehost ls
ssh tapehost ls
```

- These commands must be executable without prompting for a password.
- It is not necessary for `tapehost` to be able to execute commands on `myhost`.

Remote Resources get the same treatment as local *Resources*. That is, *BackupEDGE* can check for media availability and write protect status, adjust *Tape Block Size* and compression as necessary, check *TapeAlert* status, and even even insert cartridges if the *Resource* is in an *Autochanger*.

NOTE: It is not possible to associate a tape drive (etc.) *Resource* on one machine with a *Data Transfer Element* of an autochanger *Resource* on another.

During *Restore*, *IFR* and *FFR* also work across the network, with only the files to be restored using any network bandwidth.

Selecting a Remote Resource

Selecting a *Remote Resource* is virtually identical to selecting a local *Resource*. From *EDGEMENU*, select `Admin -> Set Default Backup Resource`.

```
+ Select Primary Device ------------------------------------------------------+
|You are selecting the Destination Resource(s) to use for this Backup / Verify.|
|  This will be the Primary Resource used.                                     |
|                                                                              |
|+ Resource List -------+                                                     |
||   tape0               | Resource :   tape1                                  |
||-> tape1               |              HP C5713A H910                         |
||   cdrom0              | Machine :    [show1.microlite.com                 ] |
||   [NEW]               |                                                     |
||                       | To select a different resource, use the Up / Down   |
||                       | arrow keys while the Next button is highlighted.  To|
||                       | view resources on a different machine, press the TAB|
||                       | key and type the system name in the "Machine" field,|
||                       | and press ENTER.                                    |
|+----------------------+                                                     |
|                                                                              |
|[Next]                              [Prev]                          [Cancel]|
+------------------------------------------------------------------------------+
```

Instead of using **FastSelect** to select a *Resource*, press `[Tab]` to get to the `Machine:` prompt and type in the proper *System Name*. The `Resource List` above will display *Remote Resources* in this instance. Then, using **FastSelect** from the `[Next]` button, highlight the appropriate *Resource* and press `[Enter]`.

*Recover**EDGE*** for *UW7* and *Linux* may use *ssh* or *rsh* as defined here for restoring from remote tape drives. *Recover**EDGE*** for *OSR5* will always be configured to use *rcmd*.

NOTE: Remote access **into** a system booted from *Recover**EDGE*** media is always done using the *telnet* protocol.

The user can switch Network Transports at any time by logging in as `root` and executing the following command...

```
/usr/lib/edge/bin/edge.install -network
```

This will re-run only the *Remote Transport Selection* section of the *Installation Manager*.

25 - Encryption

25.1 - Overview

*Backup**EDGE*** incorporates data encryption to allow the safe storage and transport of information. The goal of this chapter is to familiarize the reader with how *Backup**EDGE*** can be used toward this end, and to provide information about common mistakes and pitfalls inherent in data security.

NOTE: *Backup**EDGE*** requires a separate serial number and activation code in order to enable encryption of archive data. This serial number and activation code are in addition to the ones used for the base product. Although encryption is available while the product is in demo mode, once the demo period expires or the base product is activated permanently without an encryption serial number and activation code, then encryption will be disabled.

*Backup**EDGE*** allows for a list of files, directories, and/or patterns to be encrypted. While it is possible to encrypt all files in a backup, normally this is not necessary. System files, and other non-sensitive data, can be stored normally on the backup media. Only those files which represent sensitive information need to be encrypted. For much of this chapter, “encrypted backup” or “encrypted archive” will be used to talk about an archive that has one or more encrypted files, even if not all the files are encrypted.

Encryption algorithms use what are called “keys” to control the encryption and decryption of data. When one wants to encrypt data, one gives that data to the encryption algorithm, along with the “encryption key”. The output of the algorithm is the encrypted data. Similarly, to decrypt the data, one provides the encrypted data along with the correct “decryption key” to the decryption algorithm to recover the original, unencrypted data.

In some types of encryption algorithms, which are known as “symmetric ciphers”, the encryption and decryption keys are identical. In other words, if one has the power (key) to encrypt data with a symmetric cipher, one also has the power (key) to decrypt it, and vice-versa. It is from this symmetry that this class of cipher gets its name.

There is another class of ciphers, known as “asymmetric ciphers”, in which two different keys are employed. Whatever is encrypted with one key cannot be decrypted by that same key. Rather, the other key must be used to decrypt it. This is a very important point to remember: in an asymmetric cipher, it is possible to encrypt a message without also having the ability to decrypt it, if only one key is known. Clearly, asymmetric ciphers can do something that symmetric ciphers alone cannot.

It may be helpful to think of an asymmetric cipher as two rooms connected by a mail slot. Messages may be dropped into the slot, but cannot be recovered except by those in the other room. For backups, this idea is very powerful: it is helpful to be able to create an encrypted backup without necessarily being able to read it. For example, using this method, several systems can share a key without risk of the decryption key being discovered due to a mistake at any one of them.

Further, it is helpful to label one of the keys in an asymmetric cipher as the encryption key, and the other as the decryption key, even though both can be used in either context. For the purposes of *Backup**EDGE***, one key will be used only to encrypt data, while the other is used only to decrypt it. These keys, taken together, are referred to as a “key pair”.

*Backup**EDGE** Encryption* is based on two separate encryption algorithms. One of these is the *Advanced Encryption Standard* (*AES*), an encryption system developed with an open, peer-reviewed process sponsored by the *National Institute of Standards and Technology* (*NIST*). The details of the algorithm are freely available, along with many reference implementations.

AES is called a “symmetric cipher”, because the encryption key and the decryption key are identical.

*Backup**EDGE*** also uses the well-known asymmetric RSA algorithm as part of its encryption strategy. Like AES, its design and implementation details are easily obtained. However, unlike AES, it uses a different key for encryption than it does for decryption.

The security of *Backup**EDGE** Encryption* is not found in the secrecy of its implementation; this information is available to all. Indeed, it is largely because of the peer-review process that AES and RSA are considered to be “secure”. For more information on AES, visit the NIST website at *www.nist.gov*. For more information about how AES has been applied to *Backup**EDGE***, please consult the Technical Reference Manual.

One might ask, “How does a freely available algorithm, applied to data in a known way, allow for any extra measure of security for that data?”

The answer is, “It is not the algorithm that must be kept secret in order to maintain security.” Instead, during the encryption setup procedure, *Backup**EDGE*** creates unique encryption and decryption keys for RSA. The decryption key is exactly the information that must be kept secret. Because the key is generated randomly during installation, no two copies of *Backup**EDGE*** are likely to have the same key. Further, ***without the decryption key, encrypted data cannot be recovered by any currently known means***.

Unfortunately, asymmetric ciphers such as RSA are not without disadvantages. For *Backup**EDGE***, the major disadvantage is speed; asymmetric ciphers tend to be much slower than symmetric ciphers. For a backup in which many gigabytes of data are encrypted, faster is generally better.

*Backup**EDGE*** optimizes this by using a combination of symmetric (AES) and asymmetric (RSA) ciphers on a single backup. It gains the flexibility of an asymmetric cipher with the speed of a symmetric one.

25.2 - What Encryption Cannot Do

Encryption provides the means of securing archive media against many types of intrusion, but it is not a “cure-all” for data security. Like any other tool it must be used correctly before it is effective. Even then, there are problems that it simply is not designed to solve.

For example, one must consider the ways in which data could be received by unauthorized parties. If someone who has physical access to the machine(s) in question is determined to get the data, then he or she will almost certainly be successful. It does not matter in a case like this whether or not backups have sensitive data protected by encryption; the point of failure is not the backup media, but rather the original copy of the data!

Similarly, if a user of a system is able to gain access as the ***root*** user, then there is no need to for him or her to attack the encrypted backups. Instead, he or she will simply copy the original data. Alternatively, important system programs could be replaced with malicious counterparts that record sensitive data over time, so that future intrusions are not even necessary! *Backup**EDGE*** itself might be replaced, or configured not to encrypt data.

*Backup**EDGE*** is not designed to fix these problems. It is designed to provide a secure way to store data for archival purposes without making that data available to anybody who happens upon archive media. It is designed with *very strong, publicly-reviewed encryption algorithms* so that even a determined attacker should have great difficulty extracting the original data given only the archive media.

However, if the attacker has access to the original data, or is allowed to get the *Backup**EDGE*** decryption keys, then the encrypted archive is not secure. As an analogy, performing backups

regularly is not enough to make sure that no data is lost; one must also allow for proper storage of the media, rotation of the media used, and so on.

*Backup**EDGE*** assumes that the system is secure enough that the ***root*** user is trusted; since the ***root*** user is able to replace *Backup**EDGE*** anyway, and access any other data he or she cares to, this is not a restrictive assumption. While *Backup**EDGE*** tries to protect sensitive information from observation by non-root users in all reasonable cases, and provides several options for additional security in this area, it is not designed to protect a site from its own users. In practice, such an attempt would probably not work very well anyway, assuming the attacker has a few minutes and a screwdriver to open the machine and extract the hard drive.

In other words, *Backup**EDGE*** with encryption does not "prevent" an attacker from getting the data, any more than forcing the users of a system to pick good UNIX passwords will "prevent" an attacker from gaining unauthorized access to the system. Both simply make sure that an attack is harder than it would otherwise be, by making the backup (or the login prompt) not the weakest link. *If the cheapest attack is more expensive than the original data is worth, then the data is probably safe.*

As in any security-related application, no amount of encryption or other technical features can replace sound planning and procedures for data storage and protection.

25.3 - How *BackupEDGE* Encrypts Data

Initially, encryption is disabled. No files will be encrypted by *Backup**EDGE*** until this feature is specifically enabled via the `Set up Encryption` option in *EDGEMENU*. First, an overview of the entire encryption process will be presented.

During encryption setup, *Backup**EDGE*** creates an *Asymmetric Key Pair* for the RSA encryption algorithm. One is labelled the *Encryption Key*, while the other is the *Decryption Key*. While *Backup**EDGE*** actually uses AES to encrypt most of the sensitive data on an archive, functionally it is the RSA keys that the user is concerned about. The AES key for any particular backup is generated randomly when the backup is made, and stored on the backup *after having been encrypted* with the system-wide RSA *Encryption Key*.

This randomly-generated AES key is called the *Session Key* for a particular backup. It is this key which is used to encrypt data for the rest of the backup. When reading the backup, the *Session Key* is recovered from the archive itself, since it is stored after being encrypted with the RSA *Encryption Key* for the system, as mentioned earlier.

The RSA *Encryption Key* is also called the *Public Key*, since it is not kept secret. It is stored in a file that is world readable, and could be made public knowledge without risk of compromising encrypted data. It is this key that is needed to perform encrypted backups. Recall that in an asymmetric cipher such as RSA, the *Encryption Key* cannot decrypt data that was encrypted with that same key; only the *Decryption Key* can do that.

Therefore, it is the RSA *Decryption Key*, also called the *Private Key*, that must be kept secret to ensure that encrypted backups are secure. Further, ***without this key, data encrypted with the corresponding public key cannot be recovered. There is no known "back door" that can be opened to recover data in the event the private key is lost or damaged***. It is the decryption key that is required to read/restore backups.

*Backup**EDGE*** actually understands two variants of the *Private Key*: the *Hidden Private Key*, and the *Plaintext Private Key*. The *Plaintext Private Key* is all that is needed to recover data encrypted with the public key. The *Hidden Private Key* is encrypted with a *Passphrase* entered during installation. This passphrase must be entered before the *Hidden Private Key* is used. Whether either or both of these *Private Keys* are stored on the system is configurable by the user. The effects of this choice are outlined later.

The *Public Key* is always stored in plaintext format; it is never hidden by the passphrase. This is because knowing the *Public Key* only helps to encrypt data, not to decrypt it. Because "hidden" and "plaintext" are never used to talk about a *Public Key*, *Plaintext Private Key* is sometimes abbreviated as *Plaintext Key*, and *Hidden Private Key* is sometimes shortened to *Hidden Key*. These phrases do not refer to the *Public Key*.

Note that the *Hidden Private Key* is not to be considered secure against attack because of its passphrase protection; it is stored in this way merely to provide a level of protection against the casual observer. Details of how it is encrypted can be found in the *Technical Reference Manual*. Be aware that the simplest attack on a *Hidden Private Key* would most likely be an attack on the *Passphrase*; an easily guessed passphrase is not secure regardless of how the data is encrypted.

During installation, *Backup**EDGE*** will ask if it should keep the *Plaintext Private Key* on the system as a file readable only by root. If it does so, then decryption will be transparent whenever root reads a backup that was encrypted with the *Public Key*. If it does not, then it will ask for the *Passphrase* for the *Hidden Private Key* whenever it attempts to read from an encrypted archive.

There is at most one *Public Key* at a time on any given system. All encrypted backups will use this key. However, more than one *Private Key* may be kept on a system. Because *Backup**EDGE*** can identify which *Private Key* is needed to read a particular archive, having more than one *Private Key* on a system can be useful if reading media from multiple systems, each with different *Private Keys*.

Also note that *Backup**EDGE*** can have plaintext or hidden versions of any given *Private Key*, or both. It will first look for a plaintext version of a required key, and use it if it is found. If not, it will search for the hidden version of that key. If found, it will prompt the user for a *Passphrase* to decrypt the key, and then use it as it would the *Plaintext Private Key*. If neither key is found, *Backup**EDGE*** will inform the user that decryption is not possible until the key is installed. The *EDGEMENU* user interface will ask for instructions if it encounters this situation.

By default, *Private Keys* will not be stored in an archive unless they are encrypted; including the (plaintext) decryption key on the archive largely misses the point. The exact behavior of *Backup**EDGE*** can be found in "Encryption and Backups" on page 268.

Finally, remember that it is not necessary to have any *Private Keys* installed on a system to perform encrypted backups. Only a *Public Key* is required. By default, *Backup**EDGE*** does not provide an option to remove the *Hidden Private Key*; if desired, this should be done manually. Of course, if the *Private Key* is destroyed, then all data encrypted with the corresponding *Public Key* are irrevocably lost.

The choice of whether to store *Plaintext Private Keys* and/or *Hidden Private Keys* on the system requires careful thought. There are advantages and disadvantages to all combinations. Below is a list of some of the more obvious combinations, along with notes about each one.

25.4 - Decryption Key Options

Plaintext and Hidden Private Keys on System

In this scenario, *Backup**EDGE*** keeps both *Plaintext Private Keys* and *Hidden Private Keys* on the system. Note that the *Hidden Private Keys* will be ignored in most cases, since the *Plaintext Private Keys* will be used automatically.

Of course, as mentioned elsewhere, neither *Plaintext Private Keys* nor *Hidden Private Keys* are stored on the archive itself except in encrypted form.

In this case, verifies and restores of encrypted backups will not prompt the root user for a *Passphrase*, and will transparently decrypt whatever data is requested. This will very closely resemble how *Backup**EDGE*** behaves with unencrypted backups. However, the data selected for encryption will be stored in the archive encrypted; if one moves the media to a system without a

copy of the *Plaintext Private Keys* or *Hidden Private Keys*, the encrypted data will not be recoverable there until the appropriate *Private Key* is installed from a key backup.

As an additional bonus, *Scheduled Jobs* will be able to decrypt the encrypted copy of the AES session key, and compare it to the original during a verify. For a comparison with a case in which *Backup**EDGE*** cannot do this, please refer to the next section.

One disadvantage to this method is that the *Plaintext Private Key* is stored on the system. It is a relatively small file that can be copied to a floppy diskette or other convenient medium. Combined with an encrypted archive, someone with physical access to the machine can carry off the data and make use of it. However, it is worth noting that without *Plaintext Private Keys* available, the intruder simply has to make an unencrypted backup. Alternatively, many computers can be carried under one arm anyway.

If an attacker somehow gets access to an encrypted backup, and can somehow get the *Plaintext Private Key* file from the system, then the attacker can recover encrypted data.

Only Hidden Private Keys on System

If *Backup**EDGE*** is instructed *not* to keep *Plaintext Private Keys*, and if *Hidden Private Keys* are not removed, then attempts to verify or restore data will require a *Passphrase* if the encrypted data is to be processed. If a *Passphrase* is not available, encrypted data will be skipped.

As a special case, *Scheduled Jobs* that perform a verification can be run without the benefit of a *Passphrase*. By temporarily storing a copy of the AES session key between the backup and verify, *Backup**EDGE*** can avoid having to decrypt the session key stored in the archive. It also remembers the encrypted version of the session key, to compare against the the one read from the archive.

For all other encrypted data, the memorized unencrypted session key is used to decrypt it, and compare it against the original data on the hard drive, assuming, of course, that *Backup**EDGE*** is performing a Bit-Level verify.

Unfortunately, this does not strictly guarantee that the archive can be read successfully later. In order to decrypt the data once the *Scheduled Job* is complete, the session key must be recovered from the archive. To do this, it must be decrypted using the correct *Private Key*. Since this operation has not been tested during the verification process (recall that no private key is available, since the hidden private key is useless without the passphrase), it is technically possible that the decryption will fail.

For example, consider that the session key is corrupted in memory after being encrypted, but before being written to the archive. In this case, *Backup**EDGE*** might also remember the corrupted version of the encrypted session key between the backup and verify, so that the comparison between them during the verify might succeed. Further, since the unencrypted session key is not affected by this memory corruption in our example, *Backup**EDGE*** would both use it during the backup and memorize it for the verify. Thus, the decryption of user data for the verify would produce the correct results.

When this hypothetical archive is later used to restore data, *Backup**EDGE*** would try to recover the session key from the (corrupted) encrypted session key stored on the archive, using the private key. Either this operation would fail, or it would not produce the correct session key. In either case, the encrypted data is not recoverable.

One might ask, “Why does *Backup**EDGE*** not re-encrypt the session key, and compare that against the archived copy?” Without going into too much detail here, suffice it to say that encryption does not work that way. Please see the *Technical Reference Manual* for more information.

No Private Keys on System

This is the most restrictive scenario.

Scheduled Jobs operate identically to the case in which only *Hidden Private Keys* are available, including the caveats mentioned above. Recall that the *Hidden Private Keys* were not actually used by *Scheduled Jobs* since they require a *Passphrase*.

Attended verify and restore operations will be forced to skip encrypted files, since no *Private Key* is available. In order to restore encrypted data, the correct *Plaintext Private Key* or *Hidden Private Key* must be installed on the system.

Note that *Backup**EDGE*** will not remove the *Hidden Private Key* automatically; this must be done manually. Of course, it is imperative that there is a copy made of the *Private Key*, or else encrypted data is not recoverable.

Also note that *Private Keys* are never stored unencrypted on normal archives! One must use the "Key Backup" option in *EDGEMENU* before erasing a new *Private Key*, or else data encrypted with the corresponding *Public Key* will not be recoverable!

25.5 - Key Backups

Normal backups *do not include unencrypted Plaintext Private Keys or Hidden Private Keys* for obvious security reasons. However, that does not mean that they do not have to be carefully archived!

EDGEMENU provides a *Key Backup* option under the Setup menu (`Setup -> Decryption Key Backup`). After selecting it, and choosing the *Resource* which will hold the private keys, *EDGEMENU* will back up and verify all *Hidden Private Keys* and *Plaintext Private Keys* that are currently installed. The *Public Key* is not archived for reasons that will be explained later. Note that the *Public Key* is not excluded from backups specially, so there is little need to include it here anyway.

It is very important that such a *Key Backup* is kept safe. It contains data that is absolutely necessary to read an encrypted backup!

It is possible to restore this *Key Backup* onto any other *Backup**EDGE*** installation. Doing so installs all the keys the backup contains, so that *Backup**EDGE*** can begin using them to read encrypted data. *Backup**EDGE*** automatically keeps track of which key is needed for which archives.

The *Public Key* is not included in the key backup for exactly this reason. If it were, restoring a *Key Backup* from one system onto another would replace the *Public Key*! This is definitely not desirable, since the next encrypted backup would begin using the restored *Public Key* to encrypt data. While the *Public Key* may be replaced if this is the desired effect, generally this is not what a key backup is designed to do.

It is strongly recommended that at least three key backups be made whenever a new key pair is generated. These should be stored in separate, secure places. Preferably, more than one type of archive medium should be used. Many of today's solid-state digital media are an excellent choice. CD-R media is also a good candidate. Floppy diskettes are acceptable, but remember that they are easily damaged. Using a combination of different media is generally a good idea. Storing a printout of the key file itself can be used if all else fails, by manually re-typing the key data.

Also note that *Key Backups* can be useful during disaster recovery on those operating systems that are supported by *Recover**EDGE***. It contains a menu option to restore a *Key Backup*, enabling disaster recovery from an encrypted backup. While it is possible to include *Private Keys* on the *Recover**EDGE*** media itself, this allows new keys to be added during recovery. Also, in some cases, the *Recover**EDGE*** media cannot be stored securely, so that including the *Private Keys* would represent a security risk.

Remember, ***decryption keys are not stored on*** *Recover**EDGE media***! You must provide a Decryption Key Backup during recovery, or else encrypted files will not be restored!

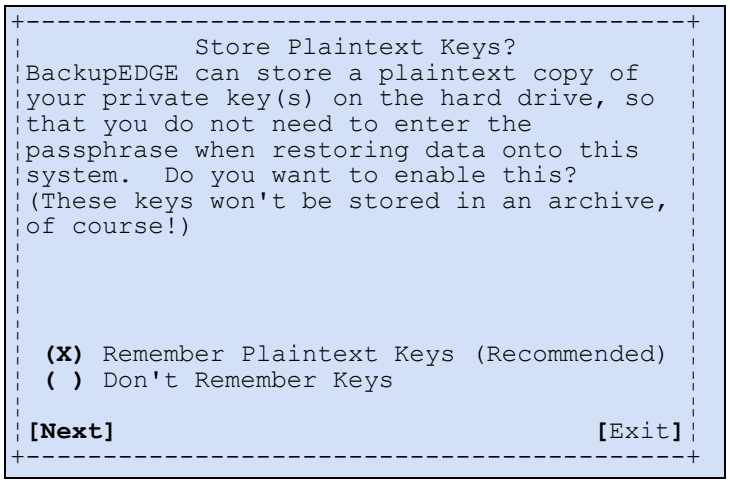
Please note that trying storing decryption keys on the *Recover**EDGE*** media requires editing *Recover**EDGE*** configuration files manually; there is no menu option to enable this. The reason for this is simple: storing keys on *Recover**EDGE*** media is generally a bad idea.

Also remember that *Backup**EDGE*** treats the directories with the *Hidden Private Keys* and *Plaintext Private Keys* specially; see "Encryption and Backups" on page 268 for more information on this.

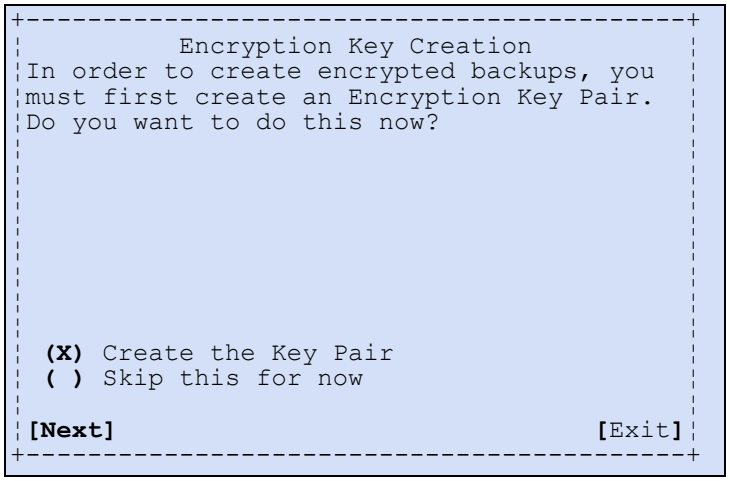
25.6 - Setting Up Encryption

To enable encryption, *EDGEMENU* provides the option
`Setup -> Configure BackupEDGE -> Configure BackupEDGE Encryption.`

When selected, this enables additional menus for encryption, and runs the encryption setup wizard. At any time after encryption is enabled, you may re-run the setup wizard with
`Setup -> Configure BackupEDGE -> Configure BackupEDGE Encryption.`



The encryption setup wizard first asks if *Plaintext Private Keys* should be stored on the system. For details about this option and its effects, please read "Plaintext and Hidden Private Keys on System" on page 262.



Next, the wizard offers to create a new key pair. If a key pair already exists, you will be informed of this. In this case, the old *Private Key(s)* will be retained so that backups made with the outgoing *Public Key* can still be read, but the *Public Key* itself will be replaced.

```
+ Key Pair Setup ------------------------------------------------------------+
¦Please enter a description for this key pair.                               ¦
¦                                                                            ¦
¦[Enc. key, mlite.microlite.com on Jan 03 2012                             ] ¦
¦                                                                            ¦
¦                                                                            ¦
¦                                                                            ¦
¦[Next]                                                              [Exit]  ¦
+------------------------------------------------------------------------------+
```

You may enter a description for the key pair by pressing `[Up-Arrow]` and typing your own description, or you may leave the default description in place.

```
+ Key Pair Setup ------------------------------------------------------------+
¦Please enter the PASSPHRASE to protect the private key. Be very sure not to ¦
¦pick an easily-guessed passphrase!                                          ¦
¦[********************                                                    ] ¦
¦Please re-enter the PASSPHRASE.                                             ¦
¦[********************                                                    ] ¦
¦                                                                            ¦
¦                                                                            ¦
¦[Next]                                                              [Exit]  ¦
+------------------------------------------------------------------------------+
```

You will be prompted to enter a *Passphrase* with which to protect the *Hidden Private Key*. You will be required to enter it twice, to be sure it is entered repeatably. Once this is done, *Backup**EDGE*** will begin generating the new RSA key pair. This can take a few minutes.

```
+ Key Pair Testing ----------------------------------------------------------+
¦Please re-enter the passphrase for the hidden key. This will be used to verify¦
¦ that the key can be unlocked properly.                                     ¦
¦[********************                                                    ] ¦
¦                                                                            ¦
¦                                                                            ¦
¦                                                                            ¦
¦[Next]                                                              [Exit]  ¦
+------------------------------------------------------------------------------+
```

Once the keys are created, they must be tested. *Backup**EDGE*** will prompt for the *Passphrase* again, in order to try unlocking the *Hidden Private Key*. If successful, it will perform some tests of the *Public Key* and *Private Keys* by encrypting and decrypting data. If all goes well, you will be informed.

In the event of a failure, please contact *Microlite Technical Support*.

```
+ BackupEDGE Installation / Upgrade / Configuration --------------------------+
+-------------------------------------------------------------------------------+
|Provide Absolute Paths of Files to Encrypt, or Wildcards.                      |
|Type filenames, TAB to Navigate, Up/Down to Change Lines, ENTER to Modify.     |
|F6 Deletes the highlighted filename.                                           |
|Filespec:  [                                                                 ] |
|                                                                               |
|                                                                 [Erase List]  |
|- Currently Selected Files ----------------------------------------------------|
|   /u/appl/filepro                                                             |
|   /u/acct/rwc9                                                                |
|-> [ Add Line ]                                                                |
|                                                                               |
|                                                                               |
|                                                                               |
|                                                                               |
|                                                                               |
|                                                                               |
|                                                                               |
|                                                                               |
|[Save]                                                             [Cancel]    |
+Editing File: mlite.microlite.com:/etc/edge.encrypt--------------------------+
+ (c) Copyright 1997-2012 by Microlite Corporation ----------------------------+
```

After the keys are generated, you will be given the option to edit the list of files which will be encrypted by the *Basic Schedule*. You may enter any filenames or patterns you like. `[Tab]` to and press `[Save]` when the list is complete.

```
+Selection Box-----------------------------------+
|                                                |
|A new key backup should be generated.  Do this  |
|                      now?                      |
|                                                |
|                                                |
|                                                |
|                                                |
|                                                |
|                                                |
|   [Yes]                              [No]      |
+------------------------------------------------+
```

Finally, if a new key pair was generated, then you are given the option to perform a *Key Backup*. It is strongly recommended that you do this.

```
+ Select Primary Device -------------------------------------------------------+
|Select the resource on which to store the key backup.                          |
|                                                                               |
|                                                                               |
|+ Resource List -------+                                                       |
||   cdrom0              | Resource :   floppy0                                  |
||   dvd0                |              Primary Floppy Drive                     |
||   tape0               | Machine :    [mlite.microlite.com                   ] |
||   tape1               |                                                       |
||   tape9               | To select a different resource, use the Up / Down     |
||-> floppy0            | arrow keys while the Proceed button is highlighted.   |
||   NullDevice          | To view resources on a different machine, press the   |
||                       | TAB key and type the system name in the "Machine"     |
||                       | field, and press ENTER.                               |
|+----------------------+                                                       |
|                                                                               |
|[Proceed]                                                          [Cancel]    |
+-------------------------------------------------------------------------------+
```

Simply select the archive device from your *Resource List* and follow the instructions. Generally, you should run two or three *Key Backups* to different media types, as mentioned above.

25.7 - Encryption and Backups

To select which files are encrypted, *Backup**EDGE*** uses a file list. This list can contain the absolute pathnames of files or directories to be encrypted, possibly with wildcards. These should be stored one per line. This list can be edited by using the encryption setup wizard as described above, or by hand with a UNIX text editor. It can also be edited in the *Domain Editor* (`Schedule -> Create/Edit Domain` and ***FastSelect*** the *Domain* to be edited), by highlighting the "`Encryption`" line and pressing `[F4]`.

If you elect to edit this file with the encryption setup wizard, be sure not to generate new encryption keys accidentally. You do not have to generate new keys in order to change the files that are encrypted with them!

The list of files to be encrypted may contain on filename, directory name, or pattern per line. For example, `/usr/secret_file` would encrypt that file, while `/usr/secret_dir` would encrypt all files under that directory, recursively. `/usr/secret*` would encrypt all files directly under the `/usr` directory that start with `secret`, including for example `/usr/secret` and `/usr/secret_files`. If any directories are selected by it, their contents would be encrypted recursively as well.

The pattern `*.c` would encrypt all files ending with `.c`, in any directory. If a directory is found to end in `.c`, then all files under it would be encrypted.

When setting up encryption in *EDGEMENU*, you will be given the option to edit the contents of this file.

Once the file exists, *Backup**EDGE*** must be told to use it.

For backups of *Domains*, the file is listed in the *Domain Editor*, much like the list of virtual files or raw devices. The file's contents may also be edited in the *Domain Editor* using the `[F4]` key, as mentioned earlier. For backups from the command line with `/bin/edge`, the `-zENCRYPT=/tmp/my_encryption_list_file` flag is used to select the file list.

NOTE: Including a file in the encryption list does not actually cause it to be backed up. Instead, this list indicates which files will be encrypted ***if they are included in the backup.***

Encryption has several effects on backup, besides actually encrypting the selected data.

Files that are to be encrypted are first compressed, if the file is larger than the compression limit and hasn't been excluded from compression. This occurs even if software compression is disabled for the backup. Since encrypted data generally compresses very badly, the hardware compression that is found in tape drives tends to produce little benefit. To counter this, *Backup**EDGE*** employs its own software compression prior to encryption. Compression also removes redundancy in the files, making certain types of attacks on the encrypted data less likely.

If checksumming is enabled, the checksums are computed for the encrypted data. Thus, it is possible to verify a checksum even without having the decryption key.

When any file on a backup is to be encrypted, the private keys are ***automatically added to the list of files that will be encrypted if they are included in the backup***. While an encrypted copy of the *Private Keys* may seem pointless, it does have a purpose: during disaster recovery, these keys are restored onto the system so that when the recovery is complete, the system is quite ready to function as before, without requiring the operator to manually re-load them via restores of *Key Backups*.

Of course, the encrypted copies will not help decrypt any data on the archive. Because of this, it is still necessary to have at least one working *Key Backup* that can be used to restore the archive!

If encryption is not enabled, then the *Private Keys* are ***automatically excluded*** from backup. This prevents a backup from having a plaintext copy of the keys unintentionally. Of course, this means that special care must be taken to include the *Private Keys* on a backup; ***if one simply***

does an unencrypted "Master Backup", the private keys will be excluded. In order to force *Backup**EDGE*** to include them unencrypted, the `-zKEYBKP` option must be given on the command line. This option works only for the `/bin/edge` program itself; there is no way to use it with *EDGEMENU* except by performing a "`Setup -> Decryption Key Backup`".

Encryption may be applied to any type of file, including raw devices and virtual files. Of course, the file must have one or more bytes of data or else encryption is skipped. This is not considered an error.

In a multi-volume archive, the encrypted *Session Key* is repeated at the beginning of each volume. This enables a restore to start on any volume if required.

A copy of the encrypted *Session Key* is also stored immediately before every encrypted file. While this is not normally used, it is intended to help recover data in the event of a medium failure, such as a snapped tape. If the session key were stored only at the beginning of the volume, then any damage to the front of the volume could render all encrypted data on it unusable, even if the encrypted data itself were not affected. Of course, in the case of a multi-volume archive, the *Session Key* from another volume could be used.

Note that while the *Session Key* is generally less than two kilobytes, encrypting many small files can cause a significant increase in archive size.

The backup summary will include the number of files that were encrypted during the backup. Be sure that it agrees with the number that you expect.

25.8 - Restoring Encrypted Backups (EDGEMENU)

Restoring data from an encrypted backup through *EDGEMENU* is very simple. You just perform a normal restore as you would from an unencrypted backup.

*Backup**EDGE*** will take one of three actions, depending on the state of your decryption keys...

Plaintext Keys Available

If the *Plaintext Private Key* for your archive is available, the files will simply be restored.

Hidden Keys Available

If the *Hidden Private Key* is available, but not the *Plaintext Private Key*, you will be prompted for the *Passphrase* before any encrypted files are restored.

```
+-----------------------------------------+
|A passphrase is required for this archive. |
|                                         |
|  (X) Enter Passphrase                   |
|  ( ) Skip Encrypted Files               |
|                                         |
|[Continue]                [Abort Operation]|
+-----------------------------------------+
```

Select `Enter Passphrase` and type your passphrase to continue. You may also elect not to type the passphrase by choosing `Skip Encrypted Files`. In this case the restore will continue but encrypted files will not be restored.

No Private Keys

If neither private key is found on the hard drive, you will be asked if you wish to install the necessary decryption keys from a *Key Backup*.

```
+-----------------------------------------+
¦This backup requires a decryption key that ¦
¦is not present on mlite.microlite.com.  You¦
¦may restore it from a key backup, skip     ¦
¦encrypted files, or cancel the restore.    ¦
¦                                           ¦
¦  (X) Use Key Backup                       ¦
¦  ( ) Skip Encrypted Files                 ¦
¦                                           ¦
¦[Next]                     [Cancel Restore]¦
+-----------------------------------------+
```

You may also read the decryption key into memory only, rather than storing it on the hard disk, if you do not want the decryption key permanently recorded on the filesystem. *EDGEMENU* will ask which of these you prefer.

```
+-----------------------------------------+
¦You may restore the key onto the hard      ¦
¦drive, or you may read it into memory.     ¦
¦Reading it into memory will use the key    ¦
¦only for this single restore.              ¦
¦                                           ¦
¦  (X) Restore to HD                        ¦
¦  ( ) Read into Memory Only                ¦
¦                                           ¦
¦[Next]                     [Cancel Restore]¦
+-----------------------------------------+
```

In either case, you'll get a *Resource List* popup prompting you for the appropriate device containing the *Key Backup*.

25.9 - Restoring Encrypted Backups (Command Line)

EDGE.RESTORE and the `/bin/edge` program each understand encrypted backups. They require that at least a *Private Key* exist on the hard drive before restoring files. If no *Plaintext Private Key* exists and a *Passphrase* is required to unlock a *Hidden Private Key*, these programs will request it. If the *Passphrase* is incorrect, they will produce a warning and offer to accept a new guess or skip encrypted files entirely.

25.10 - Restoring Encrypted Backups (*RecoverEDGE*)

*Recover**EDGE*** disaster recovery has a menu option for loading in decryption keys before beginning a restore. You'll be asked to specify the UNIX or Linux device name of the device containing the *Key Backup* to be loaded.

25.11 - Using Identical Keys on Multiple Systems

In large corporations, it may be to have the same keys protecting more than one system. A procedure for this is available. See "How do I use the same Encryption Key on multiple systems?" on page 388 for additional instructions.

25.12 - Hiding and Disabling Encryption

It is possible to remove the encryption options from *EDGEMENU*. To do so you must edit a variable in the master configuration file `/usr/lib/edge/config/master.cfg`.

```
ENC_HIDDEN={YES|NO}
```

If set to `YES`, *EDGEMENU* will hide encryption options. This is useful to keep end-users out of the encryption configuration. Note that encryption itself *is not disabled or enabled because of this*; only *EDGEMENU*'s user interface is affected.

To totally disable encryption, *causing backups to be unencrypted*, set the variable `ENC_ENABLED` to `NO` in `/usr/lib/edge/config/master.cfg`

```
ENC_ENABLED=NO
```

26 - Product Registration and Activation

License Management ensures that all clients register their products, so that they can be notified in a timely fashion of updates and enhancements.

The *License Manager* allows on-line, fax in, or web-based registration for all *Backup**EDGE*** users. Each package is shipped in demo / evaluation / unregistered mode, and will run for 60 days from the time it is installed. During that time it is necessary to run the *Registration / Activation Manager* and fill out **all** of the appropriate information. This information may be sent via electronic mail to Microlite Corporation, may be printed out and faxed, or may be typed in to the electronic registration system at `http://www.microlite.com` on the World Wide Web.

Within 24 business hours (3 business days), a return fax with a *Permanent Activation Code* will be provided. The *Registration / Activation Manager* must be run again and the *Permanent Activation Code* typed in, which will permanently activate *Backup**EDGE*** for the registering company and system. Typical turn-around time for legible activations is less than one business day.

The faxed form with the *Permanent Activation Code* should be ***PERMANENTLY STORED*** with the installation media, so that the product can be re-installed without having to re-register.

In addition to the base product, *Backup**EDGE*** includes separate features which may be licensed if desired. Each of these requires a separate *Activation Code*, in addition to the one that activates the base product.

A license for the base product includes all backup / verify / restore functionality, and Disaster Recovery functionality (if available for your platform). For those familiar with older versions of *Backup**EDGE***, this is what older versions provided as well.

Optional features, such as an *Encryption License*, enable additional functionality that not every user will care about. These can be added later if desired in most cases, simply by adding the appropriate *Feature Serial Number* using the registration system described here.

26.1 - Finding Your Serial Number

Your *Backup**EDGE** Base Product License* serial number and optional *Encryption License* serial number are always found on separate license forms. Please do not lose these forms. When a final *Activation Form* is received from the *Microlite Registration System*, please file it with the license form.

26.2 - Running The Registration / Activation Manager

To start the *Registration / Activation Manager* program, from *EDGEMENU* choose:

```
EDGEMENU -> Setup -> Activate BackupEDGE.
```

or from the `root` prompt (`#`) type...

```
/usr/lib/edge/bin/edge.activate
```

```
+Serial Number Entry Screen-----------------------------------------------------+
|Please enter one or more BackupEDGE Product / Feature serial numbers separated|
| by ',' .                                                                      |
|[                                                                             ]|
|                                                                               |
|                                                                               |
|                                                                               |
|                                                                               |
|[Next]                                                              [Cancel]|
+-------------------------------------------------------------------------------+
```

Type in the product serial number and select `[Next]`.

Product Registration Screen (Blank)

```
+ BackupEDGE Product Registration Information ---------------------------------+
¦Company Name:       [                                                        ]¦
¦Address 1:          [                                                        ]¦
¦Address 2:          [                                                        ]¦
¦Company City:       [                                                        ]¦
¦Company Country:    [                                                        ]¦
¦State / Province:   [                  ]     Zip:      [                    ]¦
¦Contact Person:     [                                                        ]¦
¦Contact Email:      [                                                        ]¦
¦Voice Phone with Area Code:   [                                              ]¦
¦Fax Phone with Area Code:     [                                              ]¦
¦Optional Additional Fax:      [                                              ]¦
¦Purchased From:     [                                                        ]¦
¦                                                                             ¦
¦[Save]                                                              [Cancel] ¦
+-------------------------------------------------------------------------------+
```

To *Register* the product:

- Enter the serial number(s) for your product when prompted. Alternatively, the `New` option from the main menu can be used to add one or more serial numbers at any time. Simply type the serial number that you will find on the installation media, sleeve, box or product manual, plus any for separate features such as encryption. If this number contains **demo** or **eval**, the product is not licensable. Please purchase a permanent license from whomever you received your copy of *Backup**EDGE*** before proceeding. Notice that after you enter the serial numbers, the screen under the main menu will display them.
- You will be prompted for end user contact information. Fill in all information listed above. Use the arrow keys and `[Enter]` key to navigate around the screen. When you first run the registration program, you will be prompted for this information immediately after providing serial numbers, if needed. It may be edited later by selecting the `Info` option from the main menu if you desire.

```
+ BackupEDGE Product Registration Information ---------------------------------+
¦Company Name:       [Microlite Corporation                                   ]¦
¦Address 1:          [2315 Mill St.                                           ]¦
¦Address 2:          [                                                        ]¦
¦Company City:       [Aliquippa                                               ]¦
¦Company Country:    [USA                                                     ]¦
¦State / Province:   [PA                 ]     Zip:      [15001               ]¦
¦Contact Person:     [Ed Smertz                                               ]¦
¦Contact Email:      [eds@microlite.com                                       ]¦
¦Voice Phone with Area Code:   [724 375 6711                                  ]¦
¦Fax Phone with Area Code:     [724 375 6908                                  ]¦
¦Optional Additional Fax:      [                                              ]¦
¦Purchased From:     [Dealer name goes here                                   ]¦
¦                                                                             ¦
¦[Save]                                                              [Cancel] ¦
+-------------------------------------------------------------------------------+
```

- After you have entered the information, you will be taken to the main menu.

```
+ BackupEDGE Product License Manager ----------------------------------------+
|+-------+-------+----------+--------+------+------+-------------------------+|
|  [New] [Send] [Activate] [Delete] [Info] [Quit]                             |
|+Add A Serial Number-------------------------------------------------------+|
|                                                                            |
|Company Name: Microlite Corporation                                         |
|Product Type: linux60                  System Name:      microlite          |
|EDGE Version: 03.03.01                 Operating System: 2.6.32-754.17.1    |
|                                                                            |
|Serial Number       Feature            Status              EX DATA         |
|XAR10000101         Base License       Demo                                |
|(None)              Encrypted Backups  Demo                                |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
+----------------------------------------------------------------------------+
```

- Use the `Send` option from the main menu to generate a registration fax, email, or printout.

NOTE: Registration data MUST be ***end user information***. Reseller/VAR/OEM information cannot be placed in the contact information fields.

Press the *Field Help* `[F1]` key for help if desired.

Product Registration Mail / Print Screen

```
+ Send BackupEDGE Registration Info ---------------------------------+
|[ ] Join Support / Update Mailing List                              |
|[ ] Email to registration@microlite.com                             |
|[ ] Print Registration on PCL5 Compatible Printer                   |
|[ ] Print Registration on Postscript Compatible Printer             |
|[X] Print Registration on Line Printer                              |
|[ ] Display Registration On-Screen                                  |
|Spooler Command:                                                    |
|[lp                                  ]                              |
|                                                                    |
|[Next]                                                   [Cancel]   |
+--------------------------------------------------------------------+
```

This screen will appear when you select the Send option from the main menu. Use the the arrow keys and `[Space]` to select each option, and type the proper command and press `[Enter]` at the spooler command option. You must:

- Select **Yes** or **No** for the `Join Support / Update Mailing List` option. Microlite Corporation will notify you of support and update issues related to this release.
- Select **Yes** or **No** for the `Email to registration@microlite.com` option. If you have Internet electronic mail access, the form can be transmitted electronically (it will be sent to *registration@microlite.com*).
- Select **Yes** for *one* of the printer types. All print the same information. If you have a PostScript or PCL5 compatible printer, the form is much easier to read.
- Type in a different spooler command if the default will not send the registration form to the correct printer.

Use `[Next]` to complete the registration process. This will send the electronic registration if appropriate, or just print the *Registration Form*.

NOTE: You may press `[Cancel]` to return to the main menu if for any reason you have entered registration information incorrectly, or do not want to send it now.

Here is an example of a completed mail / print screen.

Product Registration Mail / Print Screen - Complete

```
+ Send BackupEDGE Registration Info ---------------------------------+
¦[X] Join Support / Update Mailing List                              ¦
¦[ ] Email to registration@microlite.com                             ¦
¦[X] Print Registration on PCL5 Compatible Printer                   ¦
¦[ ] Print Registration on Postscript Compatible Printer             ¦
¦[ ] Print Registration on Line Printer                              ¦
¦[ ] Display Registration On-Screen                                  ¦
¦Spooler Command:                                                    ¦
¦[lp -d optra1                          ]                            ¦
¦                                                                    ¦
¦[Next]                                                    [Cancel]  ¦
+--------------------------------------------------------------------+
```

The above screen will print a PCL5 compatible *Registration Form* on the printer `optra1` using the `lp` command. It will also notify Microlite Corporation that you'd like to be notified about product updates via electronic mail.

If you have not sent the *Registration Form* via email, you may print it and fax it to Microlite Corporation (instructions are listed on the form). If you wish, you may connect to the Microlite Corporation World Wide Web Site (`http://www.microlite.com`) and type the registration data EXACTLY as it exists on this form. This will speed the registration process. Otherwise just file the *Registration Form* with the installation media for reference. An example of a printed *Registration Form* is shown on page 278.

Within 24 business hours, a return form will be faxed with a *Permanent Activation Code* (or codes, if you have serial numbers for optional features, such as an Encryption License). Follow the instructions in the next section to permanently activate *Backup**EDGE***.

26.3 - Permanently Activating BackupEDGE

Start the *Registration / Activation Manager* program as previously described. From *EDGEMENU* choose:

```
EDGEMENU -> Setup -> Activate BackupEDGE.
```

Select `[Activate]`

or from the `root` prompt (`#`) type...

