IBM Rescue and Recovery Deployment Guide
Version 2.0

Updated: October 22, 2004

Third Edition (October 2004)

Preface

Note: This version of this Guide is intended to provide a preliminary review of the features and commands of IBM Rescue and Recovery Version 2.0. A follow-on version will be posted in the future.
This guide is intended for IT administrators, or those who are responsible for deploying the IBM® Rescue and Recovery program to computers throughout their organizations. Rescue and Recovery is an essential tool that enables users and administrators to restore backups, access files, diagnose problems, and make Ethernet connections in case the Microsoft® Windows® operating will not open or run correctly. This guide provides the information required for installing the Rescue and Recovery application on one or many computers, provided that licenses for the software are available for each target computer.

Rescue and Recovery provides function and application helps. For questions and information about using the various components included in the Rescue and Recovery workspace refer to the helps for the components.

This guide is organized in the following way:

Chapter 1, “IBM Rescue and Recovery Overview,” on page 1 introduces the components of and installation requirements for Rescue and Recovery.

Chapter 2, “Preparing to install IBM Rescue and Recovery,” on page 7 describes pre-installation considerations, including IBM computer configurations.

Chapter 3, “Installing IBM Rescue and Recovery,” on page 15 details the procedures for installing Rescue and Recovery.

Chapter 4, “Customizing the IBM Rescue and Recovery installation,” on page 19 describes how to customize the installation of Rescue and Recovery.

Chapter 5, “Customizing the Windows Environment for Rescue and Recovery,” on page 23 describes how to customize the Windows environment for Rescue and Recovery.

Chapter 6, “Customizing the Pre Desktop Environment of Rescue and Recovery,” on page 27 describes how to customize the Rescue and Recovery component.

Chapter 8, “Best Practices,” on page 45 discusses a usage scenario for best practices in deploying Rescue and Recovery.

Chapter 9, “Issues, conflicts, and limitations,” on page 55 describes issues, conflicts, and limitations of Rescue and Recovery.

IBM deployment guides are developed with IT professionals and the unique challenges that they encounter in mind. If you have suggestions or comments, communicate with your IBM authorized representative. We will periodically update these guides, so check this Web site for later versions:
`www.pc.ibm.com/us/think/thinkvantagetech/rapidrestore.html`

Contents

Preface iii

Chapter 1. IBM Rescue and Recovery Overview 1
Major components of Rescue and Recovery 1
The Rescue and Recovery Pre Desktop environment 1
IBM Rescue and Recovery Windows environment 2
| Password Persistence 3
Installation requirements 3
Requirements for IBM computers 3
Requirements for installing and use on non-IBM computers 4

Chapter 2. Preparing to install IBM Rescue and Recovery. 7
Application interfaces 7
Rescue and Recovery for the Windows environment 7
Rescue and Recovery 7
| Considerations for over-install 12
| Password Persistence 13
Preparing computers with Rapid Restore Ultra versions 3.x and Rapid Restore PC 2.x 13
Uninstalling Rapid Restore Ultra versions 3.x and Rapid Restore PC 2.x 13
Saving backups to a network 14
Setting up user accounts for network backups. . . 14

Chapter 3. Installing IBM Rescue and Recovery. 15
Installing IBM Rescue and Recovery on a single computer 15
Installing IBM Rescue and Recovery on multiple computers. 15
Various methods for installing on single or multiple computers. 16
Installing the application silently 16
Simple install without taking a base backup . . 16
Performing an administrative install 16
Including IBM Rescue and Recovery in a disk image 17
Using PowerQuest Drive Image based tools . . 17
Using Symantec Ghost based tools 18

Chapter 4. Customizing the IBM Rescue and Recovery installation . . . 19
Producing a simple deployment with a "Create base backup" icon on the desktop. 19
| Capturing a Sysprep image in the base backup . . 20
| Capturing multiple partitions in a Sysprep backup 20

Chapter 5. Customizing the Windows Environment for Rescue and Recovery. 23
Including and excluding files in backups 23
| IBMFILTER.TXT 23
Customizing other aspects of IBM Rescue and Recovery 24
Disabling password synchronization 25
| Trouble Ticket 25
| OSFILTER.txt 25

Chapter 6. Customizing the Pre Desktop Environment of Rescue and Recovery. 27
Using IBMRRUTIL.EXE 27
Example: PEACCESSIBMXX.INI 28
Example: Adding device drivers to the Rescue and Recovery area 29
Customizing the Preboot environment 29
Changing the main GUI font 29
Changing the environment background 30
Changing entries and functions in the left panel 30
Changing entries and functions in the right panel 33
| Configuring the Opera browser. 34
| E-mail 35
| Disabling the address bar. 35
| Customizing bookmarks 35
| Changing proxy settings 36
| Enabling or specifying the full download path. . 37
| Adding a specific file extension to the downloadable files list. 37
| Changing the behavior of files with specific extensions 38
| Adding a Static IP Address 39
Changing the video resolution 40

| Chapter 7. Antidote Delivery Manager Infrastructure 41
| Repository. 41
| Antidote Delivery Manager Commands and Available Windows Commands. 42
| Typical Antidote Delivery Manager Utilization . . 43
| Major Worm Attack. 43
| Minor Application Update 44
| Accommodating VPN's and Wireless Security . . . 44

Chapter 8. Best Practices. 45
Installing IBM Rescue and Recovery in a new roll-out on IBM computers 45
Preparing the hard disk drive 45
Installation 47
Customization 47
| Password considerations 48
Updating 49
Enabling the Rescue and Recovery desktop. . . . 49

Installation of IBM Rescue and Recovery on non-IBM computers 51
Best practices for hard drive setup: Scenario 1 . . 51
Best practices for hard drive setup: Scenario 2 . . 52
Installing IBM Rescue and Recovery into a type 12 service partition 53

Chapter 9. Issues, conflicts, and limitations 55
Changing the system board 55
Backing up encrypted files 55
Limitations 55
Compatibility with previous versions 55
Drives and drive letters 56
DVD-RAM disks and IBM and recovery 56
IBM Rescue and Recovery installed on non-primary hard disk 56
Large backup files and "Not responding" messages 56
Pointing device functions 56
Restoring while the IBM Rescue and Recovery help system is open 56
Screen flashes when IBM Rescue and Recovery opens 56
USB memory key and startup 56
Wireless and dial-up connectivity 56
USB memory key inserted during installation . . 57
Video RAM and performance 57

Appendix A. Installation command-line switches 59
Administrative installation procedure and command-line parameters 59

Appendix B. TVT.TXT settings and values 63
TVT.txt Backup and Restore 70
Scheduling backups and associated tasks 70
Managing Different TVT.txt files 71
Mapping a network drive for backups 71
Setting up user accounts for network backups . . 72

Appendix C. Command line tools for IBM Rescue and Recovery 73
Rescue and Recovery Boot Manager control (BMGR32) 73
RRUCMD 74

Appendix D. User Tasks 79
Windows XP 79
Windows 2000 79

Appendix E. Antidote Delivery Manager Command Reference and Examples . . 81
Antidote Delivery Manager Command Guide . . . 81
Supported Microsoft Commands 84
Installation and Preparation 85
Preparation 85
Configuration 85
Repository 85
Schedule Information 85
Signing Key 85
Network Drives 86
Installation on Clients 86
Server Infrastructure 86
Simple System Test – Display Notification 86
Script Preparation and Packaging 86
Major Worm Attack. 86
Go.RRS 86
NETTEST.CMD 88
PAYLOAD.TXT 88

Appendix F. Notices 89
Non-IBM Web sites 89
Trademarks 90

Chapter 1. IBM Rescue and Recovery Overview

Rescue and Recovery represents a unique combination of IBM ThinkVantage™ Technologies. This integrated application provides a suite of powerful tools that can be used even if the Microsoft Windows operating system will not start.

In the corporate environment, these technologies can directly and indirectly help IT professionals. All the ThinkVantage Technologies will benefit IT professionals because they help make IBM personal computers easier to use and more self-sufficient. IBM provides powerful tools that facilitate and simplify rollouts at the outset. On a continuing basis, ThinkVantage Technologies help IT professionals spend less time solving individual computer problems and more time on their core tasks.

Major components of Rescue and Recovery

Rescue and Recovery has these major components:

- IBM Rescue and Recovery Pre Desktop environment starts even if the Windows operating system will not boot.
- IBM Rescue and Recovery Windows environment allows for backing up, file rescue, and recovery of the operating system and files.

Note: Some features of Rescue and Recovery run under the Windows operating system. In some instances system information used in the Rescue and Recovery environment are gathered while Windows is running. If the Windows operating system malfunctions, that malfunction alone will not prevent the Rescue and Recovery environment from operating normally. The functions that run under the Windows operating system, however, are not configurable, therefore these functions are not addressed in this deployment guide.

The Rescue and Recovery Pre Desktop environment

The Rescue and Recovery environment provides an emergency workspace for end users who are unable to start Windows on their computers. Running under Windows PE (Preinstallation Environment), the environment offers the Windows look, feel, and function, and helps end users solve problems without consuming IT staff time.

The Rescue and Recovery environment has four major categories of functions:

- **Rescue and Restore**
  - **Recovery overview:** links users to help topics about the various recovery options that IBM provides.
  - **Rescue files:** end users can copy files created in Windows applications to removable media or to a network, and can continue to work even with a disabled workstation.
  - **Restore from backup:** end users can restore files that have been backed up with Rescue and Recovery.
  - **Restore factory contents:** provides a way to erase the hard disk and reinstall the software that IBM preinstalled on the computer.
- **Configure**
  - **Configuration overview:** links to Rescue and Recovery environment help topics that cover configuration.

  - **Set recovery password:** an end user or administrator can password protect the Rescue and Recovery environment.
  - **Access BIOS:** opens the IBM BIOS Setup Utility program.
- **Communicate**
  - **Communication overview:** links to related help topics in the Rescue and Recovery environment.
  - **Open browser:** starts the Opera Web browser (Web or Intranet access requires a wired Ethernet connection).
  - **Download files**
  - **Map network drive:** helps end users access network drives for software downloads or file transfer.
- **Troubleshoot**
  - **Diagnostic overview:** links to Rescue and Recovery diagnostics help topics.
  - **Diagnose hardware:** opens the PC Doctor application that can perform hardware tests and report results.
  - **Create diagnostic disks**
  - **Boot from another device**
  - **System information:** provides details regarding the computer and its hardware components.
  - **Activity and asset log viewer:** details recent user activity and computer hardware to aid in problem determination and resolution. The log viewer provides a readable way to view activity and asset log entries.
  - **Warranty status**

Rescue and Recovery is available on IBM personal computers that come with IBM preinstalled software. It is also available for purchase as a download so that organizations can benefit from Rescue and Recovery on non-IBM computers as well.

Chapter 2, "Preparing to install IBM Rescue and Recovery," on page 7 addresses configuring the Rescue and Recovery environment for deployment. Although installing Rescue and Recovery includes the installation of Rapid Restore Ultra, this guide treats them as individual components in discussions of customization, configuration, and deployment.

IBM Rescue and Recovery Windows environment

The IBM Rapid Restore environment enables end users to rescue lost data, applications and operating systems with the touch of a button. This capability reduces time-consuming help desk calls, which result in support cost savings.

You can schedule backups of all end users' computers, thereby limiting risk and downtime. IBM Rescue and Recovery offers your clients an extra layer of support by pre-configuring automatic external backup to a server or external storage.

"Installing IBM Rescue and Recovery on a single computer" on page 15 covers configuring IBM Rescue and Recovery features for deployment.

Password Persistence

The following table shows considerations for deciding whether to use Password Persistence

Table 1. Password Persistence considerations

Issue	Impact if Password Persistence is enabled
If a user logs in to and old backup with the current account and password, then none of the Encrypted File system files and folders will work because those files were encrypted against the original account and and password, not the persistend account and password.	• User will lose Encrypted File System data • You cannot use Encrypted File System and Password Persistence together.
If the user didn't exist on that particular backup, then they don't have any of their User Folders or files. All Internet Explorer Favorites and Application data will not exist.	• The User ID Documents Settings are gone • Potential data loss
Deleting user in the current accounts and passwords will remove their authentication information from all the backups.	• User will not have access to data
If a manager or a network administrator let go of several employees and wanted to restore to the base backup to reset the system to remove all of the employees authentication accounts, the employees would still have access with Password Persistence.	• Is against the recommendation of Microsoft User ID maintenance practices and recommendations. •

Installation requirements

This section addresses system requirements for installing Rescue and Recovery. For best results, go to the following IBM Web site to make sure that you have the latest version of the software:

`www-307.ibm.com/pc/support/site.wss/MIGR-4Q2QAK.html`

A number of legacy computers from IBM can support Rescue and Recovery, provided that they meet the requirements specified. Refer to the download page on the Web for information about IBM computers that support Rescue and Recovery.

Requirements for IBM computers

IBM computers must meet or exceed the following requirements to run Rescue and Recovery:

- Operating System: Microsoft Windows XP or Windows 2000
- Processor: As specified by Microsoft for Windows XP (Home or Professional) and Windows 2000
- Memory: 128 MB
  - In shared memory configurations, the BIOS setting for maximum shared memory must set to no less than 4 MB and no greater than 8 MB.
  - In non-shared memory configurations, 120 MB of non-shared memory.

  Note: If a computer has less that 200 MB of non-shared memory, Rescue and Recovery will run. However, the user might be unable to start more than one application in the Rescue and Recovery environment.

- 1.5 GB of free hard disk space (the base installation requires 930 MB and does not include space required for Rapid Restore Ultra backups)
- VGA-compatible video that supports a resolution of 800 x 600 and 24-bit color
- Supported Ethernet card

Requirements for installing and use on non-IBM computers

Installation on non-IBM computers has the following requirement:

Installation requirements

1.5 GB of free hard disk space. The base install uses 930 MB.

Minimum system memory requirements

The non-IBM computer must have 128 MB system RAM to install Rescue and Recovery.

Hard disk drive configuration

The Rescue and Recovery program is not supported on the ″factory preloads″ for original equipment manufacturer (OEM) computers (non-IBM). For OEM computers, the hard disk drive must be configured according to recommendations in “Installation of IBM Rescue and Recovery on non-IBM computers” on page 51.

Network adapters

The Rescue and Recovery environment supports only wired PCI-based, Ethernet network adapters. Network device drivers included in the Rescue and Recovery environment are the same drivers that are pre-populated in Microsoft Windows XP Professional operating system and are independent of the Windows operating system. For supported IBM computers, required drivers are included with Rescue and Recovery software.

If an OEM network device in your computer is not supported, refer to the documentation that came with the device for instructions to add support for system-specific network drivers. Request drivers from your OEM.

Support for booting from external media (CD/DVD and USB)

Non-IBM computer and devices (USB hard disk drive, CD-R/RW, DVD-R/RW/RAM, or DVD+R/RW) must fully support one or more of the following specifications:

- ATAPI Removable Media Device BIOS Specification
- BIOS Enhanced Disk Drive Services - 2
- Compaq Phoenix Intel BIOS Boot Specification
- El Torito Bootable CD-ROM Format Specification
- USB Mass Storage Class Specification Overview. (Each device must comply with the command block specification in the section 2.0 Subclass code in the ″USB Mass Storage Class Specification Overview.″)
- USB Mass Storage Specification for Bootability

Video requirements

- **Video compatibility:** VGA-compatible video that supports a resolution of 800 x 600 and 24-bit color
- **Video memory:**
  - On non-shared video memory systems: a minimum 4 MB of video RAM
  - On shared video memory systems: a minimum of 4MB and maximum of 8 MB can be allocated for video memory.