```
/usr/lib/edge/bin/edge.activate -a
```

You will be prompted to enter one or more *Activation Codes*. Type in all the *Activation Codes* found on the *Activation Form* as sent to you by Microlite. Each code will be applied automatically to the corresponding serial number. You may elect to enter activation codes at any time from the *Activation Manager* main menu by selecting the `Activate` option.

Save the form containing your *Permanent Activation Code*(s) as previously discussed.

26.4 - Changing Registration Data

Sometimes a client may need to re-enter the *Registration / Activation Manager* to change information. For instance, the serial number may have been typed incorrectly or the client name spelled wrong, or the contact information may need to be changed.

This *Registration / Activation Manager* can be run in "change fields" mode.

From *EDGEMENU* choose:

```
EDGEMENU -> Setup -> Activate BackupEDGE.
```

Select `[Info]`

or from the `root` prompt (`#`) type...

```
/usr/lib/edge/bin/edge.activate -r
```

Alternatively, the `Info` option of the main menu in the *Activation Manager* can be used to access this data at any time.

Changing information in this form will require that the product be re-registered and a new *Permanent Activation Code* issued. Please follow the procedures listed on the preceding pages to email and/or print and fax the file.

If you care to remove one or more serial numbers, perhaps because they have been mis-typed, use the `Delete` option from the main menu. Simply enter the serial number(s) to be deleted.

26.5 - Removing Registration Menus from EDGEMENU

It is possible to remove the registration / activation options from *EDGEMENU* after activation. To do so you must edit a variable in the master configuration file `/usr/lib/edge/config/master.cfg`.

```
HIDE_REG={YES|NO}
```

If set to `YES`, *EDGEMENU* will hide the registration / activation options. This is useful to keep casual users from accidentally changing the registration information.

26.6 - Registration Without a Printer

On rare occasions, the system will have no printer, or the spooler will not have been configured yet at the time *Backup**EDGE*** is installed. For this reason an ASCII text copy of the registration information is stored in the following file:

```
/usr/lib/edge/config/info.register
```

This file may be printed after the spooler is set up, or copied to another system and printed. An example of this file is shown on page 278.

If for some reason this is not possible, the user may call (724) 375-6711 and request that a registration form be faxed. Return fax information may be left on the voice mail system if an operator is not available. This form should be TYPED ONLY with the information EXACTLY (character for character) as it appears on the registration screen or in the `info.register` file.

26.7 - Registration Problems

The registration system was conceived to provide as little inconvenience as possible for the end user. Electronic mail, PCL5 and PostScript registration form printing were designed to get registration information to Microlite Corporation with maximum accuracy **and** legibility.

Delays in receiving a *Permanent Activation Code* will result when:

- The registration form is incomplete.
- The registration form contains contact information referencing a reseller/VAR/OEM instead of the end user.
- The registration information is typed, and not exactly the same as the data contained in the `info.register` file.
- The information is hand written or otherwise illegible.

Please remember that if we cannot read the registration information, we cannot issue a valid *Permanent Activation Code*.

26.8 - Changing The System Name

*Backup**EDGE*** is registered to the system it is installed upon. If you change the *System Name*, *Backup**EDGE*** will detect the change and assume it has been moved to a different system. This will cause the *License Manager* to place the product in *Expired Mode*. *Scheduled Jobs* will fail and request that you run *EDGEMENU*. Running *EDGEMENU* right after a *System Name* change will place *Backup**EDGE*** into *Emergency Activation Mode*. It will run for **three days** in this mode. During this time, you must run the *Registration Program* as described on page 272, save and send a new *Registration Form* to Microlite Corporation, along with a brief note describing why the *System Name* has changed (replaced system, changed network, etc.).

You will receive warnings on the *EDGEMENU* screen, and in your electronic mail and printed reports, when *Backup**EDGE*** is running in *Emergency Activation Mode*.

26.9 - Emergency Activation

In an emergency, any of the following can be used to get *Backup**EDGE*** functioning:

- Remove and re-install *Backup**EDGE***. This will place *Backup**EDGE*** into 60 day evaluation mode, giving the user plenty of time to deal with the disaster.
- Call Microlite Corporation for a three day emergency activation. This is available during Microlite business hours only.
- Contact the Microlite Corporation World Wide Web site at `http://www.microlite.com`. You will be able to type in all registration data and receive a three day *Emergency Activation Code* immediately.
- Boot from *Recover**EDGE*** media. If you have a system with *Recover**EDGE***, *Backup**EDGE*** will *always* function when booted from the media, even if the program was never activated. Of course, if you restore a system from a backup that does not have a licensed copy of *Backup**EDGE***, when you reboot the system *Backup**EDGE*** will still not be licensed.

26.10 - Re-Installing BackupEDGE

*Backup**EDGE*** can be re-installed at any time. The registration procedure is as follows:

- Re-install the program as outlined in the installation guide.
- Run the *Registration / Activation Manager* once and type the registration information EXACTLY as it appears on your permanent registration and activation form. Save the information with `[Save]`, but do ***not*** print or email a fax form. Depending on what information is present, you may need to use the `New` option from the *Activation Manager* main menu to enter serial numbers, and the `Info` option to change the company name, etc.
- Use the `Activate` button from the main menu of the *Activation Manager* to enter your activation code(s).

*Backup**EDGE*** is now re-activated.

The permanent registration information (in machine readable format) is stored in the file:
`/usr/lib/edge/config/edge.register`

The english text version of the initial registration form is stored in the file:
`/usr/lib/edge/config/edge.register`

It is also possible to copy these files, re-install, and then replace the new files with the copies.

26.11 - Old BackupEDGE Serial Numbers

Serial numbers from *BackupEDGE* releases prior to 03.00.00 are **not** compatible with this release. You must purchase a new retail license with a new serial number in order to register and activate *BackupEDGE* 03.00.00 or later.

26.12 - Example Registration and Activation Form

```
================================================================================
Microlite BackupEDGE                                  Product Registration Form
Email or Fax and RETAIN
================================================================================
END USER REGISTRANT INFORMATION
Organization Name:          Microlite Corporation
Address 1:                  2315 Mill St.
Address 2:
Company City:               Aliquippa
Company Country:            USA
Company State/Province:     PA
Company Zip/Postal Code:    15001
END USER CONTACT INFORMATION
Primary Contact Name:       Ed Smertz
Contact Email:              eds@microlite.com (Subscribe)
Voice Phone with Area Code: 724 375 6711
Fax Machine with Area Code: 724 375 6908
RESELLER INFORMATION
Purchased From:             Acme Industrial Carpet
Fax / Email Activation To:  joe@acmeindustrialcarpet.com

PRODUCT INFORMATION
Registration Date:  Sep 11, 2019
Product Type:       linux60
System Name:        web2v
BackupEDGE Version: 03.03.00
OS Version:         2.6.32-754.17.1.el6.x86_64
Registration Code:  S36Y4SJD0WJFLYJ3T

REGISTRATION INFORMATION
Product/Feature     Serial Number
Base Product        XAR10000101


================================================================================
Thank you for purchasing and registering Microlite BackupEDGE.

Please scan and email this form to: registration@microlite.com
Or, you may also fax this form to: 724-375-6908

Your activation will be processed and sent by return fax within
24 business hours.

If you have an email, fax transmission or other problem, please call the
Registration Hotline at 724-375-6711 (US/Can toll-free 888-257-3343) Monday
through Friday from 9:00am to 5:00pm US Eastern Time.

Per the terms of the Microlite Corporation End User License Agreement
(EULA), forms containing anything but current and correct end-user
information will be considered invalid. No activation code will be issued.
Resellers may only place their contact information in the designated area.

Microlite Corporation
2315 Mill Street
Aliquippa PA USA 15001-2228
(724) 375-6711                  Voice
(724) 375-6908                  Fax
registration@microlite.com      Registration Department
```

27 - Disaster Recovery - Preparation

Disaster Recovery is the process of rebuilding a system after a data disaster, such as a lost hard drive, without having to re-install the operating system, *Device* drivers, applications and user data separately.

*Backup**EDGE*** includes a component called *Recover**EDGE***, which supports disaster recovery when using the following operating systems...

- *Linux* - Supported Intel IA32 processor distributions with 2.6.x, 3.x, 4.x kernels.
- *Linux* - Supported EM64T / AMD64 processor distributions with 2.6.x, 3.x, 4.x and 5.x kernels.
  - See the Linux Support Tables on the Microlite Web Site for more information.
  - See the Linux GPT Support Page on the Microlite Web Site for more information.
  - See the Linux UEFI Support Page on the Microlite Web Site for more information.
- *Xinuos SCO OpenServer 6 (OSR6)* - release 6.0.0, 6V and 6 Definitive.
- *Xinuos SCO OpenServer 5 (OSR5)* - release 5.0.5 through 5.0.7, 5.0.7V and 5 Definitive.
- *Xinuos UnixWare 7 (UW7)* - release 7.1.4, 7.1.4+and 7 Definitive.

On other operating systems, it is necessary to re-install a base operating system and *Backup**EDGE***, then restore data from your *Backup**EDGE*** backups, to perform a disaster recovery.

27.1 - Anatomy of a Disaster Recovery

With *Backup**EDGE*** and *Recover**EDGE***, recovering from a data disaster is simple...

- Solve the hardware problem.
- Boot from the *Boot Media*.
- Prepare all hard drives and filesystems.
- If you are using encrypted backups from the optional Encryption Module, the decryption keys must be made available from a Decryption Key Backup.
- Restore from *Backup**EDGE*** backups.
- Re-boot.

The “traditional” model for disaster recovery is to...

- boot from a specially prepared set of floppy diskettes containing the system kernel, *Device* drivers, disk preparation programs and tape programs.
- prepare hard drives, partitions and filesystems by hand.
- mount the filesystems by hand.
- restore any decryption keys needed from a Decryption Key Backup if the system backup was made with the optional Encryption Module.
- manually issue a restore command to the tape drive.
- unmount the filesystems.
- reboot the system.

*Backup**EDGE*** improves on this model in many ways...

- The *Boot Media* may be floppy diskettes, optical or SharpDrive media, or even *Bootable Tapes*.
- The *Boot Media* boot directly into the *Recover**EDGE*** system, allowing easy, menu driven system preparation.
- The data to be restored may come from a any valid *Backup**EDGE** Resource*.
- *BootableBackups*™ are also supported, using optical media, *SharpDrive* media and *Bootable Tapes*. *Bootable Backups* are backups that contain all of the boot programs *and* the files to be restored reside on the same medium.

The *Boot Media* contain modem and networking capabilities, allowing two additional functions...

- The data to be restored may come from a *Device* attached to the local system, or from a *Device* or archive file on another system on the network.
- A system administrator may work sitting at the system console, or may remotely connect to the system via modem or *telnet*.

27.2 - Boot Media vs. Bootable Backups

As mentioned, you may now create *Boot Media* on floppy diskettes, *Optical* media, and *SharpDrive* media, as well as network images (PXE booting). You boot from the *Boot Media* into the *Recover**EDGE*** system, then restore your files from separate backup media.

Boot Media should be re-generated whenever there is a significant change to the system configuration. After adding or removing filesystems, hard drives or storage *Devices*, it is a good idea to re-create the *Boot Media* so that it includes the new configuration and can replicate the system when required.

Bootable Backups work by pre-pending all of the information necessary to boot into the *Recover**EDGE*** system to the front of each full system backup. This information is stored in a file called a *Boot Image* which becomes part of each backup. As every backup is self-contained, there is no more worry about not being able to remember where you put the *Boot Media* when you really need it!

Remember, however, that decryption keys for the optional Encryption Module are never included in the *Boot Media* or on a backup (unless they are themselves encrypted). Therefore, if you are creating encrypted backups, then you must be sure to have a Decryption Key Backup available during recovery or else encrypted files will be excluded from restore.

*Backup**EDGE*** supports creating *Bootable Backups* on *SharpDrive*[1], and *Optical* media. Additionally, backups made on tape drives with supported *Bootable Tape* BIOSes may also be made bootable.

It is also possible to create *Optical Boot Media* on a machine without a writer. The *Boot Media* created by *Recover**EDGE*** is a standard ISO image that may be copied to any other computer with CD writing software and burned onto any optical media. If the system with the optical drive also has *Backup**EDGE*** installed, you may instruct *Recover**EDGE*** to create the media there live across the network.

27.3 - Limitations - Media

Floppy Diskette

On Linux, OSR6 and UW7 it is not possible to create *Recover**EDGE*** floppy diskettes, You must use one of the other media types.

1. Linux 2.6.x kernels only.

On *OSR5* optical media is the only currently supported media type. Floppy Diskette may still work but is unsupported. It takes a minimum of three diskettes to make *Recover**EDGE*** media. These are called the *Boot Diskette*, the *Filesystem Diskette*, and the *Misc Diskette*.

It is possible to have a system with a kernel, *Device* drivers or modules that are too large to fit on floppy diskettes. Although *Recover**EDGE*** has many tuning options to accommodate this, sometimes “too big” is really “too big”. In these cases, one of the other *Boot Media* choices will almost always work.

Floppy disks boot relatively slowly.

Optical

These *Device*s require that the system BIOS (Basic Input / Output Section, or boot code) be able to boot directly from a CD-ROM. If the *Device* is SCSI, the host adapter must also support CD-ROM booting.

SharpDrive (Linux)

These *Device*s require that the system BIOS (Basic Input / Output Section, or boot code) be able to boot directly from a USB (or SATA) hard drive, as required by your device type.

Bootable Tape Drives

Bootable Tape drives work by making the tape drive emulate a CD-ROM during the boot phase. Therefore, the tape drives, the system BIOS, and the SCSI host adapter must all support CD-ROM booting.

NOTE: *Recover**EDGE*** supports *OBDR* bootable backups on Hewlett Packard DDS and Ultrium tape drives at this time. Although the HP Surestore DLT vs80 tape drive is also available with *OBDR* in the firmware, its performance at the fixed hardware block size of `2048` required to work with *Recover**EDGE*** is very poor. We highly recommend using boot floppies or optical media and using variable (0) block size and a high (at least 256) *Backup**EDGE*** block size when using this or any other DLT based *Device*. See the device compatibility pages on the Microlite web site for the most current *Bootable Tape Drive* information.

27.4 - Limitations - Operating System

Linux

*Recover**EDGE*** supports BIOS-based and UEFI-based booting depending on the Linux version and release.

- See the Linux Support Tables on the Microlite Web Site for more information.
- See the Linux UEFI Support Page on the Microlite Web Site for more information.

The LVM2 Logical Volume Manager is supported under Linux 2.6 and later kernels.

Systems using special features such as GPT and software RAID are supported only on select operating systems. Please see the See the Linux Support Tables, the Linux GPT Support Page, and the Linux UEFI Support Page on the Microlite Web Site for more information.

All optical *Devices* are supported.

Automounters should be **disabled** within the operating system and / or *GUI* desktops when optical media and / or removable disk / flash media is being used.

5.0 Kernels start forcing asynchronous disk discovery on bootup. This can have unintended consequences if non-system drives are plugged into the system during bootup. Please ensure that

all USB hard drives are not being used and mounted by your operating system by default are unplugged during boot up. This will ensure that the devices are created in a sane fashion which recoverEDGE can process

OSR6

Systems using software RAID solutions are not supported for disaster recovery.

OSR5

Systems using software RAID solutions are not supported for disaster recovery.

Only SCSI *CD-R*, *CD-RW*, and *DVD Devices* are supported on releases prior to 5.0.6. 5.0.6 and 5.0.7 require the appropriate OpenServer supplements to work with non-SCSI devices.

Even if the *Secure Shell* option was selected during installation, *Remote Device* support while booted from the *Boot Media* is handled through *Remote Shell* commands.

USB OBDR Booting is not supported.

UW7

Systems using software RAID and Logical Volume Manager (LVM) solutions are not supported for disaster recovery.

UW7 is only supported for disaster recovery under releases 7.1.4 or later.

USB OBDR Booting is not supported.

27.5 - Making Boot Media and / or Boot Images

The following types of boot media or boot images may be created...

Boot Media

These are the floppy diskettes, *SharpDrive, or Optical* media used along with tape or other archives. You boot from the *Boot Media*, then restore from the archive.

Boot Images

Boot Images are the equivalent of the *Boot Media*. However, no actual media is used when they are created. Instead, the image is stored in the *Backup**EDGE** Directory* tree for one of two purposes...

Boot Images for Remote Burning

These are *Bootable ISO Image* of the *Optical Boot Media* described above. The ISO image that is created can be copied to and burned any PC or other system with a CD-Recordable *Device*. This allows you to take advantage of the boot speed and media longevity of optical media, without having to install a writer in every system.

When you create a *Bootable ISO Image*, it is saved as:

```
/usr/lib/edge/recover2/images/cdrom.iso
```

Copy this file to any other machine with software capable of directly burning an ISO image and make your *optical media*. Be sure to test the image.

Remember to re-create your *Bootable ISO Image* any time your kernel configuration changes.

Boot Images for Bootable Backups

Again, no actual media is used when these images are created. Instead, the image is stored in the *Backup**EDGE** Directory* tree, and added to each nightly backup that is to be made bootable. This of course requires that the backup will be performed on a *SharpDrive*, *Optical*, or *Bootable Tape* capable *Device*.

If you are making images for bootable optical or SharpDrive backups, you should also read “Making Bootable SharpDrive / Optical Drive Backups” on page 289. *Bootable Tape Drive* users should also read “Making Bootable Tape Backups” on page 290.

Selecting a Default Resource

When *Recover**EDGE** Boot Media* or *Boot Images* are created, they set the *Primary Resource* currently shown in *EDGEMENU* as the default storage *Resource* for restores. If this is not currently set correctly, go to `EDGEMENU: Admin -> Set Default Backup Resource` and use **FastSelect** to temporarily set the correct *Primary Resource*. The *Primary Resource* may be configured to be a *Resource* on a remote system.

Launching RecoverEDGE

From *EDGEMENU*, select `Setup -> Make RecoverEDGE Media`

```
+ Edgemenu for BackupEDGE ------------------------------------------------------+
¦+-----------------------------------------------------------------------------+¦
¦¦ [File] [Backup] [Restore] [Verify] [Admin] [Setup] [Schedule]               ¦¦
¦+-----------------------------------------------------------------------------+¦
|-------------------------------------------|[Activate BackupEDGE]      |----|
|                                           |[Make RecoverEDGE Media]   |    |
|                                           |[Disable Advanced]         |    |
|                                           |---------------------------|    |
|                                           |[Configure BackupEDGE]     |    |
|                                           +---------------------------+    |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|+---------------------------------------------------------------------------+|
||Primary Resource : web2v:url!url0                                          ||
||  Compress: None, HW Block:  N/A, Edge Block:   64, Partition: C           ||
||                                                                           ||
||                                                                           ||
||                                                                           ||
||Last Master Backup: Tuesday Sep 10 22:00:01 2019                          ||
|+Local Machine: web2v.microlite.com  Administering: web2v.microlite.com -----+|
+Create Boot Media (re2)---------------------------------------------------------+
```

From the command line prompt (as `root`), you may also launch *Recover**EDGE*** by typing

```
# re2
```

NOTE: *Recover**EDGE*** for OSR5 runs in the character interface only at this time.

Linux and *UW7* users may proceed to page 286.

Media and Images - OSR5

When you launch *Recover**EDGE*** you’ll be presented with a pop-up list of choices about the type (floppy, CD-R/RW, etc.) of *Boot Media* or *Media Image* to be created, and where it is to be booted from.

Sample Pop-Up Media Menu (OSR5)

```
+-What Kind of Recovery Media/Image (F2 to Exit)?-+
¦ (Keep Current Settings)                         ¦
¦ Floppy Drive 0 - 3 1/2"                         ¦
¦ Image Only for cdrom0 Bootable Backups          ¦
+-------------------------------------------------+
```

For example, if your system contains a Floppy Drive and a CD-ROM drive, you will be presented with two options: making floppy diskettes or making a CD-ROM *Boot Image* to be booted from your CD-ROM drive. You are not given the choice to actually make media on the CD-ROM since it is not able to write. You would be able to burn the image with a CD-R/RW drive on another system. Here is an example with a lot of choices.

```
+-What Kind of Recovery Media/Image (F2 to Exit)?-+
¦ (Keep Current Settings)                         ¦
¦ Floppy Drive 0 - 3 1/2"                         ¦
¦ Boot Media on cdrom0                            ¦
¦ Image Only for cdrom0 Bootable Backups          ¦
¦ Boot Media on dvd0                              ¦
¦ Image Only for dvd0 Bootable Backups            ¦
¦ Boot Media on rev0                              ¦
¦ Image Only for rev0 Bootable Backups            ¦
¦ Bootable backup Tape Image                      ¦
+-------------------------------------------------+
```

Under 5.0.7, you'll have a choice of floppy types...

```
+-What Kind of Recovery Media/Image (F2 to Exit)?-+
¦ (Keep Current Settings)                         ¦
¦ 3.5" 1.44MB Floppy Diskette                     ¦
¦ 3.5" 1.68MB Floppy Diskette                     ¦
¦ Boot Media on cdrom0                            ¦
¦ Image Only for cdrom0 Bootable Backups          ¦
¦ Boot Media on dvd0                              ¦
¦ Image Only for dvd0 Bootable Backups            ¦
¦ Boot Media on rev0                              ¦
¦ Image Only for rev0 Bootable Backups            ¦
¦ Bootable backup Tape Image                      ¦
+-------------------------------------------------+
```

Select the desired *Boot Media* or *Boot Image* type and press `[Enter]`.

NOTE: Always attempt to use 1.44MB floppies before higher densities. They tend to boot faster. Use higher density only if all of the recovery tools won't fit. Always allow *Recover**EDGE*** to format your floppies.

OSR5 Menu

```
 [Generate]  Reports    Configure    View    Monochrome   About    Quit
Generate Boot And Filesystem Diskettes




+-------------------------------------------------------------------------+
¦ Configuration For System: dev507        Operating System:   SCO OpenServer 5 ¦
¦ Create Boot Diskette:     Yes           Format Diskettes:   Yes             ¦
¦ Create Filesys Diskette:  Yes           Verify Diskettes:   Yes             ¦
¦ Create Misc Diskette:     Yes           Create Diskette On: 3.5" 1.44MB Flpy ¦
¦ BTLD Support Enabled:     Yes           (Misc Disk is Now   * required *    ¦
+-------------------------------------------------------------------------+
 RecoverEDGE Data Recovery System 03.01.05  (c) 1993-2013 MICROLITE CORPORATION
```

The bottom of the screen displays the type you chose, or in other words, what will happen if the `[Generate]` button is pressed. In this case, a *Boot Diskette, Filesystem Diskette* and *Misc Diskette* will be created. All diskettes will be formatted and verified.

NOTE. Under older version of *Recover**EDGE*** for OSR5, the third diskette was an optional *Network Diskette*. Under this release, **the third diskette contains tools necessary for recovery, and is mandatory** whether or not networking is enabled.

Insert your media if appropriate, and select `[Generate]` to begin making the selected *Boot Media* or *Boot Image*, and follow the prompts.

We highly recommend that, after `[Generate]` is complete, you go to the `[Reports]` menu and print and save the report that is generated along with your media. This report provides an excellent snapshot of the configuration of your system.

We also very strongly suggest that you boot from your disaster recovery media, go into the `Utilities` menu, and read from an archive each time you generate new media. **If you don't do this, you should assume that your media do not work.**

Changing The Media Type - OSR5

The Pop-Up Menu when you start *Recover**EDGE*** is usually the easiest and fastest way to choose a *Boot Media* or *Boot Image* type, unless you are writing to a *Remote Resource*.

To manually change the media type from the default selected when you started *Recover**EDGE***, press `[Configure]`, place the cursor on the `"Boot From" Drive:` prompt, and press `[Space]` until the proper *Resource* appears.

Configure Screen - Set at Floppy

```
+-------------------------------------------------------------------------+
¦              RecoverEDGE Image Creation Configuration Menu              ¦
¦GENERAL--------------------------------------------------------------------¦
¦ Create Boot Image:         Yes    Format Diskettes:         Yes          ¦
¦ Create Filesystem Image:   Yes    Verify Diskettes:         Yes          ¦
¦ Create Misc.   Image:      Yes    "Boot From" Drive:        3.5" 1.44MB Flpy
¦ Enable BTLD Support:       Yes    Diskette Interleave:      0            ¦
¦BOOT IMAGE-----------------------------------------------------------------¦
¦ Include Following Boot String Types: ct=                                 ¦
¦ DMA_EXCL:  Allow Multiple DMA Channels                                   ¦
¦ NBUFS:         0  (Auto: 8192K)                                          ¦
¦FILESYSTEM IMAGE-----------------------------------------------------------¦
¦ FS Image Inodes: 1024    FS Ramdisk Size (512-byte blocks): 16384        ¦
¦ Tape Daemon Path:                                                        ¦
¦ Tape Daemon Command Line:                                                ¦
¦MISCELLANEOUS--------------------------------------------------------------¦
¦ Report Print Command: lp -s                                              ¦
¦ Enable Network Support:  Yes                                             ¦
¦-------------------------------------------------------------------------¦
¦   F2 Ignore Changes,   F3 - Save/Done,   F5 - Re-load                    ¦
¦   F4 - Accept For This Session Only   F6 - Edge 'SPECIAL' Boot String    ¦
+Space Bar Toggles Choices---------------------------------------------------+
```

Configure Screen - Set at cdromo

```
+-------------------------------------------------------------------------+
¦              RecoverEDGE Image Creation Configuration Menu              ¦
¦GENERAL--------------------------------------------------------------------¦
¦ Create Boot Image:         Yes    Format Diskettes:         Yes          ¦
¦ Create Filesys    Image:   Yes    Verify Diskettes:         Yes          ¦
¦ Create Network Image:      Yes    "Boot From" Drive:        optical0     ¦
¦ Enable BTLD Support:       Yes    "Create On" Drive: optical0            ¦
¦BOOT IMAGE-----------------------------------------------------------------¦
¦ Include Following Boot String Types: ct=                                 ¦
¦ DMA_EXCL:  Allow Multiple DMA Channels                                   ¦
¦ NBUFS:         0  (Auto: 8192K)                                          ¦
¦FILESYSTEM IMAGE-----------------------------------------------------------¦
¦ FS Image Inodes: 1024    FS Ramdisk Size (512-byte blocks): 16384        ¦
¦ Tape Daemon Path:                                                        ¦
¦ Tape Daemon Command Line:                                                ¦
¦MISCELLANEOUS--------------------------------------------------------------¦
¦ Report Print Command: lp -s                                              ¦
¦ Enable Network Support:  Yes                                             ¦
¦-------------------------------------------------------------------------¦
¦   F2 Ignore Changes,   F3 - Save/Done,   F5 - Re-load                    ¦
¦   F4 - Accept For This Session Only   F6 - Edge 'SPECIAL' Boot String    ¦
+Space Bar Toggles Choices---------------------------------------------------+
```

When you choose an *Optical Resource*, the `Diskette Interleave:` field changes to `"Create On" Drive:`. There are three possibilities for this field...

- Leave the field blank to create an *Image* (disk file) only.
- Type the name of the local *Resource*. This is almost always exactly the same *Resource* as indicated in the `"Boot From" Drive:` field, but you **must** type it in if you want to actually create *Boot Media* in *Recover**EDGE***. If this field is blank, *Recover**EDGE*** will create a *Boot Image* only.
- Type in the name of a *Remote Resource*. This is used for creating the *Boot Media* on a remote system. For instance, you would type `mlite:optical0` to create a bootable *CD-R* or *CD-RW* on the second cdrom *Resource* on system `mlite`.

Media and Images - Linux / OSR6 / UW7

When you launch *Recover**EDGE***, it will perform extensive checks to make sure that it can create usable *Boot Media* or *Boot Images*. This includes scanning all of the appropriate modules directories on your system.

This can take a while, especially on Linux systems where all of the modules are compressed. On Linux you'll get the message:

```
Analyzing the Kernel - Please Wait! This may take a few moments…
```

Please be patient.

When the scan is finished, you'll be presented with a pop-up list of choices about the type (floppy, optical, etc.) of *Boot Media* or *Media Image* to be created, and where it is to be booted from.

Sample Pop-Up Media Menu (Linux / OSR6 / UW7)

```
+ Select RecoverEDGE Media / Image Type ----------------------------------+
|+-------------------------------------------------------------------------+|
||-> (Keep Current Settings)                                               ||
||   Images Only for optical0 Bootable Backups, Burn on Any CD-R[W]        ||
||                                                                         ||
|+-------------------------------------------------------------------------+|
+ Press [F2] to Exit, [UP] / [DOWN] / [ENTER] to Select -------------------+
```

For example, if your system contains an Optical Drive, you will be presented with the option of making an Optical *Boot Image*. You are not given the choice to actually make media on the optical drive since it is not able to write. You would be able to burn the image with an optical drive on another system. Here is an example with a lot of choices..

```
+ Select RecoverEDGE Media / Image Type ----------------------------------+
|+-------------------------------------------------------------------------+|
||-> (Keep Current Settings)                                               ||
||   Boot Media on optical0                                                ||
||   Images Only for optical0 Bootable Backups                             ||
||   Bootable Backup Tape Image                                            ||
||                                                                         ||
|+-------------------------------------------------------------------------+|
+ Press [F2] to Exit, [UP] / [DOWN] / [ENTER] to Select -------------------+
```

Linux users configured for SharpDrive backups will see...

```
+ Select RecoverEDGE Media / Image Type ----------------------------------+
|+-------------------------------------------------------------------------+|
||-> (Keep Current Settings)                                               ||
||   Boot Media on optical0                                                ||
||   Images Only for optical0 Bootable Backups                             ||
||   Boot Media on Sdrive0                                                 ||
||   SharpDrive Boot Files for SharpDrive Booting                          ||
||   Bootable Backup Tape Image                                            ||
||                                                                         ||
|+-------------------------------------------------------------------------+|
+ Press [F2] to Exit, [UP] / [DOWN] / [ENTER] to Select -------------------+
```

The *RecoverEDGE* main menu for these platforms is similar.

```
+ RecoverEDGE Media Generator ------------------------------------------------+
|+-----------------------------------------------------------------------------+|
|| [Make Media] [Configure] [Options] [Report] [About] [Quit]                  ||
|+Write Boot Media / Image-----------------------------------------------------+|
|+-----------------------------------------------------------------------------+|
||                                                                             ||
||                                                                             ||
||                                                                             ||
||                                                                             ||
||                                                                             ||
||                                                                             ||
||                                                                             ||
||                                                                             ||
||                                                                             ||
||                                                                             ||
||                                                                             ||
||                                                                             ||
|+-----------------------------------------------------------------------------+|
||Create Node: optical0      OS: Linux version 2.6.32-754.1 BIOS: Enabled      ||
||Temp Device: /dev/loop0    System: web2v.microlite.com                       ||
||Format: Yes  P2V: YES      Kernel: /boot/vmlinuz-2.6.32-754.17               ||
||                                                                             ||
|+-----------------------------------------------------------------------------+|
+RecoverEDGE Recovery System 03.03.01 (c) Copyright 1997-2020 by Microlite Corp.
```

The bottom of the screen displays the type you chose, or in other words, what will happen if the `[Make Media]` button is pressed. In this case, *Optical Media* will be created.

Insert your media if appropriate, and select `[Make Media]` to begin making the selected *Boot Media* or *Boot Image*, and follow the prompts.

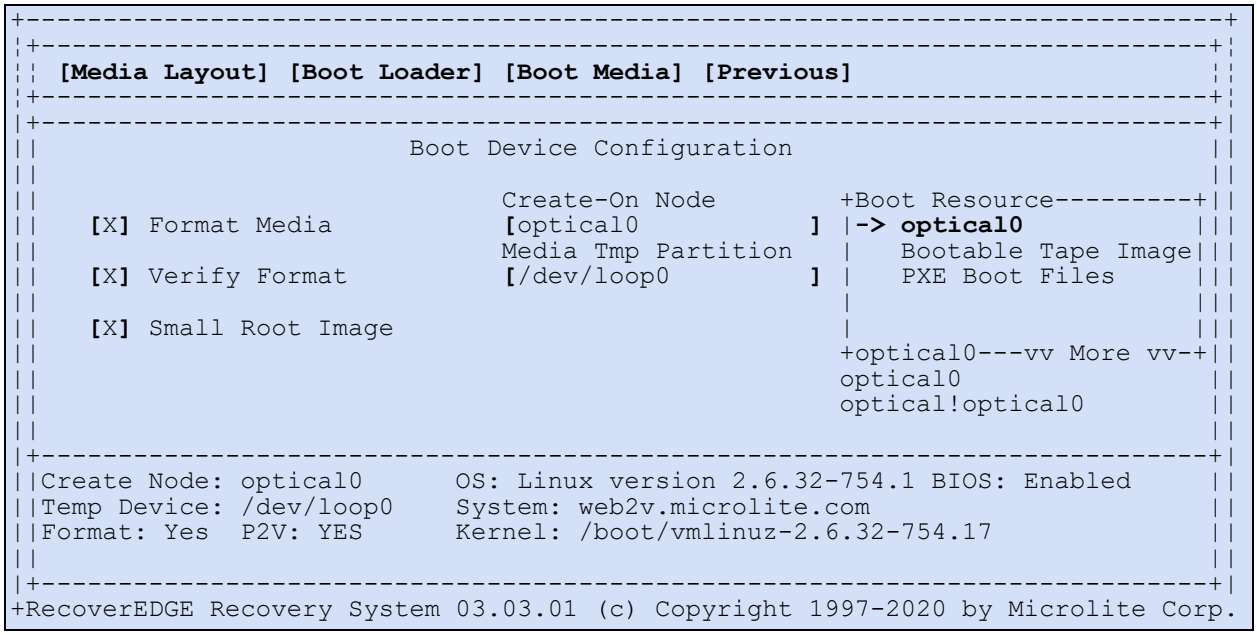
We highly recommend that, after `[Make Media]` is complete, you go to the `[Report]` menu and print and save the report that is generated along with your media. This report provides an excellent snapshot of the configuration of your system.

We also very strongly suggest that you boot from your disaster recovery media, go into the `Test Media` menu, and run the test, each time you generate new media. **If you don't do this, you should assume that your media do not work.**

Changing The Media Type - Linux / OSR6 / UW7

The Pop-Up Menu when you start *RecoverEDGE* is usually the easiest and fastest way to choose a *Boot Media* or *Boot Image* type, unless you are writing to a *Remote Resource*.

To manually change the media type, press [Configure], then [Boot Media]. Press [Tab] to put the cursor in the Boot Resource field, and use the arrows to select the proper *Resource*.



This example shows the first *Optical Media Resource* being selected (optical0).

After the proper *Resource* is selected, press [Tab] to return to the top menu bar, then press [Previous] until you get back to the main menu. Press [Make Media] to begin creating the desired media type.

- Selecting the *Resource* sets the Create-On Node automatically.
- You may type in the name of a *Remote Resource*. This is used for creating the *Boot Media* on a remote system. For instance, your would type mlite:optical1 to create bootable *optical media* on the second optical *Resource* on system mlite.
- Blank the Create-On Node field to create an *Image* (disk file) only. When the field is totally blank, the Create Node: field on the lower left will display CD/DVD Image as confirmation.

27.6 - Making Bootable SharpDrive / Optical Drive Backups

To make *Bootable SharpDrive or Optical Drive Backups*, you must follow the following rules...

- You must have a current *Media Image* created for your *Device*.
- You must have the Attempt Bootable field under the Advanced Properties (Notify/Advanced) window of a *Basic Schedule* (see “Basic Schedules” on page 212) or *Advanced Schedule* (see “Scheduling - Advanced” on page 220) set to **X**. (Under *EDGEMENU -> Full Unscheduled Backup*, you would check the Make Device Bootable flag.)

NOTE: You must test your first *Bootable Backup*. Boot the system from the *Bootable Backup* and use the *Test Media* utility to read through your complete backup. This helps to assure that everything will work when you need it most.

Most computers have the system BIOS set to boot from the *SharpDrive* or *Optical Drive* prior to the hard drive during power up.

When first in the boot order and power fails in normal mode, when there is a bootable backup in the *SharpDrive* or *Optical Drive*, the server will boot from the *SharpDrive or Optical Drive* media to the *Recover**EDGE*** boot screen (just to the boot prompt, not to the menu) when power

is restored. We recommend adjusting your system BIOS to boot from the hard drive first, and only change it to boot from the *SharpDrive or Optical Drive* if a disaster recovery is needed.

Remember that if you are using the optional Encryption Module, then you must also have a separate Decryption Key Backup available with the appropriate decryption key on it, in order to restore encrypted files. Neither the *Boot Media* nor a *Bootable Backup* will contain (unencrypted) decryption keys.

27.7 - Making Bootable Tape Backups

To make *Bootable Tape Backups*, you must follow the following rules...

- You must have a current *Media Image* created for your *Device*.
- *Bootable Tape Drives* must have their hardware, or *Tape Block Size*, set at `2048` in order to be bootable. Set this in the *Resource Manager*.
- You must have the `Attempt Bootable` field under the `Advanced Properties` (`Notify/Advanced`) window of a *Basic Schedule* (see “Basic Schedules” on page 212) or *Advanced Schedule* (see “Scheduling - Advanced” on page 220) set to **X**. (Under *EDGEMENU -> Full Unscheduled Backup*, you would check the `Make Tape Bootable` flag.)

NOTE: You must test your first *Bootable Backup*. Boot the system from the *Bootable Backup* and use the *Test Media* utility to read through your complete backup. This helps to assure that everything will work when you need it most.

Bootable Tape Devices don’t actually write the header information required to make a tape bootable until the media is unloaded after a backup. We recommend that you set the unload strategy on your *Scheduled Jobs* to always unload the media after a backup.

Always remember to unload *Bootable Tapes*, either with the eject button or via software command. Never just turn off the power with a tape in the *Device*.

Remember that if you are using the optional Encryption Module, then you must also have a separate Decryption Key Backup available with the appropriate decryption key on it, in order to restore encrypted files. Neither the *Boot Media* nor a *Bootable Backup* will contain (unencrypted) decryption keys.

27.8 - Additional Documentation

This manual covers only the basics of making *Disaster Recovery Media*. On the installation CD-ROM and on the *Microlite* ftp site (`http://www.microlite.com/documentation/documentation.html`) there is a comprehensive *Recover**EDGE** Technical Reference Manual* in PDF format.

28 - Disaster Recovery - Booting From The Media

There are two reasons for booting from the *Disaster Recovery Media*: testing the media and actually performing a *Disaster Recovery*.

Newly created *Boot Media* should be tested to...

- ensure that it will boot when required,
- make sure that your *Backup Media* can be successfully read while booted from the *Boot Media*, and
- test to ensure that modem or network based *Disaster Recovery* will function if needed.

If you are creating *Bootable Backups*, we highly recommend that you test at least the first backup created after updating your *Boot Images*.

Also remember that if you are using encrypted backups made with the optional Encryption Module, then you must have a *Decryption Key Backup* available in addition to the *Boot Media* and *Backup Media*, or *Bootable Backup* if you want to restore encrypted files.

This section describes booting from the *Boot Media* into the main *Recover**EDGE** Disaster Recovery Menu*. After booting, go to “Disaster Recovery - Testing The Media” on page 295 to test the archive media, or “Disaster Recovery - Recovering a System” on page 298, which describes the basics of performing *Disaster Recovery*.

28.1 - Booting From Boot Media or Bootable Backups

Before booting from your *Disaster Recovery* Media, you should make sure you have inserted the *Master Backup* media that will eventually be used for the restore (if it is not the actual *Disaster Recovery* media). This allows *Backup**EDGE*** to match proper *Tape Block Size* during *Device* initialization.

SharpDrive / Optical

To boot from *SharpDrive* or *Optical Boot Media* or *Bootable Backups*, make sure the correct media is in the drive when you power up or reboot.

For Optical media, your BIOS must be set to boot from the CDROM drive (that’s how it sees CD, DVD, and Blu-ray Disc *Devices*). All USB FSP / SharpDrive and Tape devices should remain unplugged until the main *Recover**EDGE*** menu is reached, then plugged in.

For *SharpDrive* media, your BIOS must be set to boot from the appropriate USB or SATA hard drive first.

All *SharpDrives* (except the one you are booting from if you are booting from a *SharpDrive*) should be ejected / unplugged until you are completely booted and reach the *Recover**EDGE*** main menu.

During the boot process, you’ll be asked to unplug / eject the *SharpDrive* media and press `[Enter]`. **All** *SharpDrives* must be unplugged or ejected at this time. After the recovery system is prepared, you’ll be asked to re-plug / re-insert it (or them).

During recovery, *Backup**EDGE*** will ignore the resource name when looking at *SharpDrive* media. It will pretend that all media has been initialized for use with whatever *SharpDrive* resource it has been told to access.

OBDR Tape

To boot from an OBDR *Bootable Backup*, you must power down the system, then hold down the `Eject` button for five seconds while powering up the tape drive (or system if it is internal) to put it in OBDR mode. The media may be in the drive when you power up, or it may be inserted after power up, but before the host adapter BIOS scans the *Device*.

Your BIOS must be set to boot from the SCSI CDROM drive (that's how it sees the OBDR *Device*) **first**. On systems with an OBDR tape drive, but an ATAPI (IDE) CDROM drive, SCSI CDROM booting may be disabled in the BIOS. The BIOS may only detect a SCSI CDROM *Device* while the tape drive is in OBDR mode. If your BIOS exhibits this behavior, so you will need to...

- power up the drive in OBDR mode.
- go in to the BIOS and enable SCSI CDROM booting.
- exit the BIOS and restart without powering down.

On some system, booting into OBDR mode involves selecting OBDR directly from the boot BIOS (USB devices) or by pressing `[F8]` at the host adapter BIOS prompt.

USB Tape

All USB tape devices should remain unplugged until the main *Recover**EDGE*** menu is reached, then plugged in.

28.2 - Booting into OSR5

When you power up the machine with the appropriate *Boot Media* inserted, you'll get a standard `boot:` prompt. From this prompt, there are four options...

- Press `[Enter]`. This will boot into the *Recover**EDGE*** main menu, with no network or modem capabilities enabled (these may be enabled later from within the menu).
- Type `modem [Enter]`. This will boot into the *Recover**EDGE*** main menu, with modem capabilities enabled automatically.
- Type `network [Enter]`. This will boot into the *Recover**EDGE*** main menu, with network capabilities enabled automatically. You'll be prompted to change the network settings or leave them at the defaults.
- Use a `link` command to add a *Boot Time Loadable Device Driver* (*BTLD*). This allows a host adapter driver to be changed during Disaster Recovery. Link commands may be combined with the `network` and `modem` boot directives.

If using floppies, you'll be prompted for the filesystem diskette and network diskette at the appropriate time. If using BTLDs, you'll be prompted for the BTLD diskettes.

When all media have been loaded, the *Recover**EDGE*** main menu will be launched.

RecoverEDGE Menu - OSR5