Application compatibility

Some applications that have complex filter driver environments (such as anti-virus software) might not be compatible with Rescue and Recovery software. For information regarding compatibility issues, refer to the ″README″ file that accompanies Rescue and Recovery software on the Web:

`http://www.ibm.com/thinkvantage`

Utilities

This guide refers to a number of utilities. These utilities can be found on the IBM Web site. Look for the links on the page that this document is placed.

Chapter 2. Preparing to install IBM Rescue and Recovery

Prior to installing Rescue and Recovery, you should understand the architecture of the entire application.

Application interfaces

Rescue and Recovery has two main interfaces. The primary interface operates in the Windows environment. The secondary interface (the Rescue and Recovery Pred Desktop environment) operates independently of the Windows operating system.

Rescue and Recovery for the Windows environment

Rescue and Recovery installs into the C:\PROGRAM FILES\IBM\IBM RAPID RESTORE ULTRA directory. The backups for IBM Rapid Restore Ultra 4.0 can be stored in multiple locations, which will be discussed later. In this document, unless otherwise noted, the location of the backups will be assumed to be in the primary location: C:\RRUBACKUPS. This directory, when placed on a local partition on the primary hard disk drive, will be protected by a filter driver that is installed as part of the Rescue and Recovery installation.

In addition to the main Rescue and Recovery application, several other supporting applets are installed on the C drive of the local client computer. You must install each applet in its correct location to ensure proper communication between the Windows operating system and the Rescue and Recovery environment. The paths for these applets are:

\IBMSHARE: used as a shared folder between the Windows operating system and the Rescue and Recovery environment.

\IBMTOOLS\UTILS: stores several applets for applications that must run in both the Windows and Rescue and Recovery environments.

\IBMTOOLS\PYTHON22: stores the Python code that is required for several Rescue and Recovery functions to work.

\IBMTOOLS\EGATHERER: holds the eGatherer code that collects system information for both the Windows and Rescue and Recovery environment.

Rescue and Recovery

Because there are several scenarios to configure hard disk drives, Rescue and Recovery must install a custom Master Boot Record (MBR). When the end user or Administrator presses the Access IBM or F11 key, the MBR launches a boot of the appropriate partition.

Default installation

If you are installing Rescue and Recovery onto a hard disk that does not have an IBM_SERVICE partition or PARTIES area, Rescue and Recovery will be installed according to the following software defaults.

- **Location:** a virtual partition that must be installed on the C drive (primary partition of the master hard disk drive) of the computer.

- **Directory structure:** Two directories (\MININT and \PREBOOT), which are protected by the same filter driver that protects the backup location \RRUBACKUPS.

See the following figure:

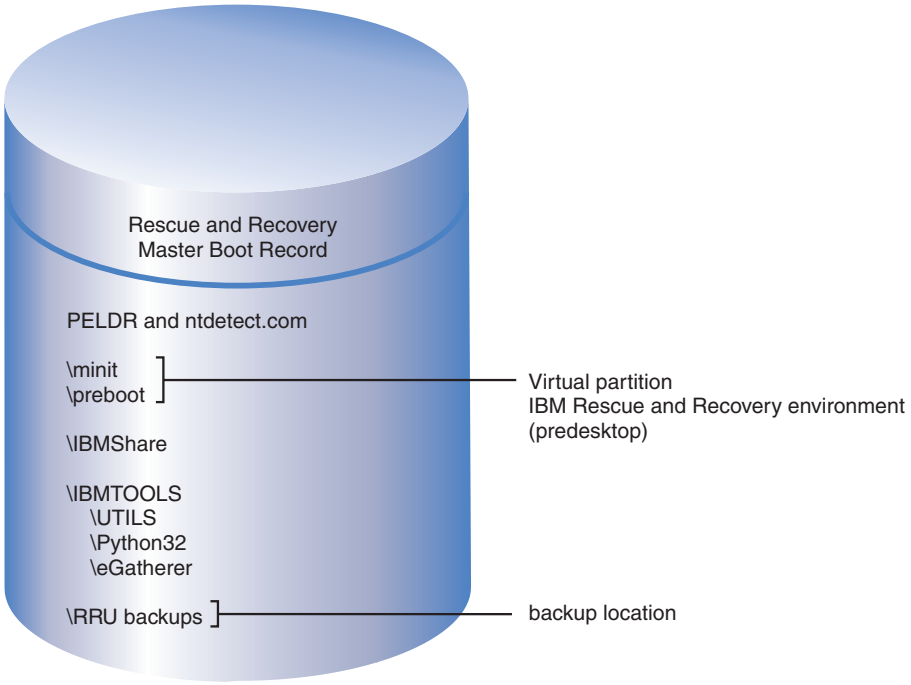

Figure 1. Default installation

Installation on IBM computers with a type 1C IBM_SERVICE partition

These IBM computers were announced prior to January 2003 or computers that have an ImageUltra™ Builder disk image.

- **Location:** a virtual partition that must be installed on the C drive (primary partition of the master hard disk drive) of the computer.
- **Partition link:** links to the IBM_SERVICE partition to restore the factory contents or the ImageUltra Builder disk image.

See the following figure:

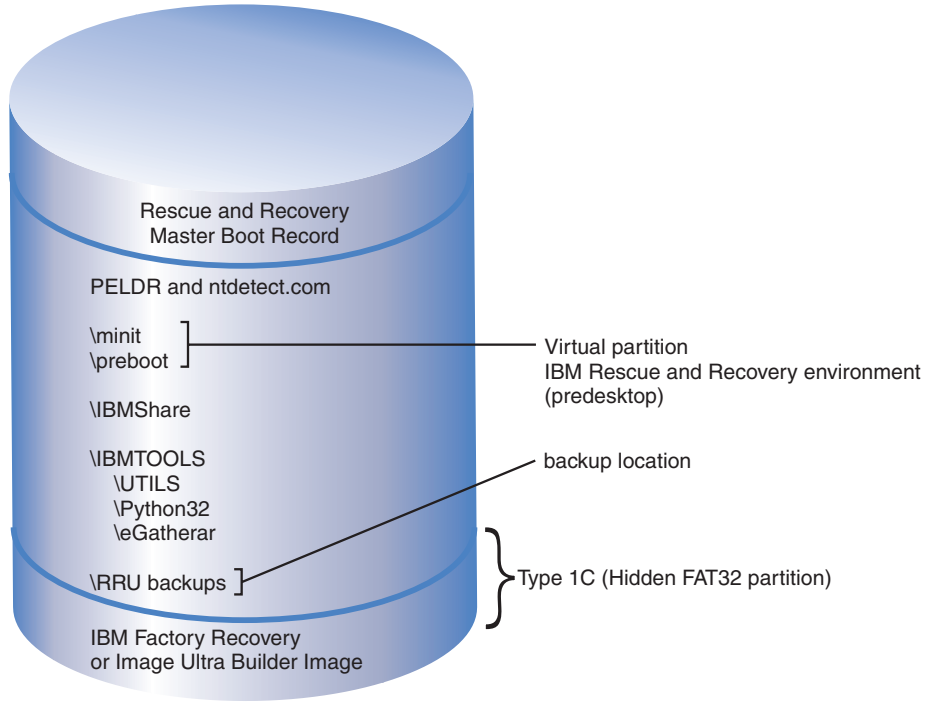

Figure 2. Installation for computers with an IBM service partition

Installation on IBM computers with a PARTIES area

IBM computers that have a PARTIES area were announced during 2003.

- **Location:** a virtual partition that must be installed on the C drive (primary partition of the master hard disk drive) of the computer.
- **Partition link:** links to the PARTIES partition to initiate a restore of factory contents or diagnostics.

See the following figure:

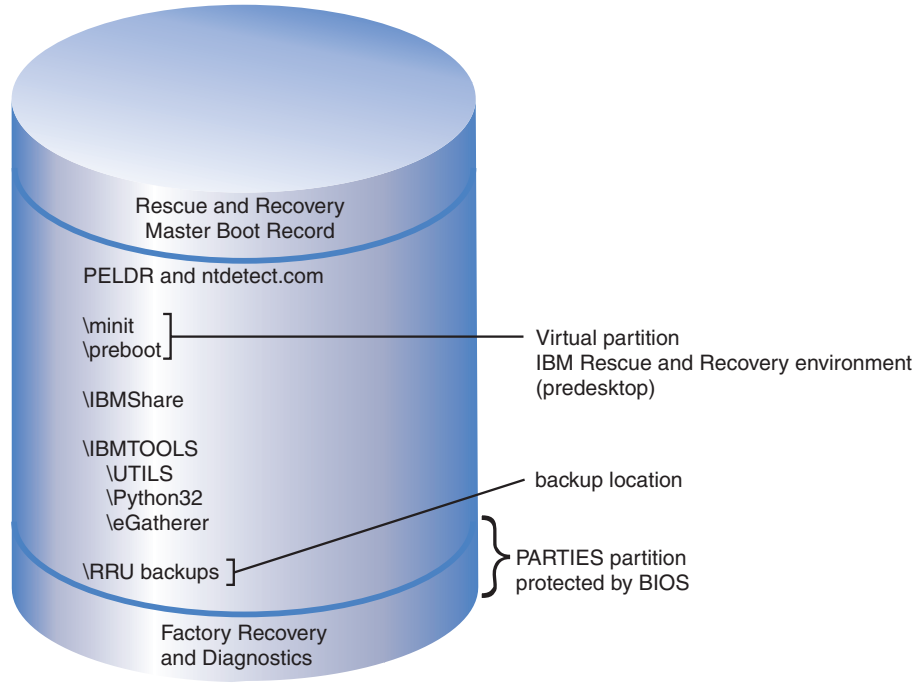

Figure 3. Installation on computers with a PARTIES area

Installation on IBM computers with a PARTIES Area and a type 1C service partition

IBM computers with this configuration were announced during 2003 and also have an ImageUltra disk image in the IBM_SERVICE partition.

- **Location:** a virtual partition that must be installed on the C drive (primary partition of the master hard disk drive) of the computer.
- **Partition link:** links to the PARTIES partition to initiate a restore of factory contents or diagnostics.

See the following figure:

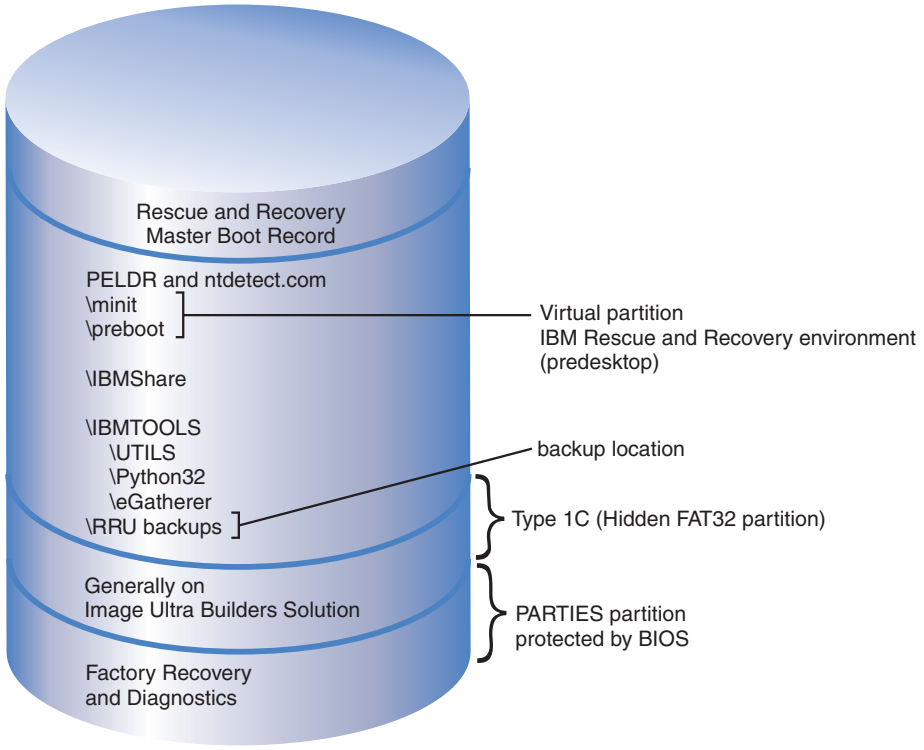

Figure 4. Installation on IBM computers with a PARTIES Area and a type 1C service partition

Installation on IBM computers with the Rescue and Recovery application preinstalled in a type 12 partition

IBM computers that are announced in the first quarter 2004 and come with the Rescue and Recovery environment preinstalled will feature this configuration. See the following figure.

- **Location:** 100% in a type 12 partition.
- **Location of factory recovery and system diagnostics:** entirely in a type 12 partition.
- **Location of backups:** NOT in the type 12 partition.
- **Partition link:** Links to the PARTIES partition to initiate a restore of factory contents or diagnostics.
- **Advantage of a type 12 partition:** When the Rescue and Recovery environment is placed in a virtual partition, several files are placed in the root of the C drive where an end user could possibly delete them. The filter driver does not protect these files because some are common with Windows boot files (for example, NTDETECT.COM). If they are deleted or otherwise become unusable, the end user would be unable to boot to the Rescue and Recovery environment. However, when the Rescue and Recovery environment is placed in a type 12 partition, Windows will prevent all users from accessing that partition and the files required to open the Rescue and Recovery environment are highly protected.

  Note: With the Rescue and Recovery environment secured in the type 12 partition, only a corrupted MBR would prevent access to the Rescue and Recovery. In that case, an external version of the Rescue and Recovery environment must be used. Currently IBM supports CD and USB hard disk

drive-based versions of the Rescue and Recovery environment that are created with the Create Rescue Media applet in the Access IBM folder of the Start Menu.

This guide discusses installation of the Rescue and Recovery environment into a type 12 partition. Please note that the recovery and diagnostics will be available only on IBM computers with the standard IBM factory preinstalled software and disk image.

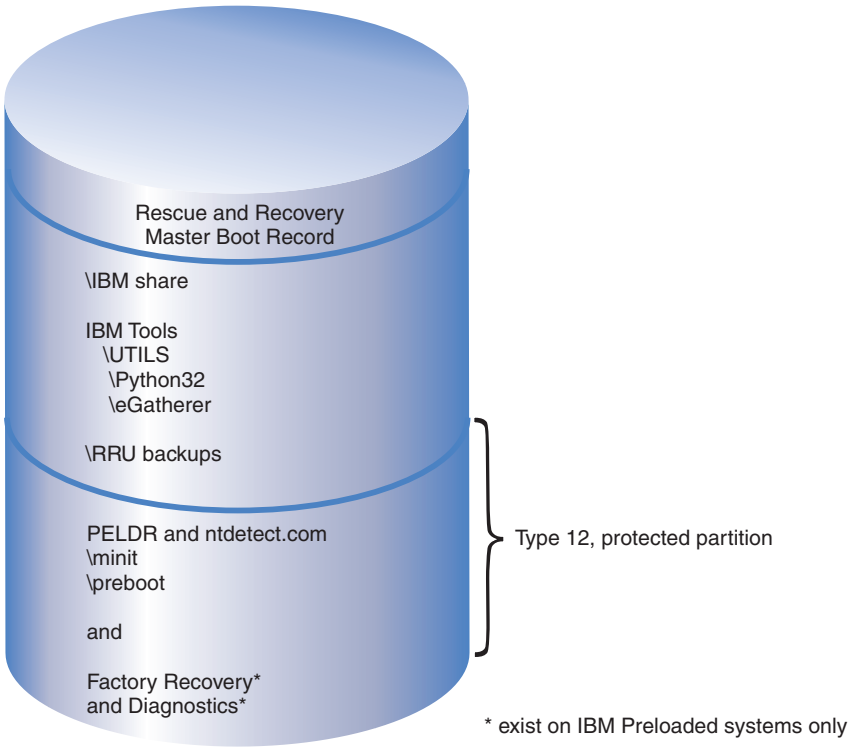

Figure 5. IBM computers with the Rescue and Recovery application preinstalled in a type 12 partition

Considerations for over-install

IBM Rescue and Recovery Version 2.0 supports an over-install operation of Rescue and Recovery 1.0.

It is recommended that a new backup be taken after installation of Rescue and Recovery 2.0. This can be done by using either a script or the user interface.

These are the basic steps you follow you get a clean backup set:

1. Copy Previous Backups to a CD/DVD drive or a USB HDD drive (if desired)
2. Delete current backups
3. Perform a base backup

The following Script will Copy Backups to a USB HDD, Delete the Current Backups Then perform a base backup.

```
@echo off

:Change directories to \Program Files\IBM\IBM Rapid Restore Ultra
cd %rru%
```

```
:copy backups to the USB drive
rrucmd copy location=U

:Delete All backups from local HDD silently
rrucmd delete location=L level=0 silent

:Perform a New Base Backup to local HDD silently
rrucmd backup location=L name="Rescue and Recovery 2.0 Base" silent
```

Password Persistence

The following table shows considerations for deciding whether to use Password Persistence

Table 2. Password Persistence considerations

Issue	Impact if Password Persistence is enabled
If a user logs in to and old backup with the current account and password, then none of the Encrypted File system files and folders will work because those files were encrypted against the original account and password, not the persistent account and password.	• User will lose Encrypted File System data • You cannot use Encrypted File System and Password Persistence together.
If the user didn't exist on that particular backup, then they don't have any of their User Folders or files. All Internet Explorer Favorites and Application data will not exist.	• The User ID Documents Settings are gone • Potential data loss
Deleting user in the current accounts and passwords will remove their authentication information from all the backups.	• User will not have access to data
If a manager or a network administrator let go of several employees and wanted to restore to the base backup to reset the system to remove all of the employees authentication accounts, the employees would still have access with Password Persistence.	• Is against the recommendation of Microsoft User ID maintenance practices and recommendations. •

Preparing computers with Rapid Restore Ultra versions 3.x and Rapid Restore PC 2.x

Before installing Rescue and Recovery, you must first uninstall earlier versions of the software.

Uninstalling Rapid Restore Ultra versions 3.x and Rapid Restore PC 2.x

You must uninstall all previous Rapid Restore applications. If an older version of Rapid Restore is detected during the Install, you will be prompted to uninstall the older application.

To uninstall earlier versions of Rapid Restore do the following:

1. Click **Start→Settings→Control Panel**.
2. Double-click **Add/Remove Programs**.
3. Select **IBM Rapid Restore PC** or **IBM Rapid Restore Ultra**, and then click **Change/Remove**.

4. Follow the on-screen instructions to complete the software removal. If IBM Rapid Restore Ultra is not in this list of programs, continue to step 5.
5. In the Add/Remove Programs applet, select **Access IBM**. This will open an Access IBM uninstall program that lists multiple IBM applications. If IBM Rapid Restore Ultra is not in this list of programs, continue to step 6.
6. Run the following command from a command prompt:

   ```
   c:\program files\xpoint\rmvmpc.exe
   ```

Saving backups to a network

If you have decided to have backups saved to a network drive (see Appendix B, "TVT.TXT settings and values," on page 63 for settings and values information), it is important to note the following: When a backup is performed, Rescue and Recovery creates a hidden directory called "RRUBACKUPS" to store the backup files in. If the destination for the backup is a common network share (for example, \\Servername\SharedFolder), you must create and share separate directories for each client computer, NOT EACH USER. The following illustrates a sample directory tree on the server.

Figure 6. Sample directory tree on a shared network resource set up to receive Rescue and Recovery backups

In Figure 6, when Network is chosen as the backup location, \\SERVERNAME\MACHINE1 would be the UNC for Machine1. The UNC for Machine2 would be \\SERVERNAME\MACHINE2.

Setting up user accounts for network backups

When the Rescue and Recovery backups directory is created on the network share, the service makes it a *read only* folder, and assigns it access rights so that only the user account that created the folder has full control over the folder. In order to complete a merge operation at the end of the incremental backups, MOVE permissions must exist for the user account. If logged in with an account other than the account that created the folder initially (i.e., administrator) the merge process will fail.

Chapter 3. Installing IBM Rescue and Recovery

This chapter discusses less complex installations of Rescue and Recovery. This will establish a foundation for complex rollouts and deployments discussed in Chapter 4, "Customizing the IBM Rescue and Recovery installation," on page 19 and Chapter 5, "Customizing the Windows Environment for Rescue and Recovery," on page 23.

Three methods of installing Rescue and Recovery exist, two of which are discussed in this chapter.
- Single-computer installation
- Multiple-computer installation

The third method, remote installation with application and installation customization, is discussed in Chapter 4, "Customizing the IBM Rescue and Recovery installation," on page 19.

You have various installation options, all of which can be employed for installation on a single computer or on multiple computers.

Finally, this chapter discusses using PowerQuest or Ghost tools for creating a disk image.

Installing IBM Rescue and Recovery on a single computer

To install on a single computer, complete the following procedure:
1. Obtain the latest version of code from the following Web site:

   `http://www.ibm.com/thinkvantage`
2. Install the Rescue and Recovery program by either of the following methods:
   - Follow the instructions on the IBM Web download page OR
   - Start the installation from a command prompt by typing the following:

     `<Source Directory> \setup_ibmrr`*`XXXX`*`.exe`

     (where *XXXX* is the build ID).

See "Various methods for installing on single or multiple computers" on page 16 to install the application silently, perform a simple install without taking a base backup, or perform an administrative install.

Installing IBM Rescue and Recovery on multiple computers

If you plan to install IBM Rescue and Recovery on multiple computers AND if you plan to customize the settings for IBM Rescue and Recovery before installation, extract the MSI-based installation code from the SETUP_IBMRR*XXXX*.EXE (where *XXXX* is the build ID) file that you downloaded. Because the Web executable file extracts itself to a temporary directory during the first stage of installation, performing this step once and then avoiding it during subsequent installations will greatly improve the install time on each computer.

See the following section to install the application silently, perform a simple install without taking a base backup, or perform an administrative install.

Various methods for installing on single or multiple computers

Installing the application silently

You have two choices for this type of installation.

- **With reboot:** Prepare a command file that silently installs Rescue and Recovery followed by a reboot:

  ```
  start /WAIT setup_ibmrrXXXX.exe /s v/qn
  ```

  (where *XXXX* is the build ID).
- **Reboot suppressed:** Prepare a command file that silently installs Rescue and Recovery, but suppresses the reboot after installation:

  ```
  :: Perform a silent install with no reboot
  Start /Wait setup_ibmrrXXXX.exe /s /v"/qn REBOOT="R""
  ```

  (where *XXXX* is the build ID).

Note: For an enterprise rollout, the required reboot at the end may be undesirable for various reasons, including interruption of a scripted process or batched installation of multiple applications. You can configure Rescue and Recovery not to reboot at the end of the installation phase, or you can script it to perform a base backup without rebooting. However, you should be aware that data backed up before the reboot will not be protected from corruption until the reboot is performed.

Simple install without taking a base backup

To install Rescue and Recovery without taking a base backup, do the following:

1. Install and configure Windows and your application suite.
2. Install Rescue and Recovery by typing `setup_ibmrrXXXX.exe` (where *XXXX* is the build ID) from a command prompt and then follow the on-screen instructions to complete the install.
   - If you desire, customize your TVT.TXT file as described in Appendix B, "TVT.TXT settings and values," on page 63.
3. Prepare the image by using Sysprep, and then shut down Windows.
4. Create an image of the entire hard disk, as described in "Using PowerQuest Drive Image based tools" on page 17 or "Using Symantec Ghost based tools" on page 18, depending on your image-creation process.

After the master image is deployed to client computers, the end user will complete the first-use procedures of Windows inserted with Sysprep, configure the basic Windows settings, and perform a backup.

Performing an administrative install

The Microsoft® Windows® Installer can perform an administrative installation of an application or product to a network for use by a workgroup or for customization. For the Rescue and Recovery installation package, an administrative installation unpacks the installation source files to a specified location. To run an administrative installation, you need to execute the setup package from the command line using the `/a` parameter.

Launching an administrative installation presents a wizard that prompts the administrative user to specify the location to unpack the setup files. The default extract location is C:\IBMRNR. You can choose other locations, including drives other local drives, mapped network drives, or new directories.

To perform the administrative install, use either the SETUP.EXE or the MSIEXE method:

- **Install Rescue and Recovery using SETUP.EXE :** Specify the target directory directory for an administrative install and extract the setup files to that directory by typing the following command:

  ```
  :: Extract the WWW EXE to the directory C:\IBMRR
  start /WAIT setup_ibmrrXXXX.exe /a /s /v"/qn TARGETDIR="C:\IBMRR"" /w
  ```

  (where *XXXX* is the build ID)
- **Install Rescue and Recovery using MSIEXE:**
  1. For all MSIs, add the following install-log generation code:

     ```
     /L*v %temp%\rrinstall.txt
     ```
  2. To install the setup files using MSIEXE, type the following command:

     ```
     :: Perform the install of Rescue and Recovery
     msiexec /i "C:\IBMRR\IBM Rescue and Recovery with Rapid Restore.msi"
     ```
  3. To silently install the setup files using MSIEXE:
     - **With reboot** at the end, type the following command:

       ```
       :: Silent install using the MSI with a reboot
       start /WAIT msiexec /i "C:\IBMRR\IBM Rescue and Recovery
       with Rapid Restore.msi" /qn
       ```
     - **Reboot suppressed**, type the following command:

       ```
       :: Silent install using the MSI without a reboot
       start /WAIT msiexec /i "C:\IBMRR\IBM Rescue and Recovery
       with Rapid Restore.msi" /qn REBOOT="R"
       ```

  To uninstall silently with MSIEXE, type the following at a command prompt:

  ```
  msiexec /x "C:\IBMRR\IBM Rescue and Recovery with Rapid Restore.msi" /qn
  ```

For more detailed information about the Windows Installer, see Appendix A, “Installation command-line switches,” on page 59.

Including IBM Rescue and Recovery in a disk image

You can use your tool of choice to create a disk image that includes Rescue and Recovery. This deployment guide provides basic information regarding PowerQuest and Ghost as it applies to this application and installation. It is assumed that you have expertise in your image creation tool and that you will include other options that you require for your applications.

Note: If you plan to create an image, you must capture the Master Boot Record. The Master Boot Record is critical for the Rescue and Recovery environment to function correctly.

Using PowerQuest Drive Image based tools

Assuming that the PowerQuest DeployCenter tool PQIMGCTR is installed in the following location (X:\PQ), you can create and deploy an image with Rescue and Recovery with the following scripts:

Minimum script files

Table 3. X:\PQ\RRUSAVE.TXT

Script language	Result
`SELECT DRIVE 1`	Select first hard disk drive

Table 3. X:\PQ\RRUSAVE.TXT (continued)

Script language	Result
SELECT PARTITION ALL (Needed if you have a type 12 partition or if you have multiple partitions in your image.)	Select all partitions
Store with compression high	Stores the image

Table 4. X:\PQ\RRDEPLY.TXT

Script language	Result
SELECT DRIVE 1	Select first hard disk drive
DELETE ALL	Delete all partitions
SELECT FREESPACE FIRST	Select first free space
SELECT IMAGE ALL	Select all partitions in image
RESTORE	Restore image

Image creation

Table 5. X:\PQ\PQIMGCTR / CMD=X:\PQ\RRUSAVE.TXT /MBI=1 / IMG=X:\IMAGE.PQI

Script language	Result
SELECT DRIVE 1	Select first hard disk drive
X:\PQ\PQIMGCTR	Image program
/CMD=X:\PQ\RRUSAVE.TXT	PowerQuest script file
/MBI=1	Capture the Rescue and Recovery Boot Manager
/IMG=X:\IMAGE.PQI	Image file

Image deployment

Table 6. X:\PQ\PQIMGCTR / CMD=X:\PQ\RRDEPLY.TXT /MBI=1 / IMG=X:\IMAGE.PQI

Script language	Result
SELECT DRIVE 1	Select first hard disk drive
X:\PQ\PQIMGCTR	Image program
/CMD=X:\PQ\RRDEPLY.TXT	PowerQuest script file
/MBR=1	Restore the Rescue and Recovery Boot Manager
/IMG=X:\IMAGE.PQI	Image file

Using Symantec Ghost based tools

When you create the Ghost image, you must use the command line switch (which might be incorporated into the GHOST.INI file) `-ib` to capture the Rescue and Recovery Boot Manager. Also, the image must capture the whole disk and all partitions. Refer to the documentation provided by Symantec for specific details on Ghost.

Chapter 4. Customizing the IBM Rescue and Recovery installation

This chapter describes more complex installations that:
- create base backup icons on the desktop
- capture a Sysprep image in the base backup

You must follow this basic process when doing a custom installation of Rescue and Recovery:
1. Extract the file SETUP_IBMRR*XXXX*.EXE (where *XXXX* is the build ID) to a MSI based installation package as described in "Performing an administrative install" on page 16.
2. Customize the control file TVT.TXT.
3. Perform the MSI-based installation, deferring the reboot as described in "Performing an administrative install" on page 16.
4. Customize the Rescue and Recovery environment.
   - If the computer you are working on will be a donor system for an image deployment, run Sysprep, and then capture an image of the hard disk.

Note: The base backup in Rescue and Recovery can be restored to a computer independent of any incremental backups. Therefore, IBM does not support deploying an image that includes a non-Sysprep image as the base backup since the identical base image with the same machine name and SID could be restored to multiple computers, creating unnecessary complications in your environment.

Producing a simple deployment with a "Create base backup" icon on the desktop

To perform a simple deployment that places a backup icon on the desktop for the user, do the following:
1. Extract the SETUP_IBMRR*XXXX*.EXE (where *XXXX* is the build ID) to a temp directory:

   ```
   start /WAIT setup.exe /a /s /v"/qn TARGETDIR="C:\IBMRR"" /w
   ```
2. Customize the TVT.TXT file, as required. For example, you might want to schedule a weekly backup at 3:00 pm every Tuesday. Add the following entries in the [Rapid Restore Ultra] section of TVT.TXT to accomplish this. (See Appendix B, "TVT.TXT settings and values," on page 63 for additional setting information.)