```
 Configure  Restore  Utilities  Automatic  Monochrome  About  Network  Quit
Configure / Reconfigure Hard Disk(s)
+------------------------------------------------------------------------------+
¦ Drive Type &   CAP.   DKINIT    BADTRK OR           ¦   FDISK               ¦
¦ Host Adapter   (mb)  or DPARAM  SCSIBADBLK   FDISK  ¦ PART.(mb)     DIVVY   ¦
¦-----------------------------------------------------------------------------¦
¦  0 SCSI blad   0       ========   Not Done   Not Done    1 1735     Not Done ¦
¦                                                                              ¦
+F1: HELP    F2: QUIT-------------------------------------------- --- --- ---  +
```

The above example is from a system with a single SCSI hard drive.

28.3 - Booting into Linux

When you power up the machine with the appropriate *Boot Media* inserted, you'll get a *Recover**EDGE** Splash Screen*. From this prompt, there are up to three options...

- Press `[Enter]`. This will boot into the *Recover**EDGE*** main menu, with no network or modem capabilities enabled (these may be enabled later from within the menu).
- Type `modem [Enter]`. This will boot into the *Recover**EDGE*** main menu, with modem capabilities enabled automatically.
- Type `network [Enter]`. This will boot into the *Recover**EDGE*** main menu, with network capabilities enabled automatically. You'll be prompted to change the network settings or leave them at the defaults.

If using floppies, you'll be prompted for the *Root Diskette* and *Misc Diskette(s)* at the appropriate time.

If you are booting from a *SharpDrive*, you will be prompted to unplug or eject all *SharpDrive Media* (including the one you booted from) during the boot process. You'll be prompted later to re-plug / re-insert them.

When all media have been loaded, the *Recover**EDGE*** main menu will be launched.

NOTE: In some cases, *Linux* kernel modules (*Device* drivers, etc.), may fail to load. In this case, you will be brought to a `root` prompt (`#`). Run the command `cat /tmp/insmod.err` to see which modules have not loaded. If they are not necessary for *Disaster Recovery*, you may ignore them. Otherwise, you should re-make the media with a different module configuration, and possibly contact Technical Support. Type `exit [Enter]` at the `root` prompt to continue booting into *Recover**EDGE***.

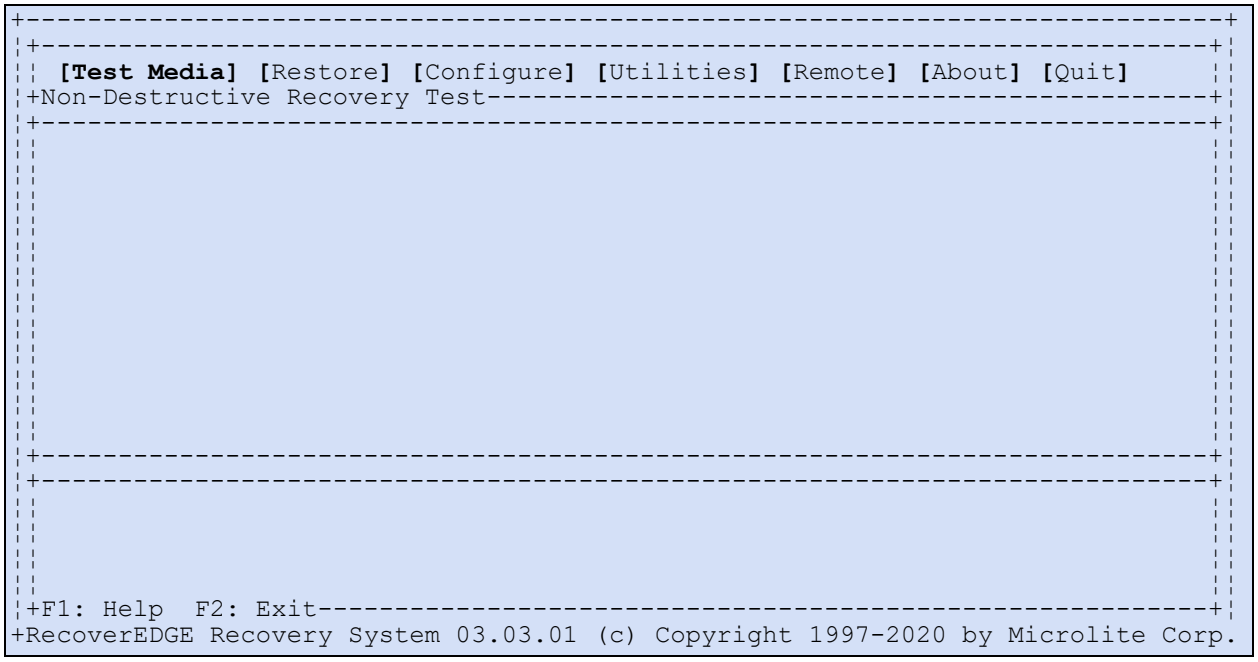
28.4 - Booting into OSR6 / UW7

When you power up the machine with the appropriate *Boot Media* inserted, you'll get a "booting" message and you'll be taken directly to the *Recover**EDGE*** main menu. Please be patient as loading modules takes a few minutes.

If using floppies under UW7, you'll be prompted for the *Root Diskette* and *Misc Diskette(s)* at the appropriate time.

In some cases, *OSR6* and *UW7* dynamic kernel modules (*Device* drivers, etc.), may fail to load. In this case, you will be brought to a `root` prompt (`#`). Run the command `cat /tmp/insmod.err /tmp/automod.err` to see which modules have not loaded. If they are not necessary for *Disaster Recovery*, you may ignore them. Otherwise, you should re-make the media with a different module configuration, and possibly contact Technical Support. Type `exit [Enter]` at the `root` prompt to continue booting into *Recover**EDGE***.

28.5 - RecoverEDGE Menu - Linux / UW7



29 - Disaster Recovery - Testing The Media

29.1 - Testing the Archive Device

To ensure the ability of *RecoverEDGE* to restore data when required, you should always try to list a backup while booted from the *Boot Media* (see page 291).

The backup may be on the *Boot Media* itself (for *Bootable Backups*), or on a local or remote *Resource*.

Remember that if you are using encrypted backups made with the optional Encryption Module, then you must have a Decryption Key Backup available in addition to the *Boot Media* and *Backup Media*, or *Bootable Backup* if you want to restore encrypted files.

Testing an OSR5 Archive

Go to the `Utilities -> Archive Utilities` menu. If you will be testing an encrypted backup, you should first restore the decryption keys from a Decryption Key Backup via the `Read Keys` option. Once you have done that, or if that is not applicable, then you should use the `Test Drive` option. Make sure a valid archive is inserted, and press `[Enter]` through all the defaults.

This procedure lists the entire archive from media. Although a complete test involves reading the entire archive, you may wish to stop the listing after a few minutes if you are satisfied that the media is being read properly. Press the `[Delete]` key to stop the listing and use the `Exit Immediately` option from the ensuing popup menu. In this instance *RecoverEDGE* will indicate that that verify failed, but that is only because it was interrupted.

Testing a Linux Archive

Select `Test Media` from the main menu. You will be prompted to insert the backup media. If the backup contains encrypted files, then you will be prompted to load the decryption keys from a Decryption Key Backup. Remember that these keys are not stored on the *Boot Media*.

This procedure first lists the entire archive from media. Although a complete test involves reading the entire archive, you may wish to stop the listing after a few minutes if you are satisfied that the media is being read properly. Press the `[Ctrl-C]` key to stop the listing and use the `Exit Immediately` option from the ensuing popup menu. In this instance *RecoverEDGE* will indicate that that verify failed, but it will give you the option to ignore the error since it was interrupted.

RecoverEDGE will then attempt to mount all filesystems and access them to be sure that all *Device* drivers have loaded properly. Finally, it records that the *Boot Media* have been tested, and unmounts the filesystems.

If any of these steps fail, you will be notified. In this case, you should treat the *Boot Media* as useless.

Testing an OSR6 or a UW7 Archive

Select `Test Media` from the main menu. You will be prompted to insert the backup media. If the backup contains encrypted files, then you will be prompted to load the decryption keys from a Decryption Key Backup. Remember that these keys are not stored on the *Boot Media*.

This procedure lists the entire archive from media. Although a complete test involves reading the entire archive, you may wish to stop the listing after a few minutes if you are satisfied that the media is being read properly. Press the `[Delete]` key to stop the listing and use the `Exit Immediately` option from the ensuing popup menu. In this instance *RecoverEDGE* will indicate that that verify failed, but it will give you the option to ignore the error since it was interrupted.

*Recover**EDGE*** will then attempt to mount all filesystems and access them to be sure that all *Device* drivers have loaded properly. Finally, it records that the *Boot Media* have been tested, and unmounts the filesystems.

If any of these steps fail, you will be notified. In this case, you should treat the *Boot Media* as useless.

29.2 - Testing Network Connectivity

OSR5

Select `Network -> Network Support -> Init Network Recovery`. Press `[Enter]` through all the defaults, or make changes as necessary. Insert the *Misc Diskette* if prompted. This will initialize the network stack. Usually, the *Misc Diskette* has already been loaded by this point, so you will not need to insert it.

Using an *OSR5* console or other program that emulates the *OSR5* console, telnet into the system on the port chosen in the defaults. When prompted, press `[Ctrl-L]` to take over the test session. Navigate the menus or perform an *Archive Test* (see page 295). Disconnect when you are satisfied that everything works.

If you are doing *Network Backups*, make sure to read an archive made over the network.

Linux

Select `Remote -> TCP/IP Recovery`. Press `[Enter]` through all the defaults, or make changes as necessary. This will initialize the network stack.

Using an *Linux* console or other program that emulates the *Linux* console, telnet into the system on the port chosen in the defaults. When prompted, press `[Ctrl-L]` to take over the test session. Navigate the menus or perform an *Archive Test* (see page 295). Disconnect when you are satisfied that everything works.

If you are doing *Network Backups*, make sure to read an archive made over the network.

OSR6 / UW7

Select `Remote -> TCP/IP Recovery`. Make sure a modem is attached to one of the COM ports. Press `[Enter]` through all the defaults, or make changes as necessary. This will initialize the network stack.

Using an *AT386* console or other program that emulates the *AT386* console, telnet into the system on the port chosen in the defaults. When prompted, press `[Ctrl-L]` to take over the test session. Navigate the menus or perform an *Archive Test* (see page 295). Disconnect when you are satisfied that everything works.

If you are doing *Network Backups*, make sure to read an archive made over the network.

29.3 - Testing Modem Connectivity

OSR5

Select `Network -> Modem Support Init Modem Support`. Make sure a modem is attached to one of the COM ports. Press `[Enter]` through all the defaults, or make changes as necessary. This will initialize the modem and prepare it to answer.

Using an *OSR5* console or other program that emulates the *OSR5* console, dial up the system to be tested. When prompted, press `[Ctrl-L]` to take over the test session. Navigate the menus or

perform an *Archive Test* (see page 295). Disconnect when you are satisfied that everything works.

Linux

Select `Remote -> Modem Recovery`. Make sure a modem is attached to one of the COM ports. Press `[Enter]` through all the defaults, or make changes as necessary. This will initialize the modem and prepare it to answer.

Using an *Linux* console or other program that emulates the *Linux* console, dial up the system to be tested. When prompted, press `[Ctrl-L]` to take over the test session. Navigate the menus or perform an *Archive Test* (see page 295). Disconnect when you are satisfied that everything works.

OSR6 / UW7

Select `Remote -> Modem Recovery`. Make sure a modem is attached to one of the COM ports. Press `[Enter]` through all the defaults, or make changes as necessary. This will initialize the modem and prepare it to answer.

Using an *AT386* console or other program that emulates the *AT386* console, dial up the system to be tested. When prompted, press `[Ctrl-L]` to take over the test session. Navigate the menus or perform an *Archive Test* (see page 295). Disconnect when you are satisfied that everything works.

30 - Disaster Recovery - Recovering a System

Remember that this manual only briefly describes the *Disaster Recovery* process. The on-line *RecoverEDGE Technical Reference Manual* goes in to far more depth, and also covers many areas where you may use you *Boot Media* without actually performing a *Disaster Recovery*. It should be consulted if an actual *Disaster Recovery* must be performed.

30.1 - OK. You've had a disaster. Now what?

RecoverEDGE can put you back together again using one of two methods:

- *Automatic* or *One-Touch Restore*.
- *Configurable Restore*.

RecoverEDGE allows complete control over configuring your hard disks and filesystems. This is discussed in greater detail in the *RecoverEDGE Technical Reference Manual*.

For simple hard drive replacement, or other "just put it back together" types of *Disaster Recovery*, the *One-Touch Restore* method is easier. Simply perform the following steps...

- Identify the problem which resulted in your data loss and have it corrected.
- Boot from your *RecoverEDGE Boot Media* or *Bootable Backup* (see page 291).
- Choose the *Automatic* or *One-Touch* menu, which will prepare your hard drive and prompt you to insert your last backup(s). If you are using an encrypted backup, you must also be able to supply a valid Decryption Key Backup in order to restore the encrypted files.
- Restore your last *Master Backup*.
- Restore your last *Differential Backup*, and any *Incremental Backups* (if you have them and it is more recent than your last *Master Backup*).
- Shut down and re-boot your system.

Linux

From the main *RecoverEDGE* menu, select `Restore -> One-Touch`. You'll be prompted to acknowledge that you are sure you want to do this. When you press `[YES]`, the hard drive will be prepared, you'll be asked to insert your backup media, and the *Disaster Recovery* will proceed.

If you have any encrypted files on the backup, you will be prompted to load the appropriate decryption keys from a *Decryption Key Backup*. If you do not have these keys, then encrypted files will not be restored.

Expected Drive Behavior

NVME/5.0 kernel hard drives 03.05.01 Build 1 and later

Due to the asynchronous disk discovery hard drives are no longer able to be matched to the wire they are attached and may get a different device node during every reboot. Due to this replacing drives are now decided by size. If you have old drives from the system and have to replace a single drive, the old drives will be matched via their filesystem UUID and the new drive will replace the missing one. However if you have to replace multiple drives at once they will be paired to the old drives based on size as compared to the old devices. For example If your original system had a 400 Gigabyte drive (Drive A) and a 1 Terabyte drive (Drive B) and you had to replace both of these with a 1 Terabyte drive and a 2 Terabyte Drive. The 1 Terabyte Drive would be drive A because it is the smaller of the two, and the 2 Terabyte Drive would be Drive B.(Note that the 1 Terabyte drive does not pair with the old 1 Terabyte drive it pairs to the small 400 Gig Drive)

Filesystems will be scaled automatically if the new hard drive is larger than the original.

NOTE: If for any reason you changed a *Resource* definition after you've created *RecoverEDGE* media and *RecoverEDGE* cannot find or initialize the old version of the *Resource*, you may edit the *Resource* definition by going to the *RecoverEDGE* command line and typing: `/tmp/resource` to start the *BackupEDGE Resource Manager*. (03.00.05b6 or later)

Virtualization - Linux P2V - VMware Esxi

Linux P2V (physical to virtual) recovery to VMware is also available in 03.00.07 and later. See "Disaster Recovery - Linux P2V - VMware" on page 300 for additional information.

Virtualization - Linux P2V - Microsoft Hyper-V

Linux P2V (physical to virtual) recovery to Hyper-V is also available in 03.01.03 build 5 and later. See "Disaster Recovery - Linux P2V - Hyper-V" on page 307 for additional information.

OSR6 / UW7

From the main *RecoverEDGE* menu, select `Restore -> One-Touch`. You'll be prompted to acknowledge that you are sure you want to do this. When you press `[YES]`, the hard drive will be prepared, you'll be asked to insert your backup media, and the *Disaster Recovery* will proceed.

If you have any encrypted files on the backup, you will be prompted to load the appropriate decryption keys from a *Decryption Key Backup*. If you do not have these keys, then encrypted files will not be restored.

Filesystems will be scaled automatically if the new hard drive is larger than the original.

NOTE: If for any reason you changed a *Resource* definition after you've created *RecoverEDGE* media and *RecoverEDGE* cannot find or initialize the old version of the *Resource*, you may edit the *Resource* definition by going to the *RecoverEDGE* command line and typing: `/tmp/resource` to start the *BackupEDGE Resource Manager*. (03.00.05b6 or later)

OSR5

From the main *RecoverEDGE* menu, simply select `Automatic`. You'll be prompted to acknowledge that you are sure you want to do this. When you press `[YES]`, the hard drive will be prepared, you'll be asked to insert your archives, and the *Disaster Recovery* will proceed.

If you have any encrypted files on the backup, you will be prompted to load the appropriate decryption keys from a *Decryption Key Backup*. If you do not have these keys, then encrypted files will not be restored.

Filesystems will be scaled automatically if the new hard drive is larger than the original.

31 - Disaster Recovery - Linux P2V - VMware

31.1 - Linux P2V Overview - VMware

NOTE: This feature **does not run in demo mode**. Your *Backup**EDGE*** must be fully registered and activated to use this capability.

Beginning with *Backup**EDGE** 03.00.07*, Linux physical-to-virtual (**P2V**) conversion/recovery is built into *Recover**EDGE***.

31.2 - P2V Pre-requisites - VMware ESXi

- *Backup**EDGE*** 03.00.07 or later *must be licensed and activated*. P2V capability is not available in 60 day demo mode.
- Must be virtualizing to VMware ESXi 5 or later.
- Must be using a supported Linux distribution. 03.00.07 build 1 supports:
  - Red Hat Enterprise Linux 6.x or 5.x.
  - CentOS Server 6.5 or 5.x.
  - Oracle Linux Server 6.x.
- 03.03.00 build 1 and later also supports:
  - Red Hat Enterprise Linux 7.8.
  - CentOS Server 7 .8-2003.
  - Oracle Linux Server 7.8

NOTE: In the 7.x series of these products, P2V conversion is not currently supported if LVM has been used. Only servers with standard filesystems can be converted. Servers must be fully patched to the 7.8 level or later for P2V to be supported.

31.3 - Making RecoverEDGE P2V Media/Images (VMware ESXi)

To make *Recover**EDGE*** images that are capable of P2V conversion...

- Install and license one of the *Backup**EDGE*** releases listed above on the physical server and configure it to store data on something accessible to VMware ESXi.
- Make sure you communicate with the storage device before making media to ensure that any and all drivers are loaded.

NOTE: NAS / FTP server is the recommended and tested storage *Resource*.

- Make new *Recover**EDGE*** optical media or ISO image. Make sure the *Recover**EDGE*** "**P2V:**" notice is set to "**YES**" on the main *Recover**EDGE*** screen. See the bold indication below.

```
+-------------------------------------------------------------------------------+
|+-----------------------------------------------------------------------------+|
|| [Make Media] [Configure] [Options] [Report] [About] [Quit]                  ||
|+Write Boot Media / Image---------------------------------------------------+|
|+-----------------------------------------------------------------------------+|
||                                                                             ||
||                                                                             ||
||                                                                             ||
||                                                                             ||
||                                                                             ||
||                                                                             ||
||                                                                             ||
||                                                                             ||
||                                                                             ||
||                                                                             ||
||                                                                             ||
||                                                                             ||
|+-----------------------------------------------------------------------------+|
|+-----------------------------------------------------------------------------+|
||Create Node: CD/DVD Image  OS: Linux version 3.10.0-1127. UEFI: Enabled     ||
||Temp Device: /dev/loop0    System: ts140.microlite.com                      ||
||Format: Yes  P2V: YES      Kernel: /boot//vmlinuz-3.10.0-1127.              ||
||                                                                            ||
|+-----------------------------------------------------------------------------+|
+RecoverEDGE Recovery System 03.03.01 (c) Copyright 1997-2020 by Microlite Corp.
```

NOTE: If P2V says "**NO**", your release of *Backup**EDGE*** has not been properly registered and activated, or your Linux distribution is not supported by our P2V process.

- If you've made an ISO image, copy it to a location accessible to the VMware console of the virtual server. It's filename is: `/usr/lib/edge/recover2/images/cdrom.iso`.

31.4 - Making Backups for P2V Conversion

- **After** the *Recover**EDGE*** optical media or ISO image have been made, perform a *Master Backup* to the storage resource.
- If desired, after the conversion is complete, you may make a final *Differential Backup* of the physical server and restore it to the virtual server. This will lessen downtime during the conversion.

31.5 - Virtual Machine Creation Guidelines

Create a new, blank virtual machine on the VMware ESXi host, using the following guidelines...

- Set the operating system type to match the name and architecture of the source machine. Recommended:
  - Red Hat Enterprise Linux 7 .x - 64bit
    `Red Hat Enterprise Linux 7 (64-bit)`
  - Red Hat / CentOS / Oracle 6.x - 64bit
    `Red Hat Enterprise Linux 6 (64-bit)`
  - Red Hat / CentOS / Oracle 6.x - 32bit
    `Red Hat Enterprise Linux 6 (32-bit)`
  - Red Hat / CentOS 5.x - 64bit
    `Red Hat Enterprise Linux 5 (64-bit)`
  - Red Hat / CentOS 5.x - 32bit
    `Red Hat Enterprise Linux 5 (32-bit)`

- Set the HBA and NIC to one of the types shown in the table below:

Operating System Category	HBA Type	NIC Type
Red Hat Enterprise Linux 6.x and 7.x	LSI SAS or Paravirtual	E1000 or VMXNET3
CentOS 6.x and 7.x	LSI SAS or Paravirtual	E1000 or VMXNET3
Oracle Linux Server 6.x and 7.x	LSI SAS or Paravirtual	E1000 or VMXNET3
Operating System Category	HBA Type	NIC Type
Red Hat Enterprise Linux 5	LSI SAS	E1000
CentOS 5	LSI SAS	E1000

- **Paravirtual** and **VMXNET3** are the recommended HBA and NIC types for 6.x and 7.x servers.
- Number of virtual hard drives must match physical server hard drives. Virtual hard drives may be larger, but not smaller. Attach to the host adapter you chose above.
- Number of virtual network interface cards (NICs) must match number of physical NICs, at least during the conversion process.
- Make sure the CD-ROM drives settings are similar to those from the original server. We recommend IDE (0:0) if not sure.
- Use VMware ESXi 5 or later. Other VMware products may work but are not tested or supported.
- If the original server was in *BIOS* mode, select *BIOS* under `VM Options` -> `Boot Options` for the VM. It *UEFI*, select *EFI* mode. Make sure *Secure Boot* is disabled.

31.6 - P2V Disaster Recovery Procedure

Restore the *Master Backup* (and optional *Differential Backup*) made at the end of "Making RecoverEDGE P2V Media/Images (VMware ESXi)" on page 300 using this procedure...

- Attach the *Recover**EDGE*** optical media or ISO image to the virtual machine and boot. You may type "`network`" at the boot prompt and initialize the network using a different IP address if the original physical service is still running. Otherwise, shut down the physical server.
- You'll get the following message, indicating that modules from the older server won't load under VMware:

```
RecoverEDGE: An error occurred while loading kernel nodules.
Check /tnp for the file insmod.err, and try to load the modules manually.
Exit the shell to resume normal recovery fron the RecoverEDGE menu.

Type exit Then Press [ENTER] For The RecoverEDGE Menu
```

  You may safely type `exit` and press `[Enter]` to continue.

- If the hard disks on the physical machine are not logical scsi devices (`/dev/sda`, `/dev/sdb` etc.) you will get the following two messages during boot:

```
+WARNING-------------------------------------------+
+                                                  +
+ Your system state appears to be inconsistent     +
+Please use the Configure menu to manually adjust  +
+              fdisk settings, etc.                +
+                                                  +
+                       [Ok]                       +
+--------------------------------------------------+
```

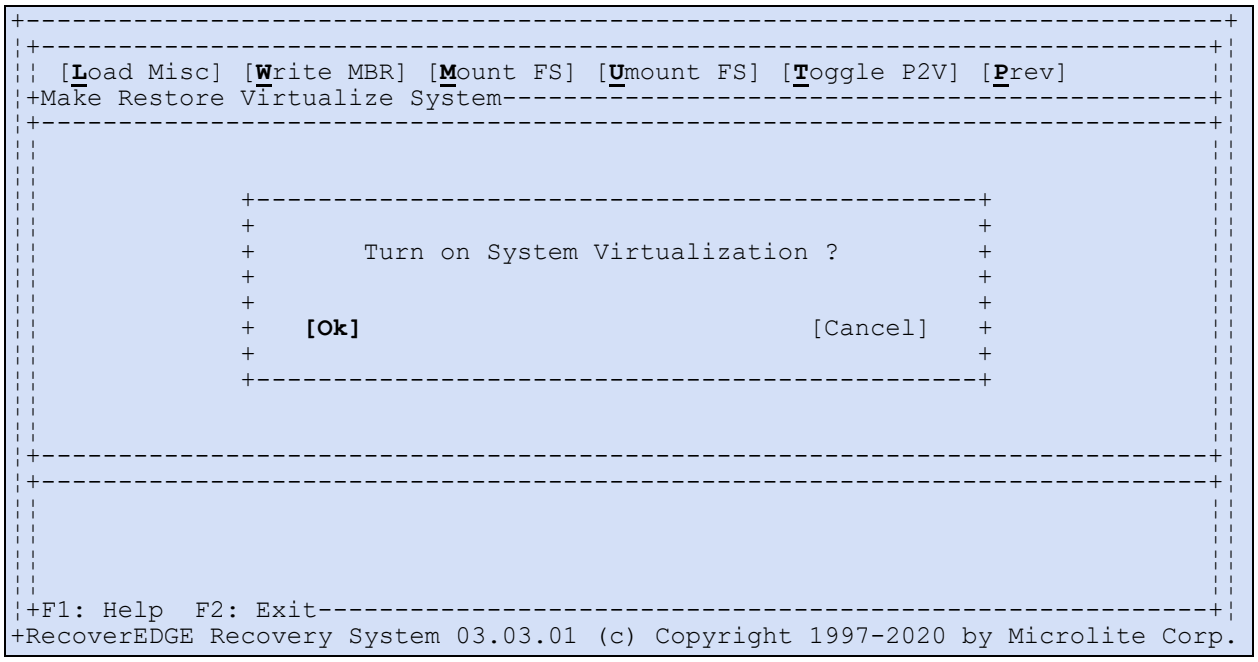
  followed by:

```
+NOTICE--------------------------------------------+
+                                                  +
+       Some Hard Drives Have Been Added           +
+      Please Review The Mapping Status.           +
+                                                  +
+                       [Ok]                       +
+--------------------------------------------------+
```

  In these cases, please see "Drive Mapping" on page 305.

- Test connectivity to the storage resource. Use "**Test Media**" from the main *Recover**EDGE*** menu and read at least part of one of your backups. You may safely ***ignore test result errors*** for part 2 (mounting the hard drive filesystems) as they don't yet exist.

- Turn on **P2V** mode from the *RecoverEDGE* menu. Go to "**Utilities - Other - Toggle P2V**" and answer "**YES**" to the "**Turn on System Virtualization**" prompt. This will ensure that, after restore, the correct HBA driver will be used as the boot driver by the operating system.



- Perform an automatic "OneTouch Restore" to the virtual machine.
- When the restore is finished, you may restore any optional differential backups.
- When all backups have been restored, the operating system on the hard drive will be modified to boot from the appropriate host adapter, and you'll be returned to the main *RecoverEDGE* menu.

NOTE: Various automated error messages may appear during the virtualization phase. You may ignore them, and if necessary, press `[F8]` on the console to restore / refresh the screen.

- Quit *RecoverEDGE*, then power off the **VM** and remove the attached CD-ROM or image.

31.7 - What if I forgot to "Toggle P2V"

If you didn't remember to "Toggle P2V" before doing your restore, you don't have to start over. From the main *RecoverEDGE* menu (either while still booted or after rebooting into the *RecoverEDGE* CD or Image)...

- Go to the "**Utilities - Other"** menu as shown above.
- Select "**Toggle P2V**" and answer "**YES**" to the "**Turn on System Virtualization**" prompt.
- Select "**Prev**" to return to the "Utilities" menu and select "**Exc Loader**".

This will correct the host adapter driver issue. When complete, quit *RecoverEDGE*, then power off the **VM** and remove the attached CD-ROM or image.

31.8 - Booting the Virtualized Operating System

Networking will need to be changed upon first reboot. We recommend booting to single user mode and running your favorite tool to correct any networking issues.

Remember, if you are going to keep the same IP address, shut down the physical server first.

- Boot the **VM**.

- Run the operating system networking commands and fix any networking issues. from the command line this command is usually:

  ```
  system-config-network-tui
  ```

  or

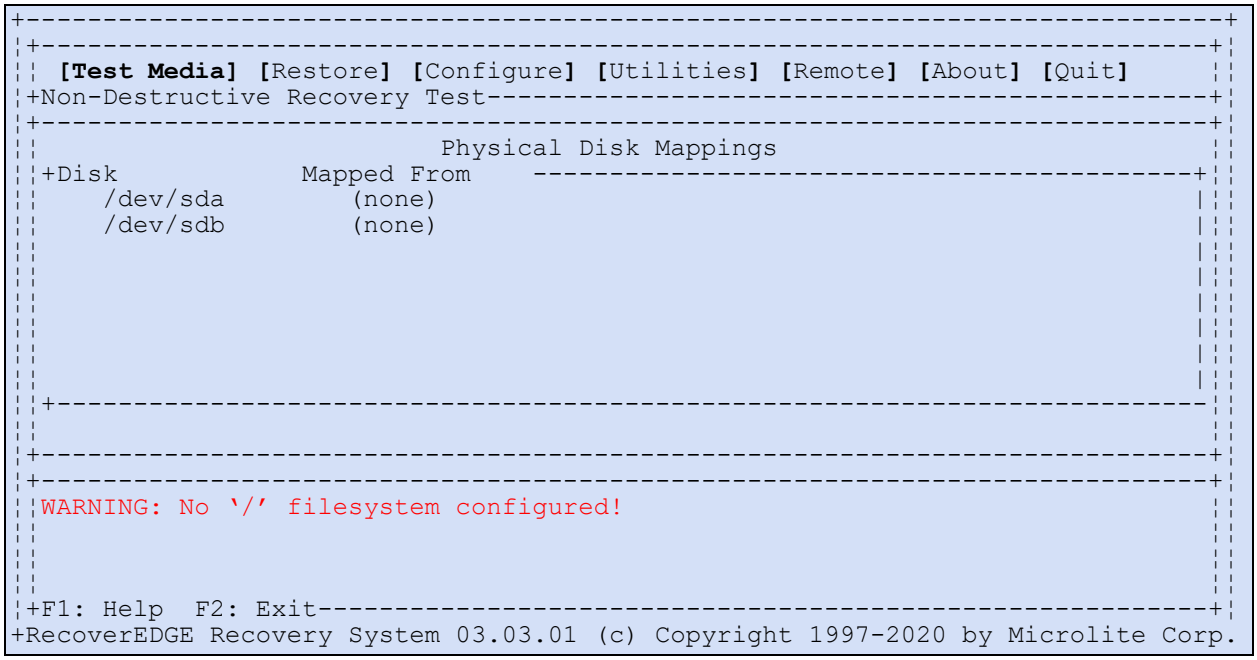
  ```
  nmtui
  ```

  although some linux variants are different, and in some cases people prefer to make manual changes.
- You'll probably have to remove the old network adapter (NIC) and add in a new one to have Linux detect the proper VMware NIC.
- Adjust any IP address information, name servers, hostname information, etc.
- Reboot and go into multi-user mode.

Changing the hostname will invalidate the *BackupEDGE* license, but if you are under a valid ***Support and Maintenance Subscription*** there is no charge to have it re-activated on the **VM**, as long as the old server will no longer be used.

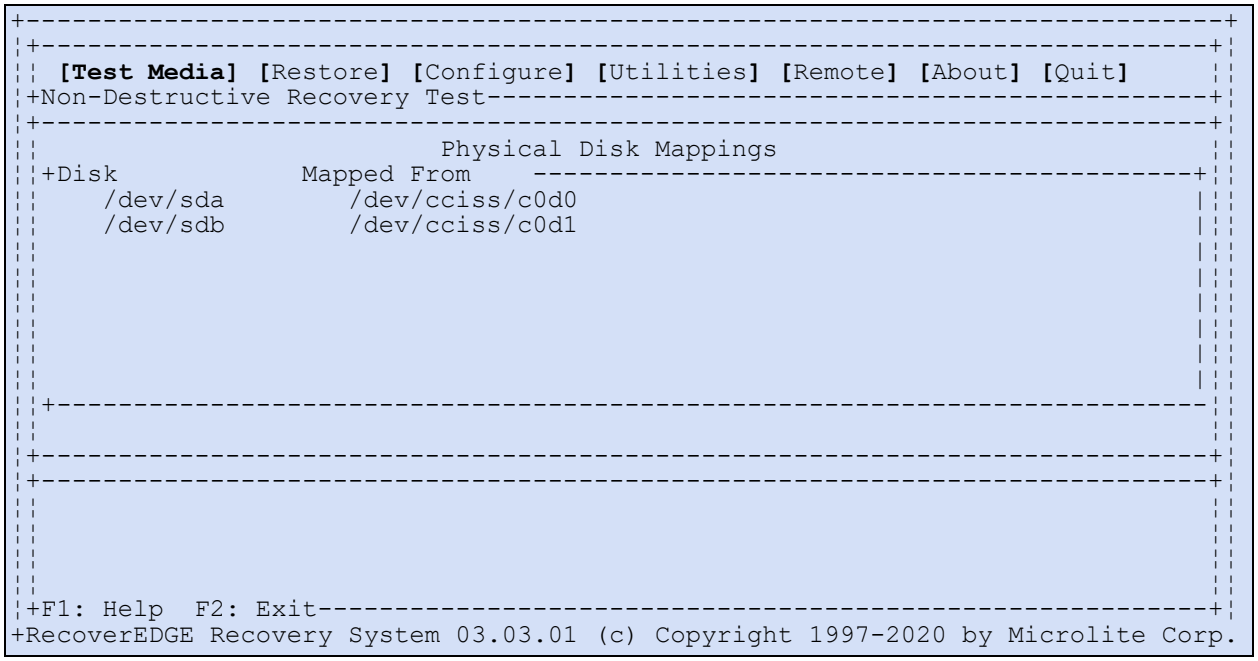
31.9 - Drive Mapping

If you were using physical hard disks on a host adapter that does not map the drives as logical scsi devices (`/dev/sda`, `/dev/sdb` etc.) you see this when you get to the *RecoverEDGE* main menu:



Go to the "**Configure - Drive Mappings Menu**". Select the first logical hard disk (`/dev/sda`) and hit **Enter**. Choose the proper boot drive from the available list (may only be one), then press **Tab** and select "**Perform Mapping**". The "`Current Drive`" may show device like `/dev/hdX` or `/dev/cciss/cXdX`. If there is more than one drive, map each of the other drives to be `/dev/sda`, `/dev/sdb`, etc.

When finished, the screen should look like this:



Return to the main *Recover**EDGE*** menu. The `WARNING: No '/' filesystem configured!` should have disappeared. Continue with "Test connectivity to the storage resource on page 303."

32 - Disaster Recovery - Linux P2V - Hyper-V

32.1 - Linux P2V Overview - Hyper-V

NOTE: This feature **does not run in demo mode**. Your *Backup**EDGE*** must be fully registered and activated to use this capability.

Beginning with *Backup**EDGE** 03.01.03 build 5*, Linux physical-to-virtual (**P2V**) conversion/recovery with Hyper-V is built into *Recover**EDGE***.

32.2 - P2V Pre-requisites - Microsoft Hyper-V

- *Backup**EDGE*** 03.03.01 build 1 or later *must be licensed and activated*. P2V capability is not available in 60 day demo mode.
- Must be virtualizing to Microsoft Hyper-V on Windows Server 2012 R2.
- 03.03.01 build 1 and later supports:
  - Red Hat Enterprise Linux 7.8.
  - CentOS Server 7.8-2003
  - Oracle Linux Server 7.8.

NOTE: P2V conversion is not currently supported if LVM has been used. Only servers with standard filesystems can be converted. Servers must be fully patched to the 7.8 level or later for P2V to be supported.

32.3 - Making RecoverEDGE P2V Media/Images (Hyper-V)

To make *Recover**EDGE*** images that are capable of P2V conversion...

- Install and license one of the *Backup**EDGE*** releases listed above on the physical server and configure it to store data on something accessible to Hyper-V.
- Make sure you communicate with the storage device before making media to ensure that any and all drivers are loaded..

NOTE: NAS / FTP server is the recommended and tested storage *Resource*.

- Make new *Recover**EDGE*** optical media or ISO image. Make sure the *Recover**EDGE*** "**P2V:**" notice is set to "**YES**" on the main *Recover**EDGE*** screen. See the bold indication below.

```
+------------------------------------------------------------------------------+
¦+----------------------------------------------------------------------------+¦
¦¦ [Make Media] [Configure] [Options] [Report] [About] [Quit]                 ¦¦
¦+Write Boot Media / Image----------------------------------------------------+¦
¦+----------------------------------------------------------------------------+¦
¦¦                                                                            ¦¦
¦¦                                                                            ¦¦
¦¦                                                                            ¦¦
¦¦                                                                            ¦¦
¦¦                                                                            ¦¦
¦¦                                                                            ¦¦
¦¦                                                                            ¦¦
¦¦                                                                            ¦¦
¦¦                                                                            ¦¦
¦¦                                                                            ¦¦
¦¦                                                                            ¦¦
¦¦                                                                            ¦¦
¦+----------------------------------------------------------------------------+¦
|+----------------------------------------------------------------------------+|
||Create Node: CD/DVD Image  OS: Linux version 3.10.0-1127. UEFI: Enabled     ||
||Temp Device: /dev/loop0    System: ts140.microlite.com                      ||
||Format: Yes  P2V: YES      Kernel: /boot//vmlinuz-3.10.0-1127.              ||
||                                                                            ||
|+----------------------------------------------------------------------------+|
+RecoverEDGE Recovery System 03.03.01 (c) Copyright 1997-2020 by Microlite Corp.
```

NOTE: If P2V says "**NO**", your release of *Backup**EDGE*** has not been properly registered and activated, or your Linux distribution is not supported by our P2V process.

- Go into "Configure".

```
+----------------------------------------------------------------------------+
¦ [Media Layout] [Boot Loader] [Boot Media] [Hyper-V] [Previous]             ¦
+Select to turn on P2V for Hyper-V ------------------------------------------+
```

- and select Hyper-V. You'll see : "`Turning On HyperV P2V conversion Settings`".
- When you return to the main menu, the `P2V` flag at the bottom left will be set to "`HV`".
- After you've made an ISO image, copy it to a location accessible to the Hyper-V console of the virtual server. It's filename is: `/usr/lib/edge/recover2/images/cdrom.iso`.

32.4 - Making Backups for P2V Conversion

- **After** the *Recover**EDGE*** optical media or ISO image have been made, perform a *Master Backup* to the storage resource.
- If desired, after the conversion is complete, you may make a final *Differential Backup* of the physical server and restore it to the virtual server. This will lessen downtime during the conversion.

32.5 - Virtual Machine Creation Guidelines

Create a new, blank virtual machine on the Hyper-V host, using the following guidelines...

- Use the default IDE hard drive controller and Intel Network Adapter.
- Number of virtual hard drives must match physical server hard drives. Virtual hard drives must be slightly larger than the hard drives on the physical server. This is because Hyper-V calculates hard drive space using a different method, and it may come up short if you enter an identical hard drive size. Always pad the hard drive size by one or 2 gigabytes to be safe.
- Number of virtual network interface cards (NICs) must match number of physical NICs, at least during the conversion process.

- Use the default virtual DVD-ROM (CD-ROM) setting.
- Use Hyper-V on Windows Server 2012 R2. Other Microsoft products may work but are not tested or supported.

32.6 - P2V Disaster Recovery Procedure

Restore the *Master Backup* (and optional *Differential Backup*) made at the end of "Making RecoverEDGE P2V Media/Images (Hyper-V)" on page 307 using this procedure...

- Attach the *Recover**EDGE*** optical media or ISO image to the virtual machine and boot. You may type "`network`" at the boot prompt and initialize the network using a different IP address if the original physical service is still running. Otherwise, shut down the physical server.
- You'll get the following message, indicating that modules from the older server won't load under VMware:

```
RecoverEDGE: An error occurred while loading kernel nodules.
Check /tnp for the file insmod.err, and try to load the modules manually.
Exit the shell to resume normal recovery fron the RecoverEDGE menu.

Type exit Then Press [ENTER] For The RecoverEDGE Menu
```

You may safely type `exit` and press `[Enter]` to continue.

- If the hard disks on the physical machine are not logical scsi devices (`/dev/sda`, `/dev/sdb` etc.) you will get the following two messages during boot:

```
+WARNING-------------------------------------------+
+                                                  +
+ Your system state appears to be inconsistent     +
+Please use the Configure menu to manually adjust  +
+              fdisk settings, etc.                +
+                                                  +
+                       [Ok]                       +
+--------------------------------------------------+
```

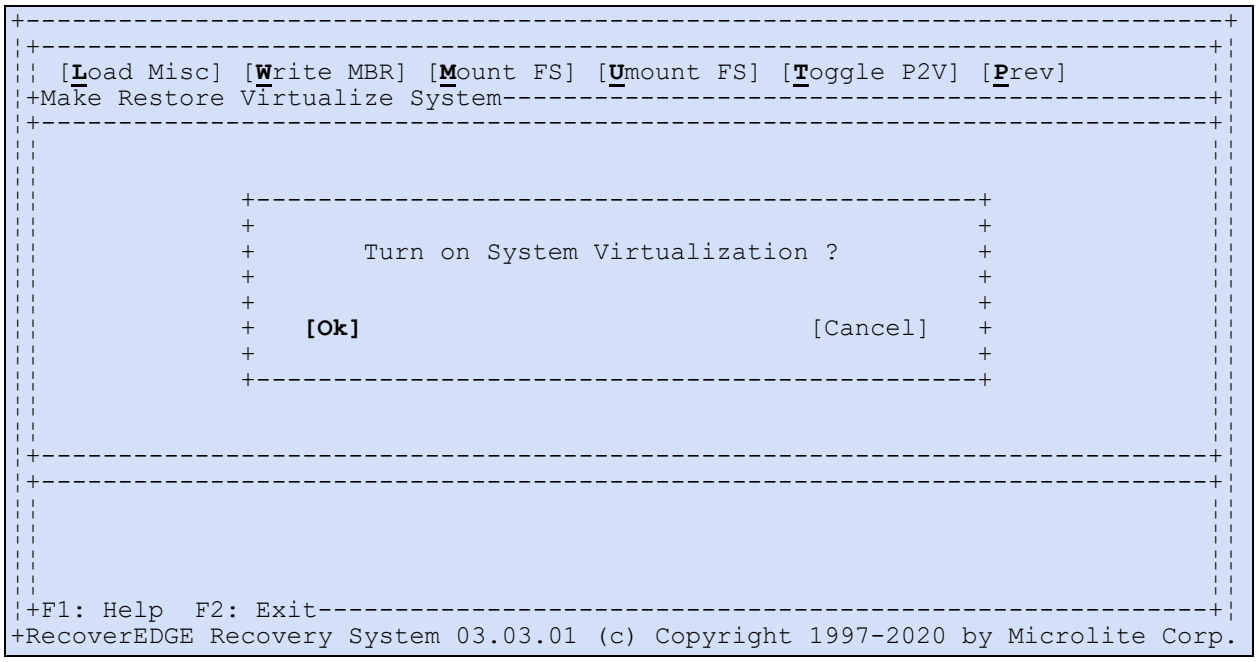
followed by:

```
+NOTICE--------------------------------------------+
+                                                  +
+       Some Hard Drives Have Been Added           +
+      Please Review The Mapping Status.           +
+                                                  +
+                       [Ok]                       +
+--------------------------------------------------+
```

In these cases, please see "Drive Mapping" on page 311.

- Test connectivity to the storage resource. Use "**Test Media**" from the main *Recover**EDGE*** menu and read at least part of one of your backups. You may safely ***ignore test result errors*** for part 2 (mounting the hard drive filesystems) as they don't yet exist.

- Turn on **P2V** mode from the *RecoverEDGE* menu. Go to "**Utilities - Other - Toggle P2V**" and answer "**YES**" to the "**Turn on System Virtualization**" prompt. This will ensure that, after restore, the correct HBA driver will be used as the boot driver by the operating system.



- Perform an automatic "OneTouch Restore" to the virtual machine.
- When the restore is finished, you may restore any optional differential backups.
- When all backups have been restored, the operating system on the hard drive will be modified to boot from the appropriate host adapter, and you'll be returned to the main *RecoverEDGE* menu.
- Quit *RecoverEDGE*, then power off the **VM** and remove the attached CD-ROM or image.

32.7 - What if I forgot to "Toggle P2V"

If you didn't remember to "Toggle P2V" before doing your restore, you don't have to start over. From the main *RecoverEDGE* menu (either while still booted or after rebooting into the *RecoverEDGE* CD or Image)...

- Go to the "**Utilities - Other"** menu as shown above.
- Select "**Toggle P2V**" and answer "**YES**" to the "**Turn on System Virtualization**" prompt.
- Select "**Prev**" to return to the "Utilities" menu and select "**Exc Loader**".

This will correct the host adapter driver issue. When complete, quit *RecoverEDGE*, then power off the **VM** and remove the attached DVD-ROM image.

32.8 - Booting the Virtualized Operating System

Networking will need to be changed upon first reboot. We recommend booting to single user mode.

Remember, if you are going to keep the same IP address, shut down the physical server first.

- Boot the **VM**.
- Run the operating system networking commands and fix any networking issues. from the command line this command is usually:

```
system-config-network-tui
```

or

```
nmtui
```

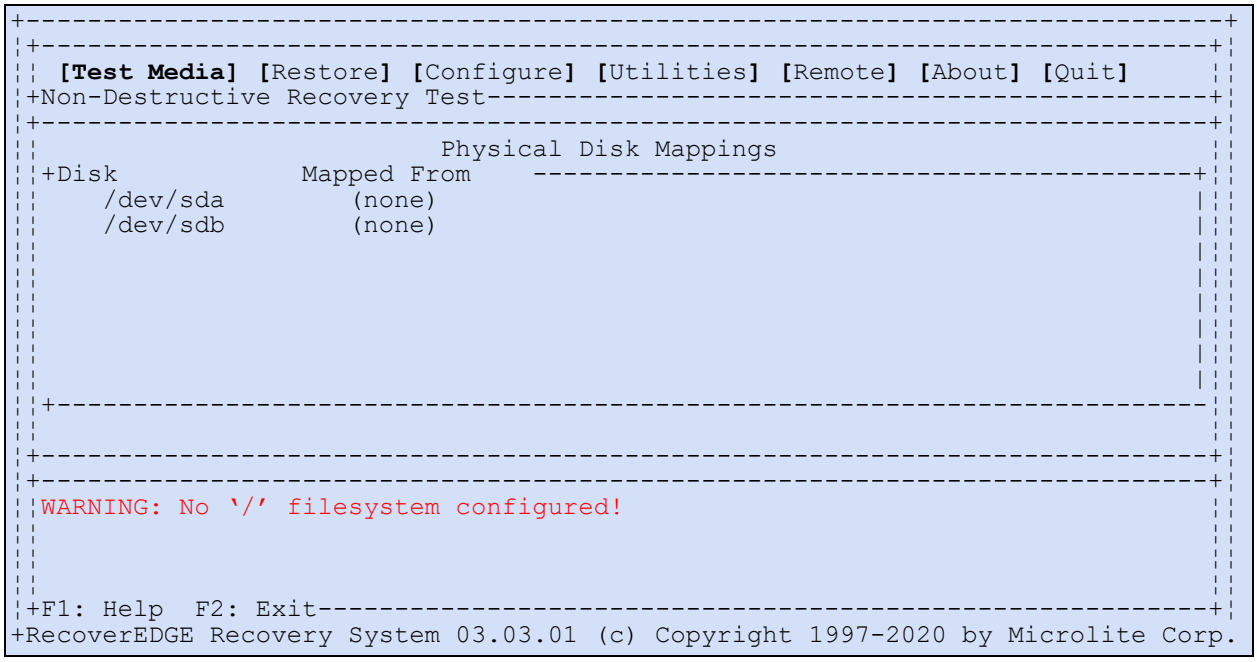
although some linux variants are different, and in some cases people prefer to make manual changes.

- You'll probably have to remove the old network adapter (NIC) and add in a new one to have Linux detect the proper VMware NIC.
- Adjust any IP address information, name servers, hostname information, etc.
- Reboot and go into multi-user mode.

Changing the hostname will invalidate the *BackupEDGE* license, but if you are under a valid ***Support and Maintenance Subscription*** there is no charge to have it re-activated on the **VM**, as long as the old server will no longer be used.

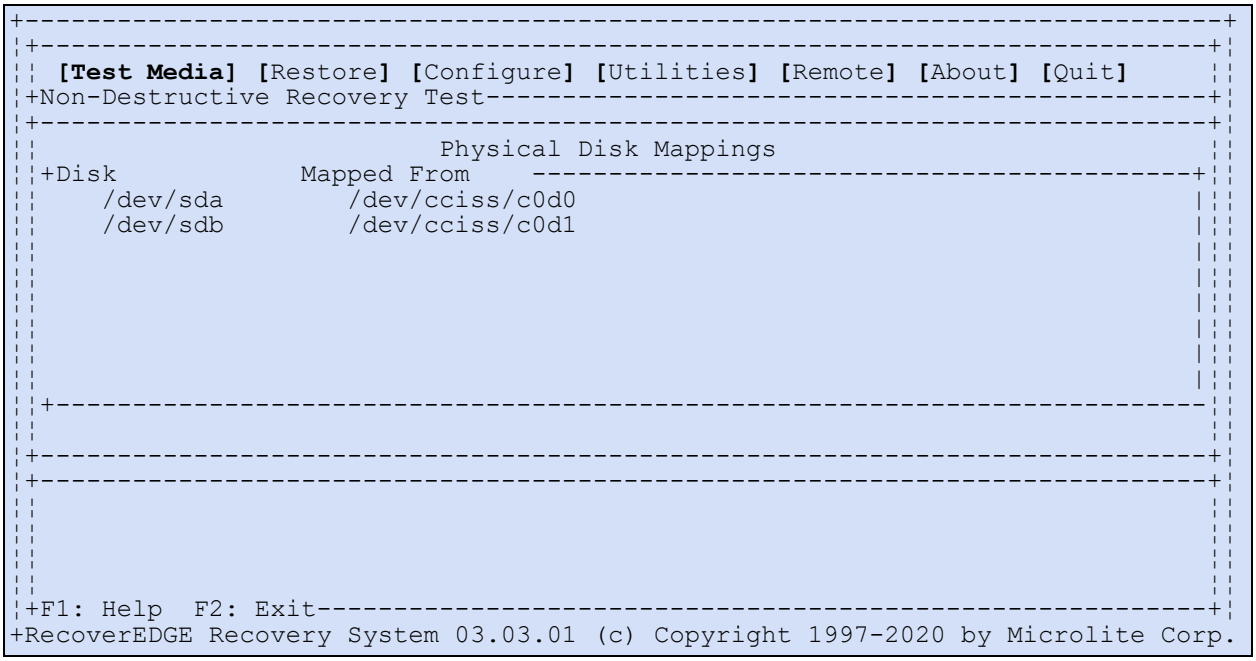
32.9 - Drive Mapping

If you were using physical hard disks on a host adapter that does not map the drives as logical scsi devices (`/dev/sda`, `/dev/sdb` etc.) you see this when you get to the *RecoverEDGE* main menu:



Go to the "**Configure - Drive Mappings Menu**". Select the first logical hard disk (`/dev/sda`) and hit **Enter**. Choose the proper boot drive from the available list (may only be one), then press **Tab** and select "**Perform Mapping**". The "`Current Drive`" may show device like `/dev/hdX` or `/dev/cciss/cXdX`. If there is more than one drive, map each of the other drives to be `/dev/sda`, `/dev/sdb`, etc.

When finished, the screen should look like this:



Return to the main *RecoverEDGE* menu. The `WARNING: No '/' filesystem configured!` should have disappeared. Continue with "Test connectivity to the storage resource on page 303."

33 - Disaster Recovery - Without RecoverEDGE

NOTE: Legacy UNIX servers and older Linux servers can utilize the information on this page. Newer Linux operating systems are much more complex and it is best to use only systems that fully support *Recover**EDGE***.

If for some reason your system is incompatible with *Recover**EDGE***, all is not lost. Use this simple method for recovering from disasters.

The nightmare of every computer user is to have a catastrophic failure resulting in the loss of all data on the hard disk. Fortunately, now that you are using *Backup**EDGE*** this can be reduced to a mere annoyance.

Here are the general steps required to completely rebuild your file systems. Your system may not require all of the steps, but you should have no difficulty adapting this procedure to your needs.

- Identify the problem which resulted in your data loss and have it corrected.
- Boot from your original *Boot Media*, initialize your primary hard disk drive, partitioning for swap space, etc. as necessary, and install your base operating system.
- If you had to install a special *Device* driver for your *Backup**EDGE*** backup *Device*, redo it now.
- If you have secondary hard drives, reformat and remount them. Some operating systems require kernel re-configuration as part of this process. Striped, mirrored, and other special hard drives must also be prepared properly.
- Make sure network filesystems, if needed, are mounted properly.

NOTE: On most systems, the boot filesystem is mounted read-only. Make sure it is mounted read-write before doing a restore.

- Install *Backup**EDGE*** from your master disk or CD-ROM. Run *EDGEMENU* and set up for your save *Device*(s).
- If you have any encrypted files on the backup you intend to restore, use *EDGEMENU* to restore the appropriate Decryption Key Backup. If you do not have these keys, then encrypted files will not be restored.
- Restore your last *Master Backup*.
- Restore your last *Differential Backup*, and any *Incremental Backups* (if you have them and it is more recent than your last *Master Backup*).
- Shut down and re-boot your system.

That's It! Your system should be back up and running, and up to date as of the time of your last *Backup*. Eventually, any UNIX filesystem gets fragmented, with portions of long files scattered all over the hard disk, reducing system performance. Periodically performing a *Master Backup* followed by the above procedure will optimize your filesystem and result in increased system throughput.

34 - Using Wildcards

*Backup**EDGE*** supports the wildcard characters `*` (asterisk) and `?` (question mark).

The `*` wildcard character represents any *zero* or more ASCII characters except the forward slash '`/`'. Its use may be restricted depending on the context in which it is used (see below).

The `?` wildcard represents exactly one ASCII character. It may be used anywhere an ASCII character may be. It will also not match a forward slash '`/`'.

Wildcards should *not* be quoted or escaped unless they are used in a command-line. If they are used on a command line, it is advisable to protect them from shell expansion.

34.1 - Wildcards During Exclusion From Backup or Restore

Wildcards may be used to exclude files or directories from backups or restores. For instance, if the following two lines were entered at the exclusion prompts when beginning a restore, then all items on the archive would be restored with the exception of the `/usr/lib/wp` directory and ANY file ending in `.idx`.

```
/usr/lib/wp
*.idx
```

Again, wildcards should ***not*** be quoted unless used on a command line.

Please note that "`*.idx`" cannot be used in `/etc/edge.exclude` or other exclude filelists that are processed by EDGEMENU or EDGE.NIGHTLY.

34.2 - Wildcard Exclusion During Nightly Backups

The same rules for exclusion wildcards apply to *Automatic Nightly Backups* from the *EDGE.NIGHTLY* program. Each line in `/etc/edge.exclude` may contain either a filename, directory name, or an unquoted wildcard. Remember, this file can contain no more than 64 separate lines with filenames and 64 lines with directory names, although wildcards may be used to exceed the actual number of files and directories excluded.

35 - BackupEDGE from the Command Line

While *BackupEDGE* has been designed to be operated primarily from a character menu system, it provides command-line tools to complete many common tasks.

35.1 - Non-interactive Installation

Usage

```
install_program -terse [-autodetect] [-autodetect_ok]
```

Description

Normally, *BackupEDGE* installation is interactive. However, in some cases it is desirable to run it without user intervention. Upgrades in particular can benefit from non-interactive installation.

In the above usage, substitute *install_program* with the full name of the self-extracting UNIX or Linux executable you wish to install, such as `/tmp/edgelnx6.elf` or `/tmp/edgesco5.elf`.

`-terse`
This option indicates that no user interaction should be requested. All output will be in text mode to standard output. Device autodetection will be skipped, so it is not necessary to load media into all devices. However, you may be warned that the autodetector should be run manually. To allow this to occur automatically if needed, please see the `-autodetect_ok` option.

`-autodetect`
During installation, *BackupEDGE* will skip device autodetection if it has completed successfully in the past, and the current version supports no new device types. This option forces autodetection to occur during the installation process. You *must* have media loaded and ready in all devices before starting the installation process if autodetection will occur, or else it may not detect all of your devices properly if you are installing in terse mode. In interactive mode, this option will force the installation program to ask if autodetection should be performed.

`-autodetect_ok`
This flag instructs the installation program to perform (or ask about, in interactive mode) autodetection *if there is reason to do so*. During interactive installations, this is the default. In terse mode, you should load media into all devices in case autodetection is performed, since terse installations do not request further user input before beginning the autodetection process. This flag is differs from `-autodetect` in that it does not force autodetection to occur; it allows the installation program to decide if autodetection is necessary, and either perform it (terse mode), or ask about it (interactive mode).

35.2 - Command-Line Restores Using EDGE.RESTORE

Usage

```
edge.restore [-stux] [-f resource] [-E ExcludeFile] [-F FileList]
[-X ExcludeFilelist] [-zSEG_NUM=x] files...
```

Description

BackupEDGE can utilize the *Quick File Access* (*QFA*), capabilities of a tape *Device*, or the *Seeking Device* capabilities of a *CD-R/RW*, or DVD *Device*, to perform highly optimized media positioning and retrieval of archived data. This process also works with disk file archives. We call the retrieval process *Fast File Restore* (*FFR*) for tapes and *Instant File Restore* (*IFR*) for all other archives.

EDGEMENU and *EDGE.EMX* offer character and *GUI* interfaces for *IFR* and *FFR*.

The *EDGE.RESTORE* program the same access capabilities from the command line.

Given the *Resource* that contains the media from which to restore files, and the names of the files to be restored, *EDGE.RESTORE* will read the archive label, select the database that was created from the archive, and restore the files using *FFR* or *IFR* access techniques as appropriate. If *FFR*/*IFR* is not available, it will use a normal-speed restore.

By default, filenames should be specified like any other UNIX command. A rule of thumb is, if "`rm file_to_keep`" gets rid of it, then "`edge.restore file_to_keep`" will bring it back. Of course, you would also have to provide the `-f` option to select the *Resource* with the archive in it. For *Expert Mode* (or legacy) backups, this does not apply (see the `-x` option below).

The options are:

`-f resource`
This selects the *Resource* (which may be `machine:resource`) that contains the medium from which you wish to restore. If this option is not given, the *Primary Resource* selected *EDGEMENU* will be used.

`-u (default, cannot be used with -x)`
This option indicates that you will use UNIX-mode paths. UNIX-mode paths are the same paths you use with other UNIX commands. See below for a description.

`-x (cannot be used with -u)`
This option indicates that you will use Expert-mode paths. These are the paths that are actually stored on the archive. See below for a description. Usually, you should use UNIX-mode paths instead.

`-E exclude_file`
This option excludes some file (or wildcarded pattern) from restore. Be sure to escape any wildcards that may be expanded by the shell. If you exclude a directory, then everything in the directory will be excluded as well.

`-X filelist`
This option provides a file which contains filenames to be excluded from restore. Each one is treated as if it were entered on the command-line with the `-E` option, except that wildcards do not have to be escaped. The filenames should be listed one per line.

`-zSEG_NUM=`**`X`**
When restoring form a URL or FSP Resource, and if more than one archive resides on the Resource, you must select the proper segment from which to begin the restore. If this flag not included on the command line, a list of available segments will be displayed and no action will be taken, Repeat the command, adding this flag with **X** being replaced by the desired segment number.

`-N`
If included, the files will only be restored that do not exist on the system currently. Normally, files will be overwritten if possible.

`-s (slow mode - no FFR or IFR)`
This option disables *FFR* and *IFR*, forcing *Backup**EDGE*** to read through the archive at normal speed. If no index is found for the archive, then slow mode will be used by default. There is normally no need to specify this option.

`-t`
If included, this option prevents any files from being restored. Note that the files listed with the `-N` option may not be indicative of the files that would actually be restored. This option is generally used for troubleshooting or timing tests only.

`-F filelist`
This option specifies a file that contains filenames to be included in the restore, one per line. Wildcards should not be escaped in these filenames.

`-v (lowercase Vee)`
This enables a summary to be displayed after the operation completes.

`-V #volumes_to_expect (uppercase Vee, default is 1)`
If you are restoring from a multi-volume archive, you should indicate how many volumes (total) exist for that archive with this option. For example, use `-V 5` for a five-volume backup.

`-y`

Normally, *EDGE.RESTORE* will ask questions if it encounters an unusual situation. This option instructs it to skip this, and try the restore anyway if possible.

`-h`
If you are performing an *FFR* or *IFR*, and request that one or more hard or symbolic links are restored, the default behavior is to restore just the link (unless, of course, you also request the linked-to file). By including this option, the link is not restored. Instead, the "real file" is restored. This option has no effect for a slow file restore. See below for examples of this.

`-H`
If you are performing an *FFR* or *IFR*, and request that one or more hard or symbolic links are restored, the default behavior is to restore just the link (unless, of course, you also request the linked-to file). By including this option, both the link and the "real file" are restored. This option has no effect for a slow file restore. See below for examples of this.

After all the options, list all the files and/or directories you'd like to restore. Filenames may contain wildcards, but should be protected from expansion by the shell in most cases. Directories will have their contents restored automatically. If you want to specify a filename that contains a space, be sure to protect the space from the shell, or else `edge.restore` will see two filenames. The examples below show this.

Options may be grouped. The following commands do the same thing:

```
edge.restore -ftVh tape0 5 -u ./myfile
edge.restore -f tape0 -t -V 5 -u ./myfile
```

The order in which options is specified does not affect their operation, assuming that any arguments to those options are kept in order on the command line.

You may be prompted to enter a passphrase to unlock a decryption key, as appropriate, when restoring from a backup with encrypted files.

Examples

```
edge.restore -f tape0 ./edge\*.doc ../a_file "./my space file"
```

(Note that the wildcard '`*`' is escaped with a backslash '`\`'. Otherwise, the shell would expand it. While this is not technically an error, there may be files on the archive which match the wildcard that are not present on the system currently. In that case, the shell would expand only those files that currently exist, and *EDGE.RESTORE* would skip the others. By including the backslash, *EDGE.RESTORE* sees the wildcard and matches all the files on the archive. Both methods have their uses, but escaping wildcards generally has the intended meaning.)

UNIX-mode paths, as referred to above, indicate that the files should be named in a way that any other UNIX command might expect them. For example:

```
rm ./important.c ../really_important.c
edge.restore -f tape0 ./important.c ../really_important.c
echo hi >/stand/unix # please don't try this
btmt -w /stand
edge.restore -f tape0 /stand/unix
btmt -d /stand
```

In contrast, expert-mode paths indicates that *EDGE.RESTORE* should interpret the filenames as matching how they appear on the archive. This is identical to the way they would have been specified in versions of *Backup**EDGE*** prior to 01.02.00. Unless you are using legacy archives or archives not made with *Backup**EDGE***, you do ***not*** want to use this option.

If you wish to perform an *FFR* or an *IFR* of symbolic links, you have the option of restoring the real file data as well (or instead). For example, under *OSR5*, the user mailboxes are in the

directory /var/spool/mail. However, the directory /usr/spool is actually a symbolic link to /var/spool. Here is an example using this:

```
1 edge.restore -f tape0 /usr/spool/mail/frank
2 edge.restore -f tape0 -h /usr/spool/mail/frank
3 edge.restore -f tape0 -H /usr/spool/mail/frank
```

In command 1, nothing will be restored, and *EDGE.RESTORE* will produce an error to that effect. The reason is that there is no "real" file called /usr/spool/mail/frank. There is a file called /var/spool/mail/frank, however.

In command 2, /var/spool/mail/frank will be restored and nothing else.

In command 3, the symlink /usr/spool will be restored, along with the file /var/spool/mail/frank.

Note that if a symlink is matched only as part of a wildcard expansion (assuming the wildcard is ***not*** expanded by the shell; if it is, *EDGE.RESTORE* never sees it!), then -h and -H will not affect that symlink. For example, including a Bourne-shell wildcard escape,

```
edge.restore -f tape0 -H /usr/\*
```

will restore the symlink /usr/spool but not any of the /var/spool directory. Of course, it will also restore the rest of the /usr directory. In contrast, the command

```
edge.restore -f tape0 -H /usr/spool/\*
```

will restore the symlink /usr/spool, and /var/spool/* . Any symlinks under /var/spool will be restored but not traversed, as they would be matched by only a wildcard expansion performed by *EDGE.RESTORE*.

```
edge.restore -f tape0 -H /usr/*
```

The above command will probably restore the symlink /usr/spool, as well as /var/spool. Why? The wildcard was not protected from shell expansion, so *EDGE.RESTORE* saw the command:

```
edge.restore -f tape0 -H /usr/spool /usr/lib /usr/and_so_on
```

To see what *EDGE.RESTORE* would see, try replacing "edge.restore" with "echo".

-h and -H do not affect files that are matched as part of a directory traversal. For example,

```
edge.restore -f tape0 -H /usr
```

will restore all of the /usr directory, but will not restore /var/spool. It will restore the /usr/spool link, however. (While this may seem similar to restoring /usr/*, the difference is that in the case of /usr/*, the directory /usr itself is not restored, just its contents. Restoring /usr restores the same contents plus changes the ownership and permissions of the /usr directory to match the archive.)

Here are some other examples of using *EDGE.RESTORE*:

```
edge.restore /stand/unix
edge.restore ./myfile
edge.restore -E ./src/keep_files ./src
```

The first command restores /stand/unix. The second restores myfile under the *Current Directory*. The third restores all of the ./src *Directory* except ./src/keep_files. Each of these examples uses the *Primary Resource* as selected in *EDGEMENU*.

Using URL and FSP Resources.

```
edge.restore -f url0 -zSEG_NUM=1 /stand/unix
```

Issuing the command once without -zSEG_NUM=x will display the available backup segments on the *URL* or *FSP* Resource.

Resources may be remotely attached:

```
edge.restore -f mlite:tape1 /stand/unix
```

This command would open the *Resource* on system `mlite` and read its label. It would attempt to find a database for the tape, position the tape on `mlite`, and restore the file. This results in minimum network overhead, as only the files to be restored will pass through the network. However, it does take more time to access remote databases than local ones.

35.3 - Using EDGE.TAPE for Hardware Status / Control

Synopsis

```
edge.tape [-terse] [-arg x] [flags] device
  -*: same as -t
  -i: inquiry                      -m: media load count
  -g: get max/min block sizes      -c: report capacity left
  -s: report switch settings       -n: report density etc.
  -t: complete tape status         -a: DAT get compression status
  -R: rewind                       -T: retension
  -F: skip to next filemark        -M: skip to next setmark
  -E: erase tape partition         -D: skip to EOD
  -L: load tape                    -U: unload tape
  -I: write filemark               -K: write setmark
  -P: set speed to arg             -B: set block size to arg
  -N: set density to arg           -A: make partition of arg mbytes
  -S: set partition to argument    -C: set DAT compression to arg
  -v: show TapeAlert(tm) support   -V: display TapeAlert message
  -Q: stacker (sequential) -- HP only
  -W: prevent (arg=1)/allow media removal
```

Description

*Backup**EDGE*** can query and control storage *Devices* through the *EDGE.TAPE* program. This section of the manual describes only a few of the more popular uses of *EDGE.TAPE*.

As the *Usage* line indicates, the command accepts either a *Device Name* (`/dev/rStp0`, `/dev/st0`, `/dev/rmt/0`, etc.) or a *Resource Name*. In the examples below, we'll use `tape0` as the default *Resource* being queried or modified. More information is available from many *Devices* if media is present.

Also note that *EDGE.TAPE* is a misnomer. It can also read information about optical drives.

NOTE: The remainder of this page assumes the *Device* is a tape drive. While *EDGE.TAPE* can operate on other *Devices*, it is generally most useful only with the `-i`, `-L`, and `-U` options in those cases.

Normally, *EDGE.TAPE* reports its results with human-readable output. If the `-terse` option is specified, output is reformatted into a list of environment variables; this mode is meant to be used with the shell `eval` command.

When issuing multiple commands to a tape *Device* (e.g., *rewind* then *unload*), it is advisable to issue multiple *EDGE.TAPE* commands. The order that commands are given on the command line is not always the order they are executed.

The *Device* given to *EDGE.TAPE* should be a *Resource* name (such as `tape0`). Alternatively, you may provide a *Device Node* (`/dev/rStp0`, for example). However, *EDGE.TAPE* may use a different version of the *Device Node* than the one specified; it may try to use the control (`/dev/xStp0`) version of the *Device*, even if the data (`/dev/rStp0`, `/dev/nrStp0`, etc.) *Device* is given. This is to circumvent problems associated with drives that don't have a tape.

Likewise, if *EDGE.TAPE* requires the data *Device*, but is given the control *Device*, it will try to switch. In this case, it defaults to the no-rewind or no-rewind, no-unload version of the *Device Node*.

Usually, it is advisable to use a *Resource* name rather than a *Device Node*. If you specify a *Device Node* that is used by one or more *Resources*, *EDGE.TAPE* will select one of those *Resources* and use its settings to query the *Device*.

Informational Commands

`-i` SCSI Inquiry
This returns the product identifier, vendor name, revision, interface type (SCSI / ATAPI / Other), SCSI compliance level (i.e., SCSI-1, 2, or 3), a description of the type of *Device* (normally Sequential Access), and a flag indicating if a tape is loaded.

`-m` Media Use
This attempts to determine the number of times the tape has been loaded into the drive. If it cannot be determined, this parameter returns `0`. This count is unrelated to the usage counter presented by reading an archive label through *EDGEMENU* or *EDGE.LABEL*.

`-g` Block Sizes
EDGE.TAPE prints the maximum, minimum, and current tape block sizes. For most tapes, the current block size will be `0`, `512`, `1024`, or `2048`. The value returned is in bytes. If the *Device* supports variable block mode, a block size of `0` will select it. While in variable block mode, the *Device* will write data blocks to the medium which are equal in size to the data given to the *Device* by the host for a given write command. Note that the size of this transfer is still bounded by the minimum and maximum block sizes as reported by this command.

`-c` Capacity
EDGE.TAPE tries to determine the capacity of all partitions on the *Device*, along with the current partition number. Values reported are in kilobytes. If ECC error correction is enabled, this value is adjusted to reflect the actual user data capacity of the partitions.

`-s` Switch Settings
Some tape *Devices* can report hardware configurations through vendor-defined commands. *EDGE.TAPE* will try to retrieve them. This command is not well developed, and is likely to provide no information.

`-n` Density
EDGE.TAPE will try to determine the density (recording format) of the loaded tape. It will also make a guess as to a text description of the tape. The density code, in hex, is displayed along with this guess, and the current write-protect status of the cartridge.

`-t` Tape Status
This option tries to print as much information as possible about the tape. It also prints some relevant drive information.

`-a` DAT Compression Status
This option reports the current compression / decompression status of the drive:

`0` decompression disabled, compression disabled
`1` decompression enabled, compression disabled
`2` decompression disabled, compression enabled
`3` decompression enabled, compression enabled

`-v` TapeAlert Support (lowercase Vee)
This option displays whether or not a *Device* is TapeAlert compatible.

`0` *Device* has no TapeAlert support.
`1` *Device* can display TapeAlert messages.

`-V` TapeAlert Message (uppercase Vee)
This option queries TapeAlert compatible *Devices* and displays any queued messages in plain english. By definition this clears the tape drive message queue.

Tape Control Commands

With all tape positioning commands that leave the drive at some location other than beginning-of-partition, it is important that a rewind *Device* is not specified on the command line. For example, use `/dev/nrStp0` not `/dev/rStp0`. However, it is not guaranteed that *EDGE.TAPE* will be able to leave the *Device* in the state requested in this case.

`-R` Rewind
rewind to beginning of partition.

`-T` Retension Tape
Retension tape, typically by spooling tape all the way out, then rewinding all the way back.

`-F` Filemark
skip to the next filemark

`-M` Setmark
skip to the next setmark

`-E` Erase
Erase current partition. (**No confirmation is requested**; the partition is erased immediately). This operation can take several hours, depending on the type of tape. Note that the partitions themselves are not removed; only the data in [one of] them. For DVD+RW media, this causes a background format to be initiated. For DVD-RAM, this starts a physical format (this is usually not needed).

`-D` End of Data
skip to end of data.

`-L` Load Tape
Many drives are incapable of actually pulling the tape into the drive mechanism. The load command may still be useful, however, if an `unload` command is issued to the drive, while `prevent media removal` (see below) is in effect. In this case, it may cause the tape to be returned to an operational state, depending on the tape drive configuration.

`-U` Unload Tape.
This generally causes the tape to be physically ejected from the drive. If `prevent media removal` (see below) is in effect for the drive, this command may fail. If the drive is embedded in a changer, and the tape changer has `prevent media removal` in effect, this command may simply unthread the tape without ejecting it back into the magazine. For tape drives in an autochanger, *EDGE.CHANGER* is a more appropriate command. It can be configured to load and unload tapes as required for tape motion in the autochanger.

`-I` Write Filemark
A filemark is the lowest level of the tape mark hierarchy. Filemarks are useful because a tape drive can generally seek to them quickly. A filemark may take up a non-negligible amount of space on the tape.

`-K` Write Setmark
A setmark is a hierarchically superior tape mark to a filemark. It is generally used to demarcate entire backups stored on a single tape.

`-P` Set Speed to `Arg`
The argument (specified with `-arg`) is used to set the tape speed. This command is rarely accepted by tape drives, as most drives support only one speed.

`-B` Set Block Size to `Arg`
The low level tape block factor is set to the value of the argument. If it is given as `0`, the tape is put into `variable block mode`. Any other value indicates `fixed block mode`.

`-N` Set Density to `Arg`
The tape recording density is set to `arg`. Most drives support only one density for any given type of tape (although some drives accept more than one tape format; e.g., a Travan drive generally reads QIC-80 tapes). This option is seldom used.

`-A` Make Partition of `Arg` Megabytes
A partition is created on the given size. Some tape drives (notably QIC drives) can only make fixed-sized partitions. Other drives, such as DAT drives, can make partitions of user-defined length. Further, some tapes do not record their partition format (again, QIC), and must be re-partitioned if the tape is removed. DAT drives record their partitioning information on the media, and further partitioning operations either fail or erase the old partition. If the argument size is `0`, a previously partitioned tape is returned to one partition (and all data is erased). *EDGE.TAPE* cannot reliably partition *Devices* which support more than two partitions.

`-S` Set Partition to `Arg` (`0` or `1`, usually)
This moves the tape head to the indicated partition. Subsequent rewind operations will return the tape here, as well.

`-C` Set DAT Compression to `Arg` (`0`, `1`, `2`, or `3`)
Sets the DAT compression to the given argument (see `-a` for a description). Some tape drives refuse to change some or all of their compression status; many drives insist that decompression is always enabled. If this command fails, try changing just one of the settings.

`-Q` Restore Stacker Mode
This attempts to return an embedded tape changer/drive combination into its stacker mode. This mode, which can be disabled when software jukebox commands are issued, generally causes the `unload` command to additionally load the next tape in the magazine. Currently, this command only works on embedded HP changers. Ejecting the magazine and reloading it, or opening the magazine access door, will return most autochangers to stacker mode.

`-W` Prevent (`arg==1`)/Allow Media Removal
If an unload command is issued, or the front panel eject button is pressed, while prevent media removal is in effect, the tape drive will reject the command. For tape jukeboxes, a `prevent media removal` command effectively turns off the front panel controls, as the jukebox is prevented from moving tapes out of the embedded tape drive. Issuing an `allow media removal` to the changer (and/or tape drive) may restore front panel operation. Note that the OpenServer 5 tape drivers seem to issue prevent media removal commands at various times automatically, so this command may be needed to restore proper operation.

Environment Variables

The `-terse` option of *EDGE.TAPE* may reference the following variables:

`ET_PRODUCT`	(Name embedded by vendor into product)
`ET_VENDOR`	(Vendor Name embedded into product)
`ET_REVISION`	(Firmware revision level of *Device*)
`ET_SERIAL_NUM`	(Device Serial Number)
`ET_SCSILEV`	(SCSI conformance level)
`ET_DESC`	(text string description of the *Device* type)
`ET_IFACE`	(type of interface)
`ET_MEDIA`	(`0` if media is not loaded, `1` if it is)
`ET_PART`	(0 if partitions aren't supported, otherwise 1)
`ET_CPART`	(current partition number, `0` or `1`)
`ET_NPART`	(Number of partitions on media)
`ET_CAPTx`	(total capacity of partition `x`, in K)
`ET_CAPRx`	(remaining capacity of partition `x`, in K)

ET_CAPTC	(total capacity of current partition)
ET_CAPRC	(remaining capacity of current partition)
ET_DENS	(density code, in hex)
ET_DENSDESC	(text description of the tape)
ET_WPROT	(0 if tape is write enabled, 1 if it is write protected)
ET_BLOCKSIZE	(Hardware block size in bytes)
ET_MINBLOCKSIZE	(minimum supported block size (0 means variable is supported)
ET_MAXBLOCKSIZE	(maximum supported block size)
ET_COMPRESSION	(Hardware compression setting - 0,1,2,3)
ET_ECC	(0 if ECC error correction is disabled, 1 if it is enabled)
ET_NGROUP	(number of redundant blocks written)
ET_UNCREAD	(number of uncorrected read errors)
ET_DLYREAD	(number of corrected read errors that caused a delay)
ET_CORREAD	(number of corrected read errors that did not delay)
ET_UNCWRITE	(un-correctable read errors detected)
ET_DLYWRITE	(delayed write errors detected)
ET_CORWRITE	(correctable read errors detected)
ET_TAPEALERT	(TapeAlert compatibility 0=no, 1=yes)
ET_RETCODE	exit status of command (same as "echo $?")

For example, with the -terse flag, this might be the command and its results:

```
edge.tape terse -i tape0
 ET_PRODUCT="Ultrium 1-SCSI "
 ET_VENDOR="HP      "
 ET_REVISION="N16D"
 ET_IFACE="0"
 ET_SCSILEV="3"
 ET_DESC="Sequential Access"
 ET_MEDIA="1"
 ET_SURE_MEDIA="1"
 ET_REMOVABLE="1"
 ET_RETCODE="0"
```

As you can see, all of the English response codes have been placed into variables. Extending this, the command:

```
 eval `edge.tape -terse -t tape0`
```

would run the extended command and place all of the results into the user or shell script environment.

NOTE: It is not guaranteed that the environment variables exported by *EDGE.TAPE* will remain the same in future revisions of *Backup**EDGE***. Be sure to check the *User's Guide* for those versions before relying on the -terse flag of *EDGE.TAPE* in those versions. Remember that the primary purpose of *EDGE.TAPE* is to facilitate backup and restore operations from *EDGEMENU* or through *EDGE.NIGHTLY*.

Errors

EDGE.TAPE generally issues mildly informative error messages whenever a problem is encountered. It also sets the exit status to reflect the outcome of all operations. A message corresponding to a particular error code is usually printed on any non-zero exit, as well as various other diagnostic messages.

EDGE.TAPE requires a licensed (or demonstration) version of *BackupEDGE*.

Examples

To print the vendor information:
```
edge.tape -i tape0
```
To capture the vendor information into environment variables in a Bourne Shell script:
```
eval `edge.tape -terse -i tape0 2>/dev/null`
echo $ET_VENDOR
```
To create a 512 megabyte partition:
```
edge.tape -arg 512 -A tape0
```
To turn off hardware compression:
```
edge.tape -arg 0 -C tape0
```
To print both the vendor information and the capacity:
```
edge.tape -ic tape0
```
To print the vendor information about the primary SCSI hard drive under *OSR5*:
```
edge.tape -i /dev/rhd00
```

35.4 - The EDGE.CHANGER Program

Synopsis

```
edge.changer [-terse] {show|move src dest|unload src|eject} resource
```

Description

EDGE.CHANGER controls a media jukebox, also known as an autochanger or tape library. It can be used to display the status of the changer elements, as well as move media around.

A jukebox is generally composed of four types of elements: storage, data transfer, import/export, and media transport.

Storage elements are used to hold media when it is not in use by a *Device* serviced by the changer. These are also referred to as magazine slots.

Data transfer elements represent the *Devices* that receive media from the changer. It is important to recognize the distinction between a data transfer element (a logical part of the changer), and the actual *Device*. For example, one would instruct a changer to move media into a data transfer element, but would actually read data from the media using an entirely separate Resource. One might issue move commands to `changer0` with *EDGE.CHANGER*, but read the data from `tape0` with *EDGEMENU*.

Import/export elements provide points for the user to add or remove media from the changer. Many desktop changers do not have separate import/export elements; media is accessed by ejecting the entire magazine.

Media transport elements represent elevators, robotic arms, etc., that actually move media around. Small changers especially do not report, or do not require any user decisions about, their media transport elements.

Commands

(abbreviations are shown in parenthesis)

`show` (`sh`):
: list all tape changer elements. If the `-terse` option is given, *EDGE.CHANGER* outputs a list of assignments to environment variables suitable for use with the shell's `eval` command. This allows

scripts to determine the state of a media changer easily. See below for a description of these variables.

`move` (`mv`):
move element `src` to element `dest`. Note that if you are moving media to or from a data transfer element, it may be necessary to issue a `load` or `unload` command to the drive after or before the changer operation to actually thread the tape. Many desktop changers with embedded drives handle this automatically.

`unload` (`un`):
unload `src`, usually into the magazine slot it came from. This command may or may not be successful, depending on the state of the changer. If *EDGE.CHANGER* cannot determine where the medium in `src` came from, it will try any unused magazine slot. When in doubt, issue a move command instead.

`eject` (`ej`):
eject the magazine. Eject will **not** unload any loaded cartridges from any data transfer elements. Most changers will not eject a magazine while media is loaded in a tape drive. This command is not supported by all autochangers.

`init (in)`:
initialize and check all changer elements. Normally, this command is not needed. It is used to force a refresh of the autochanger inventory.

Multiple commands are issued in the order they are encountered. Arguments to a command should follow it, before the next command is given.

Environment Variables

The `-terse` option of *EDGE.CHANGER* may reference the following variables:

`EC_BCSUPPORT`	(does the changer support barcodes (`YES|NO`))
`EC_ST`	(number of storage elements)
`EC_STx`	(state of storage element `x`, `1` is full, `0` is empty)
`ET_STx_PVT`	(private volume tag (barcode) for media in storage element `x`, if any)
`EC_MT`	(number of media transport elements)
`EC_MTx`	
`ET_MTx_PVT`)	
`EC_DT`	(number of data transfer elements)
`EC_DTx`	
`EC_DTx_PVT`	
`EC_IE`	(number of import/export elements)
`EC_IEx`	
`EC_IEx_PVT`	
`EC_SAx`	(storage element address of media in `DTx`, `-1` is unknown, `blank` is none, i.e. when `DTx` is empty, otherwise `STx`)
`EC_RETCODE`	return code of current command

These variables are subject to change in future versions of *EDGE.CHANGER*.

Errors

EDGE.CHANGER will generally issue informative error messages, along with a text description of any non-zero exit code. *EDGE.CHANGER* requires a licensed (or demonstration) version of *Backup**EDGE***.

Examples

To show the current state of the changer:

```
edge.changer show changer0
```

To move the tape in the first data transfer element to the second storage element, and then show the state of the changer:

```
edge.changer mv dt0 st1 sh changer0
```

To capture the changer status information into environment variables in a Bourne Shell script:

```
eval `edge.changer -terse sh changer0 2>/dev/null`
echo There are $EC_DT data transfer elements.
```

35.5 - The EDGE.NIGHTLY Program

Synopsis

```
/etc/edge.nightly some_opts -H scheduled_job_name
/etc/edge.nightly some_opts -J scheduled_job_name_{master|differ|increm}
```

Description

The *BackupEDGE Scheduler* can set up `cron` to run *EDGE.NIGHTLY* and perform a *Master Backup*, a *Differential Backup*, or an *Incremental Backup* at the proper time and on the proper days of the week if the Enabled checkbox is checked. Regardless of whether the box is or is not checked, it is possible to run the *Scheduled Job* via *EDGEMENU* or from the command-line.

If you wish to run such a job from your own script or the command line, the syntax is as follows...

```
/etc/edge.nightly -H scheduled_job_name
```

For example, the command to run `simple_job`, also known as the *Basic Schedule* is:

```
/etc/edge.nightly -H simple_job
```

You must be logged in as `root` to run this program interactively.

> **NOTE:** The `-H` option uses the day of the week to select whether a *Master*, *Differential*, or *Incremental Backup* is run. If no backup is scheduled for today, then *EDGE.NIGHTLY* will complete successfully after doing nothing.

If you wish to control the type of backup manually, use one the following syntaxes instead:

```
/etc/edge.nightly -J simple_job_master
/etc/edge.nightly -J simple_job_differ
/etc/edge.nightly -J simple_job_increm
```

None of these commands will be affected by the backup type selected in the *Scheduler*. The `-J` option does not function with autochangers.

`some_opts` allows you to modify the behavior of *EDGE.NIGHTLY*. For example, you may choose whether *EDGE.NIGHTLY* will run interactively or not. These options ***must*** be given before `-H` or `-J` if they are specified at all, or they will be ignored.

`some_opts` may be some combination of:

`-f` *`resourcename`*
Sometimes, it is desirable to override the *Resource* that will be used by a *Scheduled Job* specified with the `-H` or `-J` option. Use this option to do so.

`-zMEDIA_LIST=`*`media_list`*
This option allows you to override the media list that will be used with an autochanger. In particular, if you use the `-f` option to specify a tape drive that is embedded in an autochanger, use `-zMEDIA_LIST` to actually use the autochanger to load tapes if the *Scheduled Job* isn't configured to do so already. For example, `-zMEDIA_LIST=st0,st1` would use `st0` as the first tape, and `st1` as the second if required. Of course, you may specify barcoded tapes via `bc` as with any other media list.

`-zDISPLAY_MODE=INTERACTIVE`
If present, then *EDGE.NIGHTLY* will display its progress, and by default prompt the user for intervention interactively. It will still send a summary of the results using the *Notifiers* selected by the *Scheduled Job*, however. At the conclusion of the entire operation, *EDGE.NIGHTLY* will ask for confirmation before exiting. To control this, see `-zASK_MODE` below.

If this option is omitted, *EDGE.NIGHTLY* operate entirely non-interactively; it will produce no output and will use *Notifiers* as it does for Unattended Backups, unless specifically directed to do otherwise with `-zASK_MODE`, as described below.

`-zASK_MODE=ANY|LESS|NEVER|BG`
This option controls how much user input *EDGE.NIGHTLY* will require.

In `-zASK_MODE=ANY`, it will ask any questions of the user it wants, including helping the user see the output by requesting carriage returns from time to time. This is the default behavior if `-zDISPLAY_MODE=INTERACTIVE` is given.

In `-zASK_MODE=LESS`, *EDGE.NIGHTLY* will ask only necessary questions of the user, such as requests to manually load new media.

In `-zASK_MODE=NEVER`, *EDGE.NIGHTLY* will ask nothing of the user. It will attempt to continue the backup and verify if possible by selecting whatever answer is most likely to succeed. In the case of requests for new media, the operation will fail.

In `-zASK_MODE=BG`, *EDGE.NIGHTLY* will operate non-interactively with respect to the terminal from which it is run, but will use *Notifiers* to communicate its requests. For example, if it requires new media, it will use a *Notifier* to request it, and wait for the user to run *EDGEMENU* to acknowledge the request. This is the default if `-zDISPLAY_MODE=INTERACTIVE` is not given. Usually, there is no need to give this option if running *EDGE.NIGHTLY* from the command line; it is not the default only when run with `-zDISPLAY_MODE`, but in that case one usually *wants* interactive behavior.

Regardless of how it is started, *EDGE.NIGHTLY* will exit with a zero exit status on success, and a non-zero exit status on failure. Notification of the backup results will be performed as if it were executed via the Scheduler.

Older (01.01.0x and earlier) versions of *EDGE.NIGHTLY* supported a different command-line interface. This interface has been preserved as well as possible for backwards compatibility ***only***. It is **strongly recommended** that you replace uses of *EDGE.NIGHTLY* that have the old command line options with *Scheduled Jobs* for continued compatibility with *Backup**EDGE***. These legacy options are not documented here, and may be removed in a future version.

If you intend on using *EDGE.NIGHTLY* with the legacy command-line options, it is important that you verify its behavior against what you have expected previously. Of special importance are the log files and listing files; these have changed names and format since the 01.01.0x versions of *Backup**EDGE***. For example, `LAST_Master` is now called `backup_master.log`. Again, it is recommended that you do not use the legacy flags.

Also note that *EDGE.NIGHTLY* always provides the same pathname management facilities as *EDGEMENU*; it performs only non-Expert backups. If you depend on the filenames actually used on the archive, you may need to adapt to different names or run `/bin/edge` directly (this is not recommended). Usually, the *EDGE.RESTORE* program can be used in place of a `/bin/edge` restore so that UNIX-mode paths may be used. See “Command-Line Restores Using EDGE.RESTORE” on page 315 for some information on *EDGE.RESTORE*.

Generally, enhancements to the Scheduling system allow more flexibility than any previous version of *Backup**EDGE***. Before trying to “work around” *EDGE.NIGHTLY* with the legacy options, be sure to familiarize yourself with its new abilities.

Please consult “Scheduled Jobs in More Detail” on page 342 for more information on customizing the *Scheduled Jobs* that *EDGE.NIGHTLY* will run.

35.6 - The EDGE.LABEL Program

Synopsis

```
/usr/lib/edge/bin/edge.label -G resource
```

Description

This program displays the label on whatever medium is loaded in the *Resource* `resource` in human-readable format.

It provides the same information that `EDGEMENU -> Verify -> Show Archive Label` provides, without the character interface.

EDGE.LABEL may be used with remote resources, such as:

```
/usr/lib/edge/bin/edge.label -G mlite:tape0
```

35.7 - EDGEMENU Command-Line Options

Although *EDGEMENU* is normally used without command-line options, several are present that can be useful from time to time.

Starting in Monochrome Mode

```
edgemenu -mono
```

Normally, the *EDGEMENU* interface detects whether your terminal supports color or not, and displays the user interface accordingly. If you wish to force *EDGEMENU* to start in monochrome mode, use the `-mono` option. There is no way to force *EDGEMENU* to start in color mode; it will do so automatically if it can detect color support for your terminal.

Adding Dealer Contact Information

```
edgemenu: usage: edgemenu -dealer [-name dealer_name] [-phone phone]
[-addr address] [-fax fax_number] [-email email_address] [-web url] [-clear]
```

Every text and HTML *Backup**EDGE*** summary can be configured to contain technical contact information. This is useful for Dealers and Resellers who provide support for their customers, as well as for those who manage large installations of *Backup**EDGE***.

If run without additional options, `edgemenu -dealer` will print the current contact information, if any. By specifying the additional option `-clear`, all contact information will be erased. The remaining options allow you to set or clear the name, phone number, address, fax number, email, and web URL information.

If you wish to clear just one of the fields, specify `""` as the information. For example, the following will remove the phone number without changing the other fields:

```
edgemenu -dealer -phone ""
```

Also be sure to use quotes if the information contains spaces. Do not try to include newlines in the information.

Checking Remote Connectivity

```
edgemenu -ping [machine name]
```

Running `edgemenu -ping` instructs *Backup**EDGE*** to attempt to contact the named system, which must also have *Backup**EDGE*** installed. If this test fails, you will be notified about which step failed and why.

Usually, this option is used by Microlite Technical Support, however, it is presented here as it may be helpful to others.

35.8 - The EDGE.ACP Program

This is the Autochanger Control Program. *EDGE.ACP* is a full-screen interactive program which can query the status of a tape autochanger, and interactively allow cartridge manipulation. It is the same interface that pops up when you select `EDGEMENU -> Admin -> Changer Control`.

To run from the command line, log in as root and type...