   ```
   ScheduleHour=15
   ScheduleMinute=00
   ScheduleDayOfTheWeek=2
   ```
3. Initiate the MSI install deferring the reboot:

   ```
   start /WAIT msiexec /i "C:\IBMRR\IBM Rescue and Recovery with
   Rapid Restore.msi" /qn REBOOT="R" /L*v %temp%\rrinstall.txt
   ```
4. Customize the Rescue and Recovery environment. (See Chapter 6, "Customizing the Pre Desktop Environment of Rescue and Recovery," on page 27 for detailed information.)
5. Delete the temporary files in C:\IBMRR. (Refer to Chapter 5, "Customizing the Windows Environment for Rescue and Recovery," on page 23).
6. Write a command file with the following commands:

   ```
   del "c:\Documents and Settings\All Users\Desktop\Create Base
   ```

```
Backup.lnk
"%RRU%rrucmd.exe" backup location=L name=Base level=0
```

7. Create a shortcut on the All Users Desktop called ″Create base backup.″ (Specify your path under **Type the location** of the item.)
8. Run Sysprep on the system.
9. Create the image for deployment.

After the client user receives the image and personalizes the computer, the user clicks the **Create base backup** icon to start Rescue and Recovery and saves the base backup.

Capturing a Sysprep image in the base backup

To capture a Sysprep image in the base backup, do the following:

1. If backups where made prior to running sysprep, run the following command:
   ```
   RRUCMD delete location=l level=0 silent
   ```
2. Create a batch file using the following commands:
   ```
   @ echo off
   cd %rru%
   rrucmd sysprepbackup location=L name="Sysprep Base Backup"
   ```
3. Peform your specific Sysprep implementation when you see the following message:
   ```
   ************************************************
   ** Ready to take sysprep backup.               **
   ** PLEASE RUN SYSPREP NOW AND SHUT DOWN.       **
   **                                             **
   ** Next time the machine boots, it will boot   **
   ** to the PreDesktop Area and take a backup.   **
   ************************************************
   ```
4. Shut down and reboot when Sysprep is complete.

   Note: The operating system will reboot into the Pre-Desktop area of Rescue and Recovery. You will see a status bar that says `System Restore in Progress`
5. When complete, you will see a message that says`Sysprep Backup is Complete`.
6. Power off the system using the power button.
7. Use IBMRRUTIL.exe to obtain TVT.txt from the \rrubackups directory. For more on how to run IBMRRUTIL, see “Using IBMRRUTIL.EXE” on page 27.
8. Edit your TVT.TXT file to include the *Backup0* as follows:
   ```
   [Backup0]
   BackupVersion=2.0
   ```
9. Put the TVT.txt file to rrubackups using IBMRRUTIL. See “Using IBMRRUTIL.EXE” on page 27 for more information.
10. Capture the image for deployment.

Capturing multiple partitions in a Sysprep backup

To capture multiple partitions in a Sysprep backup, do the following:

1. Before running Sysprep, update the tvt.txt file with the following changes:
   a. Change CustomPartitions to 0 for supporting multiple partitions:
      ```
      CustomPartitions=0
      ```
   b. Update the *BackupPartition* parameter to the backup location:
      ```
      BackupPartition=3
      ```

      Note: In this case, we are backing up the data to Partition 3, E for example. If you do not set the variable, it will default to C:\.
2. Update guiexcld.txt. to prevent backup of a particular partition or file.

Create guiexcld.txt file in the directory C:\Program Files\IBM\IBM Rapid Restore Ultra with following parameters:

```
E:
D:
```

Note: In this case we are not backing up the files on drives E: and D:. If you want to prevent any files from backup, enter the file names in the guiexcld.txt.

3. Use IBMRRUTIL.exe to obtain TVT.txt from the \rrubackups directory. For more on how to run IBMRRUTIL, see "Using IBMRRUTIL.EXE" on page 27.
4. Edit your TVT.TXT file to include the *Backup0* as follows:

```
[Backup0]
BackupVersion=2.0
```

5. Put the TVT.txt file to rrubackups using IBMRRUTIL. See "Using IBMRRUTIL.EXE" on page 27 for more information.

Chapter 5. Customizing the Windows Environment for Rescue and Recovery

You can customize numerous features and aspects of Windows environment, from files included and excluded from backups to scheduling backups.

Including and excluding files in backups

IBM Rescue and Recovery has extensive include and exclude capabilities. It can include and exclude an individual file or folder or an entire partition.

The files that control the include and exclude functions, listed in order of precedence are as follows. All files are located in the directory C:\PROGRAM FILES\IBM\IBM RAPID RESTORE ULTRA.

1. IBMFILTER.TXT
2. GUIEXCLD.TXT

The end user, by default, can select individual files and folders to be excluded from the backup. These files and folders are stored in the file GUIEXCLD.TXT.

If an administrator wants to ensure that a particular file or folder is always backed up, he or she can include the file names or types in the IBMIFILTER.TXT file. Any entry in this file will always be included in a backup regardless of an entry in the GUIEXCLD.TXT.

Administrators also have the ability to always exclude a file, folder, or partition from a backup.

The following are always excluded from any backup:

- PAGEFILE.SYS
- HIBERFILE.SYS
- C:\SYSTEM VOLUME INFORMATION

When restored, both PAGEFILE.SYS and HIBERFILE.SYS will be regenerated automatically by Windows. In addition, the Windows System Restore data will be regenerated with a new restore point by Windows after a backup has been restored.

Note: The format for IBMIFILTER.TXT and GUIEXCLD.TXT uses standard DOS style commands and wildcard such as ″*″ and ″?″.

IBMFILTER.TXT

The file format is:

- One line per include/exclude rule entry.
- If omre than one rule applies to a file or folder, the last rule applies. Entries at the bottom of the file take precedence.
- Entries must start with either:
  - ; for a comment
  - I must include files or folders that match the entry
  - X must include files or folder that match the entry

- i for files or folder that you can choose to include
- x for files or folders that you can choose to exclude

```
I=*.ocx
I=*.dll
I=*.exe
I=*.ini
I=*.drv
I=*.com
I=*.sys
I=*.cpl
I=*.icm
I=*.lnk
I=*.hlp
I=*.cat
I=*.xml
I=*.jre
I=*.cab
I=*.sdb
I=*.bat
I=?:\ntldr
I=?:\peldr
I=?:\bootlog.prv
I=?:\bootlog.txt
I=?:\bootsect.dos
I=?:\WINNT\*
I=?:\WINDOWS\*
X=?:\WINDOWS\prefetch\*
I=?:\minint\*
I=?:\preboot\*
I=?:\Application Data\*
I=?:\Documents and Settings\*
I=?:\IBMTOOLS\*
I=?:\Program Files\*
I=?:\msapps\*
x=?:\Documents and Settings\*\Cookies\*
x=?:\Documents and Settings\*\Local Settings\History\*
X=?:\Documents and Settings\*\Local Settings\Temp\*
x=?:\Documents and Settings\*\Local Settings\Temporary Internet Files\*
x=?:\Documents and Settings\*\Desktop\*
x=?:\Documents and Settings\*\My Documents\*
x=?:\Documents and Settings\*\Favorites\*
x=?:\WINDOWS\CSC\*
X=?:\WINDOWS\TEMP\*
X=?:\WINNT\TEMP\*
```

Customizing other aspects of IBM Rescue and Recovery

You can customize numerous aspects of Rapid Restore Ultra using an external file named TVT.TXT that is defined prior to the installation process. The TVT.TXT file is located in the following subdirectory: C:\PROGRAM FILES\IBM\IBM RAPID RESTORE ULTRA\.

The TVT.TXT file will follow the standard Windows INI file format with the data organized by sections denoted by [] and one entry per line of this format:

```
setting=value
```

For example, if you do not want to encrypt all backup data, include the following lines in the TVT.TXT file:

```
[Rapid Restore Ultra]
EncryptBackupData=0
```

The 0 parameter following EncryptBackupData directs Rescue and Recovery not to encrypt the backup.

A complete list of setting strings, parameters, and default settings for the [Rapid Restore Ultra] section of TVT.TXT are presented in Appendix B, "TVT.TXT settings and values," on page 63.

Disabling password synchronization

Password synchronization is a feature that allows the end user to have their Windows password and their pre-desktop password match. Each time a member of the administrator group changes the Windows password, the administrator user will be prompted to update the pre-desktop password. If this is not desirable, it can be disabled. To disable the password synchronization dialog, delete the following registry key:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"IBMPRC"="C:\IBMTOOLS\UTILS\ibmprc.exe"
```

Trouble Ticket

Currently, there is no way to automatically transmit via FTP or email from the WinPE environment, the end user will be directed to use the email integrated in the browser as well as the location of the files to transmit. Dynamic data transfer is not be supported, but the logging function will package the log events into a file and direct the user of the package location and filename that can be emailed. Req 115 Trouble Ticket - One XML file will be created, which combines all information displayed in System Information (Current HW, eGatherer, and PCDR diagnostic log information), that will be placed in a location which can be easily found and accessible from both PE and OS – C:\IBMTOOLS.

Diagnostics: Is a base application available in the Pre Desktop environment which aids in problem determination. Output from these tests will be stored in a manner which can be viewed or transmitted to a help desk. IBM Rescue and Recovery will supply tools to recover to a previously backed up version of the user's Windows environment.

IBM Rescue and Recovery will contain tools to do a complete restore of a user partition to a previous version as well as tools to recover individual files. The tools will provide access to a backup of the user's data. The ability to recover all or some of this data will be provided by these tools.

OSFILTER.txt

This file recovers the user's operating system and applications without impacting their data. IBM Rescue and Recovery provides the ability to selectively restore particular files and folders (including subfolders) by using explicit enumeration and wild card filtering without deleting any other data. The user only has to select "Restore OS & Apps. An external file will define what files/folders/file types (leveraging wild cards) comprise OS and Applications. This file can be customized by the administrator and a default external file will be provided. When the user selects to recover the operating system and applications only, they will choose which backup to use. Only files that match the rules contained in this external file will be restored. The administrator can customize the contents of this external file. The file follows the filter format described in section 4.5.6

To view the OSFILTER.txt file, use this path: cd %rru%. See "IBMFILTER.TXT" on page 23 for information on the file format.

Chapter 6. Customizing the Pre Desktop Environment of Rescue and Recovery

To customize parts of the Rescue and Recovery Pre Desktop environment, which will start even if the operating system will not open, you must use the IBMRRUTIL.EXE utility program to ″get″ and ″put″ files. These files and their customization options are listed in the following table:

File / Directory	Customization Options
\MININT\SYSTEM32 WINBOM.INI	Add a static IP address, change video resolution
\MININT\INF \MININT\SYSTEM32\DRIVERS	Add device drivers
MAINBK.BMP	Modify environment background
MINIMAL_TOOLBAR(1).INI	Disable address bar
NORM1.INI	Configure the Opera browser, disable the Opera address bar, change Opera proxy settings, specify fixed download directory, add specific file extension to the downloadable files list, change behavior of files with specific extensions
OPERA_010.CMD	Exclude Window users' favorites
OPERA6.INI	Configure the Opera browser, disable the address bar
PEACCESS*XX*.INI (where *XX* is the language designation)	Preboot environment: main GUI fonts, environment background, left and right panel entries and functions, HTML-based help system
STANDARD_MENU.INI	Enable display of ″Save As″ window

Using IBMRRUTIL.EXE

You can obtain IBMRRUTIL.EXE and other utilities mentioned in this guide from the Web site that contains this document.

The following procedure lists the steps to get files from and put files into the Rescue and Recovery environment. These procedures will be used for all file customizations of the Rescue and Recovery environment.

To use IBMRRUTIL.EXE perform the following:

1. Copy IBMRRUTIL.EXE to the root of the C drive.
2. Create GETLIST.TXT file with the following syntax:

   ```
   \preboot\usrintfc\[file name], and then save the file as C:\TEMP\GETLIST.TXT
   ```

3. At a command prompt, type the IBMRRUTIL.EXE command and one of the switches defined in the following table. After the switch complete the command with the appropriate parameters, as shown in the following table.

Command and switch	Result
`IBMRRUTIL -l1`	List the contents of preboot directory
`IBMRRUTIL -l2`	List the contents of minint directory

Command and switch	Result
IBMRRUTIL -14	List the contents of the root of the C drive or root of type-12 partition
IBMRRUTIL -g C:\temp\getlist.txt C:\temp	Get files from preboot partition
IBMRRUTIL -d C:\temp\ getlist.txt	Delete a file(s) from the preboot partition.
IBMRRUTIL -p C:\temp	Add or replace files in the preboot partition.
IBMRRUTIL -bp	Update or replace files in RRUBACKUPS virtual partition.
IBMRRUTIL -br	Delete the content of backup.
IBMRRUTIL -bg	Copy individual files from the \RRUBACKUPS.
IBMRRUTIL -s	Space consumed by RRUbackups.

4. After you have performed the ″get″ routine, you can then edit the file using a standard text editor.

Example: PEACCESSIBMXX.INI

This example refers to PEACCESSIBM*XX*.INI, which is a configuration file where you can customize elements of the Rescue and Recovery environment (see “Customizing the Preboot environment” on page 29).

Note: *XX* in the file name represents one of the following two-letter language abbreviations):

Two-letter language code	Language
br	Brazilian Portuguese
dk	Danish
en	English
fi	Finnish
fr	French
gr	German
it	Italian
jp	Japanese
kr	Korean
nl	Dutch
no	Norwegian
po	Portuguese
sc	Simplified Chinese
sp	Spanish
sv	Swedish
tc	Traditional Chinese

Getting the file PEACCESSIBMEN.INI from the Rescue and Recovery environment:

1. Create GETLIST.TXT file with the following parameters:

   ```
   \preboot\reboot\usrintfc\PEAccessIBMen.ini
   ```
2. Save the file as C:\TEMP\GETLIST.TXT.
3. At a command prompt, type the following command:

   ```
   c:\IBMRRUTIL-g c:\temp\getlist.txt c:\temp
   ```

Putting the file PEACCESSIBMEN.INI back into the Rescue and Recovery environment. At a command line type the following:

```
C:\ IBMRRUTIL.EXE -p C:\temp
```

Note: The ″put″ (-p) routine will use the directory structure created in the get (-g) routine. For proper placement of the edited file, ensure that the edited file is located in the same directory that is established in the GETLIST.TXT file, as in the example below:

```
C:\temp\preboot\usrintfc\PEAccessIBMen.ini
```

Example: Adding device drivers to the Rescue and Recovery area

1. Obtain device drivers from the vendor's Web site or other media.
2. Create the following directory structures:

   ```
   C:\TEMP\MININT\INF
   ```

   ```
   C:\TEMP\MININT\SYSTEM32\DRIVERS
   ```
3. Copy all network driver *.INF files to the MININT\INF directory. (For example, E100B325.INF needs to be in the \MININT\INF directory.)
4. Copy all *.SYS files to the \MININT\SYSTEM32\DRIVERS directory. (For example, E100B325.SYS needs to be in MININT\SYSTEM32\DRIVERS directory.)
5. Copy any related *.DLL, *.EXE, or other files to the \MININT\SYSTEM32\DRIVERS directory. (For example, E100B325.DIN, INTELNIC.DLL etc. needs to be in MININT\SYSTEM32\DRIVERS directory.)

   Notes:
   a. Catalog files are unnecessary, as they are not processed by the Rescue and Recovery environment. The above instructions apply to any device driver that might be needed to configure the computer.
   b. Due to the limitation of Windows PE, you may have to manually apply some configuration applications or settings as registry updates.
6. To put the device drivers into the Rescue and Recovery environment, type the following at a command line:

   ```
   C:\ IBMRRUTIL.EXE -p C:\temp
   ```

Customizing the Preboot environment

By editing the configuration file PEAACCESSIBM*XX*.INI (where *XX* is the language designation), you can customize the following elements of the Rescue and Recovery environment:

- The main GUI fonts
- The environment background
- Entries and functions in the left panel of the user interface
- The HTML-based help system for the Rescue and Recovery environment

Note: To get, edit, and replace PEACCESSIBMEN.INI refer to "Example: PEACCESSIBMXX.INI" on page 28.

Changing the main GUI font

You can change the font of the main graphical user interface. Note that the default settings might not display all characters correctly, depending on the language and characters required. In PEACCESSIBM*XX*.INI (where *XX* is the language

designation) the [Fonts] section contains the default settings for the character style that will be displayed. The following are default settings for most single-byte character set languages:

```
[Fonts]
LeftNavNorm = "Microsoft Sans Serif"
LeftNavBold = "Arial Bold"
MenuBar = "Microsoft Sans Serif"
```

Depending on your visual and character set requirements, the following fonts are compatible with the Rescue and Recovery environment. Other fonts might be compatible, but have not been tested:

- Courier
- Times New Roman
- Comic Sans MS

Changing the environment background

The background of the right panel is a bitmap, MAINBK.BMP, which is located in the \PREBOOT\USRINTFC directory. If you create your own bitmap image for the right-panel background, it must conform to the following dimensions:

- 620 pixels wide
- 506 pixels deep

You must place the file in the \PREBOOT\USRINTFC directory in order for Rescue and Recovery to present the desired background.

Note: To get, edit, and replace MAINBK.BMP, refer to "Using IBMRRUTIL.EXE" on page 27.

Changing entries and functions in the left panel

Changing the left-panel entries requires editing the PEACCESSIBM*XX*.INI (where *XX* is the language designation) file. For information regarding getting PEACCESSIBM*XX*.INI from the Rescue and Recovery environment and replacing the file, refer to "Using IBMRRUTIL.EXE" on page 27.

Rescue and Recovery has twenty-one entries in the left panel. Although functions are different, each entry has the same basic elements. The following is an example of a left-panel entry:

```
[LeftMenu] button00=2, "Introduction", Introduction.bmp, 1,
1, 0, %sysdrive%\Preboot\Opera\ENum3.exe,
```

Entry	Customization options
00-01	Fully customizable.
02	Must remain a button type 1 (see Button Type table below). Text can be changed. An application or help function can be defined. No icon can be added.
03-05	Fully customizable.
06	Must remain a type 1. Text can be changed. An application or help function can be defined. No icon can be added.
07-08	Fully customizable.
09	You can set this entry to be displayed or to be hidden. See "Defining entry types" on page 31 for field and value information. No other customization is enabled.

Entry	Customization options
10	Must remain a type 1. Text can be changed. An application or help function can be defined. No icon can be added.
11–14	Fully customizable.
15	Must remain a type 1. Text can be changed. An application or help function can be defined. No icon can be added.
16-18	Fully customizable.
19	No customization is enabled.
20	Fully customizable

Defining entry types

Button00 must be a unique identifier. The number determines the order by which the buttons will be displayed in the left panel.

Button00=[0-8] This parameter determines the button type. This number can be an integer 0 through 8. The following table explains the type and behavior of each button type:

Parameter	Button type
0	Empty field. Use this value when you want to leave a row blank and unused.
1	Section head text. Use this setting to establish a major grouping or section head.
2	Application launch. The fields that follow define an application or command file to be started when the user clicks the button or text.
3	Opera help for the Rescue and Recovery environment. The fields that follow will define a help topic to be launched using the Opera browser
4	Display a restart message window before launching. The values in the fields that follow this button type will direct the GUI to present a message to the user that the computer will need to be restarted before the specified function is executed.
5	Reserved for IBM
6	Reserved for IBM
7	Launch and wait. The fields that follow this specification forces the environment to wait for a return code from the launched application before continuing. The return code is expected to be in the environment variable, %errorlevel%.
8	Launch application. These tell the GUI to retrieve the Country Code and language before starting the application. It is used for Web links that have CGI scripts to open a Web page from a certain country or in a certain language.

Defining entry fields

Button00=[0-8], "title"

The text following the button type parameter specifies the text or title of the button. If the text exceeds the width of the left panel, the text will be cut and ellipsis points will indicate that more characters follow. On mouse over, the full title text will be displayed in a bubble.

Button00=[0-8], "title", file.bmp
Following the title text, specify the file name of the bitmap that you want to use as an icon for the button being created. The bitmap must be no larger than 15 pixels by 15 pixels to fit correctly.

Button00=[0-8, "title", file.bmp, [0 or 1]
This setting directs the environment to display or hide the entry. The value 0 hides the entry. If the value is set to 0, then the a blank line is displayed. The value 1 displays the value.

Button00=[0-8], "title", file.bmp, [0 or 1], 1
This is a reserved function and must always be set to 1.

Button00=[0-8], "title", file.bmp, [0 or 1], 1, [0 or 1]
To require a password prior to starting an application, place a value of 1 in this position. If you set this value to 0, no password will be required before a specified application is started.

Button00=[0-8], "title", file.bmp, [0 or 1], 1, [0 or 1], %sysdrive%[pathname\executable]
The value of %sysdrive@ must be the boot drive letter. Following the boot drive letter, you must provide a fully qualified path to an application or command file.

Button00=[0-8], "title", file.bmp, [0 or 1], 1, [0 or 1],%sysdrive%[pathname\executable], [parameters]
Provide any number of parameters required by the target application that is being started.

If you are not providing values for various fields, you must provide the required commas in order for the button definition to be accepted and to run correctly. For example, if you are creating a group heading, "Rescue and Recover," the following would be the code for the entry:

```
Button04=1, "Rescue and Recover",,,,,,
```

Entries 02, 06, 10 and 15 must remain type 0 (or header) entries, and they will always fall in their numerical places. The availability of entries that fall under the headers can be reduced by setting fully customizable entries to type 0-blank lines in the left panel. However, the total number of entries cannot exceed twenty-two and entries 9 and 19 must remain in those positions.

The following table shows the function and executables that you can start from the left-panel entries:

Function	Executable
Recover files	WIZRRU.EXE
Restore from backup	WIZRRU.EXE
Recover factory contents	RECOVER.CMD
Open browser	OPERA.EXE
Map a network drive	MAPDRV.EXE
Diagnose hardware	RDIAGS.CMD; launches the PC Dr application, IBM preinstallation models only
Create diagnostic diskettes	DDIAGS.CMD

Changing entries and functions in the right panel

Changing the right-panel entries requires editing the PEACCESSIBMXX.INI (where *XX* is the language designation) file. For information regarding getting PEACCESSIBMXX.INI from the Rescue and Recovery environment and replacing the file, refer to "Example: PEACCESSIBMXX.INI" on page 28.

The function links and user messages and window status of the right panel are customizable.

Customizing the function links in the right panel

To change the functions of the links that span the top of the right panel, modify the [TitleBar] section of PEACCESSIBMXX.INI (where *XX* is the language designation). These links operate the same way as the left-panel entries. The button number values are 00through 04. The same applications that can be started from the left panel can be started from the [TitleBar] entries. See the applications on page 7 for a complete list of applications that can be started from the title bar.

Modifying user messages and window status

PEACCESSIBMXX.INI (where *XX* is the language designation) contains two sections with messages to the user that you can modify:

```
[Welcome window]
[Reboot messages]
```

The Welcome window is defined in the [Welcome] section of PEACCESSIBMXX.INI (where *XX* is the language designation). Depending on the changes that you have made to the left panel, you can change the information in the title line and lines 01 through 012. You can set the font that the title, head and bold will be displayed in:

```
[Welcome]
Title = "Welcome to IBM Rescue and Recovery with Rapid Restore"
Line01 = "The IBM(R) Rescue and Recovery(TM) workspace provides a number of tools
to help you recover from problems that prevent you from accessing the Windows(R)
environment."
Line02 = "You can do the following:"
Line03 = "*Rescue and restore"
Line04 = "your files, folders or backups using IBM Rapid Restore(TM)"
Line05 = "*Configure"
Line06 = "your system settings and passwords"
Line07 = "*Communicate"
Line08 = "use the Internet and link to the IBM support site"
Line09 = "*Troubleshoot"
Line10 = "diagnose problems using diagnostics"
Line11 = "Features may vary based on installation options.
For additional information, click Introduction
in the Rescue and Recovery menu."
Line12 = "NOTICE:"
Line13 = "By using this software, you are bound by the
terms of the License Agreement. To view the license,
click Help in the Rescue and Recovery toolbar,
and then click View License."
Continue = "Continue"
NowShow = "Do not show again"
NoShowCk =0
WelcomeTitle = "Arial Bold"
WelcomeText = "Arial"
WelcomeBold = "Arial Bold"
```

The following settings are for the Title Bar Help functions on the user interface:

Command0
An HTML page to be started for the base help page

Command1
IBM License Agreement HTML page

HELP Help

LICENSE
License

CANCEL
Cancel

Commnad0
%sysdrive%Preboot\Helps\en\f_welcom.htm

Command1
%sysdrive%Preboot\Helps\en\C_ILA.htm

To hide the Welcome window altogether, change `NoShowCk=0` to `NoShowCk=1`. To change the display fonts for the title and welcome text, edit the last three lines of the section according to your design preferences.

Note: Do not change or delete lines 13 and 14.

In the [REBOOT] section of the PEACCESSIBM*XX*.INI (where *XX* is the language designation) file, you can modify the values in the following lines:

```
NoShowChk=
RebootText=
```

The two values for ″NoShowChk″ are `0` and `1`. The message can be hidden when a user chooses. When a user clicks the check box when the message is displayed the value is set to `0`. To have the message displayed, change the value to `1`. If necessary, the font for messages in the [REBOOT] section can be changed. For example, this value can be set as follows:

```
RebootText = "Arial"
```

Note: The following sections of PEACCESSIBM*XX*.INI (where *XX* is the language designation) are available in the file, but are not customizable: [Messages], [EXITMSG], and [HelpDlg].

Configuring the Opera browser

The Opera browser has two configuration files, one of which contains the default IBM configuration. The other is the ″active″ configuration. An end user can make changes to the active configuration, but will lose those changes when Rescue and Recovery is restarted.

To make permanent changes to the browser, edit the copies of both OPERA6.INI and NORM1.INI that are on the %systemdrive%, C, in the following folder path: C:\PREBOOT\OPERA\PROFILE. The temporary, ″active″ copy of OPERA6.INI is on the ramdrive (Z:) in the Z:\PREBOOT\OPERA\PROFILE directory.

Notes:

1. To get, edit and place the OPERA6.INI and NORM1.INI files, refer to “Using IBMRRUTIL.EXE” on page 27.

2. The Opera workspace has been modified to provide enhanced security. As a result, some browser functions have been deleted.

E-mail

IBM Rescue and Recovery provides support for web-based e-mail through the Opera browser. Opera provides IMAP based email which can be enabled through the large enterprise configuration, but will not be supported. To get the reference information on how to enable please go to http://www.opera.com/support/mastering/sysadmin/ and read their System Administrator's Handbook.

Disabling the address bar

To disable the address bar in Opera, complete the following procedure:

1. Get the file MINIMAL_TOOLBAR(1).INI from C:\PREBOOT\OPERA\PROFILE\TOOLBAR by using the IBMRRUTIL process in the sections "Using IBMRRUTIL.EXE" on page 28.
2. Open the file for editing.
3. Locate the [Document Toolbar] section of the file.
4. Locate the "Address0" entry.
5. Place a semicolon (; -a comment delimiter) in front of the "Address0" entry.

   Note: Stopping here and continuing to step 7 will disable the Opera toolbar, but will leave a nonfunctional "Go" button and toolbar graphic. To remove the "Go" button and the toolbar, continue with step 6.
6. Locate the following entries and then place a semicolon in front of each:

   ```
   Button1, 21197=Go Zoom2
   ```
7. Save the file.
8. Put the file by using the IBMRRUTIL process as discussed in section "Using IBMRRUTIL.EXE" on page 1. The address bar will be disabled when Opera runs.

Customizing bookmarks

IBM has configured Opera to read the bookmarks established in this ramdrive file: Z:\OPERADEF6.ADR. This file is generated when Rescue and Recovery is started from code in the startup routine. The startup routine automatically imports Windows Internet Explorer bookmarks and adds some additional IBM bookmarks. Because the ramdrive file that is generated on startup is impermanent, add bookmarks to Internet Explorer, which will be automatically imported when the Rescue and Recovery environment is started.

You can exclude some or all of the Internet Explorer favorites. To exclude specific Windows users' favorites do the following:

1. Get C:\PREBOOT\STARTUP\OPERA_010.CMD by using the IBMRRUTIL process discussed in "Using IBMRRUTIL.EXE" on page 27.
2. Open the file for editing.
3. Locate the following line in the .CMD file: PYTHON.EXE.FAVS.PYC Z:\OPERADEF6.ADR
4. At the end of this line of code type in quotations the names of the Windows users whose favorites you want to exclude. For example, if you want to exclude the favorites for All Users and Administrator, the code line will read as follows:

   ```
   python.exe favs.pyc z:\Operadef6.adr "All Users, Administrator"
   ```
5. Save the file.

6. Put the file by using the IBMRRUTIL process discussed in "Using IBMRRUTIL.EXE" on page 27.

If you do not want any of the Internet Explorer favorites to be displayed in the browser provided in the Rescue and Recovery environment, do the following:

1. Get the C:\PREBOOT\STARTUP\OPERA_010.CMD for editing by using the IBMRRUTIL process discussed in "Using IBMRRUTIL.EXE" on page 1.
2. Locate the following line in the .CMD file: PYTHON.EXE.FAVS.PYC Z:\OPERADEF6.ADR
3. Do one of the following:
   a. Type REM at the beginning of the line, as follows:

      ```
      REM python.exe favs.pyc z:\Operadef6.adr
      ```

   b. Delete the line of code from the file.
4. Save the file.
5. Put the file back by using the IBMRRUTIL process discussed in "Using IBMRRUTIL.EXE" on page 27.

Changing proxy settings

To change the proxy settings for the Opera browser, do the following:

1. Get the file C:\PREBOOT\OPERA\PROFILE\NORM1.INI for editing by using the IBMRRUTIL process discussed in "Using IBMRRUTIL.EXE" on page 27.
2. Add the following section to the bottom of the NORM1.INI file:

   Note: The [0 or 1] variable indicates that the check item is either enabled (1) or disabled (0).

   ```
   [Proxy]
   Use HTTPS=[0 or 1]
   Use FTP=[0 or 1]
   Use GOPHER=[0 or 1]
   Use WAIS=[0 or 1]
   HTTP Server=[HTTP server]
   HTTPS Server=[HTTPS server]
   FTP Server=[FTP server]
   Gopher Server= [Gopher server]
   WAIS Server Enable HTTP 1.1 for proxy=[0 or 1]
   Use HTTP=[0 or 1]
   Use Automatic Proxy Configuration= [0 or 1]
   Automatic Proxy Configuration URL= [URL]
   No Proxy Servers Check= [0 or 1]
   No Proxy Servers =<IP addresses>
   ```

3. Save the file.
4. Put the file back by using the IBMRRUTIL process discussed in "Using IBMRRUTIL.EXE" on page 27.

To add an HTTP, HTTPS, FTP, Gopher, or WAIS proxy, type `=<address of proxy>` after the appropriate line. For example, if the address of your proxy server is http://www.your company.com/proxy, the HTTP Server line would read as follows:

```
HTTP Server=http://www.your company.com/proxy
```

To add the port to the entry, place a colon after the address and type the port number. The same holds for the "No Proxy Servers" and "Automatic Proxy Configuration URL" fields.

z:\preboot\opera\profile\opera6.ini.

Enabling or specifying the full download path

There are numerous settings that you can set to enable display of the ″Save As″ window. The most straightforward method is offered here.

1. Get the C:\PREBOOT\OPERA\DEFAULTS\STANDARD_MENU.INI file by using the IBMRRUTIL process discussed in “Using IBMRRUTIL.EXE” on page 27.
2. In the [Link Popup Menu] section, locate this string: ;;Item, 50761.
3. Remove the two semicolons, and then save the file. When Rescue and Recovery is closed and reopened, an end user will be able to right-click a link and the ″Save Target As″ option will be displayed. This will result in display of the ″Save As″ window.

   Note: Straight links (not redirected links) will work with the above procedure. For example, if a link targets a .PHP script, Opera will save the script only, not the file to which the script points.
4. Put the file back to the directory structure by using the IBMRRUTIL process discussed in “Using IBMRRUTIL.EXE” on page 27.

To specify a fixed download directory, do the following:

1. Get the C:\PREBOOT\OPERA\NORM1.INI file by using the IBMRRUTIL process defined discussed in “Using IBMRRUTIL.EXE” on page 27.
2. In the file, locate this line:

   ```
   Download Directory=%OpShare%
   ```
3. Change %OpShare% to the full path of the directory to which you want downloaded files to be saved.
4. Save the NORM1.INI file. When Rescue and Recovery is closed and reopened, Opera will save downloaded files to the specified directory.
5. Put the file back by using the IBMRRUTIL process discussed in “Using IBMRRUTIL.EXE” on page 27.

Note:

- Customizing the full path for downloading does not enable users to save the target file, even if the link is redirected.
- IBM has configured Opera to download only the .ZIP, .EXE, and .TXT file types, and will only change Opera behavior for these file types. (There are potentially thousands of file types using a three-letter file extension. Just as the Rescue and Recovery environment is not intended to be a replacement for the Windows environment, the Opera browser is not intended to replace a full-service browser. Internet access is provided to help users get up and running. The number of recognized file types is necessarily limited. For the purposes of rescue and recovery, .TXT, .EXE, and .ZIP should be sufficient. If another file type needs to be transferred, best results will be realized by creating a .ZIP file, which can then be extracted.)
- File types are recognized by mime type rather than by file extension. For example, if a .TXT file is named with .EUY as an extension, the file will still open in the Opera browser as a text file.

Adding a specific file extension to the downloadable files list

You can add to the list of files that can be downloaded through the Rescue and Recovery browser. To add to the list, complete the following procedure:

1. Make sure that Opera is closed and that all Opera windows are closed, including the Rescue and Recovery help files.

2. Get the C:\PREBOOT\OPERA\NORM1.INI file using the IBMRRUTIL process discussed in "Using IBMRRUTIL.EXE" on page 27.
3. Locate the [File Types] section of the file.
4. Use the search function to discover whether the file extension you want is listed, but does not work; then do one of the following:
   - If the extension is found, but files with that extension do not work correctly, complete the following steps:
     a. Change the value following the extension from 8 to 1. (A value of 8 tells the browser to ignore the file. A value of 1 instructs the browser to save the file.) For example, change the following:

        ```
        video/mgpeg=8,,,,mpeg,mpg,mpe,m2v,m1v,mpa,|
        ```

        to

        ```
        video/mgpeg=1,,,,mpeg,mpg,mpe,m2v,m1v,mpa,|
        ```

     b. Scroll up to the [File Types Extension] section of the NORM1.INI file, and then search for the mime type of the file. For example, find the following: VIDEO/MPEG=,8
     c. Change the ,8 value to the following:

        ```
        %opshare%\,2
        ```

        Note: If the value already set as specified, do not change the value.
     d. Save the file, and then copy the file to OPERA6.INI, and then restart Rescue and Recovery for the changes to be effective.
   - If the extension is not present and files of the desired type do not work correctly, do the following:
     a. In the [File Types Extension] section of NORM1.INI, locate the temporary mime entry. The following is an example: temporary=1,,,,lwp,prz,mwp,mas,smc,dgm,|
     b. Add the file type extension to the list. For example, if you want to add .CAB as a recognized extension, add it according to the following sample entry:

        ```
        temporary=1,,,,lwp,prz,mwp,mas,smc,dgm,cab,|
        ```

        Note: The trailing comma and pipe symbol are essential for this setting to work. If either is omitted, all file extensions in the list might be disabled.
     c. Save the file to the directory path C:\TEMP\. Copy the file to OPERA6.INI, and then restart the IBM Rescue and Recovery workspace for the changes to be effective.

Changing the behavior of files with specific extensions

You can change the behavior of files by replacing values in the NORM1.INI file. To change file behavior by extension, do the following:

1. Close Opera and all active Opera windows, including IBM help files.
2. Open the PREBOOT\OPERA\NORM1.INI file for editing by using the IBMRRUTIL process discussed in "Using IBMRRUTIL.EXE" on page 27.
3. Locate the [File Types] section of the file, and then search for the extension you want to work with. For example, you want all .TXT files to be saved to the IBMSHARE folder.
4. Find the following entry: TEXT/PLAIN=2,,,,TXT,|

   Note: A value of 2 instructs the browser to display the text in Opera. A value of 1 instructs the browser to save the target file in the IBMSHARE folder.
5. Continuing with the .TXT example, change the line to read as follows:

   ```
   TEXT/PLAIN=1,,,,TXT,|
   ```

6. Save the file and put it back by using the IBMRRUTIL process as discussed in "Using IBMRRUTIL.EXE" on page 27.
7. Restart the IBM Rescue and Recovery workspace for changes to be effective.

Adding a Static IP Address

To add a Static IP address, you need to change the following files.

1. Get the \MININT\SYSTEM32 WINBOM.INI file by using the IBMRRUTIL process discussed in "Using IBMRRUTIL.EXE" on page 27.
2. Add `[WinPE.Net]` section before `[PnPDriverUpdate]` in WINBOM.INI file. For example, consider the following file: WINBOM.INI

```
[Factory]
WinBOMType=WinPE
Reseal=No
[WinPE]
Restart=No
[PnPDriverUpdate]
[PnPDrivers]
[NetCards]
[UpdateInis]
[FactoryRunOnce]
[Branding]
[AppPreInstall]
```

   You must add the following lines to the `[WinPE.Net]` section.

```
[WinPE.Net]
Gateway=9.44.72.1
IPConfig =9.44.72.36
StartNet=Yes
SubnetMask=255.255.255.128
```

Entry	Description
`Gateway`	Specifies the IP address of an IP router. Configuring a default gateway creates a default route in the IP routing table. **Syntax:** `Gateway = xxx.xxx.xxx.xxx`
`IPConfig`	Specifies the IP address that Windows PE uses to connect to a network. **Syntax:** `IPConfig = xxx.xxx.xxx.xxx`
`StartNet`	Specifies whether to start networking services. **Syntax:** `StartNet = Yes | No`
`SubnetMask`	Specifies a 32-bit value that enables the recipient of IP packets to distinguish the network ID and host ID portions of the IP address. **Syntax:** `SubnetMask = xxx.xxx.xxx.xxx`

3. Get the PREBOOT\IBMWORK NETSTART.TBI file by using the IBMRRUTIL process discussed in "Using IBMRRUTIL.EXE" on page 27.
4. Change

```
factory -minint
```

   to

```
factory -winpe
```

5. Comment out the following lines:

   ```
   regsvr32 /s netcfgx.dll
   netcfg -v -winpe
   net start dhcp
   net start nla
   ```

6. Put the \IBMWORK NETSTART.TBI and \MININT\SYSTEM32 WINBOM.INI files back by using the IBMRRUTIL process discussed in "Using IBMRRUTIL.EXE" on page 27.

Changing the video resolution

You can change the video resolution by changing the default predesktop resolution settings of 800 × 600 × 16-bit. To change the settings, do the following:

1. Get the MININT\SYSTEM32\WINBOM.INI file by using the IBMRRUTIL process discussed in "Using IBMRRUTIL.EXE" on page 27.
2. In the file WINBOM.INI, add the following entries:

   ```
   [ComputerSettings]
   DisplayResolution=800x600x16 or 1024x768x16
   In the file preboot\ibmwork\netstart.tbi change factory-minint to factory-winpe
   ```

   When the Rescue and Recovery environment starts, you will see an additional window during startup that is titled ″Factory preinstallation.″ Furthermore, the colors will be reduced from thousands to 256.
3. Put back the MININT\SYSTEM32\WINBOM.INI file by using the IBMRRUTIL process discussed in "Using IBMRRUTIL.EXE" on page 27.

Chapter 7. Antidote Delivery Manager Infrastructure

Antidote Delivery Manager is the name for an anti-virus, anti-worm infrastructure included in IBM Rescue and Recovery. It's objects are reliable and quick to implement, and efficient, and allows an administrator to initiate blocking and recovery within minutes, It can be kicked off by one administrator, and it will function even for systems that are unlocated or not network attached. This complements existing antivirus tools, so maintaining virus scanning tools and obtaining patches is still required. Antidote Delivery Manager provides the infrastructure to stop the destruction and apply the patches.

Antidote Delivery Manager works by delivering instructions from an administrator to each system and by supporting commands to combat a virus or a worm. The administrator prepares a script containing the actions desired on each system. The repository function delivers the script securely to the system within minutes and executes the commands. Commands include restricting network connections, displaying messages to the end users, restoring files from backups, downloading files, executing other system commands, and rebooting the machine either to the same operating system or to switch into or out of the Rescue and Recovery environment. Both the repository function and the commands will work in either the normal operating system (such as Windows XP) or in the Rescue and Recovery environment

The overall strategy to combat a virus is reduce the spread and damage of the malicious code, apply patches and cleanup to each system, then bring the restored machines back onto the network. For a highly destructive and fast spreading virus, it may be necessary to remove systems from the network and conduct all repair operations in the Rescue and Recovery environment. Although this is the safest method, it is also disruptive to end users if applied during normal working hours. In some circumstances, shifting to the Rescue and Recovery environment can be delayed or avoided by restricting the network capabilities. The next step is to get patches and cleanup code downloaded, clean code run and patches set up for installation. In general, patches are designed to be installed while the operating system is running, but clean up and other operations may be more appropriate in the Rescue and Recovery environment. Once the corrective actions are complete, the system can then be restored to normal operation with Windows XP running and network configurations restored.

The next two sections will describe the repository operation and commands in detail. Then installation and configuration of the function will be presented. The following sections are examples of how to use the system for the common tasks of testing, responding to destructive viruses, addressing machines connected by wireless or Virtual Private Networks (VPNs), and fixing less destructive problems.

Repository

The repository function runs on each system and periodically checks for new messages from the administrator. It checks at a scheduled time interval or at the occurrence of several interesting events (boot, resume from suspend or hibernate, detection of a new network adapter, assignment of a new IP address, etc). The repository function looks for messages in a set of directories, in a Windows share location, such as \\machine\share\directory, at HTTP URLs, and at FTP URLs . If more than one message is found, it will process them in "directory sort by name"

order. Only one message will be processed at a time. A message will only be processed successfully once. If processing a message fails, by default, it will not be attempted again, but retrying on failure may be specified in the message itself.

A message must be packaged by an administrator before being placed in a directory to be processed by the repository function. To create the package, the administrator places all of the files that constitute the message into a directory (or its subdirectories). One of the files must be named "GO.RRS" the primary command script. The administrator may optionally use a signature key for this message, but if used the key must be available to all of the target systems. The repository function will check the package for integrity, check the signature if supplied and unpack all of the files into a local directory before executing GO.RRS.

The primary command script file (GO.RRS) follows the syntax of a Windows Command File. It may contain legitimate Windows commands and any of the commands listed in the next section. Also, a Python command interpreter is installed as part of the Rescue and Recovery environment, so Python scripts may also be called from the GO.RRS script.

At the end of execution of the script, all files unpacked from the message will be deleted, so if files will be required after the script exits (for example, installing a patch on reboot) the files must be moved out of the message directory.

Each system will have a configuration of repositories to check. It may be appropriate for the IT administrator to divide the population of systems into groups and assign different repositories (network shares) to each group. For example, system's might be grouped geographically be proximity to a file server. Or, system's could be grouped by function, such as engineering, sales, or support.

Antidote Delivery Manager Commands and Available Windows Commands

The Antidote Delivery Manager system provides several commands to facilitate the operation of the system. In addition to the command to create messages and adjust settings, there are commands to control networking, determine and control operating system state, examine XML files from system inventories and notify the end user of progress of the Antidote Delivery Manager script on the client machine. The NETWK command enables or disables networking or restricts networking to a limited group of network addresses. The INRR command may be used to determine if the Windows XP operating system is running or if the computer is in the Rescue and Recovery environment. The REBOOT command can be used to shutdown the computer and specify that it should boot either to Windows XP or to Rescue and Recovery. The MSGBOX application allows for communication with the end user by displaying a message in a pop-up box. The message box can optionally contain "OK" and "Cancel" buttons so the message can act differently based on input from the end user.

Certain Microsoft commands are also available to Antidote Delivery Manager. The permitted commands include all commands built into command shell such as DIR, CD, etc. Other useful commands such as REG.EXE to change the registry and CHKDSK.EXE to verify disk integrity are available.

Typical Antidote Delivery Manager Utilization

The Antidote Delivery Manager system can be used to complete a wide variety of tasks. Several examples are provided below to demonstrate how the system might be used.

- **Simple System test - Display Notification**

  The most basic use of the system is to display a single message to the end user. The easiest way to run this test and also test other scripts before deployment is to place the message in a repository that is a local directory on the administrator's personal computer. This allows rapid testing of the script with no impact to other machines.

- **Script preparation and packaging**

  Write a GO.RRS script on any machine where Antidote Delivery Manager has been installed. Include a line MSGBOX /MSG "Hello World" /OK. Run the APKGMSG command on the directory containing GO.RRS to create a message.

- **Script Execution**

  Place the message file in one of the repository directories on your machine and observe correct operation. When the mail agent next runs, a message box will display with the "Hello World" text. Such a script is also a good way to test network repositories and to demonstrate features such as the checking of repositories on resume from suspend.

Major Worm Attack

The example demonstrates one possible approach to combating a major virus. The basic approach is to turn off networking, then reboot to Rescue and Recovery, retrieve fixes, perform repairs, then boot back to Windows XP, install patches, and finally restore networking. A single message may be used to perform all of these functions through the use of flag files and the RETRYONERROR command.

1. **Lockdown phase**

   The first thing to accomplish is to inform the end user what is about to happen. If the attack is not extremely serious, the administrator may give the End User the option to defer the fix until later. In the most conservative case, this phase would be used to disable networking and provide a short window such as 15 minutes for the End User to save work in progress. RETRYONERROR is used to keep the script running and then the machine may be rebooted into the Rescue and Recovery Environment.

2. **Code distribution phase an repair phase**

   Now that the threat of infection has been removed by disabling the network and rebooting to Rescue and Recovery, additional code may be retrieved and repairs accomplished. The network may be enabled or only certain addresses may be permitted for the time required to retrieve additional files. While in Rescue and Recovery, and virus files may be removed and the registry may be cleaned up. Unfortunately, installing new software or patches will not be possible since the patches will assume that Windows XP is running. With networking still disabled and all virus code removed, it is safe to reboot to Windows XP to complete repairs. A tag file written at this time will direct the script to the patch section after the reboot.

3. **Patch and recovery phase**

   Once the machine reboots in Windows XP, Antidote Delivery Manager will begin processing again even before the End User can log in. Patches should be installed at this time. If necessary, the machine can be rebooted for a final time

if the newly installed patches require it. Now that all cleanup and patching has been completed, the network may be enabled and the End User informed that normal operation is possible.

Minor Application Update

No all maintenance will require the drastic measures described above. If a patch is available, but a virus attack is not in progress, a more relaxed approach may be appropriate.

Once again, a single script can control the operation through the use of RETRYONERROR and tag files.

1. **Download Phase**

   The process begins with a message box informing the End User that a patch will be downloaded for later installation. Then the patch can be copied from the server.

2. **Patch phase**

   Now that the patch code is ready for installation, it is time to warn the End User and start installation. If the End User requests a delay, a tag file could be used to track the delay. Perhaps later requests to install the patch might be more urgent. Note that Antidote Delivery Manager will maintain this state even if the End User powers off or reboots their system. Once the End User has granted permission, the patch is installed and system rebooted if required.

Accommodating VPN's and Wireless Security

The Rescue and Recovery environment does not currently support either remote access Virtual Private Networks (VPN) or wireless network attachments. If a machine is using one of these network attachments in Win XP, and then reboots to Rescue and Recovery, network connectivity will be lost. So a script like the example above will not work because networking will not be available in RR to download files and fixes.

The solutions are to package all needed files in the original message or download the need files before rebooting. This is done by placing all necessary files in the directory with GO.RRS. The script file must take care to move the required files into their final positions before exiting the script (when the directory containing GO.RRS on the client will be deleted). Placing patches in the message file may not be practical if the patches are very large. In this case, the End User should be informed, then networking restricted to only the server containing the patch. Then the patch can then be downloaded while still in Windows XP. Although this may length the exposure of Windows XP to a virus, the extra time probably will not be significant.

Chapter 8. Best Practices

This chapter presents a usage scenario to illustrate the best practices of Rescue and Recovery. This scenario starts with the configuration of the hard disk drive, moves through several updates, and follows the life cycle of a deployment. Installation on both IBM and non-IBM computers is described.

Installing IBM Rescue and Recovery in a new roll-out on IBM computers

This section describes installing Rescue and Recovery in a new roll-out.

Preparing the hard disk drive

The first thing to consider when deploying a system is preparing the hard disk drive of your donor system. If you want to start with a clean hard disk, you must clean out the Master Boot Record on the primary hard disk.

1. Remove all storage devices (second hard disks, USB hard disks, USB memory keys, PC Card Memory, and so on) from the donor system, except the primary hard disk that you are going to install Windows on.

   Attention: Running this command will erase the entire contents of the target hard disk drive. After running, you will be unable to recover any data from the target hard disk drive.
2. Create a DOS boot diskette and place the file CLEANDRV.EXE on it.
3. Boot the diskette (only one storage device attached). At the DOS prompt, type the following command:

   ```
   CLEANDRV /HDD=0
   ```
4. Install the operating system and applications. Build your donor system as though you were *not* installing Rescue and Recovery. The last step in the process is to install Rescue and Recovery.

Installation

This first step in the install process is extraction of the InstallShield executable to the directory C:\RRTEMP. If you are going to install Rescue and Recovery on multiple systems, performing this process one time will reduce the install time on each machine by roughly one-half.

1. Assuming that the install file is located in the root of the C drive, create a file EXE_EXTRACT.CMD, which will extract the file C:\SETUP_IBMRR*XXXX*.EXE (where *XXXX* is the build ID) to C:\RRTEMP.

   ```
   :: This package will extract the WWW EXE to the directory c:\RRTemp for an
   :: administrative install.
   @ECHO OFF
   :: This is the name of the EXE (Without the .EXE)
   set BUILDID=setup_ibmrr1033
   :: This is the drive letter for the Setup_ibmrr1033.exe
   :: NOTE: DO NOT END THE STRING WITH A "\".  IT IS ASSUMED TO NOT BE THERE.
   SET SOURCEDRIVE=C:
   :: Create the RRTemp directory on the HDD for the exploded WWW EXE
   MD c:\RRTemp
   :: Explode the WWW EXE to the directory c:\RRTemp
   ```

```
start /WAIT %SOURCEDRIVE%\%BUILDID%.exe /a /s /v"/qn TARGETDIR=c:\RRTemp"
 TARGETDIR=c:\RRTemp"
```

2. You can make many customizations prior to the installation of Rescue and Recovery. Some examples in this scenario are:
   - Change maximum number of incremental backups to 4.
   - Set Rescue and Recovery to perform an incremental backup every day at 1:59 p.m. to the local hard disk and call it ″Scheduled.″
   - Hide the Rescue and Recovery User Interface to all users not in the local Administrators Group.
3. Create a custom TVT.TXT (modified entries are in **bold**):

```
[Scheduler]
Task1=RapidRestoreUltra
Task2=egatherer
[egatherer]
ScheduleFrequency=2
Task=c:\IBMTOOLS\eGatherer\launcheg.exe
ScheduleHour=0
ScheduleMinute=0
ScheduleDayOfTheWeek=0
ScheduleWakeForBackup=0
[RapidRestoreUltra]
LastBackupLocation=0
CustomPartitions=0
Exclude=0
Include=0
CustomStorageSettings=1
MaxNumberOfIncrementalBackups=4
MaxBackupSize=0
EncryptBackupData=1
UUIDMatchRequired=0
PasswordRequired=0
DisableArchive=0
DisableRestore=0
DisablePreferences=0
DisableSFR=0
CPUPriority=3
Yield=0
Ver=4.0
Task=C:\Program Files\IBM\IBM Rapid Restore Ultra\rrucmd.exe
TaskParameters=BACKUP location=L name="Scheduled"
ScheduleFrequency=1
ScheduleHour=13
ScheduleMinute=59
HideGUI=0
GUIGroup=Administrators
[RestoreFilesFolders]
WinHiddenFolders=%RRUBACKUPS%,%MININT%,%PREBOOT%
PEHiddenFolders=%RRUBACKUPS%,%MININT%,%PREBOOT%,Z:\
AllowDeleteC=FALSE
```

4. In the same directory as the new TVT.TXT, create a file INSTALL.CMD, which will perform several actions:
   - Copy the custom TVT.TXT into the install package created in c:\RRTemp.
   - Perform a silent install of IBM Rescue and Recovery without a reboot at the end.
   - Start IBM Rescue and Recovery so that a base backup can be performed.
   - After the service is started, set up the environment to create an ISO image of the RRE Rescue CD (this is normally performed as part of a reboot).
   - Create the ISO image.
   - Create the base backup and reboot the system.
5. Modify the INSTALL.CMD code. The following represents the code for INSTALL.CMD:

```
:: Copy custom TVT.txt here
copy tvt.txt "c:\RRTemp\program files\IBM\IBM Rapid Restore Ultra"
:: Install using the MSI with no reboot (Remove "REBOOT="R"" to force a reboot)
start /WAIT msiexec /i "c:\RRTemp\IBM Rescue and Recovery with Rapid
 Restore.msi" /qn REBOOT="R"
:: Start the service. This is needed to create a base backup.
start /WAIT net start "IBM Rapid Restore Ultra Service"
:: Make an ISO file here - ISO will reside in c:\IBMTOOLS\rrcd
```

   Note: You do not need to set up the environment if the system is rebooted.

```
:: Set up the environment
set PATH=%PATH%;%SystemDrive%\IBMTOOLS\Python22
set PATHEXT=%PATHEXT%;.PYW;.PYO;.PYC;.PY
set TCL_LIBRARY=%SystemDrive%\IBMTOOLS\Python22\tcl\tcl8.4
set TK_LIBRARY=%SystemDrive%\IBMTOOLS\Python22\tcl\tk8.4
set PYTHONCASEOK=1
set RRU=c:\Program Files\IBM\IBM Rapid Restore Ultra\
set PYTHONPATH=C:\IBMTOOLS\utils\support;C:\IBMTOOLS\utils\logger
:: The next line will create the ISO silently and not burn it
c:\IBMTOOLS\Python22\python c:\IBMTOOLS\utils\spi\mkspiim.pyc /scripted
:: Take the base backup... service must be started
c:
cd "c:\Program Files\IBM\IBM Rapid Restore Ultra"
RRUcmd.exe backup location=L name=Base level=0
:: Reboot the system
c:\IBMTOOLS\Utils\bmgr32.exe /R
```

Customization

Assume that you have deployed Rescue and Recovery in your environment and now you realize you would like to change the following things with Rescue and Recovery :

- You would like more than 4 incremental backups and would like to change it to 10.
- The backup time of 1:59 p.m. interferes in some way with your environment. You would like to change the time to 10:24 a.m.
- You would like to allow all users on your systems to access the Rapid Restore 4.0 user interface.

- You would like to yield the system to other processes during a scheduled backup. Your evaluation after experimentation determines that the proper value of `Yield=` in your environment should be `2` instead of the standard value of `0`.

To do this on multiple machines:

1. Create a mod file called UPDATE.MOD (using a text editor) with the following contents:

```
[RapidRestoreUltra] MaxNumberOfIncrementalBackups=10
[RapidRestoreUltra] ScheduleHour=10
[RapidRestoreUltra] ScheduleMinute=24
[RapidRestoreUltra] GUIGroup=
[RapidRestoreUltra] Yield=2
```

2. You can then create a short INSTALL.CMD file and using a systems management tool of your choice push the INSTALL.CMD and UPDATE.MOD files to your target systems. After the systems run INSTALL.CMD the updates will be effective. The contents of INSTALL.CMD are as follows:

```
:: Merge the changes into TVT.TXT
"%RRU%cfgmod.exe" "%RRU%tvt.txt" update.mod
:: Reset the scheduler to adopt the new scheduled backup time without a
reboot
"%RRU%reloadsched.exe"
```

Password considerations

IBM Rescue and Recovery has an option that allows you to disable Windows Password Persistence in case you want a separate Pre Desktop Area (PDA) password.

Then you preload the PDA, you do not set a password. The first time a user changes the password you can ask them if they want to set a PDA password per above. If they download and install the PDA area separately, the install program can prompt them to set a password after the install.

When the IT administrator is setting up the system for the user, they will be logged in as Administrator. If they set up a new user account (either Administrator or limited user) the administrator will be offered the opportunity to set a PDA password, or synchronize the new user's password with the PDA.

The IT administrator may choose to allow the new user full access to the PDA area by synchronizing the passwords. If the user has limited access to the system, they will not be offered the option to synchronize when they change the password. The limited user can still change the PDA password by booting to it and choosing to change the password.)

The administrator may also choose to set a different password in which case the limited user would not have access to the PDA area

The following applications will be created to allow password management. These applications will be available under the customers primary operating system, and under the pre-boot operating system:

- password.pyc /s [[/p < password>] /n <new password>] [/a <hint text>]
- password.pyc /v [/p <password>]
- password.pyc /a
- Password configuration utility

Password configuration utility This application can be run in three modes a command line interface, a graphical UI, and a library api. The command line interface is out lined below.

Variable	Description
/s	Set the password used with /n, and optionally /p. If /s is provided by itself, a UI will open asking for the additional information
/p	The password that is currently set
/n	The new password
/v	Verify a password (This is used to log in) If /v is provided by itself, an you will be prompted for the additional information. After second try, the /v option will print the hint to stdout.
/c	Check to see if the password has already been entered correctly. A return code of 0 return means that the password was entered correctly. A return code of 151 means that the password has not been entered correctly
/a	Retrieve or set the hint. If /a is supplied without /s, the hint is returned to stdout.
/?	Provides help information. If /s is provided without /a any current hint will be cleared when the new password is set.
//help	Will return help information

Updating

Now assume that you need to make a major change to your system, such as a service pack update to Windows. Before you install the service pack, you would like to force an incremental backup on the system and identify that backup by name.

1. Create a file FORCE_BU.CMD and push it down to your target systems.
2. After the file FORCE_BU.CMD is on the target system, launch it.

The contents of FORCE_BU.CMD are:

```
:: Force a backup now
"%RRU%rrucmd" backup location=L name="Backup Before XP-SP2 Update"
```

Enabling the Rescue and Recovery desktop

After realizing the benefits of Rescue and Recovery for a period of time, you want to benefit from the Rescue and Recovery environment. For demonstration purposes, a sample UPDATE_RRE.CMD script is provided in the following section that will extract the control file for the Rescue and Recovery environment, which you can edit and then put back into the Rescue and Recovery environment using IBMRRUTIL.EXE. See “Using IBMRRUTIL.EXE” on page 27 for more information.

To modify the desktop of the Rescue and Recovery environment, the UPDATE_RRE.CMD script demonstrates several processes:

- Use IBMRRUTIL.EXE to get a file from the Rescue and Recovery environment. The files to be extracted from the Rescue and Recovery environment are defined by the file GETLIST.TXT.
- Create a directory structure to put files back into the Rescue and Recovery environment after finishing.
- Make a copy of the file for safe keeping and then edit it.

In this example, you want to change the home page that is opened when an end user clicks on the **Open Browser** button in the Rescue and Recovery environment. This example will open the Web page `http://www.ibm.com/thinkvantage`.

To make the change, when Notepad opens with PEACCESSIBMEN.INI,

1. Change the line:

   ```
   button13 = 8, "Open browser", Internet.bmp, 1, 1, 0,
   %sysdrive%\Preboot\Opera\Opera.EXE, http://www.pc.ibm.com/cgi-
   bin/access_IBM.cgi?version=4&link=gen_support&country=__
   COUNTRY__&language=__LANGUAGE__
   ```

   TO

   ```
   button13 = 8, "Open browser", Internet.bmp, 1, 1, 0,
   %sysdrive%\Preboot\Opera\Opera.EXE,
    http://www.ibm.com/thinkvantage
   ```

2. Put the new version into the directory structure for placing files into the Rescue and Recovery environment. For details, refer to "Using IBMRRUTIL.EXE" on page 27.
3. Reboot the system into the Rescue and Recovery environment.
4. You have done some analysis and determined that there are files that you must get backed up and there are other files that do not need to be backed up since they reside on the server and can be obtained after a system restore. To do this you would create a custom set of IBMINCLD and IBMEXCLD files. These files would be placed in a directory with NSF.CMD, which copies these files into the proper location. In addition:

   NSF.CMD:

   ```
   copy ibmincld "%RRU%"
   copy ibmexcld "%RRU%"
   ```

   IBMEXCLD:

   ```
   .nsf
   ```

Table 7. UPDATE_RRE.CMD script