```
edge.acp
```

You will be prompted to **FastSelect** your autochanger.

See "Autochanger Media Manipulation" on page 250 for more information. on the *EDGE.ACP* user interface.

35.9 - NAS / etc. From The Command-Line

Since media writing is now fully integrated, the `/bin/edge` command can be used to perform backups to any type of resource directly in *Backup**EDGE 2.1*** or later.

```
edge cvf url0 .
edge cvf ftp://ftp.mydomain.com/backups .
edge tvf url0
```

Note that the listing command ('`tvf`') may prompt for user intervention when the listing starts if more than one archive is present. In this case, you will be given a list of archive numbers and a short description of each. You may enter the archive number to list it, or '`i`' then the archive number to get more information about it (e.g., '`i1`'). If there are more archives than can be displayed at once, you may press [Enter] to see more of them listed.

If you know the slot name of the archive you want to read, you may specify that on the command-line with `-zSLOTNAME=` :

```
edge tvf url0 -zSLOTNAME=simple_job.monday
```

If you know the archive number before running the command, you may specify it on the command line:

```
edge tvf url0 -zSEG_NUM=4
```

To find the proper segment number, you may use the edge.segadm segment manager as shown in the next section.

Note that `-zSEG_NUM` does **not** apply to backups; this applies **only** to reads/restores. You do not have control over the archive number during a backup `-zSLOTNAME` applies to both backups and restores.

When writing backups, you may want to specify a different slot name. Otherwise, the default slot name will be used. Remember that doing two backups with the same slot name will cause the first one to be overwritten by the second one.

```
edge cvf url0 -zSLOTNAME=mybackup .
edge cvf url0 -zSLOTNAME=hithere .
```

Note that the slotname substitutions that are used in the Scheduler (e.g., '`%m`' for the machine) do not work on the command line. Instead, you should use the shell or some other method to construct the slot name if you want it to be variable:

```
DAY=`date +%j`
SLOT="backup.${DAY}"
edge cvf url0 -zSLOTNAME=$SLOT .
```

Do not specify a slot name with non-NAS / FSP backups.

35.10 - Maintenance Commands

*Backup**EDGE*** provides some command-line maintenance tools to manage URL / FSP resources. While you probably won't need these, they are provided for completeness.

TERMS REFRESHER

Important terminology:

Medium: something that holds data, such as a tape, Blu-ray Disc cartridge, NAS folder, etc.

Archive: a collection of files of a particular *Domain* at a particular time, such as "*Master Backup of the domain* `system` *at midnight on July 1st, 1999*".

Instance: one particular copy of an *Archive* on a *Medium*. In general, when one refers to a *Backup*, one is talking about one *Instance*.

> For example, when the *Scheduler* runs a *Scheduled Job*, it creates one instance of a new archive for each Domain that is supposed to be backed up as part of the *Scheduled Job*. If a *Scheduled Job* is supposed to back up the `System` and `mysql` *Domains*, then the *Scheduler* will create one *Instance* for each of two new *Archives*.

Segment: a unit of storage on a *Medium*. A NAS, for example, might hold many *Segments*. An *Instance* is composed of one or more *Segments*, possibly contained on more than one *Medium*. The different *Media* can be of different types (tape, NAS, etc.). A *Segment* belongs to exactly one *Instance*. Each *Segment* is given a number, starting from 1, that records the order that it is to be used when reading that *Instance*.

> This may sound complicated, but it isn't. A *Backup* using more than tape, for example, may be said to have one *Segment* on each tape. When writing to a NAS, SharpDrive, etc., *Backup**EDGE*** typically breaks a single *Backup* into *Segments* of 1GB each, which gets around file size limits. When S3CLOUD or re-startable NAS backups are performed, the *Backup* is broken (by default) into small 50MB *Segments*. In the event of a network failure, this provides for a smaller amount of data that needs to be cached and re-transmitted after a re-start.

*Label: Backup**EDGE*** includes information about every *Segment* at the start of that *Segment*. This *Label* tells roughly what the *Backup* contains, when it was made, what *Instance* this *Segment* belongs to, the order of this *Segment* relative to the other *Segments* in this *Instance*, etc.

> If two *Instances* of the same *Archive* exist, it is not the case that one can necessarily interchange the *Segments* which comprise them. For example, one cannot generally read the first *Segment* of *Instance 1* then the second *Segment* of *Instance 2*, and expect to get anything useful from it. While they contain the same data if extracted, that data might be stored differently between the two *Instances*. The number of *Segments* might not even be the same.

Archive ID: an identifier that uniquely identifies an *Archive*. All *Instances* of the same *Archive* have the same *Archive ID*. It is stored in the *Label* for every *Segment* of every *Instance*. If you copy an *Archive* using the *Scheduler* or ***edge.xfer***, the copy will have the same *Archive ID* as the original.

Instance ID: an identifier that uniquely identifies an *Instance*. All *Instances* have a unique *Instance ID*. Each *Segment* of the *Instance* has this *Instance ID* stored in it. If you copy an *Archive* using the *Scheduler* or ***edge.xfer***, the copy will have the same *Archive ID* as the original. but a different *Instance_ID*.

Job ID: an identifier that uniquely identifies a run of a *Scheduled Job*.

> Every *Instance* created by a single run of a *Scheduled Job* shares a *Job ID*. If a *Scheduled Job* is supposed to back up the `System` and `mysql` *Domains*, both *Instances* would share the same *Job ID*, but no other *Instance* would.

EDGE.SEGADM

edge.segadm manages the archives and segments on NAS/S3CLOUD/SharpDrive/FSP *Resources* (or anything else, really). It can be used to:

- Initialize and erase all contents of a *Resource*.
- Initialize non-destructively, simply recalculating the control file of a *Resource*.
- Identify *Archive Instances* and *Jobs*. Once identified, they can then be either deleted by calling ***edge.segadm*** with the `-d` flag and unique archive information, or copied by the ***edge.xfer*** program.
- Delete unwanted archives and jobs.

It can also delete individual *Segments*, but as they represent only parts of an archive, this is generally not a good idea.

The output of ***edge.segadm*** can be returned as text (the default) or as environment variables which may be used by other programs (use the `-terse` flag)...

```
edge.segadm [-terse] [-f resource] [filters] [commands]

Filter options:
-zSEG_NUM=# : use given segment number (starting from 1)
-r: reclaimable segments only
-R: non-reclaimable segments only
-s slotname : must match slot name
-zARCHID=archid : must match archive id
-zJOBID=jobid : must match job id
-zJOB=job : must match job name
-zSEQUENCE=sequence : must match sequence
-zDOMAIN=domain : must match domain
-zDATEBEFORE=date : must be older than date
-zNEWEST: only select most recent segment(s)

Command options:
-b: reinitialize nondestructively
-B: reinitialize destructively (ERASES EVERYTHING)
-d: delete all matching segments
-l: lists all matching segments
-t: list; synonym for -l
-L: lists all matching segments verbosely
-T: list; synonym for -L
```

You may include '`-f resource`' on any of the commands given below to select the *Resource* to use. By default, the *Primary Resource* selected in edgemenu will be used.

Examples:

```
/usr/lib/edge/bin/edge.segadm -f url0 -l
```

this will list all the segments on whatever medium is loaded in this *Resource*. Each *Segment* listed will be given a number that can be used to reference it later. Here is the format for one the first *Segment* of a typical response.

```
Segment 1 (1023MB) --
ml310 system Edgemenu 03.00.00 Master 2010/11/24 14:34:01
```

```
/usr/lib/edge/bin/edge.segadm -terse -f url0 -l
```

this will return the same information as above, except as environment variables. It is typically used to identify unique *Archives*. Here is the format for one the first *Segment* of a typical response.

```
SEGADM_SEG0_SEGMENT=1
SEGADM_SEG0_SIZE_MB=1073709056
SEGADM_SEG0_ARCHID=095736af418ad0a1
SEGADM_SEG0_INSTID=687aada76fd48c42
SEGADM_SEG0_JOBID=1f38f39d61f0648b
SEGADM_SEG0_JOB=ml310.microlite.com:simple_job_master
SEGADM_SEG0_SEQ=ml310.microlite.com:onsite
```

```
SEGADM_SEG0_DOM=ml310.microlite.com:system
SEGADM_SEG0_SEG=1
SEGADM_SEG0_DATE=1290627241
SEGADM_SEG0_SYS=ml310.microlite
```

```
/usr/lib/edge/bin/edge.segadm -f url0 -zSEG_NUM=# -l
```

(Replace `#` with a segment number.) This will list the entire label for the given segment number.

```
/usr/lib/edge/bin/edge.segadm -f url0 -zDATEBEFORE="11/25/2010" -d
```

This will delete ALL the *Archives* on `ulr0` with creation dates prior to 11/25/2010 at midnight, and possibly re-number the *Segments*.

```
/usr/lib/edge/bin/edge.segadm -f url0 \
-zDOMAIN="ml310.microlite.com:system" -zDATEBEFORE="11/25/2010" -l
```

This will list ALL (and ONLY) the *Archives* on `url0` that were created by the *Domain* `system` of `ml310.microlite.com`.

```
/usr/lib/edge/bin/edge.segadm -f url0 -zDOMAIN="ml310.microlite.
com:system" -NEWEST -l
```

This will list the latest *Archives* on `url0` that were created by the *Domain* `system` of `ml310.microlite.com`.

Typical Usage:

```
/usr/lib/edge/bin/edge.segadm -f url0 -b
```

This will non-destructively re-initialize *Resource* `url0`, re-calculating the control file.

```
/usr/lib/edge/bin/edge.segadm -f url1 -B
```

This will **destructively** re-initialize *Resource* `url0`, resetting the control file and **erasing** all *Segments* in the Resource.

```
eval `/usr/lib/edge/bin/edge.segadm -terse -f url0 \
-zJOB=ml310.microlite.com:simple_job_master -l -zNEWEST 2>/dev/null|head -11`

/usr/lib/edge/bin/edge.xfer -from url0 -from_archid ${SEGADM_SEG0_ARCHID} \
-to s3cloud0
```

This will identify the latest *Archive* created on *Resource* `url0` and, using its unique *Archive ID* number, copy it to *Resource* `s3cloud0`.

Experiment with different commands and IDs to create programs that perform the archive and media manipulation you desire.

EDGE.URLUTIL

edge.urlutil is the archive listing utility. It is used list the contents of archives, but may also be used to manage and find specific directories and folders in S3CLOUD archives.

```
# /usr/lib/edge/bin/edge.urlutil
edge.urlutil: usage:
    -f resource
    -r (recursive)
    -D (delete)
    -u url (override url)

example: edge.urlutil -f url0
```

It may also be used for deleting individual archive segments, and should be used very carefully as improper use can damage archives.

Examples:

The only example (and only recommended use) for this utility is to identify lost directories in S3CLOUD backups.

From the Unix/Linux command line you can manipulate *Backup**EDGE*** buckets.

Identifying / Listing Buckets

Try some of these commands from the root shell.

```
# /usr/lib/edge/bin/edge.urlutil -f s3cloud0
```

will return the "Bucket name" of a resource, as in...

```
edge.urlutil: info: opening resource
'uewo-ghpc-wgaz-dbsq' (unknown size)
(end of directory listing)
0 bytes listed
```

With the bucket name (example in **bold** above) known,

```
# /usr/lib/edge/bin/edge.urlutil -f s3cloud0 -r -u uewo-ghpc-wgaz-dbsq
```

(using YOUR Bucket Name) will walk the entire url, or...

```
# /usr/lib/edge/bin/edge.urlutil -f s3cloud0 -r -u uewo-ghpc-wgaz-dbsq  |grep
ctl
```

will show just the directory names of the *Resource*, for instance:

```
edge.urlutil: info: opening resource
(end of directory listing)
'backups/ctl' 7
'mlite/ctl' 3272
```

Would identify "`/backups`" and "`/mlite`" as *Resource Directories* in this example.

Deleting Archives

Using the *Resource Directory* names shown above, you could define an *S3CLOUD Resource* with each of the directory names (`/backup`s and `/mlite`) in turn, then use EDGEMENU to delete any unneeded archives. You could also define the *Resources* in EDGEMENU, then use *EDGE.SEGADM* (page 330) which is the command line tool for this purpose.

Deleting Entire Resource Directories

In the example above, you could also permanently delete the entire "`/mlite`" *Resource Directory* and ALL its contents (including the directory name itself, all archives, and the *ctl* file with:

```
# /usr/lib/edge/bin/edge.urlutil -f s3cloud0 -D -u uewo-ghpc-wgaz-dbsq/mlite
```

Hint 1 for the power user: ***edge.urlutil*** and ***edge.segadm*** are not limited to S3CLOUD *Resources*.

Hint 2: These programs were upgraded in 03.00.03 build 3. The syntax here and in the manual reflects this release, and may not be the same in older versions.

EDGE.XFER

edge.xfer is the archive copy utility. It is used to copy one complete *Archive*, *Instance* or *Job* from one *Resource* to another. It is used internally by the `copy to`: function in the *Scheduler*, but may be called by the end user from either the command line or from a script or program.

Archive ID, *Instance ID* or *Job ID* may be obtained from **edge.segadm**, above.

```
edge.xfer [-terse] -from resource [-from_slot slotname] [-from_archid archive_id]
[-from_instid instanceid[ [-from_jobid jobid] -to resource [-to slotname]

-from requires a resource name
-to requires a resource name

Options:
-from_slot requires a slot name
-to_slot requires a slot name
-from_archid
-from_archid requires an archive id
-from_instid
-from_instid requires an instance id
-from_jobid
-from_jobid requires a job id

Modifiers:
-add_seq
```

Archives are automatically re-segmented to fit the destination *Resource*. If a particular software compression mode is specified in the *Resource* definition, the *Archive* is automatically compressed to that specification. If to a *Resource* where `No` or `Hardware` compression is specified, no re-compression will occur.

Examples:

```
/usr/lib/edge/bin/edge.xfer -from url0 -from_archid archive_ID -to url1
```

assuming a valid *Archive ID*, this will copy the *Archive* from `url0` to `url1`.

```
/usr/lib/edge/bin/edge.xfer -from url0 -from_archid archive_ID -to tape0 \
-add_seq
```

assuming a valid *Archive ID*, this will copy the *Archive* from `url0` to `tape0`. effectively turning the *multi-Segment* NAS backup into a single *Segment* tape backup (if it fits on one tape. It will also make the copy a part of the *Sequence*. This means that, for example, the original *Archive* could be deleted and *Differential* or *Incremental Backups* would know to base themselves on the copy.

EDGE.NASMGR

edge.nasmgr is the NAS/AF/FSP management tool. It has several options:

```
/usr/lib/edge/bin/edge.nasmgr -U af0
```

This will forcibly unmount the named AF resource, and mark it as unused. If *Backup**EDGE*** somehow gets confused and thinks that an AF is in use when it is not, you can use this command to force it to mark the device as unused.

For example, if the unmount command fails, *Backup**EDGE*** might have no choice except to leave the AF mounted. You can use **edge.nasmgr** to mark the resource as not in use and unmounted once you figure out why the unmount failed.

```
/usr/lib/edge/bin/edge.nasmgr -I af0
```

This will manually initialize the AF. No backups will be erased. Note that this does not rebuild the control file for any FSPs that use the AF. This will initialize the AF itself for use with *Backup**EDGE***. Generally, you won't need to run this command. If you want to rebuild the control file of one particular FSP, use **edge.segadm** as described below.

36 - Error Return Codes

*Backup**EDGE*** command-line tools return an error code indicative of the status of the operation performed. A return code of `0` means the operation was successful. These codes are also reported by *EDGEMENU* when an operation fails.

The following list shows the possible return codes and their respective meanings:

`0 - complete success`
Congratulations!

`1 - error in command usage`
If you are entering `/bin/edge` commands directly, you have mis-typed the command line. Please Consult the *Technical Reference Guide* for more information on this subject. You may also want to consider not running `/bin/edge` directly.

If you are using *EDGEMENU*, this error may be caused by an incorrect field in the *Resource Manager*. If you have not edited any *Resources* manually, or if you do not see an error in the Resource, you should contact *support@microlite.com* for assistance.

`2 - miscellaneous error, not otherwise defined below`
This error is of historical value.

`3 - error reading from the archive device`
While verifying or restoring data, *Backup**EDGE*** received an error from the Operating System indicating that the data could not be obtained from the archive. Usually, this indicates a hardware read error of some sort, and may be accompanied by *TapeAlert*™ messages in the verify or restore summary.

`4 - error writing to the archive device`
This message means that some failure occurred while writing an archive. If this error occurs near the expected end of the medium, it may be an incorrect (too large) volume size in the *Resource Manager*. If the volume size is `0` (unlimited), try setting it to the appropriate size for this medium. It may be a hardware write error from the operating system indicating a bad spot on the medium, a failing tape (etc.) drive, etc. If you are writing to CD-R/RW's, it can also indicate that the burn process failed because of a buffer underrun (try increasing the buffer size in the `Resource Manager`, disabling Software Compression, or lowering the burn speed).

`5 - error opening or accessing a file or device`
*Backup**EDGE*** could not open a file while performing a backup. Consult the log file in `/usr/lib/edge/lists/(jobname)` or the summary for the file that failed, and try reading that file yourself. If it is not readable, you may have filesystem corruption or a failing hard drive. Otherwise, contact *support@microlite.com* for assistance.

`6 - error while reading a file from the hard disk`
When performing a backup or verify, *Backup**EDGE*** encountered a read error from the Operating System while reading a file from the filesystem. This generally indicates that one or more files (mentioned in the summary) are not accessible, and may be the result of filesystem corruption or a failing hard drive. It is generally not related to the archive *Device*. Try backing up just the file(s) which failed.

`7 - error while writing a file to the hard disk`
While restoring data, *Backup**EDGE*** could not write a file to the filesystem. The most likely cause is that the filesystem ran out of space. If you did not back a virtual file up as virtual, this error is very common, since virtual files take up much more physical disk space after a restore if they were not marked as virtual for the backup.

`8 - not enough memory available`
*Backup**EDGE*** was unable to allocate memory. Exceptionally large *EDGE Block Factors* (the default value is `64`) may cause this problem. Remember that the *EDGE Block Factor* is measured in 512-byte blocks.

`9 - unused`
This error is no longer used.

`10 - the header block of the file to be restored is bad`

*Backup**EDGE*** read a file header from an archive that had an incorrect checksum. Either the data has been corrupted on the medium, or it is being transferred incorrectly to the operating system. If the *EDGE Block Size* or *Tape Block Size* in the *Resource Manager* do not match what the archive was written with, this error can sometimes result even with a good tape. In this case, correct the settings in the *Resource Manager* and try again. If the problem persists, contact *support@microlite.com* for assistance.

11 - interrupted
*Backup**EDGE*** was interrupted by the user, either by cancelling a backup or refusing a request for new media.

12 - error seeking on archive device
*Backup**EDGE*** was unable to seek while reading or writing an archive. Be sure that the *Device* can actually perform random access. Tape drives are never seeking *Devices*. Check the *Resource Manager* to see if the *Seeking* option is set.

If you are using a DVD *Device*, try toggling the *Indexing* flag to its opposite state to see if the error persists.

13 - error while verifying data
An error occurred during the verify phase. The archive should not be trusted.

14 - byte level compare during level 2 verify
*Backup**EDGE*** found differences between the data on the archive and the original data. This indicates that the backup **SHOULD NOT BE USED**. Modifying files on the hard disk after a backup but before the verify should **NOT** produce this error, unless the timestamps on the files were reset to match those on the archive. Otherwise, *Backup**EDGE*** will report that the file has been modified since it was backed up, which is not an error.

15 - incomplete operation
*Backup**EDGE*** could not backup or restore all the requested files. For a backup, this means that some files weren't found on the filesystem, or could not be accessed. For a restore, this means that some files weren't on the archive. Verification can fail with this error if encrypted files are found on the archive, but no key is available to decrypt them.

16 - unused
This error is no longer used.

17 - unused
This error is no longer used.

18 - dual process synchronization error
This error indicates that *Double Buffering* failed because the reading and writing processes became un-synchronized. Contact *support@microlite.com*, or disable *Double Buffering*.

20 - Cannot Get Temporary Database
While Indexing an archive, *Backup**EDGE*** could not open a temporary database. It is possible that the filesystem containing `/usr/lib/edge/database` is full, mounted read-only, or that the directory is missing altogether. Disabling *Indexing* in the *Scheduler* (Notify / Advanced) will get around this problem, but no database will be created for *Fast / Instant File Restore*!

21 - Cannot Open Database
*Backup**EDGE*** was unable to open an archive database. Usually, this indicates that the user does not have sufficient permissions on the files in `/usr/lib/edge/database`, or that directory is missing.

22 - Exec Failed
*Backup**EDGE*** could not run some external program. The exact cause of this error depends on what it was trying to do. Contact *support@microlite.com* for assistance.

23 - Cannot Open Resource
This error indicates that the resource could not be accessed. Check the *Device Node*(s) in the *Resource Manager* to be sure they are spelled right. Also be sure those *Device Nodes* are present, and can access the *Device*. Also be sure that the resource name is spelled correctly if you are using a command-line tool such as *EDGE.TAPE*.

24 - Unlabeled Tape Detected

You tried to perform an action that requires a labelled tape, such as *Indexing* for *Fast File Restore*. It is also possible that the archive cannot be read, possibly due to a *Tape Blocksize* mismatch.

25 - Unexpected EOM / Corrupt Database
While reading from an archive, the End-of-Medium was found unexpectedly. If this occurs during indexing, it means the medium most likely has a read error (try running a verification of the archive with indexing disabled from *EDGEMENU*). If this is during a restore, it is possible that a read error occurred in much the same way, or that the positioning information in the database doesn't reflect the data that is on the archive.

26 - EDGE Failed
Some error occurred during a *Fast File Restore* or *Index* operation. Repeat the operation using normal (not *FFR/IFR*) restore, or with *Indexing* disabled. This may produce a more descriptive error message.

27 - Maximum Path Length Exceeded
*Backup**EDGE*** cannot archive files with pathnames longer than `400` characters. If the file is a symlink, or a hard link, neither the filename nor its link target may be more than `170` characters long. A file with a path larger than this was encountered.

28 - Filename Not Found
A given filename wasn't found. The cause of this error depends on what issued it.

29 - Cannot Get Tape Blocksize
An error occurred trying to read the hardware parameters from a tape drive or other *Device*. Make sure the *Device* is accessible to the operating system, and that the *Resource Manager* has correct values for it.

30 - Cannot Reopen Control Device
Low-level SCSI control of a *Device* failed. Contact *support@microlite.com* for assistance.

31 - Erase / Reten / Etc. Command Failed
A command that (probably) produces tape motion failed. Usually, this indicates that the *Device* refused the command. For example, attempting to erase a write-protected tape might cause this error.

32 - Cannot Scan Changer
*Backup**EDGE*** was unable to scan a tape autochanger to determine its inventory. This indicates that the *Device* may be improperly set up in the operating system or busy. It is also possible that the *Device Node* setting in the *Resource Manager* is incorrect.

33 - Move Failed
*Backup**EDGE*** received an error while moving tapes in an autochanger. This may be because the source element was empty, the destination element was full, an unknown element was specified, or the *Device* encountered some physical obstruction of some kind. Loading a cleaning cartridge generally produces this message also, although the cleaning cycle takes place.

34 - No Tape
A requested operation requires a medium, but none was detected. Either no medium is present, or the detection process is mis-configured. Make sure the Resource Manager settings are correct. Also, use `edgemenu -> View -> Primary Resource Status` to see if media is detected.

35 - Can't Get Sense Data
An error occurred, but *Backup**EDGE*** was unable to get specific information about it. Generally this error is not reported, in favor of the one that occurred that caused *Backup**EDGE*** to try to get additional information in the first place.

36 - SCSI Command Failed
A SCSI command sent by *Backup**EDGE*** failed. This may be the result of an improper setting in the *Resource Manager*. If the *Device* is generally working properly with *Backup**EDGE*** (try `edge.tape -t resource_name` and see if you get any useful output), it may be the case that the *Device* simply doesn't support whatever *Backup**EDGE*** is asking it to do.

37 - Error Getting Device Parameters
*Backup**EDGE*** could not determine the basic *Device* parameters, such as low-level block size, etc. This may indicate a communications problem between *Backup**EDGE*** and the operating system, or the operating system and the *Device*. Make sure the *Resource Manager* settings are correct, and that the *Device* can be accessed from the operating system. Also be sure that all needed kernel modules (such as '`sg`' in Linux) are loaded.

38 - Erase Failed
*Backup**EDGE*** was unable to erase a tape or blank a CD-RW. If this is a CD-RW, the disc may be damaged.

39 - Error Setting Device Parameters
*Backup**EDGE*** was unable to set the *Device* parameters, such as low-level block size. This may indicate that a communications error has occurred, but may also indicate that the *Device* wasn't ready when *Backup**EDGE*** attempted to access it. If this occurs after a backup or verify, you may need to adjust the setting of `SETTLE_TIME` in `/usr/lib/edge/config/devices.def` for the *Resource* in question, to give it more time to become ready (**CAUTION**: modifying `devices.def` without a full understanding of the variables and formats involved incorrectly can result in a non-functional installation of *Backup**EDGE***.)

40 - Create Partition Failed
*Backup**EDGE*** was unable to partition a tape. Most likely, the partition size was too big, or the *Device* does not support partitioning.

41 - Not Implemented
*Backup**EDGE*** does not support the attempted operation, such as sending an `Eject` command to a disk file.

42 - Locate / Read Position Failed
*Backup**EDGE*** was unable to use *Fast File Restore*. Be sure the *Device* supports it by running *Manual Check* from the *Resource Manager* (**CAUTION**: have a tape in the drive that can be overwritten safely!).

43 - Startup Error
*Backup**EDGE*** has encountered a licensing error. Contact *support@microlite.com* for assistance.

44 - Internal Error
An internal error occurred. Contact *support@microlite.com* for assistance.

45 - Error Compiling Device Database
The file `/usr/lib/edge/config/devices.def` is missing or corrupt. Running *EDGE.TAPE* from the command line will provide more information about what went wrong.

46 - Media Is Write-Protected
*Backup**EDGE*** does not believe the medium can be written to. This also indicates that it has been told (in `devices.def`) that writing is not possible for the given medium type.

47 - Error Initializing X-Windows
*Backup**EDGE*** could not start *EDGE.EMX*. Make sure that the `DISPLAY` shell variable is set and exported correctly, and that the client (`edge.emx`) has "`xhost`" permission on the X Server.

48 - Initialize Elements Failed
*Backup**EDGE*** could not scan an autochanger. See Error 32.

49 - Database Append Failed
*Backup**EDGE*** could not perform an append operation on a database.

50 - Write Failed
*Backup**EDGE*** encountered a failure while writing. Normally, this indicates a full filesystem or bad medium.

51 - Device Is Not Removable
*Backup**EDGE*** tried to load / unload / etc. some medium that is not removable, such as a hard disk.

52 - Cannot Create Pipe
*Backup**EDGE*** is unable to create a named pipe for inter-process communication. Make sure the directory `/usr/lib/edge/system/pipes` exists and is writable. Also make sure that "`df -i`" reports some free inodes on that filesystem. This error is not related to Error 9, which involves using pipes for software compression.

53 - Cannot Start Operation
*Backup**EDGE*** encountered a failure during the startup phase of a backup / verify / restore. Normally, the summary will provide more descriptive information. This error shows up for anything that stops a backup before data is actually transferred to or from the medium (excluding any attempt to read the label).

54 - Script Failed
An external script, such as a *Domain* start/stop script, exited with a `nonzero` status. The summary should detail which script failed.

55 - Changer Problem
Some error occurred while trying to load media for a *Scheduled Job* using an autochanger. Be sure the media list in the *Scheduler* is correct, and that tapes are loaded into the indicated slots. The summary may provide more information.

56 - Machine Not Available
A remote machine could not be contacted. Try '`edgemenu -ping machinename`' to get more specific information.

57 - System Name Changed
The system's name has changed. This can cause problems with *Backup**EDGE***'s configuration. Please see "Changing The System Name" on page 277.

58 - RecoverEDGE Token File Error
*Recover**EDGE*** could not create a token file to describe aspects of the system configuration. Please contact *support@microlite.com* for assistance.

59 - No Read/Write Command Found
This error indicates that *Backup**EDGE*** could not find the appropriate command to write to a *Device*. It probably indicates a configuration error of some kind. Contact *support@microlite.com* for assistance.

60 - Failure Finishing Optical Medium
An error occurred while closing an optical medium, such a a CD-R. This could indicate a bad medium.

61 - Indexing Failed
An error occurred while Indexing during *Verify*. It may indicate a read error on the tape. Disable *Indexing* and try the *Verify* again. If the *Verify* fails again, the error message returned should be more complete and indicate the true cause of the failure. If no error occurs, contact *support@microlite.com*.

`105 - Tape Open Failed`
This error indicates that a tape drive or other archive device could not be opened.

`106 - HD Open Failed`
This error indicates that a file on the hard drive could not be opened.

`107 - Generic System Error`
This error is produced when the operating system reports an error that is not covered by some other error number.

`108 - Internal Error`
This error indicates that *Backup**EDGE*** has detected an internal inconsistency. Please contact Microlite Technical Support for assistance (`support@microlite.com`).

`109 - General Backup Error`
This error occurs when some operation during a backup fails that is not covered better by another error.

`110 - End-of-medium Encountered`
If *Backup**EDGE*** detects an end-of-medium marker unexpectedly, and cannot recover, this error is generated. Normally, this error is not reported since a new volume is loaded by the user.

`111 - General Double-Buffering Error`
The double buffering system has detected an error. Disable double buffering, or contact `support@microlite.com` for assistance.

`112 - Bad Password`
You have supplied an incorrect passphrase for an encrypted archive. While you can still access the unencrypted files, the encrypted ones will not be accessible.

`113 - End-of-archive Encountered`
*Backup**EDGE*** has found the end of an archive. Normally, this is not a reported error.

`114 - Informational`
This is an informational warning, rather than an error.

`115 - Receiver Shut Down`

BackupEDGE detected that some of the data pipeline it uses internally has shut down early. Please contact `support@microlite.com` for assistance.

`116 - Out-of-band Data Corrupt`
Some of the data on an archive cannot be read. This data should have included internal *BackupEDGE* information, but it did not or it was corrupt.

`117 - Callback Error`
The callback subsystem has reported an error. Please contact `support@microlite.com` for assistance.

`118 - Compress Pipe Failure`
While using pipe compression, *BackupEDGE* ran out of space. Disable pipe compression and use streaming compression (the default) instead.

`119 - Compress / Decompress Error`
An error occurred while compressing or decompressing data. This could be caused by corrupt data on the archive, if this is a read operation.

`120 - Locate Failed`
BackupEDGE is unable to position on the medium.

`121 - Locate Failed`
BackupEDGE is unable to position on the medium.

`122 - User Not Authorized`
The user that is running *BackupEDGE* does not have sufficient permissions to perform the requested operation.

`123 - Locate Failed`
BackupEDGE is unable to position on the medium.

`124 - Network Link Failed`
While sending data over a network, the connection failed. This is probably due to a network error, or the program on the remote machine exited unexpectedly.

`125 - General Filter Error`
Some data filter in *BackupEDGE* reported an error. The filter involved, along with more information about the error, is usually printed.

`126 - RNG Subsystem Error`
The Random Number Generation subsystem has detected an error.

`127 - Lock Failed`
BackupEDGE is unable to lock a file during a backup.

37 - Scheduled Jobs in More Detail

37.1 - Running Scripts to Prepare for Backup

When a *Domain* is archived by a *Scheduled Job*, it is possible to include custom scripts to prepare the *Domain* beforehand, and reset it afterwards. This *Domain Script* is run as follows:

- Before the backup, the script is run as:
  `script -begin domain_name backup 0`
  where `domain_name` is replaced by the name of the *Domain* being backed up.
- After the backup, the script is run as:
  `script -end domain_name backup return_code`
  where `domain_name` is replaced by the *Domain* name, and `return_code` is replaced by the numeric return code of the backup. Generally, `0` and `15` indicate complete and partial success, while any other return code represents failure.
- Before verification, the script is run as:
  `script -begin domain_name verify 0`
- After verification, the script is run as:
  `script -end domain_name verify return_code`

Since many users of *Backup**EDGE*** are used to configuring nightly backups in a certain way, 01.02.04 emulates the behavior of older releases by default. The Basic Schedule's *Domain*, `system`, uses *EDGE.BSCRIPT* as the *Domain Script* to do this. Other *Domains* may use any *Domain Script*(s) you like.

WARNING: Be sure that your scripts exit with a `zero` status (success) if the operation is not `backup` or `verify` as reported in the command line! Future versions of *Backup**EDGE*** may use additional operations. In particular, do not assume that if the parameter is not `backup` it must be `verify`. Avoiding this will help keep your scripts compatible with future versions of *Backup**EDGE***.

NOTE: The *Domain Script* is intended to prepare the ***data*** for archiving, and to return it to normal operation after the archive operation completes. It is not intended to perform tasks specific to any *Scheduled Job*, such as sending reports! It is also not intended to prepare the ***Resource*** for access, either!

EDGE.BSCRIPT

This is the default *Domain Script* for the `system` *Domain*. It is a wrapper that emulates the behavior of older versions of *Backup**EDGE*** (01.01.0x and earlier). Normally, ***no modifications*** should be made to this file directly. This file will be overwritten whenever *Backup**EDGE*** is (re)installed or upgraded.

At the start of a backup, *EDGE.BSCRIPT* runs the *EDGE.START* script. At the conclusion of a successful backup and verify, it runs the *EDGE.PASSED* script. If the backup or verify fails, *EDGE.FAILED* is run.

There are a few differences about this behavior from previous versions, however:

- *EDGE.PASSED* is not run unless a backup is **verified successfully**. As it is ***strongly recommended*** that all *Scheduled Jobs* include a verify, this should not affect most people. If you really want to run *EDGE.PASSED* without verifying the backup, you must change *EDGE.BSCRIPT* to do so.

- *EDGE.BSCRIPT* will not be run if certain startup errors are encountered. These involve configuration issues with the *Scheduled Job* itself. Like earlier versions, *EDGE.PASSED* or *EDGE.FAILED* will be run only if *EDGE.START* has been run first.
- Semantically, *EDGE.START*/*PASSED*/*FAILED* were in reference to the start, success, and failure of the ***backup job*** in 01.01.0x and earlier. Now, they are related to the preparation and un-preparation of the *Domain* being archived or verified. This difference shows up only if you are using these scripts for tasks such as sending notification about the status of the nightly backup process, etc., rather than preparing the system for backup or returning it to normal use. In practice, this means that the scripts might not be called as often as in previous releases. If you are using these scripts for sending notification, please review the new *Notifier* options in this release of *Backup**EDGE*** in “Notification Options” on page 218.

EDGE.START

By default, *EDGE.BSCRIPT* will execute the program `/etc/edge.start`. This program is a shell script that does nothing but exit with a zero exit status. It is designed to be user modified. You may place commands here which will shut down spoolers, log out users, etc. as required. If `/etc/edge.start` exits with a nonzero exit status, the backup (and optionally verify) will **NOT** be performed, and the program `/etc/edge.failed` will be run. Otherwise, the backup will begin.

If you are backing up a *Domain* that does not specify *EDGE.BSCRIPT*, the above discussion does not apply. It is intended only for backwards compatibility.

EDGE.PASSED / EDGE.FAILED

If the backup and verify complete successfully, *EDGE.BSCRIPT* will execute the program `/etc/edge.passed`. If the backup or verify fail, or if `/etc/edge.start` exits with a nonzero exit status, then the program `/etc/edge.failed` will be executed. The programs `/etc/edge.passed` and `/etc/edge.failed` are Bourne shell programs set up by default to do nothing but exit with the proper exit status.

These programs are also designed to be user modified. They are shell programs containing a variety of environment variables which can be used to execute custom functions. Unlike previous versions, these scripts should ***not*** be used to report the status of the backup job; this may be accomplished through *Backup**EDGE** Notifiers* (described in the User’s Guide). These scripts should be used to un-prepare the *Backup Domain* after a backup and verify. For example, an appropriate use of these scripts is to re-start databases stopped by *EDGE.START*.

If a new release of *Backup**EDGE*** is installed over an old one, the files `/etc/edge.start`, `/etc/edge.passed`, and `/etc/edge.failed` will be copied to `/etc/edge.start00`, `/etc/edge.passed00`, and `/etc/edge.failed00`, respectively, for safekeeping. Then new versions of these programs will be installed from the distribution. The user should take care to migrate any modifications into the new versions.

Older releases of *Backup**EDGE*** used these programs to print a nightly backup report. This functionality has been folded into the *Scheduler*.

If you are backing up a *Domain* that does not specify *EDGE.BSCRIPT*, the above discussion does not apply.

37.2 - Multi-Volume Nightly Backups

*Backup**EDGE*** scheduled backups should ideally fit on one volume. If a *Master Backup* fits on one volume, then it is best to perform one at least each night. If not, performing attended *Master Backups* and automatic *Differential* or *Incremental Backups* is the next best procedure.

If it is absolutely necessary to perform automatic backups which require more than one volume, a method exists for inserting the second volume and informing the *BackupEDGE* task which is waiting in the background. Simply start *EDGEMENU* on the machine performing the backup, and it will notice that a stopped *Scheduled Job* exists. You will be given the option to continue or abort the backup, along with an explanation of why it has stopped.

Generally, email notification will be used to indicate that this situation exists. If you received no email at all, you should first run *EDGEMENU*, select `Admin -> Browse Running Jobs`, and look at the status of the job that has not sent mail. Not receiving email usually constitutes a configuration problem.

Alternatively, use a `ps` command confirms that *BackupEDGE* processes are still running. If so, perform the following steps.

Check the end of the appropriate catalog file.

```
tail /usr/lib/edge/lists/(jobname)/backup_master.log[1]
```

If the normal *BackupEDGE* summary appears, the backup completed successfully. Check for the verify log similarly.

If the file doesn't appear to be complete, it is possible that the archive *Device* is hung because of a media or driver fault.

If the end of the file shows a "locked file" message, free the locked file from the appropriate terminal and the backup will continue.

This procedure requires some operating system knowledge, and so is only recommended if, even with compression, *Master*, *Differential*, or *Incremental Backups* will not fit on one volume.

REMEMBER: If you are performing multi-volume backups, you will be prompted to re-insert the first volume when the verify begins! *Indexing* for *FFA/IFA* is disabled on multi-volume backups.

37.3 - Excluding Files and Directories From Backups

When using the default *Domain* `system`, the file called `/etc/edge.exclude` is used to store `exclude` filenames. If this file exists and consists of directory names or file names, one per line, up to 128 files and 128 directories, then these directories and/or files will be excluded from the backup performed by any *Scheduled Job* which backs up the default *Domain*. A sample `/etc/edge.exclude` file is included in the distribution. It will automatically exclude the *BackupEDGE* catalog file directory from being backed up. You may add additional file and/or directory names.

If you are using a different *Domain*, you may select any file(s) to take the place of `/etc/edge.exclude`.

NOTE: Wildcards can be used to identify files and directories to be excluded. See "Wildcard Exclusion During Nightly Backups" on page 314 for further information.

37.4 - Excluding Files From Bit Level Verification

The default Domain `system` checks for the existence of a file called `/etc/edge.nocheck`. If this file exists and consists of file names, one per line, then these files will be excluded from *Bit Level Verification*, if selected. A sample `/etc/edge.nocheck` file is included in the installation. It contains filenames that frequently change between a Backup and a Verify. You may add additional file names.

1. For *Differential / Incremental Backups*, this would be `/usr/lib/edge/lists/(jobname)/backup_differential.log` (etc.).

If you are using a different *Domain*, you may select any file to take the place of `/etc/edge.nocheck`.

37.5 - Virtual File Identification

By default, the default *Domain* (`system`) looks at the file `/etc/edge.virtual` to determine which files should be treated as virtual (sometimes called sparse). *EDGEMENU* also looks at this file by default.

ALL files to be treated as virtual **must** be identified by listing their full pathnames, one per line, in the file `/etc/edge.virtual`.

For example, if the file `/etc/edge.virtual` contained...

```
/usr/mdx/data/onefile
/usr/vpix/defaults/C:
/usr/bin/vpix/C:
```

then any backups done from *EDGEMENU* or *EDGE.NIGHTLY* (using the `system` *Domain*) would automatically treat the above three files as virtual during backups.

During restore operations, files saved as virtual are automatically detected and reconstructed.

If you are using a different *Domain*, you may choose any file to replace `edge.virtual` with the file of your choice in the *EDGEMENU Domain Editor*.

Please consult “Virtual File Backups” on page 353 in the *Backup**EDGE*** User’s Guide for more information.

37.6 - Raw Filesystem Partition Identification

The default *Domain* (`system`) uses the file `/etc/edge.raw` to list, one per line, the *Device Nodes* which will also have their associated data archived. For example, if one lists `/dev/the_floppy_disk` in `/etc/edge.raw`, not only will the *Device Node* `/dev/the_floppy_disk` be archived, but any data on that *Device* as well (presumably whatever floppy disk is in the drive at the time). Unscheduled backups through *EDGEMENU* also uses the file `/etc/edge.raw` by default.

Also, by default the file `/etc/edge.rawscript` will be run before and after the data is archived.

If you are using a different backup *Domain*, you may select a different file for either or both of `/etc/edge.raw` and `/etc/edge.rawscript`.

Changing the default for unscheduled *EDGEMENU* backups involves manually editing `/usr/lib/edge/config/master.cfg`.

Please consult “Raw Filesystem Partition Backups” on page 353 in the *Backup**EDGE*** User’s Guide for more information.

37.7 - The SCHEDULE.LCK Lock File

When *EDGE.NIGHTLY* begins *Scheduled Job*, it checks for the existence of a lock file called `/usr/lib/edge/lists/(jobname)/schedule.lck`. If this file exists, *EDGE.NIGHTLY* assumes that another instance of the *Job* is currently running, and terminates without beginning a backup. An appropriate mail message is sent to the user designated in the *Scheduler* to receive failure notifications.

If the `/usr/lib/edge/lists/(jobname)/schedule.lck` file does not exist, *EDGE.NIGHTLY* creates it.

If an *EDGE.NIGHTLY* backup terminates properly, with either a pass or fail status, the `/usr/lib/edge/lists/schedule.lck` file is automatically deleted.

On most systems, the installation program creates a script called `/etc/rc2.d/S88edge`. This script runs automatically at system start-up or re-boot and checks for the existence of `/usr/lib/edge/lists/*/schedule.lck`. If the file exists, it is deleted and a console warning message is displayed. This allows the next unattended backup to proceed, since whatever process created the lock file no longer exists.

37.8 - The EDGE_PROGRESS.LOG Status File

The *`/usr/lib/edge/lists/(jobname)/edge_progress.txt`* file is used for status messages by *EDGE.NIGHTLY*. This file can be used as a diagnostic tool if there are hung backup processes or if *EDGE.NIGHTLY* is terminated improperly.

If an *EDGE.NIGHTLY* backup terminates properly, with either a pass or fail status, the `/usr/lib/edge/lists/(jobname)edge_progress.txt` file is preserved until the next time the *Scheduled Job* runs. See “Debugging A Failed Backup” on page 349 for additional detail.

37.9 - The EDGE_SUMMARY.LOG Summary File

The file `/usr/lib/edge/lists/(jobname)/edge_summary.txt` includes a text summary of the last operation performed by the named *Scheduled Job*. The information is identical to what would have been sent as a text-only status email.

37.10 - Sample Unattended Backup Summary

Below is an example of the printed backup summary created by *EDGE.NIGHTLY*. It is identical to a text-only email of the same backup.

```
================================================================================
Microlite BackupEDGE Data Archiving System       Unattended Backup Summary
================================================================================
Backup Time             = 2019-09-10 22:00:05
Message Time            = 2019-09-10 23:31:50
BackupEDGE Release      = 03.02.03 build 2 (2019-07-02 edgelx64)
Serial Number           = XAR10000101
Registered End User     = Microlite Corporation
Subscription Expires    = 111 days Left
System Name             = web2v.microlite.com
Job Name                = web2v.microlite.com:simple_job_master
Job Description         = (Master) Basic Schedule
Sequence Name           = web2v.microlite.com:onsite
Sequence Description    = On-Site Backups
Primary Device [C=3]    = web2v:url!url0
Primary Volume Size     = 300.0GB
Segment                 = web2v.microlite.com:system #1
Software Block Size(s)  = 64
Hardware Block Size(s)  = 4096
Media Usage             = 1
Number of Files         = 210975
Backup Type [Status]    = Master [PASSED!]
Verify Type [Status]    = Level-2 (Bit) [PASSED!]
================================================================================
             Detailed Information About This Unattended Backup
--------------------------------------------------------------------------------
Job ID: 431bf5965813ba2f
[Backup of web2v.microlite.com:system]
Archive ID: 7c190d430c2064fc
Instance ID: 3c306d28070cff86
File '/usr/lib/edge/recover2/re' Has Changed
SUMMARY - BACKUP
Serial Number           = XAR10000101
Date                    = Tue Sep 10 22:56:20 2019
Files Encountered       = 210969
Total Data              = 61.21GB
Data Written            = 55.99GB
Segments Used           = 57
SW Compression          = 9%
Elapsed Time            = 00:56:10
Data Transfer Speed     = 64.249 GB/hr
                        = 1096.545 MB/min
                        = 19163513 bytes/sec
Relative Speed          = 70.239 GB/hr
                        = 1198.775 MB/min
                        = 20950114 bytes/sec
Exit Status             = 0
Actual Medium Usage     = 37%
--------------------------------------------------------------------------------
[Verify of web2v.microlite.com:system]
Archive ID: 7c190d430c2064fc
Instance ID: 3c306d28070cff86
File '/usr/lib/edge/recover2/re' Has Changed
SUMMARY - BYTE-BY-BYTE VERIFICATION
Serial Number           = XAR10000101
Date                    = Tue Sep 10 23:31:49 2019
Segments Used           = 57
Data Read               = 56.14GB
Elapsed Time            = 00:35:23
Data Transfer Speed     = 95.787 GB/hr
                        = 1634.785 MB/min
                        = 28569951 bytes/sec
Files Encountered       = 210969
Files Excluded          = 4
Files Modified          = 40
```

```
Files Not Checked      = 365
Special Files          = 33342
Verified Successfully  = 177220
Change Log             = /usr/lib/edge/lists/simple_job/
                         /changedfiles_system_master.txt
Status                 = No problems found
Exit Status            = 0
Total Verify Time      = 00:35:23
-------------------------------------------------------------------------
[Summary:  BACKUP_PASS / VERIFY_PASS
(web2v.microlite.com:simple_job_master)
[End of Summary]
```

The report may contain more information than is listed here, including...

- Information and statistics on additional *Domains* being included in the backup.
- Information on copies being done as part of the backup.
- A list of files that were not backed up, if for any reason a problem occurred.
- Any *TapeAlert* messages reported by the storage *Device*.
- If the unattended backup overwrote the previous unattended backup, this will be indicated as well. Normally, this means that the medium was not changed manually. *EDGE.NIGHTLY* still performs the unattended backup in this case, however.
- Miscellaneous warnings about *Recover**EDGE*** media not being tested, encryption keys not being archived, etc.

37.11 - Backup Log

Both *EDGEMENU* and *EDGE.NIGHTLY* appends a one-line log message to the log file `/usr/lib/edge/lists/logfile.txt` for each operation it performs. A sample of this file might look like this:

```
Listing of web2v:logfile.txt
2019-09-08 22:02:36 [edge.nightly:3] Verify2    P   0     1521
2019-09-08 22:02:37 [edge.nightly:3] Verify2    P   0        6
2019-09-09 22:58:12 [edge.nightly:3] Master     P   0   211333
2019-09-09 22:58:18 [edge.nightly:3] Master     P   0        6
2019-09-09 23:31:36 [edge.nightly:3] Verify2    P   0   211333
2019-09-09 23:31:36 [edge.nightly:3] Verify2    P   0        6
2019-09-10 13:53:18 [edge.nightly:3] Master     P   0        6
2019-09-10 13:53:20 [edge.nightly:3] Verify2    P   0        6
2019-09-10 22:56:20 [edge.nightly:3] Master     P   0   210969
2019-09-10 22:56:26 [edge.nightly:3] Master     P   0        6
2019-09-10 23:31:49 [edge.nightly:3] Verify2    P   0   210969
2019-09-10 23:31:50 [edge.nightly:3] Verify2    P   0        6
2019-09-11 13:53:15 [edge.nightly:3] Master     P   0        6
2019-09-11 13:53:17 [edge.nightly:3] Verify2    P   0        6
```

The columns provide information about each unattended operation, including...

- Date and time the log entry was generated;
- Program generating the message (typically *EDGEMENU* or *EDGE.NIGHTLY*)
- Intended operation (*Master Backup*, *Level-2 Verify*, etc.);
- "`P`"assed or "`F`"ailed;
- Exit code;
- Number of files processed;
- Error information on failure

If an error occurs, more than one line may be printed to provide a better description of what went wrong.

37.12 - EDGE.NIGHTLY Exit Codes

These are described in detail in “Error Return Codes” on page 336.

37.13 - Debugging A Failed Backup

As previously mentioned, the log files for each operation are stored in:
`/usr/lib/edge/lists/`**`jobname`**

where **`jobname`** is the name of the *Scheduled Job* that created them. For the Basic Schedule, this is `simple_job`. If the log files were created in *EDGEMENU*, replace **`jobname`** with `menu`.

In this directory, some or all of the following files may be present:

`backup_system_master.txt`	Log file of last *Master Backup* made by this *Scheduled Job* of the *Domain* `system`. If another *Domain* is also included (such as mysql) there will be another, similar log.
`verify_system_master.txt`	Log file of the last verification of the *Domain* `system`.
`changedfiles_system_master.txt`	List of all files which were changed on the hard disk between the backup and verify of the *Domain* `system`.
`edge_summary.txt`	Text version of the last summary created.
`edge_progress.txt`	Step-by-step list of actions performed when this *Scheduled Job* was last run.
`schedule.lck`	Lockfile for this *Scheduled Job*.

The `edge_progress.txt` is highly detailed and can usually pinpoint the exact point of failure for any particular job.

The following is an example of an `edge_progress.log` listing. As you can see, it can be extensive. Most logs will not be this long, as this one is from a device which is both in a library and has capacity reporting available.

```
2019-09-10 22:00:05 [edge.nightly:0] Successfully Opened Unattended Progress
File
2019-09-10 22:00:05 [edge.nightly:0] Checking For Media List
2019-09-10 22:00:05 [edge.nightly:0] Using Datespec Media List
2019-09-10 22:00:05 [edge.nightly:0] No Media List Found
2019-09-10 22:00:05 [edge.nightly:0] Checking For Slot Names
2019-09-10 22:00:05 [edge.nightly:0] Using Datespec Slot Name
2019-09-10 22:00:05 [edge.nightly:0] No Slot Name Found
2019-09-10 22:00:05 [edge.nightly:0] Beginning BackupEDGE Job simple_job:
Basic Schedule (Enabled, 22:00)
2019-09-10 22:00:05 [edge.nightly:1] Starting backup of domain
web2v.microlite.com:edomain/system
2019-09-10 22:00:05 [edge.nightly:1] Starting Operation
2019-09-10 22:00:05 [edge.nightly:2] Running Domain Script (begin)
2019-09-10 22:00:05 [edge.nightly:3] Domain Script Exited With 0
2019-09-10 22:00:05 [edge.nightly:2] Configuring EDGE Backup
2019-09-10 22:00:05 [edge.nightly:3] Instantiating NAS Manager On
web2v:url!url0
2019-09-10 22:00:05 [edge.nightly:4] NAS Manager Instantiation Succesful
2019-09-10 22:00:05 [edge.nightly:3] Generating Archive Label
2019-09-10 22:00:10 [edge.nightly:4] Label Generated Successfully
2019-09-10 22:00:10 [edge.nightly:3] Starting EDGE
2019-09-10 22:56:20 [edge.nightly:3] Master     P   0   210969
2019-09-10 22:56:20 [edge.nightly:3] EDGE Returned Exit Code 0
2019-09-10 22:56:20 [edge.nightly:2] Including Capacity Info
```

```
2019-09-10 22:56:20 [edge.nightly:2] Running Domain Script (end)
2019-09-10 22:56:20 [edge.nightly:3] Domain Script Exited With 0
2019-09-10 22:56:20 [edge.nightly:2] Operation Finished, Exit Code 0
2019-09-10 22:56:26 [edge.nightly:1] Starting verify of domain
web2v.microlite.com:edomain/system
2019-09-10 22:56:26 [edge.nightly:1] Starting Operation
2019-09-10 22:56:26 [edge.nightly:2] Running Domain Script (begin)
2019-09-10 22:56:26 [edge.nightly:3] Domain Script Exited With 0
2019-09-10 22:56:26 [edge.nightly:2] Configuring EDGE Listing / Verify
2019-09-10 22:56:26 [edge.nightly:3] Starting EDGE
2019-09-10 22:56:26 [edge.nightly:3] Instantiating NAS Manager On
web2v:url!url0
2019-09-10 22:56:26 [edge.nightly:4] NAS Manager Instantiation Succesful
2019-09-10 23:31:49 [edge.nightly:3] Verify2    P   0   210969
2019-09-10 23:31:49 [edge.nightly:3] EDGE Returned Exit Code 0
2019-09-10 23:31:49 [edge.nightly:3] Listing / Verify Succeeded
2019-09-10 23:31:49 [edge.nightly:2] Running Domain Script (end)
2019-09-10 23:31:49 [edge.nightly:3] Domain Script Exited With 0
2019-09-10 23:31:49 [edge.nightly:2] Operation Finished, Exit Code 0
2019-09-10 23:31:50 [edge.nightly:1] Job Completed Successfully
2019-09-10 23:31:50 [edge.nightly:0] Compressing / Purging Databases
2019-09-10 23:31:50 [edge.nightly:0] Mailing Summary (If Configured)
2019-09-10 23:31:50 [edge.nightly:0] Mailing Failure Report (If Configured)
2019-09-10 23:31:51 [edge.nightly:0] Removing Lock File
```

Reading through this log will allow you to identify the failure point and take appropriate action. For instance...

If the *Backup* had failed (the exit code in the last line of the example above, you'll get a pretty detailed error message in your emailed or printed report. This is also duplicated in the `edge_summary.txt` file. However, looking at the bottom of the backup log with "`tail backup_system_master.txt`" might provide even more specific information about the error.

If the *Verify* had failed (not in the example above, you'll also get a pretty detailed error message in your emailed or printed report and in `edge_summary.txt` file. Again, looking at the bottom of the verify log with "`tail verify_system_master.log`" might provide even more specific information about the error.

Individual file verification errors are found in `changedfiles_system_master.txt`.

Examining these logs may allow you to solve your own problems more easily. If not, having this information available when contacting your service provide or Microlite Technical Support will probably help provide a faster resolution to your problems.

38 - Integration Guide

This section is intended to describe how the installation of *BackupEDGE* may be streamlined for many similar systems. It also provides some ideas on how to better integrate *BackupEDGE* with your operating system.

Remember that you must have a valid *BackupEDGE* license for every system on which you install it.

38.1 - Duplicating BackupEDGE Installations

BackupEDGE provides many options to provide a flexible backup environment. However, it comes at the expense of additional installation time if the configuration is repeated manually for each of many identical systems.

Luckily, it is not necessary to do this. This section describes how to avoid this repetition.

The first step is to configure *BackupEDGE* correctly once. This involves creating any *Scheduled Jobs*, *Sequences*, *Domains*, *Notifiers*, etc.

The second step is to produce a configuration file that contains all of this information. The command `edge.cfgmgr` provides an easy interface to do this:

```
/usr/lib/edge/bin/edge.cfgmgr export [-devices] [-fqhn]
[-F filelist] [-pubkey] configuration_filename
```

This will create a file that contains all of the *BackupEDGE* configuration, including the *Device* database (optionally), and *BackupEDGE*'s idea of the system name (optionally). It does not allow you to avoid re-licensing each machine in any event.

If you want to write the configuration to a floppy diskette, you may specify its device node name for `configuration_filename`.

If present, the `-F filelist` option specifies the name of a file that contains the filenames of additional files to be included in the configuration output file. These should be listed one per line. You may include any additional files you wish, except the decryption keys for the optional Encryption Module. ***Remember that decryption keys will be excluded automatically, so including them here will do nothing!***

If present, the `-pubkey` option includes the encryption key for the optional Encryption Module. When the resulting configuration file is imported, this key will replace the public encryption key on that system. Note that decryption keys, either plaintext or hidden, are not included. These must be restored manually from a Decryption Key Backup.

To clone this configuration, repeat the installation of *BackupEDGE* on the target machine. You may skip *Device* autodetection if the *Devices* are the same also (and you elected to save the *Device* configuration with `edge.cfgmgr` above). You do not have to schedule a backup, however. You should also obtain an activation key for this system, and permanently activate it.

Once you have done this, run:

```
/usr/lib/edge/bin/edge.cfgmgr import configuration_filename
```

to import the configuration created above. This will restore all *Domains* (including *Virtual File* lists, Include Lists, etc.), *Sequences*, *Scheduled Jobs*, *Notifiers*, and (optionally) *Resources*. This will work even if you have not permanently activated *BackupEDGE*, but it will *not* affect the expiration date.

By default, this will not copy any program used as the *Notification Command* in any *Notifier*. If you wish to duplicate this as well, include it with a `-F filename` option when running `edge.cfgmgr` to create the configuration file.

It is important that you check the first duplicated machine's functionality to be sure you didn't forget anything in the copy operation, and that it will do what you expect. Of course, if you run into any problems, you may contact your *BackupEDGE* reseller or Microlite Corporation Technical Support (`support@microlite.com`).

If you wish to see exactly what files will be copied, you may run the following command:

```
edge tvf configuration_filename
```

38.2 - Performing Command-Line Backups

In earlier versions of *BackupEDGE* (01.01.0x and earlier), performing a backup via the command line was accomplished in one of two ways:

- Running `/bin/edge`
- Running `/etc/edge.nightly` (or `/usr/lib/edge/bin/edge.nightly`)

Running `/bin/edge` is very similar to running the UNIX utility `tar`. While more powerful (i.e. it can write directly to optical media, URL and FSP backup media), it creates archives as an ACTION and not as a PROCESS (see "Anatomy of a BackupEDGE Backup" on page 40). You still have to do a lot of script writing and you can't easily use many of the advanced features of *BackupEDGE*, especially when it comes to indexing, quick file access, automatic verification, logging, and notification. The command line remains useful for simple tasks.

Running `/etc/edge.nightly` is now the preferred way to accomplish backups while maintaining all of the benefits of *BackupEDGE*. To do this, however, you must define Storage Resources (see "Resources" on page 41), Backup Domains (see "Domains" on page 42)and Schedules Jobs (see "Scheduled Jobs" on page 45), then use the EDGE.NIGHTLY command-line syntax described on page 326 to manage running the jobs.

38.3 - Performing Command-Line Restores

For those familiar with older versions of *BackupEDGE* (01.01.0x and earlier), the preferred method of performing a command-line restore was to use the `/bin/edge` program. This emulated the *UNIX* `tar` program. This method is still available, but is no longer the easiest way for most applications.

Starting with *BackupEDGE* 01.02.00, the preferred way to perform a restore from the command-line is to use *EDGE.RESTORE*. This allows the same transparent access to *Fast / Instant File Restore*, *Resources*, and *Summaries* from the command-line as are provided in *EDGEMENU*. It also provides the benefits of supplying UNIX-mode pathnames, rather than the old-style expert-mode pathnames.

For example, to restore the file `/etc/passwd` as quickly as possible from the medium loaded in the *Resource* `dvd0`, one would use:

```
edge.restore -f optical0 /etc/passwd
```

If an archive database (*Index*) is available, *EDGE.RESTORE* will use it to perform an *Instant File Restore* from the archive. Otherwise, it will use normal speed.

If you are in the `/etc` directory already, you might also run:

```
edge.restore -f s3cloud0 ./passwd
```

Note that as long as the archive was not an Expert-Mode archive, *EDGE.RESTORE* handles finding the filenames automatically. As a general rule, if the `rm` command would remove a file given some filename (ignoring whether or not it actually exists), then that same filename can be used to restore the file from an archive with *EDGE.RESTORE*:

```
rm ../some_file.c
edge.restore -f tape0 ./some_file.c
```

Another benefit of using *EDGE.RESTORE* involves hard- and symbolically-linked files. On many systems, `/etc/passwd` is actually a symbolic link to another file. If an archive database is available, *EDGE.RESTORE* can look up this symlink (and any others required) and restore the original data and the symlinks, or just the original data:

```
edge.restore -fH optical0 /etc/passwd
```

This would restore the symlinks and the real target, while

```
edge.restore -fh optical0 /etc/passwd
```

would restore the target only. If specified without `-h` or `-H`, then the symlink itself will be restored, but not the target.

Please consult “Command-Line Restores Using EDGE.RESTORE” on page 315 for a detailed explanation of *EDGE.RESTORE*,

38.4 - Virtual File Backups

Virtual Files are files whose reported size is much greater than the actual amount of data contained in the file. This is because the data not accounted for is null data, e.g. binary zeroes. Since the null data does not take up any real space on the filesystem, the file appears to *UNIX* to contain more data than actually exists. The places in the file where the null data occurs will be referred to here as “black holes”. The ability of a file to contain “black holes” is unique to *UNIX*.

If a *Virtual File* is archived without any special attention, all of the null data will be read from the file and placed on the archive media. This is very inefficient and a waste of archive media capacity. Furthermore, when the file is restored, the null data will be restored as ***real*** nulls, causing the file to consume much more disk space than need be. After the restore, the file is no longer *Virtual*; it is a very large file with null data in it. Therefore it is wise to mark *Virtual Files* for special consideration before backing them up, so that *Backup**EDGE*** can both archive them efficiently and upon restore recreate the “black holes” so as to consume a minimal amount of disk space.

A list of all *Virtual Files* should be placed, one per line, in a data file. The list may contain either absolute or *Relative Pathnames*; *Absolute Pathname*s are preferred. The filename for the default *Domain* is `/etc/edge.virtual`. This is also the file used for unscheduled backups through *EDGEMENU*.

Each file in this list will receive special attention during *Backup**EDGE*** backups. During backup, *Backup**EDGE*** identifies all of the “black holes” in the file, then archive all of the real data plus the “black hole” markers. If compression is enabled, the actual data (but not the “black hole” markers) is compressed.

Upon restore, the data is decompressed if necessary, and the file is restored with all of the “black holes” placed exactly where they were originally. This process is known as “re-virtualizing”. It is not necessary to identify *Virtual Files* during restores; *Backup**EDGE*** knows when an archived file is *Virtual*.

Virtual Files may be identified by using the *Backup**EDGE*** *Virtual File* scanner. This can be run during a normal *Backup**EDGE*** installation. If you wish to run the command at a different time, the command is...

```
/usr/lib/edge/bin/edge.vfind
```

38.5 - Raw Filesystem Partition Backups

A *Device Node* is typically a pointer into the system kernel that allows access to a particular device. When *Backup**EDGE*** encounters a *Device Node*, it usually backs up only the information necessary to re-create the node itself.

Some database programs do not store their data within files residing on the UNIX filesystem. Instead, they use a partition on a hard disk which does not contain an actual UNIX filesystem, and read and write data using their own routines.

For these data partitions, and for any other type of non-filesystem partition, *Backup**EDGE*** has a special procedure called a *Raw Filesystem Partition Backup*.

To archive a *Raw Filesystem Partition*, *Backup**EDGE*** treats the *Device Node* as if it were an actual data file, that is, it opens the node for input, reads all the input, and writes it to the archive media with a standard archive header. During restore, in addition to creating the *Device Node*, all data is written back in to the node.

Further, *Backup**EDGE*** can automatically run a user process just before, and just after, the data in the *Raw Filesystem Partition* is archived. When archiving databases, such as Oracle, Informix and Sybase applications, this user program typically shuts down and re-starts the database, or otherwise places it into a ready-to-archive mode.

The default *Backup**EDGE** Domain* defines `/etc/edge.raw` as the default file list for *Raw Filesystem Partitions*. *EDGEMENU* also uses this file for unscheduled backups. To treat a partition as a *Raw Filesystem Partition* for archive purposes, simply place its *Device Node* in the `/etc/edge.raw` file (one *Device Node* per line). To have special start/stop commands run, you may modify the default user script (`/usr/lib/edge/bin/edge.rawscript`) or create your own script and use the *Domain Editor* to identify it. To see how to run your own start/stop programs, print out the `edge.rawscript` program and examine its contents; it contains a sample implementation.

38.6 - Themes (Java / Web Services)

The Java and *Web Services* interfaces were designed with user customization in mind. By default, the following theme is used:

```
/usr/lib/edge/system/themes/java/default
```

As delivered, this is actually a symbolic link to:

```
/usr/lib/edge/system/themes/java/microlite
```

Users may create any number of theme directories and modify virtually any color or graphic shown on the screen. See the `colors` file in the default theme for more information.

The HTML code, borders and graphics used by *Backup**EDGE** Web Services* may also be changed as desired.

38.7 - Color Palettes (Character Interface)

If you don't like the colors you see when you run *EDGEMENU* in character mode, you may change them. *EDGEMENU* has two separate color palettes: the full-color palette you see when you run *EDGEMENU* in default mode, and the monochrome palette you see when you run *EDGEMENU* from a monochrome terminal, with the `-mono` startup flag, or by selecting `File -> Toggle Color/Mono` from within *EDGEMENU*.

There are a wide variety of changeable colors in the color palette file. If you create a color palette which is easily readable on a specific type of terminal or terminal emulator, please send it to us, with documentation on why you designed it and what you like about it. We'll place it on our *ftp* site and possibly within future releases of *Backup**EDGE***.

By default, the following color palette is used:

```
/usr/lib/edge/system/themes/ncurses/default/colors
```

As delivered, this is actually a symbolic link to:

```
/usr/lib/edge/system/themes/ncurses/microlite/colors
```

Users may create any number of palette directories and modify virtually any color shown on the screen. See the `colors` file in the default palette for more information.

This color palette does not affect *Recover**EDGE*** for *OSR5*. It also does not affect the registration program, *EDGE.ACTIVATE*.

38.8 - Defining Resources Manually

NOTE: *Backup**EDGE*** autodetection is generally sufficient to find all tape, optical drives, loaders and changers on your system. If it does not there is probably a device or driver incompatibility issue. While this mode may work, it is not recommended.

Although the *Installation Manager* autodetects most *Resources*, you may occasionally find the need to create your own. For example, you may want to create a *Resource* entry for a tape drive that has very old firmware, or that is on a bus that is not detected by the *Installation Manager*. Or, you may want to create a *File* to use to create backups instead of a *Device*.

Manually Creating a Tape Drive Resource

Let's manually create a tape drive *Resource*. From *EDGEMENU*, select `Admin -> Define Resources`. **FastSelect** `[New]` to create a new *Resource*.

```
+ Select Resource Name And Type ---------------------------+
|Resource Type:  +----------------------------+            |
|                |Tape Drive                  |            |
|                |Optical Drive               |            |
|                |FTP Server (url)            |            |
|                |Directory (fsp)             |            |
|                |Attached Filesystem         |            |
|                |SharpDrive (sdrive)         |            |
|                |Other Device                |            |
|                |AutoChanger                 |            |
|                +----------------------------+            |
|Resource Name:  [tape1                      ]            |
|[Next]                    [Prev]                 [Cancel]|
+UP / DOWN  Arrows To Change Resource Type-----------------+
```

If desired, change the *Resource Name*. Use only numbers and letters; no spaces or special characters.

With the cursor in the *Resource Type* field, use the right arrow and left arrow to display the different `Resource Types` available. When finished, set the `Resource Type` to `Tape Drive` and press `[Next]`.

Creating a Tape Drive Resource - Before

```
+ BackupEDGE Resource Information ------------------------------------------+
|- General Resource Information ------------------------------------------- |
|Resource Type       Tape Drive                                             |
|Resource Name       [tape1             ] Change as appropriate             |
|Description         [                  ]                                  |
|Changer Assoc       [Standalone Device]                                    |
|Interface           [Other      ]                                          |
|                                                                           |
|- Tape Drive Information ------------------------------------------------- |
|Data Node           [                          ] [A] TapeAlert(tm) Support |
|No Rewind Node      [                          ] [X] Multiple Archives?    |
|Tape Block Size     [-1                        ] [C] Partition             |
|Locate Threshhold   [-1                        ] [ Manual Check ]          |
|                                                                           |
|                                                                           |
|- Default Backup Properties ---------------------------------------------- |
|Volume Size         [0           ] [H] Compression                         |
|Edge Block Size     [64          ] [Y] Double Buffering                    |
|[Next]                             [Prev]                          [Cancel]|
+---------------------------------------------------------------------------+
```

Fill in the proper responses for each field, then press `[Next]` to save the *Resource*.

Here is an example for an old legacy tape drive running on a *UNIX* system.

Creating a Tape Drive Resource - After

```
+ BackupEDGE Resource Information ------------------------------------------+
|- General Resource Information ------------------------------------------- |
|Resource Type       Tape Drive                                             |
|Resource Name       [tape1             ] Change as appropriate             |
|Description         [Quantum DLT       ]                                  |
|Changer Assoc       [Standalone Device]                                    |
|Interface           [Other      ]                                          |
|                                                                           |
|- Tape Drive Information ------------------------------------------------- |
|Data Node           [/dev/st0                  ] [A] TapeAlert(tm) Support |
|No Rewind Node      [/dev/nst0                 ] [X] Multiple Archives?    |
|Tape Block Size     [-1                        ] [C] Partition             |
|Locate Threshhold   [-1                        ] [ Manual Check ]          |
|                                                                           |
|                                                                           |
|- Default Backup Properties ---------------------------------------------- |
|Volume Size         [99953664    ] [N] Compression                         |
|Edge Block Size     [64          ] [Y] Double Buffering                    |
|[Next]                             [Prev]                          [Cancel]|
+---------------------------------------------------------------------------+
```

Since this tape drive does not properly respond to SCSI inquiry commands, we've set the `Interface` to `Other`.

Pressing `[F1]` for help at each field describes the proper settings for that field. By pressing the `[F1]` key on the *Volume Size* key, you can scroll up and down through a long list of suggested *Volume Sizes* for various storage media.

Manually Creating a File Archive Resource

NOTE: *BackupEDGE* file Resources created with this method are not as fully functional as when creating *Attached Filesystem Resources*. This information is included for legacy purposes only. See "Configuring Legacy Disk-to-Disk Backups" on page 158 for additional information on setting up *Attached Filesystem Resources* for directory backups.

Let's manually create a file archive *Resource*. From *EDGEMENU*, select `Admin -> Define Resources`. **FastSelect** `[New]` to create a new *Resource*.

```
+ Select Resource Name And Type ---------------------------+
|Resource Type:  +----------------------------+            |
|                |Tape Drive                  |            |
|                |Optical Drive               |            |
|                |FTP Server (url)            |            |
|                |Directory (fsp)             |            |
|                |Attached Filesystem         |            |
|                |SharpDrive (sdrive)         |            |
|                |Other Device                |            |
|                |AutoChanger                 |            |
|                +----------------------------+            |
|Resource Name:  [other1                      ]            |
|[Next]                    [Prev]                  [Cancel]|
+-----------------------------------------------------------+
```

If desired, change the *Resource Name*. Use only numbers and letters; no spaces or special characters. In our example, we'll create a *Resource* called `file0`.

With the cursor in the *Resource Type* field, use the right arrow and left arrow set the `Resource Type` to `Other Device` and press `[Next]`.

Creating a File Archive Resource

```
+ BackupEDGE Resource Information ------------------------------------------+
|- General Resource Information ---------------------------------------------|
|Resource Type       Other Device                                           |
|Resource Name       [file0             ] Change as appropriate             |
|Description         [Accounting Archive File     ]                         |
|Changer Assoc       [Standalone Device]                                    |
|                                                                           |
|                                                                           |
|- Other Device Information -------------------------------------------------|
|Data Node           [/tmp/archive0.edge          ] [Y] Device Can Seek?     |
|                                                                           |
|                                                                           |
|                                                                           |
|                                                                           |
|- Default Backup Properties ------------------------------------------------|
|Volume Size (K)     [0                           ] [S] Compression          |
|Edge Block Size     [64                          ] [Y] Double Buffering     |
|[Next]                                 [Prev]                    [Cancel]  |
+---------------------------------------------------------------------------+
```

Fill in the proper responses for each field, then press `[Next]` to save the *Resource*.

In the *Installation and Removal* section of this manual the section called "Examples of Storage Resources" on page 61 has very detailed information on creating *Resources* of various types.

38.9 - Background - *BackupEDGE* Configuration Files

BackupEDGE stores information in several configuration files:

`/etc/default/edge.cfg` - "bootstrap" configuration

`/usr/lib/edge/config/master.cfg` - main configuration file

`/usr/lib/edge/system/pconfig/*/*` - various files

The file `/etc/default/edge.cfg` contains information about where to find the rest of the *BackupEDGE* installation, and several options which are very basic to proper operation. ***This file will be overwritten*** with every new *BackupEDGE* installation or upgrade, so it is generally advisable not to change it. This file **may contain** any (Bourne) shell script.

`/usr/lib/edge/config/master.cfg` contains most of the global options for *BackupEDGE*. Changes made here will be preserved across upgrades. As new options are added, they will be merged with any changes you have made here. If the default value of a variable is changed during an upgrade, it will be modified in `master.cfg` if and only if you have not changed it from its previous default. This file may ***not*** contain any shell script code, except comments and variable assignments. Remember: this file not parsed by the shell, although it retains the same form as a shell script for editing convenience.

The `pconfig/` files are used to store information about *Backup Domains*, *Sequences*, *Scheduled Jobs*, *Notifiers*, and more. While it is recommended that you ***do not modify them directly*** in general, it is possible to view them. These files may ***not*** contain any shell script code except comments and variable assignments.

The `master.cfg` file is actually a symlink to a `pconfig/` file, although editing it directly is permitted.

All `pconfig`s have their settings preserved across upgrades. (Incidentally, the name `pconfig` stands for ***P***ersistent ***Config***uration.)

38.10 - Configuration Variables Explained

This section describes `master.cfg`, the main *BackupEDGE* configuration file.

NOTE: This information is provided to help you read *BackupEDGE* configuration files for diagnostic purposes. The information may change from release to release, and should be treated as "internal" to the operation of *BackupEDGE*. When upgrading to a newer version, it is important that you re-familiarize yourself with this information in case it has changed.

The file starts with a header similar to the following:

```
# Microlite BackupEDGE System-Wide Configuration File
# Copyright 2002-2019 by Microlite Corporation
# All Rights Reserved
#
# NOTE: THIS FILE MAY CONTAIN ONLY COMMENTS, BLANK LINES, AND
# VARIABLE ASSIGNMENTS (TO CONSTANT VALUES).
# IT MAY CONTAIN NO OTHER SHELL CONSTRUCTS!
```

General Options

`ENABLE_OVERFLOW={YES|NO}`
If set to `YES`, *BackupEDGE* will allow selection of *Overflow Resources*. An *Overflow Resource* is used if the medium in the *Primary Resource* fills up during a backup, or runs out of data during a listing / restore. Normally, you will use only the *Primary Resource* and load the next medium as required. An *Overflow Resource* is only used if you wish to (for example) perform a two volume backup using two separate tape drives.

Most installations ***do not*** require the use of *Overflow Resources*.

`SITECODE=000`
This is the 3-digit site code that will represent this system. It may be set to any desired 3-digit number. Numeric pages sent via *Notifiers* will use this value as the first three digits. For information on how to interpret the rest of a numeric page, please refer to "Numeric Pagers" on page 236.

DBDELT="14"
After a *Scheduled Job* is run through *EDGE.NIGHTLY*, it checks this parameter to decide whether or not to delete any of the existing archive indexes (databases). If it is unset, no indexes are erased. Otherwise, indexes older (in days) than the value of DBDELT will be deleted from the system.

NOTE: All indexes stored the system are checked, even if they were created by another *Scheduled Job*.

DBCOMT=2
This setting is similar to DBDELT, except that databases are compressed rather than deleted. Compressed databases are automatically decompressed before use, although the first access requires slightly more time than normal to allow for the decompression.

TMPDIR=/tmp
This is the directory where the *Software Compress Pipe* is stored during a backup. It should be set to a readable / writable directory in the filesystem with the most available free space. If it is unset, it will default to a reasonable value for most systems. If a backup with software compression enabled produces an Error 9 during the backup, consider changing this parameter.

NOTE: /tmp is not the default on all systems. Some systems (such as *UW7*) use /usr as the temporary filesystem.

ZBUFFERS=5
This parameter selects the number of *Backup***EDGE** buffers to allocate for *Double Buffering*. The default is 5 on most systems. This will affect all double-buffered backups through *EDGEMENU* or *EDGE.NIGHTLY*.

Each buffer requires enough shared memory to hold one software block of data. The size of this block is the *Backup***EDGE** software block size in the *Resource Manager* times 512 bytes.

LOCAL_DB_ONLY={YES|NO}
LOCAL_DB_ONLY, if set to YES, will restrict searches for *FFR*/*IFR* indexes (databases) to the local machine. Normally this is not necessary, but if you are experiencing hanging at the outset of a restore, it is possible that changing this setting will resolve it.

LOCAL_DOM_ONLY={YES|NO}
Setting LOCAL_DOM_ONLY to YES will cause *Backup**EDGE*** to treat any machine that is not part of the local DNS domain as if it were not accessible. If set to NO, *Backup**EDGE*** will treat machines in the local DNS domain identically to machines in remote domains. Normally, this only affects behavior when importing tapes from other sites.

WARN_RECOVERY={YES|NO}
Setting this to YES enables *Backup**EDGE*** Disaster Recovery checking during backups. Various warnings about the state of your Disaster Recovery media may be included on the summary of a backup / verify / restore operation if this is enabled. If your operating system does not support Disaster Recovery (*Recover**EDGE***), then this option has no effect.

If you are receiving warnings about your *Recover**EDGE*** media, it is advisable to create or test the media as indicated, rather than disabling this option.

ENABLE_ADVANCED={YES|NO}
Setting this to YES enables the advanced scheduling options in *Backup**EDGE***. If it is disabled, any existing advanced schedules will be accessible via *EDGE.CRONSET*, but *EDGEMENU* will not let you create or edit them.

This setting is normally changed from NO to YES via the *Schedule* menu of *EDGEMENU*.

ENABLE_OBDR_POPUP={YES|NO}
If set to YES, *Recover**EDGE*** will offer HP-OBDR™ as an option on the initial *Media Type* popup

list. HP-OBDR is always available for selection manually on the `Configure` (*OSR5*) or `Configure -> Boot Media` (*Linux/UW7*) screens. This field is set automatically on installation. If your operating system does not support Disaster Recovery (*Recover**EDGE***), this option has no effect.

Generally, it is not necessary to edit this parameter manually.

`ENC_HIDDEN={YES|NO}`

If set to `YES`, *EDGEMENU* will hide encryption options. This is useful to keep end-users out of the encryption configuration. Note that encryption itself is not disabled or enabled because of this; only *EDGEMENU*'s user interface is affected.

`ENC_ENABLED={YES|NO}`

If set to `NO`, encryption will be entirely disabled. If set to `YES`, encryption will be enabled, assuming that it is licensed and set up. Please consult "Encryption" on page 259 for more information.

EDGEMENU Options

`NO_CENTER=NO`
By default, *EDGEMENU* centers pathnames as it scrolls them in a window during backup. Setting this variable to YES causes the pathnames to be left justified, which may make them easier to read.

`EDGEMENU_RAW_LIST=/etc/edge.raw`
Set raw file list for unscheduled *EDGEMENU* backups. *Scheduled Jobs* use *Backup Domains*, and thus ignore this in favor of the Domain settings.

`PRESERVE_ATIME={NO|YES}`
If set to `YES`, unscheduled backups through *EDGEMENU* will attempt to preserve the *UNIX* `atime` setting (at the expense of `ctime`). Otherwise, `ctime` will be preserved but `atime` will be modified.

NOTE: This setting affects only *EDGEMENU* backups that are not *Scheduled Jobs*! Unattended jobs (or those run via `Backup -> Run Scheduled`) will use the *Domain* setting for preserving `atime`.

Backup Domain Defaults

These settings may be set on a per-*Domain* basis also. Setting them here provides a default for those *Domains* that do not have any value selected. Normally, these should have no effect since *Domains* should have these values filled in already by the *Domain Editor* in *EDGEMENU*.

`EDOM_COMPBIN={YES|NO}`
If set, software compression will include files with the e*x*ecute permission set. Otherwise, these files will be excluded from compression. Normally, this option should be enabled.

`EDOM_COMPLIM=4`
This is the minimum size (in 512-byte blocks) that a file must be before it is considered for software compression. Files smaller than this are not compressed.

`EDOM_COMP_EXCL="/u/images"`
Files in this directory are not subject to software compression.

`EDOM_SUFFIXES=".gz .tgz .TGZ .bz .BZ .bz2 .BZ2 .zip .ZIP"`
Files ending in these suffixes are not compressed when software compression is enabled. The extensions `.gz .tgz .TGZ .bz .BZ .bz2 .BZ2 .zip` and `.ZIP` are automatically excluded. By default, no additional suffixes are excluded by `EDOM_SUFFIXES`. The above list is provided to

show the proper syntax, and would not actually change anything since they are already excluded by default.

`EDOM_LAST_FILE=/tmp/last_file`
If this option is set, the named file will be stored as the last file on the archive.

`EDOM_RAW_SCRIPT=/usr/lib/edge/bin/edge.rawscript`
If set, this script will be run before and after a *Raw Filesystem Partition* backup occurs.

`EDOM_VIRTUAL_LIST=/etc/edge.virtual`
Set virtual file list default for unscheduled backups run through *EDGEMENU*.

38.11 - Level 1 and 2 Differential/Incremental Backups

*Backup**EDGE*** can perform two types of *Differential Backups* and *Incremental Backups*: *Level 1* and *Level 2*. Normally, the default of *Level 2* is appropriate for most systems. The description below should help you determine if this is right for your application. If you're unfamiliar with the terms involved, it is likely that *Level 2* is the right answer.

Which level is selected is based on the variable `EDOM_INCREM1` in the `pconfig` for the *Domain* in question. This value may be changed from the *Domain Editor* in *EDGEMENU*. This setting affects both *Differential Backups* and *Incremental Backups*.

An option that is closely related to `EDOM_INCREM1` is `EDOM_PRESERVE_ATIME`. If set to `NO`, every file that is backed up will have its access time (`atime`) set to the time of the backup. This is the default behavior, and is generally correct; the access time is a *UNIX* file attribute designed to record when a file is read. However, UNIX provides a way to preserve the access time during a backup, at the expense of changing the change time (`ctime`) of that file. The change time records when a file's attributes are changed. Setting `EDOM_PRESERVE_ATIME` to `YES` will cause *Backup**EDGE*** to preserve `atime` at the expense of `ctime`. This option may be changed in the *Domain Editor*.

The following describe the four combinations of these two settings:

`EDOM_INCREM1` is set to `YES`. `EDOM_PRESERVE_ATIME` is set to `NO`. This performs a *Level 1 Differential Backup*. This compares the file modification time (`mtime`) of each file against the start time of the last successful *Master Backup*. If `mtime` for the file is newer, then the file is archived. Modifications to a file which change `mtime` include creation, writing, and updating. Older release of *Backup**EDGE*** were only capable of *Level 1 Incremental Backups*. After every backup, the access time (`atime`) of every file is set to the time at which *Backup**EDGE*** read it. This is the default behavior.

`EDOM_INCREM1` is set to `YES`. `EDOM_PRESERVE_ATIME` is set to `YES`. *Backup**EDGE*** performs a *Level 1 Differential Backup*. The access time (`atime`) of each file is not affected by the backup, but the `ctime` of each file is set to the time at which *Backup**EDGE*** accessed it. (It is not possible to leave both the `atime` and the `ctime` unchanged when a file is backed up). *Backup**EDGE*** compares the file modification time (`mtime`) of each file against the start time of the last successful *Master Backup*. If `mtime` for the file is newer, then the file is archived. Modifications to a file which change `mtime` include creation, writing, and updating.

`EDOM_INCREM1` is set to `NO`. `EDOM_PRESERVE_ATIME` is set to `NO`. *Backup**EDGE*** performs a *Level 2 Differential Backup*. This compares the file change time (`ctime`) of each file against the start time of the last successful *Master Backup*. If `ctime` for the file is newer, then the file is archived. Modifications to a file which change `ctime` include creation, writing, updating, moving, linking, and changing mode or ownership. The `atime` of each file is set to the time at which *Backup**EDGE*** accessed the file. The `ctime` is unchanged by *Backup**EDGE***.

`EDOM_INCREM1` is set to `NO`. `EDOM_PRESERVE_ATIME` is set to `YES`. This combination will produce an error, since it would try to perform a *Level 2 Differential Backup*, which checks the change

time (`ctime`) of each file, but would be forced to change the `ctime` in order to preserve the access time (`atime`). Thus, the second backup of this type would back up every file!

Some programs (like `tar` and `cpio`) purposely modify `mtime` when they restore a file. Therefore if a new program is installed, or if a file is restored from a backup, its `mtime` may be set to a time previous to the last *Master Backup*, which means that a *Level 1 Incremental Backup* will ignore it. So a *Level 2 Incremental Backup* (which is the default) is much more robust, although it may take up more archive space.

39 - BackupEDGE Licensing

*Backup**EDGE*** version numbers consists of the 3 sets of digits and a build number. Understanding this may help when contacting us regarding upgrades or technical support.

The version number may look like this: `03.03.00b1`.

We would pronounce this as: `Oh-three-dot-oh-three-dot-oh-oh-build-one`.

The first two digits (03 in this example) are reserved for ***major new releases***.

The next two (02) change with ***significant enhancements for features***.

The third two (00) change whenever we add a new ***minor feature*** or to ***fix a significant problem***.

The build number (b1) is for bug fixes. These fixes might not be applicable to all operating systems supported by *Backup**EDGE***; the fictional *Backup**EDGE*** 03.03.00 for OpenServer 5 might be at a different build level than *Backup**EDGE*** 03.03.00 for Linux, if some fixes are needed for one platform but not another.

39.1 - Update / Upgrade Eligibility

New *Backup**EDGE 3.x*** licenses are eligible for no-charge upgrades to all new versions whose build 1 release is first shipped while under a ***Support and Maintenance Subscription***, plus all subsequent builds (bug fixes) released for those versions. This is based on the date-encoded activation code created during product registration. For example, the date-encoded activation code would make clients eligible for...

1. Free updates to all builds of the current release of *Backup**EDGE***, i.e. 03.00.01 in effect on the date the activation code is generated, up through:
2. Free upgrades to all builds of the current release of *Backup**EDGE***, i.e. 03.00.02, 03.01.00, etc. shipping while the ***Support and Maintenance Subscription*** is in effect.
3. Free cross-platform upgrades while the ***Support and Maintenance Subscription*** is in effect.

All new releases of *Backup**EDGE*** first shipped after a ***Support and Maintenance Subscription***n has expired are ***not eligible*** for a free upgrade. ***Support and Maintenance Subscription*** extensions and renewals are available.

Support and Maintenance Subscription extensions and renewals come with a new date-encoded activation code good for another year from the date the previous **Subscription** expired (extension) or from the date the activation code is generated (not the date it is entered into *EDGEMENU*).

Bug fix builds made available for eligible releases will be downloadable regardless of ***Support and Maintenance Subscription*** status.

If a client attempts to activate a version of *Backup**EDGE*** they are not eligible for, i.e after a ***Support and Maintenance Subscription*** has expired, our activation department will inform them that it is not eligible and point them to the original reseller to purchase a ***Support and Maintenance Subscription*** renewal.

39.2 - Why Version Numbers Are Important

These numbers may sound complicated, but they really aren't. They allow us to identify easily exactly when a product was shipped, to find the correct version of source code should we have to

help you with a problem, and to help to identify whether your version needs an upgrade in order to fix a particular problem.

39.3 - How To Find Your Version Number

All products since 01.01.07 (November 1999) can view their version number within *EDGEMENU* by selecting `File -> About Edgemenu`. This information is also contained in the file `/usr/lib/edge/config/edge.build`.

Older releases can see the version number on the right side of line three of the main *EDGEMENU* screen.

40 - The Indispensable *BackupEDGE* QA Guide

This guide is intended to answer common questions pertaining to the care and feeding of Microlite *BackupEDGE*. It was produced from user feedback received since the initial release of 01.02.00. If you have anything to add to this guide, please feel free to email it to `qaguide@microlite.com` for possible inclusion in the next release.

40.1 - Index To Questions

Pg. ***Q# - Question***

40.2 - The Questions

Question 1 - How do I install *BackupEDGE*?

This topic is discussed in "How Do I Install BackupEDGE?" on page 49 in the *BackupEDGE* User's Guide. It is recommended that you consult that document (available from `http://www.microlite.com/documentation/documentation.html`) for complete instruction.

Question 2 - I have a numeric/alpha-numeric pager, or an HTML-capable e-mail reader. Can I use it with *BackupEDGE*?

Yes, *BackupEDGE* can be configured to send short alpha-numeric or very short numeric-only messages to summarize the result of a *Scheduled Job*, or to request operator intervention. *BackupEDGE* can also send HTML messages with embedded images.

If you will be using a pager, you will need a way of sending a message to it. Most pagers permit paging via e-mail. If yours does, then you should enter that e-mail address in the *Scheduler* as you normally would. However, the first time you do this on a particular installation of *BackupEDGE*, you must tell *BackupEDGE* to use a different message format, or else it will try to send a full-length summary! If your pager does ***not*** support receiving e-mail, you will have to follow slightly different instructions, presented below.

If you would like to send HTML (MIME-encoded) e-mail, just enter the e-mail address as you normally would. After saving the *Scheduled Job*, you must tell *BackupEDGE* to use HTML rather than plain text as the message type.

To change the type of message sent, use `edgemenu -> Schedule -> Edit Notifiers` after entering the e-mail address into at least one *Scheduled Job*. Use the `[Up]` and `[Down]` arrows to select the *Notifier* for your pager/HTML recipient (it will have the same e-mail address you entered earlier). Press `[Enter]` to edit this Notifier.

One of the fields for the *Notifier* is "Message Type". Use the `[Up]` arrow to highlight this field, and use the `[Right]` and `[Left]` arrow keys to select "HTML", "Numeric" or "Alpha-Numeric", as appropriate. It is possible that this field is set correctly already, since *BackupEDGE* will guess that any e-mail that looks enough like a phone number should be treated as an alpha-numeric pager.

As an aside, if you would like to copy the message to multiple addresses, you may enter a space-separated list of e-mail addresses in the "Recipient(s)" field. An identical message will be sent to each, by running the command given in the "Command" field once per address, substituting any `%n` on the command line with the address being used. This is an easy way to create an alias for several different addresses, so you do not have to update multiple *Scheduled Jobs* to change who receives information about it. Of course, if you wish different people to receive different format messages (for example, HTML and plain text), you must use multiple *Notifiers*.

Once you have made any changes to the *Notifier*, use the `[Down]` arrow or `[Tab]` key to highlight `[Save]`, and press `[Enter]`.

Any time you use this e-mail address in a *Scheduled Job*, it will automatically format the e-mail appropriately. There is no need to re-edit the Notifier if you later add this e-mail address to another job on this installation of *BackupEDGE*.

If you wish to send a message to a pager that does ***not*** support e-mail as a method of communication, you will need some external program that is capable of accepting text to send to that pager. If your pager does not accept e-mail and you do not have an external program to page it, then *BackupEDGE* cannot communicate with the pager.

Assuming you do have such a program and your pager requires it, you will have to configure a *Notifier* to use it. To do this, simply add `mypager` or some other descriptive name to the list of

Notifiers for the appropriate *Scheduled Job(s)* in place of an e-mail address. Then, save the *Scheduled Job* and use `edgemenu -> Schedule -> Edit Notifiers` to edit `mypager`, and set the "Message Type" field to Numeric or Alpha-Numeric, as described above. Do not save the *Notifier* yet, however.

Once the Message Type has been set, highlight the "Command" field, and enter the full path to your external paging program. If you want the text of the page to be sent to this command's standard output, precede the pathname with a pipe symbol (e.g., "`|/usr/local/bin/program`"). If you would like to provide the paging program with a filename of a file that contains the text to be sent, use the string `%f` as an argument (e.g., "`/usr/local/bin/program %f`"). You may also include other arguments on the command line, as required by your external paging program.

Once you have done this, save the *Notifier*. Any future use of `mypager` will now send pages using this program.

More information on Notifiers can be found in"Working with Notifiers" on page 235 in the *BackupEDGE* User's Guide.

Question 3 - Can I restore files quickly from the command line?

Yes.

To do this, use the program *EDGE.RESTORE*. This provides easy access to the restore engine of *BackupEDGE*. The basic syntax is:

```
edge.restore -f resource_name file(s)_to_restore
```

For example, the following commands are typical:

```
rm ./my_program.c ../makefile
edge.restore -f tape0 ./my_program.c ../makefile
```

`edge.restore` provides many more options. Please consult "Command-Line Restores Using EDGE.RESTORE" on page 315 in the *BackupEDGE* User's Guide.

Question 4 - I want to be notified when any of my clients' backups fail. How do I do this?

When entering *Notifiers* for a *Scheduled Job*, you may choose to include some in the "Mail Failures To" field. These *Notifiers* will be used only when the Scheduled Job fails. If you do not specify a "Mail Summary To" or "Print Summary To" *Notifier*, then the "Mail Failure To" *Notifiers* will receive requests for new media during nightly backups.

Note that including a "Mail Failure To" or "Print Failure To" *Notifier* does not change what is sent to the "Mail/Print Summary To" *Notifiers*. These will still receive all *Scheduled Job* summaries, whether successful or not.

If desired, you can configure these *Notifiers* to send Alpha-Numeric or purely Numeric message, suitable for pages as described in "I have a numeric/alpha-numeric pager, or an HTML-capable e-mail reader. Can I use it with BackupEDGE?" on page 367. Also consult "Anatomy of a BackupEDGE Backup" on page 40 in the *BackupEDGE* User's Guide.

Question 5 - *BackupEDGE* did not detect my tape (or other) device. What do I do now?

BackupEDGE will offer to perform autodetection of all your *Devices*, in order to create *Resources* from them. (Recall that a *Resource* is the name *BackupEDGE* gives to a physical *Device* that can use.) You may start autodetection from *EDGEMENU* using `Setup -> Configure BackupEDGE -> Autodetect New Devices` at any time.

If autodetection completes but does not detect one or more *Devices*, you can add them manually later.

If autodetection does not complete (it hangs), repeat the installation but skip autodetection by using the `[DOWN ARROW]` key to select 'Skip Autodetection' when prompted. You will also have to skip creating a default *Scheduled Job*, as there will be nothing onto which to write the archive! It is possible to add the *Resources* manually if necessary in this case.

Before adding any *Resources* manually, one must ask why the *Device* wasn't autodetected. Some causes for this are:

1. The *Device* is not configured into the operating system. If the operating system doesn't know about the *Device*, *Backup**EDGE*** will be unable to use it even if it is configured manually.

For example, under *OSR5* one must run `mkdev tape` or `mkdev cdrom` when adding a new tape drive or cdrom, respectively. `mkdev juke` adds an autochanger to the operating system. Remember that ATAPI devices under 5.0.6 and earlier cannot be used except as read-only devices. Starting with OSR 5.0.7, ATAPI devices can be accessed for writing as well. In this case, they will (should) be detected as SCSI devices in *Backup**EDGE***.

Under Linux, you may have to install kernel modules yourself. If you add a SCSI tape drive, be sure that the command `cat /proc/scsi/scsi` shows your tape drive. If not, *Backup**EDGE*** (and any other software package, probably) will be unable to use the *Device* until you correct the situation.

You may need to use the `insmod` command to add the appropriate SCSI kernel modules. Exactly which modules are needed depends on your system configuration, but some common ones are listed below. To see what modules are loaded, run the command `cat /proc/modules`.

`scsi_mod`: If the directory `/proc/scsi` or the file `/proc/scsi/scsi` do not exist, this module is probably missing. It is sometimes named `scsi`.

`aic7xxx`: This module controls just about any non-RAID Adaptec host adapter

`st`: If `/proc/scsi/scsi` shows your tape drive but trying to write to it with the command `tar cvf /dev/st0 /tmp` fails immediately with no tape motion and the error `No such device or address`, you might be missing the `st` (`S`csi `T`ape) module.

`sr_mod`: This is the `S`csi `C`drom module. It is to CD-ROMs what `st` (see above) is to tape drives.

`ide-scsi`: If you have an IDE/ATAPI *Device*, it is suggested that you run the *Device* using the `ide-scsi` driver. This causes Linux and *Backup**EDGE*** to treat the *Device* as a SCSI *Device*. If you want to do this, be sure that `ide-scsi` is loaded.

`ide-tape`: If you are using an IDE/ATAPI *Device* without `ide-scsi`, this driver provides access to it. If you are using `ide-scsi`, this module must NOT be loaded, or else `ide-scsi` will have nothing to do!

`ide-cdrom`: This is the same as `ide-tape` for CD-ROM drives. It is called `ide-cd` on some systems.

Under *UW7*, the operating system should detect the new *Device* automatically. However, if it is the first *Device* on a host adapter (including IDE), you may need to install the appropriate host adapter support into the kernel.

2. *Device Nodes* are missing. These are how *Backup**EDGE*** does the majority of its communication with the *Device*.

OSR5: `/dev/rStp0` C 46,0 (scsi tape drive)

Linux: `/dev/st0` C 9,0 (scsi tape drive, or ATAPI drive under `ide-scsi`), `/dev/ht0` C (IDE/ATAPI tape drive that is not running under `ide-scsi`)

UW7: `/dev/rmt/ctape1` C (*Device* numbers vary)

3. *Backup**EDGE*** cannot communicate with the *Device*, but the operating system can. Sometimes, you can run `tar cvf /dev/st0 /tmp` (replacing `/dev/st0` with the appropriate *Device Node* name for your tape drive -- this doesn't work for CD-R/RW's!) and have the tape drive run. Be sure that the drive is actually moving! If `/dev/st0` doesn't exist, `tar` will store all the data in a ***file*** called `/dev/st0`, with no tape motion. This is obviously *not* what you want! If this happens, you may be missing a *Device Node* (described above).

Assuming `tar` can access the *Device*, then try using `edge cvf /dev/st0 /tmp`. If this works, then *Backup**EDGE*** can write data to the *Device* as well. If this is true, then at worst you will have to define the *Device* manually.

If you are running Linux with a SCSI (or ide-scsi) tape drive or other device, do not add the *Device* manually yet. First, try running the command
`edge.tape -i /dev/st0`
(as always, replace `/dev/st0` with the appropriate *Device Node* if this is not a tape drive), and see if it can identify your *Device* information. For SCSI *Devices*, this should print the model and vendor information correctly. If it does not, try running the command `insmod sg` and then repeating the *EDGE.TAPE* command. If it now shows the correct information, autodetection will probably find your *Device*. You must be sure to run `insmod sg` every time after rebooting your machine!

To set up a *Device* manually, run *EDGEMENU* and select `Admin -> Define Resources`. Then use the `[Up]` and `[Down]` keys to select `[New]`, and press `[Enter]`.

QUESTION 6 - LAST NIGHT'S BACKUP FAILED. CAN I REPEAT IT NOW? - OR - I WANT TO PERFORM PART OF MY BACKUP SCHEDULE USING EDGEMENU.

If you want or need to run jobs through *EDGEMENU*, use the `Backup -> Run Scheduled` option. You will be directed to select (using the `[Up]` and `[Down]` keys, then `[Enter]` to select one) a *Scheduled Job* to run.

You will be given information about the *Scheduled Job* and the *Sequence* to which it contributes backups. Then, you may be given the option of choosing the backup type (*Master*, *Differential*, or *Incremental*) that you want to perform. Note that if you have not yet completed a *Master Backup* successfully, you will not be given the option of a *Differential* or *Incremental Backup* -- these backups must be based on a *Master Backup* in the same *Sequence*. Similarly, an *Incremental Backup* requires at least one successful *Differential Backup* in that *Sequence*.

After selecting the backup type, you will be prompted to insert the first medium into the appropriate *Device*, or be prompted for the *Media List* to use if the *Job* uses an *Autochanger*. Once you do this, the *Scheduled Job* will start. If it requires more volumes, you will be notified with a pop-up window in *EDGEMENU* rather than via email or print notification. Once complete, the Backup Summary will be printed and/or e-mailed normally, in addition to being displayed in a pop-up window in *EDGEMENU*.

For more information, please consult "Navigating EDGEMENU" on page 194 in the *Backup**EDGE*** User's Guide.

QUESTION 7 - HOW DO I BACK UP TO A FILE?

To back up to a file, you must create a *Resource* for it in the *Resource Manager*. Use `edgemenu -> Admin -> Define Resources`.

Use the `[Up]` and `[Down]` arrow keys to highlight, "`[New]`", and press `[Enter]`. Then, use the `[Up]` arrow key to highlight "Resource Name", and enter the name for your *Resource*, such as "fileo". By default, the *Resource Manager* will be creating a Tape Drive, and will call the *Resource* "tapeo" (perhaps using some other number). You should change this name for clarity.

One you enter the *Resource Name*, use the `[Down]` arrow to highlight the "Resource Type" field. Use the `[Left]` and `[Right]` arrows to select the type, in this case "Other Device".

Use the [Down] and [Left] arrow keys to highlight the [Next] button, and press [Enter].

You will now have a screen which allows you to edit the *Resource*. Use the [Up], [Down], and [Tab] keys to navigate. Be sure to fill in all the fields, including "Description". Note that you probably do NOT want to press [Enter] on the [Standalone Device] button, as it is used for autochanger associations.

For the "Data Node", enter the filename. For the "Volume Size", enter the maximum size this file should consume. Note that if you attempt to make a backup that exceeds this size, you will be prompted for another "medium", but will not be given the opportunity to change the filename. While you can move the file out of the way manually, it is much more convenient if backups to files do not span volumes.

Please note that before performing a backup, the file itself must exist. To create an empty file (for example /tmp/myfile), type >/tmp/myfile from the UNIX/Linux shell. This will create the file if it does not exist, and ERASE its contents if it does.

For more information, please consult "Navigating Resource Screens" on page 60 in the *Backup**EDGE*** User's Guide.

Question 8 - I want to do Master Backups to tape, and Differential Backups to optical/rev/nas/etc. How do I set this up?

(This will assume that you are backing up your entire system with the *Basic Schedule*, and wish to expand it to include *Differential Backups* to urlo.)

To do this, you must create two *Scheduled Jobs*. One *Scheduled Job* will perform the *Master Backups* to tape. The other will perform *Differential Backups* to urlo.

Set up the *Basic Schedule* to perform *Master Backups* as described elsewhere.

Once you have done this, run *EDGEMENU*. Select Schedule -> Advanced Schedule (you may need to select Schedule -> Enable Advanced to make this option available). You will be presented with a list that contains the *Basic Schedule* along with the options [New] and [New From Wizard]. Select [New From Wizard] by using the [Down] key to move the arrow to it, and pressing [Enter]. This will create a new *Advanced Scheduled Job*.

You will be prompted to select a *Sequence* to which this new *Scheduled Job* will add backups. Since this *Scheduled Job* will be making *Differential Backups* based on the *Master Backups* run by the *Basic Schedule*, they must be part of the same *Sequence*. (If you are unfamiliar with these concepts, consult the *BackupEDGE* manual.) This *Sequence* is called onsite (which stands for 'On-site Backups of this System'). Use the [Up] and [Down] arrows to select this *Sequence*, and press [Enter].

You will then be prompted to select the *Resource* to which the *Differential Backups* will be written. Select the *Resource* for your NAS (urlo, etc.).

You will now be prompted to enter the time, in 24-hour format (00:00 is midnight), that the *Differential Backup* will occur. If you wish to schedule them at different times, please pick one of the times now. You can repeat this procedure and create multiple *Differential Jobs* for each of the times you want. Press [Enter] on the [Next] button to continue.

Press the space bar on each day of the week until Differ (Differential) appears.

When you are happy with the layout, highlight the [Next] button and press [Enter] to continue.

You must enter a short name for this *Scheduled Job*, and a description. Once you do this, you will be shown a summary of the *Scheduled Job*. You may save the job, or make further modifications to it. It is highly recommended that you add notification options to this job. If you wish to use a pager or HTML-enabled email reader for this, please consult "I have a numeric/alpha-numeric pager, or an HTML-capable e-mail reader. Can I use it with BackupEDGE?" on page 367.

Question 9 - My unattended backup *Scheduled Job* requires more than one volume. What do I do?

First, you must be sure to specify a volume size in the *Resource Manager* before attempting multi-volume backups to that *Resource*. Otherwise, it is likely that your backups will fail with a write error at the end of the first volume.

If you are using a tape autochanger (also called a library or jukebox), you should consult the question "How do I use an autochanger?" on page 374. The remainder of this answer assumes you must change media manually.

Next, you must be sure that the *Scheduled Job* contains some e-mail and/or print *Notifier* in the "Mail / Print Summary To" field. This *Notifier* will be used to request more media. If both an e-mail and print *Notifier* are present, the e-mail *Notifier* alone will be used for media requests.

When the *Scheduled Job* is run unattended (i.e., scheduled), it will send an e-mail message requesting more media. Once you receive this message and insert new media, you must tell the *Scheduled Job* to continue. To do this, run *EDGEMENU*. (If the *Scheduled Job* uses a remote *Resource*, run *EDGEMENU* on the machine on which you scheduled it, not the machine with the *Resource*.) If you are already in *EDGEMENU*, use `Schedule -> Acknowledge All` instead.

When *EDGEMENU* starts, or when you select `Schedule -> Acknowledge All`, it checks for stopped *Scheduled Jobs* that were run unattended on the local machine. If it finds any, it will notify you and give you the option to let the *Scheduled Job* continue, or force it to abort. Presumably, you will want to accept the default "continue" message. The *Scheduled Job* will then start on the next medium.

You will receive additional requests for media as necessary. When the backup completes, you will then be e-mailed with a request to re-insert the first volume for verification (it is ***strongly*** recommended that you accept the default bit-level verification option for all *Scheduled Jobs*!).

Question 10 - Where can I find product updates?

The easiest way to get eligible updates to *Backup**EDGE*** is to use the update manager (`EDGEMENU -> File -> Check for Updates`). You may also check Microlite's website, (*http://www.microlite.com*). Updates will be available for download from the Downloads page.

New *Backup**EDGE 3.x*** licenses are eligible for no-charge upgrades to all new versions whose build 1 release is first shipped while under a ***Support and Maintenance Subscription***, plus all subsequent builds (bug fixes) released for those versions. This is based on the date-encoded activation code created during product registration. Contact your *Backup**EDGE*** reseller, Microlite Corporation for additional information.

Question 11 - I want to use a remote tape (or other) device with BackupEDGE. How do I set this up?

First, install *Backup**EDGE*** on the machine that has the *Device* physically attached. The installation process should autodetect the *Device*. If not, please see the appropriate question for how to resolve this.

From now on, this machine will be called `tapehost` for the purpose of example. You should use whatever the real name of this machine is, of course.

Once the installation is complete, make sure that *Backup**EDGE*** can access the *Device* by running a backup and verify through *EDGEMENU*. Since you probably want to back up this system anyway, be sure to schedule the appropriate *Scheduled Job* to do so, probably as part of the installation.

Once the machine that is physically attached to the *Device* can use it, the next step is to get any remote machine(s) working with it as well. For this to happen, you must allow `rsh` and/or `ssh` commands to run on the tape host from the remote host. In other words, while logged-in as

'`root`' on the remote host, '`rsh tapehost ls`' should produce a listing of `root`'s home directory, which is usually `/` or `/root`. If you get errors, such as '`Permission denied`', then you have not set up remote access correctly.

For `rsh`/`rcmd`, there must be a `.rhosts` file in the `/` (`/root` for Linux) directory on `tapehost` that contains the names of the machines that are allowed to access it, one per line. This file must be owner-readable and nothing else (`chmod 400 .rhosts`).

For `ssh`, you copy the appropriate keys into one of several different places (depending on how you have set up `ssh`). Consult the `ssh` documentation for exactly how to do this.

Once `rsh`/`rcmd` or `ssh` works, you can install *Backup**EDGE*** on the remote machine(s). During installation, you may be prompted whether or not to use `rsh`/`rcmd` or `ssh`. Select whichever is appropriate by using the `[Up]` and `[Down]` arrows. It does not matter what you selected when installing *Backup**EDGE*** on `tapehost`, however.

You may skip autodetection on the remote host(s) if there are no *Devices* of interest. However, even if there are CD-ROM drives, you should allow autodetection to proceed so that *Resources* are created for them. It is perfectly acceptable to access *Remote Devices* even if local *Devices* are defined as *Resources*.

All that is left is to tell *Backup**EDGE*** to use the *Remote Device*. To do this, when at a 'Select Device' popup screen (such as when scheduling an unattended backup), use the `[Tab]` key to switch to the machine name box. Type '`tapehost`' (or whatever machine you want), and it should list the *Backup**EDGE*** defined on that machine. Select from the list as you would for local *Resources*.

If you ever change the parameters for the *Resource* on tapehost, all *Scheduled Jobs* (etc.) that use it will use the new parameters as well automatically.

For more information, please consult "Selecting a Remote Resource" on page 258 in the *Backup**EDGE*** User's Guide.

Question 12 - How can I check the status of an unattended *Scheduled Job* while it is running?

Use `edgemenu -> Schedule -> Browse Running Jobs` to get a list of all *Scheduled Jobs*. Use the `[Up]` and `[Down]` keys to highlight the *Scheduled Job* you wish to see. Then press `[Enter]` to view the last status message received from it.

If the *Scheduled Job* requires operator intervention, such as a manual load of new media, *EDGEMENU* will display the information and give you the option of telling the *Scheduled Job* to continue. Note that *EDGEMENU* automatically checks for stopped *Scheduled Jobs* when it is first started, and tells you if any are found. It does not automatically repeat this check, however, so if a *Scheduled Job* requires user intervention after you are in *EDGEMENU*, you must use `Browse Running Jobs` to view that *Scheduled Job's* status, or ask it to repeat this check with `Schedule -> Acknowledge All`.

Question 13 - How do I set up a Backup Schedule that contains only unattended Master Backups?

If all of your data fits onto one volume (tape, optical, whatever), and your system load permits it, performing unattended *Master Backups* is almost certainly the best option. The reasons are simple: unattended backups happen automatically, and the resulting volume contains all the data you want to protect.

To set up such a backup, you can use the *Basic Schedule* option in *EDGEMENU* by running *EDGEMENU*, then selecting `Schedule -> Basic Schedule`.

See "Scheduling - Basic" on page 210 in the *Backup**EDGE*** User's Guide for additional information.

QUESTION 14 - HOW DO I USE AN AUTOCHANGER?

To configure an autochanger (sometimes called a "library" or "jukebox") for use with *Backup**EDGE***, you must first take any steps necessary to tell your operating system about it.

For *OSR5*, this requires running '`mkdev juke`' and rebooting. If you have an autochanger that uses a Logical Unit Number (LUN) other than `0`, you must also make sure that LUN scanning for you host adapter is enabled The file to edit is `/etc/conf/pack.d/(your_adapter)/space.c`.

For *Linux*, this should require no additional steps, assuming your tape drive(s) are accessible also.

For UW7, this should require no additional steps, assuming the Host Bust Adapter (HBA) driver for your SCSI card is already loaded. Unless you just installed a new SCSI card, this should be the case.

If this has been done correctly, *Backup**EDGE*** should autodetect your autochanger during installation. If you have already installed *Backup**EDGE*** before taking the above steps, use `edgemenu -> Admin -> Autodetect New Devices` to repeat autodetection.

If *Backup**EDGE*** finds your autochanger, the next step is to associate the *Resource* for it with whatever tape drives or other *Devices* it serves. This allows *Backup**EDGE*** to figure out what tape drives are affected by the autochanger.

For this example, assume that `changer0` is the *Backup**EDGE*** name of the autochanger, and `tape0` is the *Backup**EDGE*** name of the tape drive installed in it. If your autochanger contains multiple tapes, simply repeat this process.

After autodetection, *Backup**EDGE*** will display a screen that allows you to associate `tape0` with `changer0`. Simply highlight `changer0:dt0` and press `[Enter]`. This will list all the un-associated tape drives (etc.). Highlight `tape0` and press `[Enter]` again. This will associate the first Data Transfer Element (`dt0`) of `changer0` with `tape0`. Repeat this for all Data Transfer Elements on all autochangers. Be sure to get these right, otherwise *Backup**EDGE*** will load media into the wrong drive! If you want to change these associations later, you can do so by selecting the autochanger in the *Resource Manager* (`edgemenu -> Admin -> Define Resources`), and pressing `[Enter]` on the "Modify Associated Devices" button.

Once the autochanger has been detected and associated with the appropriate device(s), you may configure *Backup**EDGE*** to automatically change tapes during unattended backups.

To do this, use the Scheduler to create or edit the *Scheduled Job* you wish to change tapes automatically. Select the tape drive (NOT the autochanger, which will not even be an option) that it should use. Once you do this, *Backup**EDGE*** will ask if it should use the associated autochanger, or just treat the drive as a stand-alone drive for this *Scheduled Job*. The default will be to use the associated autochanger.

If you are editing an existing *Scheduled Job*, you will have to re-select the *Resource*, even if it is the currently selected one for this *Scheduled Job*. Otherwise, *Backup**EDGE*** will not start using the autochanger for this *Scheduled Job*.

When the cursor is position on the proper day, press `[Ctrl-D]` to get to the selection screen and insert the slot or barcode name that should be loaded for that day's backup.

Storage elements are another name for magazine slots. They are named `st0`, `st1`, etc. Using a storage element will cause *Backup**EDGE*** to load whatever medium is in that magazine element.

Barcodes are specified as `bc1234abc` where '`1234abc`' should be replaced with whatever barcode is on the tape you wish to load. If a tape with this barcode is present in the autochanger, *Backup**EDGE*** will load it. If it is not present, the `Scheduled Job` will fail if it tries to load that tape. All examples will use storage elements rather than barcodes, but you may mix and match them freely, even on the same day.

If you specify more than one storage element (or barcode) for a particular day, separate it with a comma, such as "`st0,st5`". This will cause *Backup**EDGE*** to use `st0` first, and then `st5` if `st0` fills. You do not have to have the same number of tapes specified for each day.

QUESTION 15 - WHAT IS A VIRTUAL FILE?

A *virtual file* (sometimes called a *sparse file*) is a file that appears to take up more space than it actually does. These files are generally used by database applications.

In a virtual file, some parts of the data require no appreciable disk space. These parts appear to be filled with binary zeroes (although not all binary zeroes are part of such a virtual section of file!). These virtual sections are interspersed with real data, which does take space on the hard disk. If an application decides to fill in some of those virtual zeroes with real data, then those section cease to be virtual and begin consuming disk space normally.

Database applications that use virtual files generally do so to avoid sorting the records they store. Specifically, by separating records with large numbers of virtual zeroes, the database maintains the ability to insert new records in order with existing records, while not requiring much disk space over what is actually required to store the records. Using this approach without virtual files would require that all those not-virtual zeroes be stored on the disk too! Not all database applications use this approach, as there are other ways to accomplish generally the same thing.

*Backup**EDGE*** supports virtual files. When defining a *Backup Domain*, you may include the name of a file that contains a list, one per line, of the files that are to be treated as virtual. It's important to identify any files this way, as they are by construction practically indistinguishable from normal non-virtual files from an application's point of view. If you do not, *Backup**EDGE*** will treat them like normal files, meaning all of the virtual zeroes will be stored in the archive. If you ever restore this file, the virtual zeros will be restored as real zeros!

If you list these files for *Backup**EDGE***, however, they will not take up excessive amounts of archive space. On restore, they will automatically be "re-virtualized", so the virtual zeroes again take little space.

For more information, please consult "Virtual File Backups" on page 353 in the *Backup**EDGE*** User's Guide.

QUESTION 16 - HOW DO I DECIDE WHAT MY BACKUP SCHEDULE SHOULD BE?

Before answering this, it is important to be familiar with a few commonsense assumptions that have proven themselves useful time after time:

Assumption 1: Always plan for the worst when it comes to losing data.

Two direct consequences of this are:

Assumption 2: Assume every operation stands a significant chance of failure until it completes successfully.

Assumption 3: Never have only one method of recovery from any failure.

A final assumption that comes from experience is:

Assumption 4: Failures that cause data loss are usually simple, but creative.

With these assumptions in mind, it is possible to construct a good backup schedule for your particular installation.

Tape drives and other archive *Devices* are notoriously bad at detecting failures. Simply because data was transferred without *reported* error to the medium, it does not mean that no error occurred. One of the biggest strengths of *Backup**EDGE*** is that it provides a strong, additional check for data integrity: the Bit-Level Verify. This actually reads the archive, and verifies

everything on it. Unless this test passes, you should not assume the data was recorded without incident.

This argument, along with Assumption 2, supports one of the most overlooked rules in developing a plan for data protection:

Rule 1: A backup that has not been successfully Bit-Level verified has failed.

Also by Assumption 2, you must assume media will fail at inopportune times. So, in terms of reliability, it is best to match your tape drive (or other archiving *Device*) with your data. If you can perform a nightly *Master Backup* onto one tape (etc.), you stand a much lower chance of losing data than if you require more than one tape (etc.) to recover later.

The reason is simple: more media increases the chance that one of them will be lost or damaged. By making *Master Backups* whenever possible, each medium is self-contained. As a side benefit, it is easier to automate a backup that does not require a user to manually load new media. Unless you have a tape autochanger, a multi-volume backup must have help to complete.

The drawback to performing a *Master Backup* is performance. When your system is performing a *Master Backup*, its performance will be degraded temporarily due to the extra load on the hard drives and CPU.

The easiest solution to this is to run a *Master Backup* when nobody is using the system. It is very common to have at least a nightly *Master Backup* run automatically for just this reason. This provides the first rule of building a backup *Schedule*:

Rule 1: If at all possible, run a single-volume Master Backup daily through the Scheduler.

In this case, be sure that the medium is changed nightly. It is ***very*** bad practice to leave the same media in the drive for multiple nights; Assumptions 2 and 3 both run contrary to the practice. *Backup**EDGE*** will warn you if it detects this.

The reason is, if a backup fails while overwriting the previous night's backup (for example, if the machine is befallen by some physical catastrophe, or electric power loss, etc., remembering Assumption 4), then not only will you lose your current backup, but the one from the night before, too. You must always assume that a backup will fail until it has completed successfully.

Rule 2: Never overwrite your most recent backup (or, if it is a Differential or Incremental Backup, any backup on which it depends).

If a *Master Backup* is not practical because of capacity restraints of your archive *Device*, you should consider getting a new archive *Device* that better suits the task you will be asking it to perform.

If a *Master Backup* is not practical because you *must* run it during "operating hours" (hopefully for the purpose of protecting against mid-day hard drive failures or user errors, and in addition to a regular *Master Backup*), then it is reasonable to consider *Differential Backups*.

A *Differential Backup* archives all and only that data that has changed since the last *Master Backup* [in the same *Backup Sequence*]. So, it generally takes less time and system resources to perform. The down side to this approach is that the data on the system is changing as people go about their work. If a backup on a quiescent system is a crisp photograph of that system's state, then a backup on a busy system is more like a photograph with blurred motion. Usually, this is not a significant problem because of *Backup**EDGE***'s ability to lock files during backup, but it is still a point that requires consideration.

Another down-side to using *Differential Backups* is the difficulty of recovery. Because data is located on two media, both must be restored to bring the system back to the state it was in when the *Differential Backup* was made. Even if you want to restore only one file, you must try to restore it from the *Differential Backup*, and if it is not present, then try the *Master Backup*.

*Backup**EDGE*** makes this relatively easy with tools like *EDGE.RESTORE*, but it's still more work than restoring data from a *Master Backup* alone.

It is always a good idea to keep enough data physically isolated from the machine(s) that contain it to prevent Assumption 4 from being troublesome. If you keep your entire stash of *Master Backups* next to your tape drive (or in the magazine in your autochanger) for easy access, you are not well-prepared for a natural disaster or theft.

Rule 3: Always keep up-to-date off-site backups.

Many insurance companies require off-site backups in order to qualify for any loss-of-business insurance. Make sure your backup plan periodically rotates full system backup media out of the building on a regular basis.

Exactly how many backups you keep at once, and how much trouble you go to keeping them in different locations, depends on the importance of the data you are trying to protect. It also depends on what kind of data you are using and for what types of failures you are planning. Keeping (say) one *Master Backup* from each week prior to the current one for a month or two helps in the event a file is lost or damaged, but nobody realizes immediately.

Finally:

Rule 4: Always read and check BackupEDGE Backup Summaries.

It does very little good to have a mailbox full of messages warning about failed backups, should you ever want to restore from any of them.

QUESTION 17 - HOW DO I DISABLE A *SCHEDULED JOB* TEMPORARILY?

If you will be skipping a *Scheduled Backup* (such as over a holiday), simply uncheck the '`Enabled`' box in the *Scheduler*. This is located in the upper-right-hand corner of the *Basic* and *Advanced Scheduler* windows.

When a *Scheduled Job* is disabled, it will not be run automatically. However, you may still run it manually via *EDGEMENU* using `Backup -> Run Scheduled`, or by using the command-line interface to *EDGE.NIGHTLY*.

QUESTION 18 - CAN I CONTROL MY AUTOCHANGER FROM THE COMMAND LINE?

Yes. The command *EDGE.CHANGER* can be used to do so. It can be used to move tapes around, and to find out where tapes are currently located in a changer.

While the entire command-line of *EDGE.CHANGER* is documented in the "The EDGE.CHANGER Program" on page 324 in the *Backup**EDGE*** User's Guide, a few examples are presented here.

`edge.changer`
This produces a usage message.

`edge.changer show changer0`
This provides a human-readable report of the autochanger configuration.

`edge.changer -terse show changer0`
This provides a machine-readable (and shell-readable) report of the same information.

`edge.changer move st0 dt0 changer0`
This moves the tape from *Storage Element* 0 (`st0`) to *Data Transfer Element* 0 (`dt0`). If configured in the *Resource Manager*, *Backup**EDGE*** will also issue a Load command to the tape drive to bring it online. If you attempt to move a tape from a `dt` element, *Backup**EDGE*** will issue a tape unload to the associated tape drive if configured to do so in the *Resource Manager*.

`edge.changer move bcMONDAY dt0 changer0`
This moves the tape with the barcode `MONDAY` into `dt0`.

`edge.changer eject changer0`
If possible, *EDGE.CHANGER* will unload any tape in any data transfer elements, and then eject the entire magazine. Not all autochanger support this, however.

`edge.changer unload dt0 changer0`
This causes the tape in `dt0` to be unloaded to the *Storage Element* from which it came. If *EDGE.CHANGER* is unable to determine what *Storage Element* this is, it will pick any free storage element.

The full path to *EDGE.CHANGER* is `/usr/lib/edge/bin/edge.changer`. It is also symbolically linked into the `/bin` or `/usr/bin` directory for easy access from the command line. Only `root` may use *EDGE.CHANGER* successfully.

QUESTION 19 - CAN I CONTROL MY TAPE DRIVE (OR OTHER DEVICE) FROM THE COMMAND LINE?

Yes. The command *EDGE.TAPE* may be used to query and control a tape drive, CD-ROM, DVD, or even autochanger from the command line. (Note: *EDGE.TAPE* cannot actually move tapes around in an autochanger. To do this, please see “Can I control my autochanger from the command line?” on page 377. It can be used to query the autochanger for information about its firmware revision, vendor name, and so on.)

This program is documented in “Using EDGE.TAPE for Hardware Status / Control” on page 319 in the *Backup**EDGE*** User’s Guide. However, a few examples are given here as well.

`edge.tape`
This produces a usage message.

`edge.tape -i tape0`
This produces basic identification information about tape0 in human-readable format.

`edge.tape -terse -i tape0`
This produces basic identification information about tape0 in shell-parseable format.

`edge.tape -arg 512 -B tape0`
This sets the hardware block size of tape0 to 512 bytes.

`edge.tape -R tape0`
This rewinds tape0, if it isn’t already.

`edge.tape -t tape0`
This produces a lot of (generally) informative information about `tape0`.

WARNING: The output of *EDGE.TAPE* is subject to change without notice.

The full path to *EDGE.TAPE* is `/usr/lib/edge/bin/edge.tape`. It is also symbolically linked into the `/bin` or `/usr/bin` directory for easy access from the command line. Only `root` may use *EDGE.TAPE* successfully.

QUESTION 20 - CAN I READ A TAPE LABEL FROM THE COMMAND LINE?

Yes. Run the program *EDGE.LABEL* as follows:

`/usr/lib/edge/bin/edge.label -G tape0`

You will be shown a human-readable description of the label.

WARNING: The output of *EDGE.LABEL* is subject to change without notice.

Question 21 - Can I run a *Scheduled Job* from the command line?

Yes. The program *EDGE.NIGHTLY* can be used for this purpose.

For those familiar with older versions of *Backup**EDGE***, the command line to *EDGE.NIGHTLY* has changed. While it still attempts to support the legacy options, it is strongly recommended that you take this opportunity to upgrade any scripts that may use it. *Backup**EDGE*** provides many new features and abilities, usually with very little change to existing scripts.

To run *EDGE.NIGHTLY*, use:

```
/usr/lib/edge/bin/edge.nightly -H jobname
```

where jobname is the name of the *Scheduled Job* as entered in *EDGEMENU*. For the Basic Schedule, `jobname` should be `simple_job`. Generally, no output will be produced. You may not mix new and old command-line options.

This will run the appropriate type of backup (*Master*, *Differential*, or *Incremental*) based on the day of the week as it is configured in the *Scheduler*. If no backup is configured for this day, *EDGE.NIGHTLY* will return (successfully) immediately.

To use *EDGE.NIGHTLY* to run a *Scheduled Job* from a script, it is recommended that the *Scheduled Job* be disabled in the *Scheduler*, so it does not run automatically. However, it is not an error to leave it enabled.

Remember that you may configure and disable any number of *Advanced Schedules* using *EDGEMENU*, and use scripts to control when they are run.

Also remember that prior to *Backup**EDGE*** 01.02.00, a *Differential Backup* was known as an *Incremental Backup*. There was no backup that corresponds to what is now called an *Incremental Backup* in older *Backup**EDGE*** releases. If you use the old command-line flags (which you should do only as a last-resort, and *never* if this is a new undertaking), you should still specify `-I` to perform this backup, but now it performs what is called a *Differential Backup*. In other words, `-I` does exactly what it did before.

Question 22 - What's the best *BackupEDGE* block size to use?

*Backup**EDGE*** allows you to select the *software* (or *Edge*) block size that is uses to communicate with your *Devices*. This is not to be confused with the *hardware* block size that tape drives and some other *Devices* may use (this is explained below).

The software block size is specified in the Resource Manager in the field 'Edge Block Size'. This is value is in 512-byte blocks.

Generally, it is good to be consistent about the software block size used. By default, all Resources are set up with a software block size of 64 (32KB). Larger values show speed increases on some tape drives, however, especially DLT devices.

Do not set this value too high. Depending on your operating system and *Device* setup, setting this too high can cause backup and/or verify failures. It is suggested that you do not increase it above 256.

To determine what software block size is best for your setup, you should use the program *EDGE.SPEED* to measure it. This process will ERASE the contents of the tape, and cannot be used with other media types.

```
/usr/lib/edge/bin/edge.speed
```

The *hardware* block size is used mainly with tape *Devices*. It is set in the *Resource Manager* also, under the name "Tape Block Size". It is not accessible for non-tape *Resources*. Its value is in bytes.

A tape drive generally has the ability to separate data on the tape into fixed-size blocks. The size of these blocks is equal to the hardware block size set when the data is written. Generally, trying

to read data from the tape requires that the tape drive's hardware block size matches that which was used to write the tape. If a value is specified that is greater than zero in the *Resource Manager* for a particular *Resource*, *Backup**EDGE*** will attempt to set the hardware block size to this value before performing a backup through *EDGEMENU* or a *Scheduled Job*.

Tape drives usually support the special hardware block size of `0`. Since it is not useful to write data zero bytes at a time, this value indicates that the tape blocks should be of *variable* length. Specifically, each as each block of data is received from the operating system (or requested by the operating system), the number of bytes requested is used as the block size written (or expected block size to be read). As with fixed-size blocks, the block size while reading must match the block size that is recorded for that block. Unlike fixed-size blocks, each block may be of a different length. In practice, however, *Backup**EDGE*** will write identically sized blocks in variable block mode.

If you are using variable-sized blocks, the size of the hardware blocks that are written (read) are the size of the blocks that are produced (requested) by *Backup**EDGE***. This size is the software block size described above. So, if an archive is written in variable-block mode with the software block size set to `64`, the tape blocks will be 32KB long.

*Backup**EDGE*** also supports the special value of `-1` for the hardware block size. This value is not supported by any tape drive directly, but instead instructs *Backup**EDGE*** not to set the hardware block size before a backup. Instead, it uses the current setting of the tape drive. This is the default.

Generally, the hardware block size is set to `-1`, `0`, `512`, `1024`, or `2048`.

QUESTION 23 - I WANT TO BACK UP SPECIFIC SUBSETS OF MY DATA AS PART OF MY BACKUP SCHEDULE. HOW DO I DO THIS?

*Backup**EDGE*** allows you to separate your data into different parts, called *Backup Domains*. Each of these *Domains* describes some data that you want to protect. By default, *Backup**EDGE*** uses a domain called `system`, which includes all the files, directories, *Device Nodes*, etc., on your system.

The backups of a *Domain* are organized into *Sequences*. These *Sequences* allow you to separate backups by purpose. The most common example is on-site versus off-site backups of the same data. By keeping the two sets of backups separate, off-site backups are never dependent on on-site backups, nor are on-site backups dependent on off-site backups. If all the backups were accounted for together, it would be difficult to intermix on-site *Differential Backups* with off-site *Master Backups* without the on-site *Differential Backups* being based (sometimes) on off-site *Master Backups*.

Once you create a *Domain* to describe what you want to protect, you must define one or more *Sequences* to hold backups of that data. Remember that a *Sequence* accounts for backups of exactly one *Domain*; you cannot have two *Domains* share the same (for example) on-site *Sequence*. Instead, each must have its own *Sequence*.

When you create a *Scheduled Job*, you select which *Domain* this job should protect indirectly by selecting the *Sequence* of which the resulting backup will be a member. If you elect to perform *Differential* or *Incremental Backups*, they will be based on *Master Backups* in the same *Sequence*.

For more information on *Domains* and *Sequences*, please consult "Anatomy of a BackupEDGE Backup" on page 40 in the *Backup**EDGE*** User's Guide.

To actually take these steps, you must first enable *Advanced Scheduling* through *EDGEMENU*. To do this, simply select that option from the *Schedule* menu.

Once you have done this, you must create a new *Backup Domain* using the menu option for that purpose. When asked to select the *Domain* to edit, use the `[Down]` key to select `[New From`

`Wizard]`, and press `[Enter]`. For the details of this procedure, please consult “Creating Backup Domains” on page 231 in the *Backup**EDGE*** User’s Guide.

Similarly, create at least one new *Sequence* for this *Domain*. Select a name for it that describes the purpose of the backups. Consult “The Default Backup Sequence” on page 233 in the *Backup**EDGE*** User’s Guide for more information.

Finally, you must create one or more *Scheduled Jobs* to select the type, frequency, and destination *Device* of the backups you wish to make of this *Domain*. Consult “Scheduling - Advanced” on page 220 in the *Backup**EDGE*** User’s Guide.

Question 24 - What’s the difference between an archive listing and an archive index?

An archive listing is produced when *Backup**EDGE*** creates, lists, or restores an archive as a record of the process that occurred. This contains all the filenames that were encountered and processed. This generally means “all files backed up”, “all files listed”, or “all files restored”. The listing is for informational purposes, and is stored in human-readable format.

An archive index is designed to be a machine-readable database of the files on an archive, to act as a “cache” for that information for fast access. It is created when an Indexing pass is done on the archive, usually as part of the verification process. The index records much of the same information as the archive listing, plus information about where on the medium each file is stored. It also includes information about the archive label. An index is not stored in a form humans can read easily.

When *EDGEMENU* lets you browse through the contents of an archive for restore (see “Selective Restore” on page 245 in the *Backup**EDGE*** User’s Guide), it is consulting an index for this information. When a file is restored via Fast File Restore or Instant File Restore, a database provides the necessary records of where the desired file(s) are stored on the medium. The listing files have no part in this process.

When *Backup**EDGE*** tries to overwrite an archive, it will also try to erase any index that goes with that archive since it is no longer useful. It does not care about any listing that may be present; the listing is an historical record of the process that created or read the archive.

Question 25 - How do I make OPTICAL / OBDR Bootable Backups?

This is documented in “Anatomy of a Disaster Recovery” on page 279 in the *Backup**EDGE*** User’s Guide.

Question 26 - How do I restore one/a small number of files to their original/a new location?

This answer assumes that the backup is a non-Expert mode backup. This means it was created with *Backup**EDGE*** 01.02.00 or later, and was not created with the Expert Backup option of *EDGEMENU*. All 01.02.00 unattended backups, and most 01.02.00 EDGEMENU backups are fall into this category. For backups prior to 01.02.00, please consult “Expert Restore” on page 248 in the *Backup**EDGE*** User’s Guide for information.

Write protect the medium that contains the archive, and insert it into the the appropriate *Device*. This can be the same *Device* that wrote it, or any other compatible *Device* for which a *Backup**EDGE*** *Resource* is defined, even if it is on the same machine. (Be sure that the Tape Block Size matches the original *Resource’s* Tape Block Size if this is a tape *Device*, or you may have trouble reading the tape on some operating systems. *Backup**EDGE*** tries to record this information in the archive label on the medium, but a blocksize mismatch can make it impossible to get the label!)

Then start *EDGEMENU*. Select `Restore -> Selective Restore`. If an archive database can be found for this, you will be prompted to select whether you wish to browse the contents of the

archive, or type the filenames you wish to restore. Select whichever you prefer. If you are unsure, consult “Selective Restore” on page 245 in the *BackupEDGE* User’s Guide.

If no archive database is found, you must enter the filenames manually. To do this, you should enter their full pathname(s).

NOTE: If the archive database is on a remote system, *BackupEDGE* can still use it for *Fast File Restore*, or *Instant File Restore*. However, it is suggested that you do not browse the database. Doing so can be slow.

Once you have selected the files you wish to restore, you will be presented with a screen full of options. By default, the files will be restored to their original location.

There are two options for restoring files to alternate locations: changing the working directory for the restore, and performing a *Flat File Restore* (which is not to be confused with a *Fast File Restore*). You may select none, either, or both of these options.

If you wish to change the working directory, you may edit the text box that contains it. The following table shows some examples of how changing the working directory affects the final file position:

File to be Restored	Initial Working Dir	Setting Working Dir to /tmp Restores File To...
`/usr/lib/myfile`	`/`	`/tmp/usr/lib/myfile`
`/usr/lib/myfile`	`/usr`	`/tmp/lib/myfile`

The *Initial Working Dir* was chosen automatically when the archive was created. *BackupEDGE* tries to select a working directory that provides the maximum flexibility for a later restore. However, it also must pick a directory that contains all the files to be archived. So, if you perform a backup of `/usr/lib` and `/usr/bin`, it may select `/` or `/usr` for the working directory, but not `/usr/lib`, `/usr/bin`, or `/etc` (in fact, it will pick `/usr`). If this is a backup of all files on your system, the working directory must be `/` .

The second option to move files during a restore is to select a *Flat File Restore* by placing an `X` in the appropriate checkbox. This will cause *BackupEDGE* to remove all pathnames from the restore, and restore only the filenames. For example:

File to be Restored with Flat File Restore Enabled	Working Dir (May be Original or Edited Manually)	Flat File Restore Restores File To...
`/usr/lib/myfile`	`/`	`/myfile`
`/usr/lib/myfile`	`/usr`	`/usr/myfile`

Note that *Flat File Restore* causes *BackupEDGE* to omit all directory names, even if they are deeper than the files requested. For example, given that the archive contains:

```
/usr/mydir/file_a
/usr/mydir/dir_b/file_b
/usr/mydir/dir_b
/usr/mydir
```

A *Flat File Restore* with a working directory of `/tmp` would produce:

```
/tmp/file_a
/tmp/file_b
/tmp/dir_b
/tmp/mydir
```

QUESTION 27 - HOW DO I CHANGE THE COLORS THAT EDGEMENU USES?

BackupEDGE allows you to configure the color palette for *EDGEMENU*, *RecoverEDGE* for Linux and *RecoverEDGE* for *UW7*. It does not allow the colors of *RecoverEDGE* for *OSR5* to be modified.

The file `/usr/lib/edge/config/colors` contains the color palette. It may be edited with a text editor such as `vi`. The palette is installation-wide; it cannot be varied by terminal type or user at this time. It will be preserved across upgrades to *Backup**EDGE*** if possible.

It is recommended that you make a backup copy before modifying it.

If this file is removed, then the color palette will revert to a simple color scheme, similar to what is seen during the initial installation of *Backup**EDGE***.

Question 28 - When will *BackupEDGE* create an archive index for Fast File Restore / Instant File Restore?

*Backup**EDGE*** will attempt create an archive index automatically if instructed to do so through the 'Attempt Index' option in *EDGEMENU* or the Notify / Advanced tab in the Scheduler (the default is enabled). If the *Resource* used is a tape drive and the Locate Threshold is set to -1 in the *Resource Manager,* then no index will be created. The summary will contain a warning in this case.

Question 29 - I want to make *Differential* and/or *Incremental Backups* with EDGEMENU. How do I do this?

Creating *Differential* or *Incremental Backups* with *EDGEMENU* requires that you run a *Scheduled Job* in attended mode. It is ***not*** necessary that this *Scheduled Job* ever runs unattended.

After creating the appropriate *Scheduled Job*, select `Backup -> Run -> Scheduled` from *EDGEMENU*. You will be prompted to select between any available backup types, based on what types of backups have already been performed. It does ***not*** matter what (if any) types of backups are selected in the *Scheduler* for this *Scheduled Job*.

Recall from "Anatomy of a BackupEDGE Backup" on page 40 in the *Backup**EDGE*** User's Guide that one cannot perform a *Differential Backup* unless the *Sequence* to which it will belong already has a successful *Master Backup*. If you are not given the option of performing a *Differential Backup*, it is because no *Master Backup* ***in this Sequence*** currently exists.

Question 30 - Why do I get the error...

A complete list of numeric error codes can be found in "Error Return Codes" on page 336 in the *Backup**EDGE*** User's Guide.

Question 31 - How do I configure Virtual (Sparse) Files?

A *Virtual* (or *Sparse*) *File* is a file that appears to consume more hard disk space than it actually does. The difference between the apparent and actual size is treated as binary zeros when read. These files are used mainly for databases.

The operating system presents these files as identical to normal, non-virtual files. So, *Backup**EDGE*** must be told to treat them specially. If *Backup**EDGE*** is not told to treat them as *Virtual Files*, it will back them up as regular files, including the binary zeroes that aren't physically stored on the hard disk. As a result, the file will take up more space on the archive than necessary, and will take up more space if it is ever restored.

Before continuing, you should be familiar with the concept of a *Backup Domain*. If you are not, please consult "Anatomy of a BackupEDGE Backup" on page 40 in the *Backup**EDGE*** User's Guide.

To tell *Backup**EDGE*** that a file should be backed up as a *Virtual File*, you must create a file that contains its filename (along with the names of any other *Virtual Files*, one per line). This list file is then given to the *Domain(s)* that contain the file. Any time a backup of this *Domain* is made, the files listed in the list file will be automatically backed up as *Virtual Files*.

By default, the *Domain* named system uses the contents of the file `/etc/edge.virtual` to list all the *Virtual Files* on the system.

During installation, *Backup**EDGE*** will offer to autodetect virtual files for you. If you elect to do this, they will be stored in `/etc/edge.virtual`.

For more information, please consult "Virtual File Backups" on page 353 in the *Backup**EDGE*** User's Guide.

Question 32 - How do I configure Raw Filesystem Partitions?

UNIX and Linux *Device Nodes* can be used to access physical hardware, such as floppy diskettes and hard disk partitions. Normally, *Backup**EDGE*** archives the *Device Node*, but not the data that may be accessible through that *Device Node* directly. For most applications, this is the desired behavior; the data to be backed up is contained in the UNIX or Linux filesystem. Backing up the raw data on the associated hard disk partitions would be redundant.

However, some applications store data outside of the UNIX or Linux filesystem directly into a hard disk partition (etc.). In this case, you may want to have *Backup**EDGE*** back the underlying data up, in addition to the *Device Node* that accesses it.

Before attempting this, it is important that you are familiar with basic *Backup**EDGE*** terms such as *Sequence* and *Domain*. Please consult "Anatomy of a BackupEDGE Backup" on page 40 in the *Backup**EDGE*** User's Guide for information.

To have *Backup**EDGE*** back up the data accessed by a *Device Node*, you must create a file that contains the names of the *Device Nodes* that should have their underlying data archived. These should be listed one per line. Then, this filename should be added to the *Domain* under 'Raw Dev Filelist' option. For more information on editing Domains, please consult "Default Domain" on page 231 in the *Backup**EDGE*** User's Guide.

Question 33 - How do I initialize tapes or other media?

Run *EDGEMENU*. Be sure that the *Primary Resource* (shown in the box at the bottom of the screen) is the correct one. Insert the medium to be initialized, and wait for it to become ready.

Select `Admin -> Initialize Media`. You will be given the opportunity to change the default medium usage counter, and proceed to initialize the medium.

Write-once media (such as CD-R's) cannot be initialized.

For more information, please consult "Initialize Medium" on page 202 in the *Backup**EDGE*** User's Guide.

Question 34 - What is TapeAlert™?

TapeAlert™ is a Hewlett-Packard initiative adopted by many tape drive vendors. It provides a means for a tape drive to provide you with status information and warnings. As the tape drive encounters messages, it will queue them until requested by *Backup**EDGE***.

*Backup**EDGE*** will report TapeAlert messages it finds in the summary it creates for the operation it was performing when the message was detected. These messages should be taken seriously, as they generally predict impending failures of the medium or the *Device*.

Not all *Devices* support TapeAlert. If you are unsure, select `View -> Primary Resource Status` in *EDGEMENU*. One of the properties listed will indicate if TapeAlert support is present in the *Device*.

TapeAlert messages remain queued in the tape drive until a TapeAlert query is made, and are then erased. If you get a TapeAlert labeled as "Before Backup" on an email message or printed report, consider the possibility that some prior use of the tape drive caused this message to be queued.

Question 35 - What is an Autochanger Association?

Autochangers (also called Libraries or Jukeboxes) are separate *Devices* from the tape drives they support. *Backup**EDGE*** maintains a separate *Resource* for the Autochanger itself, apart from any tape drive(s).

The Autochanger provides *Storage Elements* (magazine slots) and *Data Transfer Elements* (tape drives), along with *Import / Export Elements* (places where an operator can add or remove tapes from the Autochanger), and *Media Transport Elements* (mechanisms which physically move tapes between the other elements). When *Backup**EDGE*** issues a command to the autochanger, it instructs it to move media from one element to another. It is important to realize that to the autochanger, each of these elements is roughly just a place that a tape may located. The *Data Transfer Element*, as seen by the Autochanger, has nothing to do with actually reading from or writing to the tape.

However, *Backup**EDGE*** must be able to predict how this affect the status of the tape drives. By creating an association, the *Data Transfer Elements* of the Autochanger can be be associated with the tape drives physically installed in the corresponding location. Then, *Backup**EDGE*** can instruct the Autochanger to move a tape into a *Data Transfer Element*, and use the associated tape drive to access the tape's data. It is an Autochanger Association which tells *Backup**EDGE*** of this relationship.

For more information on setting up these associations, please refer to "Configuring a URL for FTP Backups" on page 62 in the *Backup**EDGE*** User's Guide.

Question 36 - How do I set up printing for Scheduled Jobs?

Use `edgemenu -> Schedule` to edit the *Scheduled Job* to which you would like to add printed summaries. Use the *Notify / Advanced* option to display the *Notification* options.

The field labelled "`Print Summary To`" should contain the printer **queue** name (***not*** the command used to print) that will print the summary. Save the *Scheduled Job* and exit the *Scheduler*.

If you would like to review or edit the command that will be used to print, use *EDGEMENU* to edit the *Notifier* created for that printer name, using `Schedule -> Edit Notifiers`, as described in "Edit Notifiers" on page 209 in the *Backup**EDGE*** User's Guide.

Question 37 - Where does *BackupEDGE* store its listing files?

The log files for each operation are stored in:
`/usr/lib/edge/lists/`**`jobname`**

where **`jobname`** is the name of the *Scheduled Job* that created them. For the Basic Schedule, this is `simple_job`. If the log files were created in *EDGEMENU*, replace **`jobname`** with `menu`.

In this directory, some or all of the following files may be present:

`backup_system_master.txt`	Log file of last *Master Backup* made by this *Scheduled Job* of the *Domain* `system`. If another *Domain* is also included (such as mysql) there will be another, similar log.
`verify_system_master.txt`	Log file of the last verification of the *Domain* `system`.
`changedfiles_system_master.txt`	List of all files which were changed on the hard disk between the backup and verify of the *Domain* `system`.
`edge_summary.txt`	Text version of the last summary created.

`edge_progress.txt`	Step-by-step list of actions performed when this *Scheduled Job* was last run.
`schedule.lck`	Lockfile for this *Scheduled Job*.

These are described in additional detail in “Debugging A Failed Backup” on page 349.

QUESTION 38 - I HAVE A DATABASE/OTHER APPLICATION THAT I WANT TO SHUT DOWN BEFORE ARCHIVING. HOW DO I DO THIS?

This can be accomplished by editing the Domain Script for the *Domain(s)* that include this database (or other application).

If you are using the default *Domain* `system`, these scripts default to `/etc/edge.start`, `/etc/edge.passed`, and `/etc/edge.failed`. Otherwise, the script is selected in the Domain Editor of *EDGEMENU*.

Then, perform backups of this data using *Scheduled Jobs*. These can be run unattended and/or through the Run Scheduled option of *EDGEMENU*.

For more information about Domains, please read “Anatomy of a BackupEDGE Backup” on page 40 in the *BackupEDGE* User’s Guide. For more information about Domain Scripts, please review “Running Scripts to Prepare for Backup” on page 342 in the *BackupEDGE* User’s Guide.

QUESTION 39 - WHAT IS AN “EXPERT-MODE ARCHIVE” AND WHY DOES *BackupEDGE* KEEP TELLING ME IT FOUND ONE?

Most backups performed with *BackupEDGE* 01.02.0x are called non-Expert backups. This means that *BackupEDGE* manages how the data is stored on the archive to make the restore process easier. More specifically, in a non-Expert backup, you tell *BackupEDGE* what you want to back up, and it handles the details of how it is stored on the archive.

In all versions of *BackupEDGE* before 01.02.00, you had the responsibility of telling *BackupEDGE* how data was to be stored on tape (e.g., in absolute or relative pathname format, what the current working directory of the backup would be, etc.). Because you had the freedom to store data in any way at all, *BackupEDGE* cannot help you locate it later.

The additional freedom of an Expert-mode backup brings with it significant responsibility without providing significant (or any) benefits to the average user. Its name “Expert-mode backup” derives from the assumption that only UNIX experts would require the benefits this additional control.

It is highly recommended that you use non-Expert-mode backups if possible. Normally, *BackupEDGE* can manage the pathnames on an archive in such a was as to provide exactly the same benefits as an Expert-mode backup for almost any normal circumstance.

QUESTION 40 - WILL *BackupEDGE* COMPRESS/DELETE MY ARCHIVE INDEX?

By editing `/usr/lib/edge/config/master.cfg`, you can configure *BackupEDGE* to compress and/or delete archive indexes. Please review “Environment Variables” on page 322 in the *BackupEDGE* User’s Guide.

QUESTION 41 - I WANT TO SET UP DIFFERENTIAL (AND POSSIBLY INCREMENTAL) BACKUPS OF MY SYSTEM IN ADDITION TO MASTER BACKUPS. CAN THE BASIC SCHEDULE DO THIS?

Yes.

First, you must enable *Advanced Scheduling* in *EDGEMENU*. Then, you must edit the *Basic Schedule* with the *Advanced Schedule* editor (`EDGEMENU -> Schedule -> Advanced Schedule`). You will now be able to select *Master*, *Differential*, and *Incremental Backups* on each day of the week.

As long as at least one day has a *Differential* or *Incremental Backup* scheduled, you will be able to select any backup type in the Basic Scheduler for any day of the week. However, if the *Basic Schedule* will perform only *Master Backups*, the *Basic Scheduler* will revert to its old behavior of allowing *Master Backups* only. You will then have to use the *Advanced Scheduler* to re-enable *Differential* or *Incremental Backups*.

By default, the Advanced Scheduler is disabled in *Backup**EDGE*** 01.02.04. To enable it, run `EDGEMENU -> Schedule -> Enable Advanced Scheduler` and follow the prompts.

Question 42 - How Do I Change the Font Size When Running BackupEDGE in Character Mode in X Windows?

When you click or double-click the *Backup**EDGE*** (or *EDGEMENU*) icon, the following script is executed...

```
/usr/lib/edge/bin/edgemenu.sh
```

You may change the font size by editing this script and setting the `FONT` variable. Typically, the appropriate setting for this variable would be one of the alias names from the `misc/fonts.alias` file in your X Windows libraries. An typically larger font in most systems is the 10 x 20 font. To use this, edit `edgemenu.sh` and change the...

```
FONT=""
```

line to say...

```
FONT="10x20"
```

Then launch *EDGEMENU* from the icon and observe the results.

NOTE: This does not work under OpenServer 5.

Question 43 - What's the Correct Way to do Multi-Volume, Attended Backups Without Backing Up through EDGEMENU?

If you wish to run a backup without running *EDGEMENU*, you should create a *Scheduled Job*. This *Scheduled Job* can be run in either the foreground or the background via the *EDGE.NIGHTLY* program as desired.

If the *Scheduled Job* is run in the background, it will behave as if it was run automatically via the *Scheduler*. If user intervention is required, the *Notifiers* selected in the *Scheduled Job* will be used. To acknowledge these, simply start *EDGEMENU*, and you will be told that there are *Scheduled Jobs* requiring attention. You will then be given the option to tell them to proceed.

If the *Scheduled Job* is run in the foreground, it will interactively prompt for new volumes and display a running status as it progresses.

EDGE.NIGHTLY will run a *Scheduled Job* in foreground mode if the `-zDISPLAY_MODE=INTERACTIVE` command line flag is given:

```
/etc/edge.nightly -zDISPLAY_MODE=INTERACTIVE -H simple_job
```

NOTE: The `-zDISPLAY_MODE` flag must be the first option on the command line!

These options are detailed in "The EDGE.NIGHTLY Program" on page 326.

Question 44 - What's the Best Way to Add Backups to My Own Shell Scripts?

You should run *EDGE.NIGHTLY* from the command line. Please refer to "The EDGE.NIGHTLY Program" on page 326 in the User's Guide.

Question 45 - How do I use the same Encryption Key on multiple systems?

First, you must have a permanent Encryption License in order to use encryption beyond the initial demo period. You must also set it up normally, so that one system has the public encryption key that you want to copy.

You must also install *Backup**EDGE*** with an Encryption License on each machine that will be performing encryption.

If you will be replicating systems using `edge.cfgmgr`, then you may use the option `-pubkey` to include the public key in the configuration file. Then, when this configuration file is imported onto one of the other installations, the public key will be copied as well. *Note that this does not cause the private keys to be copied! This must be done manually via a key restore!*

Alternatively, the key itself is stored in the file `/usr/lib/edge/keys/public.key`. You may make a copy of this file any way you like if you do not plan on using `edge.cfgmgr`. You must have previously set up encryption on the target machines, however, or else it will not be used. You should elect not to create a new key pair during setup, of course.

Question 46 - How do I set up a backup to an FTP server / NAS?

First, be sure to have *Backup**EDGE 2.1*** or later. Versions prior to this do not support FTP backups.

The complete instructions for this can be found in the “Configuring FTP/FTPS Backups” on page 90 in the *Backup**EDGE*** User’s Guide. Please consult that for more detailed instructions.

The quick answer is: set up a URL Resource in the Resource Manager (EDGMENU ->Admin -> Define Resources). Specify the machine, directory, username, and password for the FTP server. Then simply use this resource whenever you would like to back up to the FTP server.

Question 47 - How do I use FTPS?

To select it, highlight the Protocol field in the URL Resource definition, and use the Right Arrow key to select from FTP, which is a standard unencrypted FTP session, FTPS (FTP Data+Ctrl via SSL), which is used to encrypt both the session authentication and the actual data transferred, or FTPS (FTP Ctrl via SSL), which is used to encrypt only session authentication information.

Remember that FTPS does not write encrypted archives; it only encrypts the data during transmission to the FTP site, along with the username / password information for the FTP server. You may also want to enable encryption for the archive itself if you want it to be stored on the FTP site encrypted. To do this, please see “Encryption” on page 259 in the *Backup**EDGE*** User’s Guide.

Question 48 - What else do I need to know about SharpDrives?

When initializing *SharpDrive* media, be absolutely sure that only the desired media is selected for destructive initialization. While *Backup**EDGE*** tries to ignore those media which seem to be used for other things, it cannot always do so reliably. It is up to you to make sure that the device node(s) is/are correct, else **YOU MIGHT LOSE DATA**.

If more than one medium is available for the *SharpDrive Resource*, then *Backup**EDGE*** usually writes the archive to the medium that has the most free space on it. "Free space" is measured as the sum of unused space on the medium, plus the amount of space that is used by archives which may be reclaimed. To be reclaimable, the archive must have an expired TTL at the very least, plus some additional requirements in some cases which will be described below.

Note that *Backup**EDGE*** does not reclaim archives unless it actually needs the space; *Backup**EDGE*** cares only that the space could be reclaimed if it is needed. Also note that exceptions to the "most free space rule" will be given below.

In the case of differentials and incrementals, *BackupEDGE* will avoid reclaiming the last copy of any master, differential, or incremental backup on which the newly-created backup will depend.

For example, if it is writing a differential backup, then it will not reclaim the last copy of the corresponding master backup in order to free up space for the differential, even if that master backup has an expired TTL. Note that there may be more than one copy of an archive (see below), so that *BackupEDGE* might still choose to reclaim the master if another copy of it has been recorded.

There is one exception to this exception. Nightly backup jobs which are run unattended (not via edgemenu:Run Scheduled) have an option to allow automatic promotion due to overwrite. This option can be set in the Notify / Advanced screen of the job.

If overwrite promotion is allowed, then *BackupEDGE* may reclaim a backup on which the new backup will depend if its TTL has expired, even if it is the last copy. Of course, if it does so, the new backup will be promoted to replace the old one. Note that using edgemenu:Run Scheduled forces the user to choose the backup type manually. *BackupEDGE* will not override this choice.

Another restriction on reclaiming archives occurs when a job performs more than one backup as part of the job. For example, a job might perform a file-level backup and a MySQL backup. In this case, *BackupEDGE* will refuse to reclaim any archive that was done as part of this job. To continue with the example, *BackupEDGE* will not reclaim the filesystem backup when looking for space for the mysql backup. While we expect that the TTL would usually prevent this anyway, we did not want the individual backups in a multi-domain job with a TTL of 'immediately reclaimable' to compete for space.

There is one case in which *BackupEDGE* may write to a *SharpDrive* medium which does not contain the most free space. If *BackupEDGE* is performing a job that requires more than one backup (as in our filesystem / MySQL example), then it will use the free space rule only for the first backup that it writes. All subsequent backups will use the same medium as the first, so that the job is not silently split across multiple *SharpDrive* media.

None of this describes what *BackupEDGE* does if it does actually run out of space on whatever medium it selects. In all cases, it will prompt for more media, even if there are other sharpdrive media on which it could continue. It does this to avoid silently splitting the archive across multiple media. Note that in this case, the user must unplug the *SharpDrive* medium on which the backup was started before telling *BackupEDGE* to continue. If not, *BackupEDGE* will notice that the backup has been started on that medium and refuse to continue since there is no more space on it. In most cases, this will result in *BackupEDGE* immediately requesting more media again. This behavior is intentional.

Also note that it is not necessary that the user plugs in new media to fulfill the request; if the backup starts with multiple *SharpDrive* installed, then unplugging the one which contains the beginning of the backup and acknowledging *BackupEDGE*'s new volume request might be sufficient to let *BackupEDGE* continue (assuming, of course, that at least one of the remaining sharpdrives has space on it). The user may choose to plug in new media in any case, of course. If multiple media are plugged in, then *BackupEDGE* will use the 'free space rule' to select which one on which to continue the backup.

Remember that media which has been initialized for some other *SharpDrive resource* will be entirely ignored by *BackupEDGE*. It will not affect any of the decisions *BackupEDGE* makes when choosing media.

Again, it is recommended that only one *SharpDrive* be plugged in at any one time during a backup. It's really much simpler than remembering all of these rules.

QUESTION 49 - HOW ELSE CAN I USE A REMOVABLE HARD DRIVE?

First, be sure to have *BackupEDGE 2.1* or later. Versions prior to this do not support removable hard drive backups.

The complete instructions for this can be found in the "Configuring Legacy Disk-to-Disk Backups" on page 158 in the *BackupEDGE* User's Guide. Please consult that for more detailed instructions.

The quick answer is, set up an AF (Attached Filesystem) resource. It should contain enough information to mount and unmount the removable hard drive.

After that, set up one or more FSP resources. Select the AF created above. Be sure each FSP has its own directory on the AF.

Once you have an FSP set up and initialized, use the FSP to write backups. The slot name is important with FSP backups, since multiple backups can be on the same FSP at once. The slot name controls when a backup overwrites an existing backup (same slot name), and when the new backup is added without removing old backups first. The User's Guide provides more information on this.

QUESTION 50 - WHAT HAPPENS WHEN I CHANGE MY TAPE DRIVE / DVD DRIVE / ETC.?

When changing hardware, you must perform any necessary steps to inform the operating system. For OpenServer 5, this involves running the appropriate `mkdev` script to remove the old hardware and add the new hardware. Other operating systems do not require this.

However, once you do this, you must still tell *BackupEDGE* how to deal with the new hardware. Generally, you may do one of two things:

1. Run the *BackupEDGE* autodetector (EDGEMENU -> Setup -> Configure BackupEDGE -> Autodetect New Devices).

2. Let *BackupEDGE* determine what has changed.

Generally, option 1 is the better option, since you can decide immediately if *BackupEDGE* can talk to the new hardware. If you delete the *Resource* for the outgoing hardware before running the autodetector (EDGEMENU -> Admin -> Define Resources, then press F6 to delete the highlighted *Resource*), then you can simply name the detected resource with that name, and all existing *Scheduled Jobs* will start to use it.

Option 2 lets *BackupEDGE* discover for itself that hardware it wants to access is missing. In this case, it will try to detect any new hardware, and use it as a substitute for the missing device. Backup reports will note that a substitution has occurred. EDGEMENU will notify you on startup of this as well.

EDGEMENU will also give you the option to make the substitution permanent. If you do this, then the old *Resource* will be deleted, and the new one will be renamed to match the old *Resource*. This will cause all *Scheduled Jobs* to use the new *Resource*.

For additional information on resource handling and substitution. please see "Notes on Changing Backup Device Hardware" on page 68.

QUESTION 51 - WHY FTPS AND NOT SFTP?

BackupEDGE treats all devices alike. FTPS has a full feature set, including the ability to open an archive starting at a specific block. This is critical to the Instant File Restore capability within *BackupEDGE*. SFTP lacks this capability. It essentially copies whole files only.

FTPS is also generally easier to configure. SFTP requires keys to be transferred, special ports to be open in the firewalls, and additional daemons to be run.

41 - Support Policy

41.1 - Electronic Mail

Non-priority support via electronic mail is available at any time to anyone running *BackupEDGE* 03.00.00 or later with either a current ***Support and Maintenance Subscription*** or a ***Subscription*** that has expired within the last 5 years. or higher on a best-effort basis. No contract is required at this time. Technicians can be contacted via e-mail at `support@microlite.com`.

Support and Maintenance Subscriptions may be renewed for up to 5 years after they expire. After that the license moves to **Support End Of Life**. After **Support End Of Life** is reached, no support of any kind is available, and no updates are available.

41.2 - Pre-Sales / Evaluation Products

Those who have installed an evaluation copy of *BackupEDGE* are welcome to contact our support department for assistance in set-up and configuration of the products.

Our telephone support hours are 8:30am to 5:00pm Eastern Time. Telephone support is available for 60 days from the date of first contact for users running an evaluation program. Upon calling Microlite, please indicate that it is a Pre-Sales call. The receptionist will gather your information and you will be directed to a technician. In the event a technician is not available, your call will be returned as soon as possible.

41.3 - Commercially Licensed Products

Those who have purchased a *BackupEDGE* license will receive a *Base Product Serial Number* and a ***Support and Maintenance Subscription***. Please have the *Serial Number* available when contacting our support department. Technicians can be accessed via e-mail at `support@microlite.com`. The ***Support and Maintenance Subscription*** is generally one through five years from the date the product is activated depending on the license. If support is needed before activation, the time period begins from the date of first phone contact. The ***Support and Maintenance Subscription*** includes:

- Telephone and e-mail technical support.
- Free product upgrades.
- Free cross-platform upgrades.
- No-charge re-activation of licenses under normal circumstances.
- Access to our upgrade / update servers. See “BackupEDGE Licensing” on page 363 for more information.
- The ability to extend a current Subscription at a reduced rate.

Contact your reseller or see the Microlite Web Site for ***Support and Maintenance Subscription*** extension and renewal information.

- *Out of Subscription Support* can be purchased on an as-needed basis. The charge at the time this User Guide was created is $250.00* per hour billable in 15 minute increments of $62.50*. This may be changed at any time. There will be a minimum of 15 minutes charged for each call. Payment can be made using Visa, MasterCard, Discover or American Express. Support for *BackupEDGE 02.0x* and earlier is billed in 30 minute minimum increments.

*All prices shown are in US dollars. Prices are subject to change without notice.

41.4 - Authorized Resellers

Resellers who are registered with Microlite are entitled to no charge technical support at any time for their own in-house licenses. When calling for technical support for a registered end-user, the end-user serial number must be supplied, and it must be covered under a valid ***Support and Maintenance Subscription***.

41.5 - Telephone Support

Telephone support is available between the hours of 8:30am and 5:00pm United States Eastern time, Monday through Friday, holidays excluded.

Telephone support eligibility:

- End Users under a valid ***Support and Maintenance Subscription***.
- Registered resellers when calling for support on their own licenses or on behalf of an end-user under a valid ***Support and Maintenance Subscription***.

Upon calling Microlite, please indicate that it is a support call and be ready with the serial number of the product for which support is desired. Resellers must also have their reseller number available for verification. The receptionist will gather your information and you will be directed to a technician. In the event a technician is not available, your call will be returned as soon as possible.

Please check the Microlite Product Support web page for the most current information.

Contact Microlite Technical Support at:
724-375-6711 (Phone)
724-375-6908 (Fax)

42 - End User License Agreement (EULA)

Before installing this product, carefully read the following terms and conditions. Installation of this product indicates your acceptance of these terms and conditions. If you do not agree with them, promptly return the product unused and request a refund of the amount you paid. If you are installing this software for use by other parties, you agree to inform the users that the use of the software indicates acceptance of these terms.

1 - LICENSE. The software programs ("Software") contained in the package are copyrighted and owned by Microlite Corporation ("Microlite") and are licensed (not sold) to you by Microlite under the following conditions.

- ***Evaluation:*** You may install any of the products, whether downloaded or from distribution media, on a single computer system for a ONE TIME ONLY 60 day evaluation period without purchasing a valid license. This includes encryption, subject to export restrictions contained herein.
- ***Purchased License:*** You may install the version of this product described on your purchased license for unlimited use on a single operating system instance on a single computer system by using a permanent serial number provided by Microlite Corporation to register the product. Your permanent license goes into effect upon receipt and entry of the Activation Code provided by Microlite Corporation after receipt of a valid registration form. To be considered valid, only End-User information may be entered in the following registration form fields; Company Name, Address 1, Address 2, Company City, Company Country, State / Province, Contact Person, Contact Email, Voice Phone, Fax Phone.
- ***Encryption License:*** You must purchase, register and activate a separate encryption license in order to use encryption features after the evaluation period.
- ***Backup:*** If and only if you have a valid, purchased license, you may make a single copy of the Software for backup purposes or installation. You may not alter, decrypt, reverse assemble, reverse compile, or otherwise translate the Software. You may not copy the Software into any public network. You may not sublicense or rent the Software to any third party. The license is non-transferable.

2 - TITLE. Microlite shall retain all rights, title and interest in and to Software including, but not limited to, all copyrights, patents, patent applications, licenses, trade secrets, trademarks, trade names, service marks, inventions, franchises and all proprietary rights in and relating to the Software. During and after the term of this Agreement, you agree that you will not assert or claim any interest in or do anything that may adversely affect the validity and the enforceability of any intellectual property right relating to the Software.

3 - STATEMENT OF LIMITED WARRANTY. Microlite provides a three-month limited warranty, as measured from the date of delivery to the original customer, on the media (e.g. compact disc, etc.) on which the software is furnished, if delivery is not electronic. With the exception of the express warranty described above, the Software is not warranted and is provided "as-is". The warranties described above replace all other warranties, express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

4 - LIMITATION OF REMEDIES. Microlite's entire liability and your exclusive remedy shall be as follows: Microlite will provide the express warranty described above. If Microlite does not remedy defective media as warranted, you may terminate your license and your money will be refunded upon the return of all of your copies of the Software. For any claim arising out of Microlite's limited warranty or for any other claim whatsoever related to the subject matter of these terms, Microlite's liability for actual damages, regardless of the form of action or basis

(including breach, negligence, misrepresentation or other tort) shall be limited to the greater of $100 or the money paid to Microlite or its Authorized Remarketers for the license for the Software that caused the damages or that is the subject matter of, or is directly related to, the cause of action. This limitation will not apply to claims for personal injury or damages to real or tangible personal property caused by Microlite's negligence. In no event will Microlite be liable for any lost profits, lost savings, or any incidental damages or other consequential damages, even if Microlite or its remarketers have been advised of the possibility of such damages, or for any claim by you based on a third party claim. Some jurisdictions do not allow the limitation or exclusion of incidental or consequential damages, so the above limitation or exclusion may not apply to you. In no event will Microlite or any of its resellers be liable for any interruption of use or any loss of, inaccuracy, or damage, to data or records.

5 - GENERAL. You may terminate your license at any time by destroying all your copies of the Software or as otherwise described in these terms. Microlite may terminate your license if you fail to comply with these terms. Upon such termination you agree to destroy all your copies of the Software. Any attempt to sublicense, rent, lease or assign, or transfer any copy of the Software is void. You agree that you are responsible for payment of any taxes, including personal property taxes, resulting from this Agreement. No action, regardless of form, arising out of this Agreement may be brought by either party more than two years after the cause of action has arisen. This Agreement is governed by the laws of the United States of America. If you acquired the Software in the United States of America, the law of the Commonwealth of Pennsylvania shall govern.

6 - UNITED STATES GOVERNMENT RESTRICTED RIGHTS LEGEND. The Software and accompanying written materials are provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of The Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or in subparagraphs (c)(1) and (2) of the Commercial Computer Software-Restricted Rights clause at 48 C.F.R. 52.227-19, as applicable. The Contractor/Manufacturer is: Microlite Corporation, 2315 Mill Street, Aliquippa PA 15001-2228 USA.

7 - EXPORT RESTRICTIONS. Software contains encryption technology and is subject to export regulations under United States law. The Software is eligible for export and subject to License Exception ENC under Sections 740.17(a) and (b)(3) of the export administration regulations of the United States Department of Commerce, Bureau of Export Administration. You agree that you will not export or re-export the Software or any part thereof (i) to Cuba, Iran, North Korea, Sudan, Syria, or any other country subject to United States trade sanctions applicable to the Software, to individuals or entities controlled by such countries, or to nationals or residents of such countries other than nationals who are lawfully admitted permanent residents of countries not subject to such sanctions; or (ii) to any named party or individual on the United States Department of Treasury, Office of Foreign Assets Control (OFAC) list of Specially Designated Nationals and Blocked Persons or on the United States Department of Commerce, Bureau of Export Administration Denied Persons List or Entity List.

8 - WARNING. The Software is not fault tolerant and is not designed, manufactured, or intended for use or resale as on-line control equipment in hazardous environments requiring fail-safe performance, including but not limited to use in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of the software product could lead directly to death, personal injury, or severe physical or environmental damage (“high risk activities”).

43 - PXE Boot / Configuration Guide

Misplacement of, or damage to, boot media have long been potential sources of delay and trouble in the event of a disaster. To eliminate this potential problem, *BackupEDGE* (actually *RecoverEDGE*) is capable of performing media-free disaster recovery by using network booting capabilities of modern Network Interface Cards (NICs) to start *RecoverEDGE* from a boot image stored elsewhere on the network.

43.1 - What is PXE?

PXE (generally pronounced “pixie”) is a standard for booting a system via the network (PXE stands for Pre-Boot Execution Environment). Most modern network cards and system bioses support this. If yours doesn't, there might be a firmware update available that will allow it.

The idea is that on bootup, the network card can take a series of steps that will end up with a booted system:

1. Locate a DHCP (Dynamic Host Configuration Protocol) server
2. Get an IP address from the DHCP server
3. Get the IP address of the TFTP (Trivial File Transfer Protocol) server from the DHCP server
4. Get a boot image from the TFTP server
5. Boot from this image.

It may sound complicated, but after proper setup, these steps occur automatically whenever the NIC card becomes the boot device.

RecoverEDGE can use PXE to boot your system to the disaster recovery menu without additional boot media, such as a CD, DVD, or REV. Of course, you must still have some sort of backup available if you want to restore everything. Because *BackupEDGE* supports FTP backups, it is possible to perform a disaster recovery with no local media at all, if both FTP backups and PXE disaster recovery are used!

It is strongly recommended that you read this entire section before trying to use PXE for disaster recovery, and that you perform test booting and archive listings before putting it into a production environment.

43.2 - Which Operating Systems Does RecoverEDGE Support PXE With?

RecoverEDGE supports PXE booting on Linux 2.6, 3.x , 4.x and 5.x kernels in BIOS mode.

43.3 - How Do I Set Up PXE Booting?

Setting up PXE booting is reasonably straightforward.

Configure a DHCP Server

The first step is to make sure that a DHCP server is available on your network. During the PXE boot, the network card will get its IP address via DHCP. Even if your server normally has a static IP address (which it should for use with *BackupEDGE* or just about anything else), during PXE booting the network address will be dynamically configured via DHCP.

This document isn't going to describe how to set up a DHCP server. It will tell you what you must do (in general) to modify an existing DHCP server to allow PXE booting.

After you have configured a DHCP server, it is necessary to tell it about the TFTP boot server that actually holds the *RecoverEDGE* PXE boot images. To do this, you must tell it three things:

1 that booting and bootp are allowed from the DHCP server.

2 the “next server” address (the TFTP server in this case).

3 the filename to get from the “next server”.

Exactly how you tell your DHCP server this depends on the server in question.

A very popular server under Linux is **dhcpd**, which is easy to configure. The examples that follow assume that you're using this server.

The configuration file is `/etc/dhcpd.conf` by default. Edit this file (probably make a backup first). The start of the file might look something like this:

```
-----------------------------------------------------
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#

# option definitions common to all supported networks...
option domain-name "microlite.com";
option domain-name-servers mlite.microlite.com, www.microlite.com;
-----------------------------------------------------
```

Lines starting with “`#`” are comments. To enable PXE booting from this DHCP server, you must add these lines:

```
allow booting;
allow bootp;
```

Probably they should be put just after the initial group of comments.

Notice that these lines end with a semi-colon (`;`). All dhcp configuration lines that we'll be adding should end with a semi-colon.

Next, you must tell the server where the TFTP server is and what filename should be used for PXE booting. Where in the file you put this depends on your DHCP configuration. You may put it in one or more of the “subnet” sections, or in the outside block. If you include it in a subnet section, you could control which TFTP server is used based on the subnet. If you're not sure how to do this or why you'd want to, then probably you can just put it directly after the “allow” lines you just added:

```
# Linux
filename "pxelinux.0";
next-server 192.168.1.16;
```

The filename refers to a file that we're going to be storing on the TFTP server. While you can change the name (assuming you also rename the file, of course), for now we'll assume you don't need to. The file will be installed as `pxelinux.0` (Linux) by default when you install the boot files made be *RecoverEDGE* onto the TFTP server.

The next-server line should list the IP address of the TFTP server. In the example, this is `192.168.1.16`. Change this to the IP address of the TFTP server you've created. Note that if it is the same as the DHCP server, do **not** use `127.0.0.1` here; use the IP that is accessible from the network on which the DHCP clients will be located.

Configure a TFTP Server

After the DHCP server has been set up, you must set up a TFTP server, and install the PXE boot files on it. Again, setting up a TFTP server is beyond the scope of this document, but it's fairly straightforward. Normally, you'll already have one. It is probably disabled by default, but editing

the appropriate `inetd / xinetd` configuration file `(e.g., /etc/inetd.conf)` will enable it. Be sure to restart `inetd / xinetd` after changing the configuration file, or else nothing will happen.

Build RecoverEDGE PXE Images

The last step is to generate PXE boot files using *RecoverEDGE*. To do this, install *BackupEDGE* normally and configure it on whatever machine(s) you care to. When you run *RecoverEDGE* (`edgemenu:Setup:Make RecoverEDGE Media`), you will see the option for creating `PXE Boot Files for Network Booting`. Select this, then `Make Media` from the main *RecoverEDGE* menu to create the images.

```
+ Select RecoverEDGE Media / Image Type ----------------------------------+
|+-------------------------------------------------------------------------+|
||   (Keep Current Settings)                                               ||
||   Boot Media on Floppy Disk (1.72MB)                                    ||
||   Boot Media on Floppy Disk (1.68MB)                                    ||
||   Boot Media on Floppy Disk (1.44MB)                                    ||
||   Boot Media on dvd0                                                    ||
||   Images Only for dvd0 Bootable Backups                                 ||
||-> PXE Boot Files for Network Booting                                    ||
||                                                                         ||
||                                                                         ||
||                                                                         ||
||                                                                         ||
|+-------------------------------------------------------------------------+|
+ Press [F2] to Exit, [UP] / [DOWN] / [ENTER] to Select ------------------+
```

If you receive an error about detecting the mac address of the network adapter, or if *RecoverEDGE* selects a network card that you do not intend to boot from, then edit the value of `RE2_PXE_MAC` in `/usr/lib/edge/config/master.cfg`. This will override *RecoverEDGE*'s selection the next time PXE boot files are created.

NOTE: The DHCP and TFTP servers themselves probably cannot be booted via PXE if they are the **only** DHCP and TFTP servers on your network. Use another type of boot media for *RecoverEDGE* to protect these systems, such as CDROM, DVD, REV, or bootable tape.

Assuming image creation is successful, the PXE boot files will be stored in:
`/usr/lib/edge/recover2/images/pxe.tar`

These can be transferred to and un-tarred into the root directory of your tftp server.

The `pxe.tar` archive contains several files:

```
./pxelinux.0
./pxelinux.cfg/<mac address>
./recoveredge/<mac address>/pxelinux.0
./recoveredge/<mac address>/sysname
./recoveredge/<mac address>/<system name>
./recoveredge/<mac address>/<some other files>
```

`<mac address>` is the boot network adapter's mac address, with `01` prepended.

The `pxelinux.0` file is the PXE boot file. The copy in `./recoveredge/<mac address>` is not used normally, but is provided as a backup.

The file in `pxelinux.cfg` is the configuration file for booting from the given mac address. Note that renaming or copying this file is all that's needed to boot from a network card with a different mac address. It is not necessary to copy the entire `./recoveredge/<mac address>` directory.

The `sysname` file contains a line:

```
<mac address> <system name>
```

so that you can use Linux commands to associate mac addresses, system names, and boot files easily. The `<system name>` file is just an empty file named the same as the system itself. This file is mostly useful if you're browsing the tftp directory manually.

The remaining files in the `./recoveredge/<mac address>` directory are the *RecoverEDGE* boot files.

NOTE: Multiple systems can share the same TFTP server for disaster recovery. Each one will create a `pxe.tar` file, but the filenames will be different because of the mac address. Note also that the `pxelinux.0`.

Booting from PXE

To boot a server via PXE, you must:

1 Tell the system BIOS to boot via the network card before the hard drive or other boot media, if needed.

2 Tell the network card to try to PXE boot, if needed.

Some BIOSes have special PXE boot keys, such as `F12`. If you press this when prompted during normal bootup, the BIOS will automatically attempt to PXE boot. Other BIOSes treat network booting like a normal boot device, so you must be sure it is high enough up in the boot order. Some BIOSes use odd names for PXE booting in the boot order; if you see a boot option but don't know what it is, it might be PXE booting.

If all goes well, your system will contact the TFTP server and boot to a Microlite splash screen, as it does for other boot media types, such as CDROM or DVD.

From this point, just press [`Enter`] to boot to the *RecoverEDGE* main menu, and proceed as described in the User's Guide. Note that *RecoverEDGE* will offer to initialize the network stack after PXE booting.

44 - Index

S

W

X