```
@ECHO OFF
::Obtain the PEAccessIBMen.ini file from the RRE
c:\RRDeployGuide\IBMRRUTIL\ibmrrutil -g getlist.txt
c:\RRDeployGuide\GuideExample\RREOriginal
:: Make a directory to put the edited file for import back into the RRE
md c:\RRDeployGuide\GuideExample\put\preboot\usrintfc
:: Open the file with notepad and edit it.
ECHO.
ECHO Edit the file
c:\RRDeployGuide\GuideExample\RREOriginal\PEAccessIBMen.ini

File will open automatically

pause
:: Make a copy of original file
copy
c:\RRDeployGuide\GuideExample\RREOriginal\preboot\usrintfc\PEAccessIBMen.ini
c:\RRDeployGuide\GuideExample\RREOriginal\preboot\usrintfc\
PEAccessIBMen.original.ini
notepad
c:\RRDeployGuide\GuideExample\RREOriginal\preboot\usrintfc\PEAccessIBMen.ini
pause
copy c:\RRDeployGuide\GuideExample\RREOriginal\preboot\usrintfc\
PEAccessIBMen.ini c:\RRDeployGuide\GuideExample\put\preboot\usrintfc
:: Place the updated version of the PEAccessIBMen into the RRE
c:\RRDeployGuide\IBMRRUTIL\ibmrrutil -p c:\RRDeployGuide\GuideExample\put
ECHO.
ECHO Reboot to the RRE to see the change
pause
c:\IBMTOOLS\UTILS\bmgr32.exe /bw /r

Create GETLIST.TXT:

\preboot\usrintfc\PEAccessIBMen.ini
```

Installation of IBM Rescue and Recovery on non-IBM computers

To install Rescue and Recovery, eight free sectors must be available in the Master Boot Record on the hard disk. Rescue and Recovery uses a custom Boot Manager in order to enter into the Recovery area.

Some OEM manufacturers store pointers to their product recovery code in the Master Boot Record sector. OEM product recovery code may interfere with the Rescue and Recovery Boot Manager installation.

Consider the following scenarios and best practices to ensure Rescue and Recovery provides the desired functions and features:

Best practices for hard drive setup: Scenario 1

This scenario covers new image deployments that include Rescue and Recovery. If deploying Rescue and Recovery to existing OEM clients that contain OEM product recovery code, run the following test to determine if the OEM product recovery code interferes with Rescue and Recovery:

1. Set up a test client with the image that contains the OEM product recovery code.
2. Install Rescue and Recovery. If eight free sectors in the MBR do not exist as a result of the OEM product recovery code, you will see the following error message:

   ```
   Error 1722. There is a problem with this Windows
   ```

```
Installer package. A program run as part of the
setup did not finish as expected. Contact your
personnel or package vendor.
```

If you are using an OEM image for the base OS, ensure that the Master Boot Record does not contain the product recovery data. You can do this in the following way:

Attention: Running the following command will erase the entire contents of the target hard disk drive. After running, you will be unable to recover any data from the target hard disk drive.

1. Use CLEANDRIVE.EXE available from `http://www.ibm.com/support/us` to ensure all sectors are cleared from the MBR on the hard disk drive that you plan to use to create your base image.
2. Package the image according to your procedures for deployment.

Best practices for hard drive setup: Scenario 2

Deploying Rescue and Recovery deployment on existing clients requires some effort and planning.

If you receive Error 1722 and need to create eight free sectors, call the IBM help desk to report the error and obtain further instructions.

Creating a bootable IBM Rescue and Recovery CD

Rescue and Recovery builds and burns the rescue media CD from the current service area contents, rather than from a pre-assembled ISO image. However, if an appropriate ISO image is already present, because it was preloaded or because it had been built before, that image will be used to burn the CD, rather than to create a new one.

Because of the resources involved, only one instance of the CD burning application may be running at any given time. If it is running, attempting to start a second instance will produce an error message and the second instance will abort. In addition, due to the nature of accessing protected areas of the hard drive, only administrators can create the ISO; however, a limited end user can burn the ISO to a CD. See below for information on how to pre-create the ISO image of the Rescue and Recovery media CD.

- minint
- preboot
- win51
- win51ip
- win51ip.sp1
- scrrec.ver

Note: If you create a new ISO image, you must have at least 400 MB of free space available on the system drive in order to copy the directory trees and build the ISO. Moving around this much data is HDD-intensive, and might take 15 or more minutes on some computers.

Creating the recovery ISO file and burning to CD a sample script file: Prepare the following code:

```
:: Make an ISO file here - ISO will reside in c:\IBMTOOLS\rrcd
```

Note: The following seven lines of code (in bold font) are needed only if the system is not rebooted after install.

```
:: Set up the environment
set PATH=%PATH%;%SystemDrive%\IBMTOOLS\Python22
set PATHEXT=%PATHEXT%;.PYW;.PYO;.PYC;.PY
set TCL_LIBRARY=%SystemDrive%\IBMTOOLS\Python22\tcl\tcl8.4
set TK_LIBRARY=%SystemDrive%\IBMTOOLS\Python22\tcl\tk8.4
set PYTHONCASEOK=1
set RRU=c:\Program Files\IBM\IBM Rapid Restore Ultra\
set PYTHONPATH=C:\IBMTOOLS\utils\support;C:\IBMTOOLS\utils\logger
:: The next line will create the ISO silently and not burn it
c:\IBMTOOLS\Python22\python c:\IBMTOOLS\utils\spi\mkspiim.pyc /scripted
:: The next line will create the ISO with user interaction and not burn it
:: c:\IBMTOOLS\Python22\python c:\IBMTOOLS\utils\spi\mkspiim.pyc
/noburn
```

Installing IBM Rescue and Recovery into a type 12 service partition

This information is TBD.

Chapter 9. Issues, conflicts, and limitations

To get the latest information regarding the Rescue and Recovery program, visit www.ibm.com/pc/support. To view Hints & Tips associated with the Rescue and Recovery program, do the following:

1. Click **Hints & Tips**.
2. In the **Brand** field, use the drop-down menu to select **ThinkVantage Technologies**.
3. In the **Family** field, use the drop-down menu to select **IBM Rescue and Restore**; then click **Continue**.

Changing the system board

If you need to change a failed motherboard and you are using UUID protection as soon as you complete the motherboard replacement, perform a backup. This will capture the new UUID and propagate it to the original backups.

Backing up encrypted files

Rescue and Recovery does backup both Windows EFS and IBM Client Security Software File and Folder Encryption (FFE) files in their encrypted form.

If you use FFE, you should ensure that the database that FFE uses to keep track of what folders are protected by FFE also has a .NSF extension. To ensure that these files are always backed up, include the entry C:\PROGRAM FILES\IBM\SECURITY*FLT.NSF in the IBMINCLD file. This ensures that the database file for FFE is backed up. Loss of this file will prevent access to the FFE protected files and folders.

Single File Restore of encrypted files (FFE and EFS) does have some limitations in the Rescue and Recovery environment. When an encrypted file can be restored, using Single File Restore is best summarized in this table below. Note that during full restore of the system, all encrypted files are restored with no issues.

	Windows	**Rescue and Recovery Environment**
FFE	No	Yes
EFS	Yes (logged on user only)	No

Limitations

There are a number of limitations that administrators and end users need to note.

Compatibility with previous versions

IBM Rapid Restore Ultra 3.0 and prior versions are not compatible with the Rescue and Recovery program. If you install the Rescue and Recovery program and previous versions of Rapid Restore Ultra are installed, then the Rescue and Recovery program prompts you to uninstall any previous versions of Rapid Restore Ultra, including all backups made by prior versions of the program during installation of the Rescue and Recovery program.

Drives and drive letters

When you are transferring files, the drive letters used for the location and destination directories might not represent drive letters typically used in your Windows environment. One way of locating the drive that is known as your C drive is to expand each directory and look for folders commonly associated with the C drive such as a My Documents folder or a Documents and Settings folder.

DVD-RAM disks and IBM and recovery

The Rescue and Recovery workspace does not support booting from a DVD-RAM disk as an external device. As a result, do not create rescue media, product recovery CDs, backups, or archive backups using DVD-RAM media if you intend to boot from an external device. Other DVD formats are supported.

IBM Rescue and Recovery installed on non-primary hard disk

If you installed the Rescue and Recovery program on a hard disk drive, other than your primary drive, and the alternate drive is damaged, then you must reinstall Rescue and Recovery program if you want to continue performing rescue and recovery operations from the alternate drive. It is a good idea to perform a backup operation after the program is reinstalled.

Large backup files and ″Not responding″ messages

If you are transferring large files, you might see a ″Not responding″ message on a previous IBM Rapid Restore file transfer window. However, the file transfer operation is still underway and can be verified by the progress bar indicated on the window where the file transfer operation was started.

Pointing device functions

All pointing devices will operate as a two-button device within the Rescue and Recovery workspace. For example, just as the third button of a three-button mouse is not supported in the Rescue and Recovery workspace the scrolling capability of an IBM ScrollPoint® mouse is not supported.

Restoring while the IBM Rescue and Recovery help system is open

If you have the IBM Rescue and Recovery program and help system open while attempting to perform a ″Backup now″ backup, the program will close and you will receive an error message. However, the backup operation is underway and the error message should be closed. To check on the progress of your backup, re-open the Rescue and Recovery program. The progress will be indicated on the screen.

Screen flashes when IBM Rescue and Recovery opens

Depending on the video card installed on your computer, there might be a series of flashes when the Rescue and Recovery workspace is opened.

USB memory key and startup

You can use a USB memory key to perform read/write functions within the Rescue and Recovery workspace; however, you cannot boot from a USB memory key.

Wireless and dial-up connectivity

The Rescue and Recovery workspace has no wireless or dial-up capability. Only wired Ethernet is supported.

USB memory key inserted during installation

If you install Windows 2000 and there is a USB memory key attached to the computer at the time of installation, then a TXTSETUP.SIF is inserted in the C drive root directory. If you attempt to enter the Rescue and Recovery workspace with the TXTSETUP.SIF in the C drive root directory, your computer will not boot into the Rescue and Recovery workspace successfully. To prevent this problem, either detach the USB memory key before installing Windows 2000 or delete or rename the TXTSETUP.SIF file in the C root directory before entering the Rescue and Recovery environment.

Video RAM and performance

The video RAM that came with your computer is typically set to store a default capacity of 8MB. Having a video RAM lower than 8MB might adversely affect performance of the Rescue and Recovery program.

Appendix A. Installation command-line switches

The Microsoft® Windows® Installer (hereafter referred to as ″Installer″) provides several administrator functions through command-line switches and parameters.

Administrative installation procedure and command-line parameters

The Installer can perform an administrative installation of an application or product to a network for use by a workgroup or for customization. For the Rescue and Recovery installation package, an administrative installation unpacks the installation source files to a specified location.

- To run an administrative installation execute the setup package from the command line using the /a parameter:

  ```
  Setup.exe /a
  ```

An administrative installation presents a wizard that prompts the administrative user to specify the locations for unpacking the setup files. The default extract location is C:\. You can choose a new location which may include drives other than C:\ (other local drives, mapped network drives, etc.). You can also create new directories during this step.

- To run an administrative installation silently, you can set the public property TARGETDIR on the command line to specify the extract location:

  ```
  Setup.exe /s /v"/qn TARGETDIR=F:\IBMRR"
  ```

  Or

  ```
  msiexec.exe /i "IBM Rescue and Recovery.msi" /qn TARGERDIR=F:\IBMRR
  ```

After completing an administrative installation, the Administrator can customize the source files, such as adding settings to TVT.TXT.

Using MSIEXEC.EXE: To install from the unpacked source after making customizations, the user calls MSIEXEC.EXE from the command line, passing the name of the unpacked *.MSI file. MSIEXEC.EXE is the executable program of the Installer used to interpret installation packages and install products on target systems.

```
msiexec /i "C:\<WindowsFolder>\Profiles\<UserName>\
Personal\MySetups\<project name>\<product configuration>\<release name>\
DiskImages\Disk1\<product name>.msi"
```

Note: Enter the command line above as a single line with no spaces following the slashes.

The following table describes the available command line parameters that can be used with MSIEXEC.EXE and and examples of how to use it.

Parameter	Description

/I <package>
or
<product code>
	Use this format to install the product:
	`Othello:msiexec /i "C:\<WindowsFolder>\Profiles\`
	`<UserName>\Personal\MySetups`
	`\Othello\Trial Version\`
	`Release\DiskImages\Disk1\`
	`Othello Beta.msi"`
	
	Product Code refers to the GUID that is automatically generated in the Product Code property of your product's project view.

/a <package>	The `/a` option allows users with administrator privileges to install a product onto the network.
/x <package> or <product code>	The `/x` option uninstalls a product.
/L [i|w|e|a|r|u|c|m|p|v|+] <log file>	Building with the /L option specifies the path to the log file; these flags indicate which information to record in the log file: • `i` logs status messages • `w` logs non-fatal warning messages • `e` logs any error messages • `a` logs the commencement of action sequences • `r` logs action-specific records • `u` logs user requests • `c` logs initial user interface parameters • `m` logs out-of-memory messages • `p` logs terminal settings • `v` logs the verbose output setting • `+` appends to an existing file • `*` is a wildcard character that allows you to log all information (excluding the verbose output setting)
/q [n|b|r|f]	The `/q` option is used to set the user interface level in conjunction with the following flags: • `q` or qn creates no user interface • `qb` creates a basic user interface The user interface settings below display a modal dialog box at the end of installation: • `qr` displays a reduced user interface • `qf` displays a full user interface • `qn+` displays no user interface • `qb+` displays a basic user interface
/? or /h	Either command displays Windows Installer copyright information

Parameter	Description

TRANSFORMS	Use the **TRANSFORMS** command line parameter to specify any transforms that you would like applied to your base package. Your transform command line call might look something like this:
	`msiexec /i "C:\<WindowsFolder>\`
	`Profiles\<UserName>\Personal`
	`\MySetups\`
	`Your Project Name\Trial Version\`
	`My Release-1`
	`\DiskImages\Disk1\`
	`ProductName.msi" TRANSFORMS="New Transform 1.mst"`
	
	You can separate multiple transforms with a semicolon. Because of this, it is recommended that you do not use semicolons in the name of your transform, as the Windows Installer service will interpret those incorrectly.

Properties	All public properties can be set or modified from the command line. Public properties are distinguished from private properties by the fact that they are in all capital letters. For example, `COMPANYNAME` is a public property.
	
	To set a property from the command line, use the following syntax:
	`PROPERTY=VALUE`
	
	If you wanted to change the value of `COMPANYNAME`, you would enter the following:
	`msiexec /i "C:\<WindowsFolder>\`
	`Profiles\<UserName>\Personal`
	`\`
	`MySetups\Your Project Name\`
	`Trial Version\My Release-1`
	`\`
	`DiskImages\Disk1\ProductName.msi"`
	`COMPANYNAME="InstallShield"`

Appendix B. TVT.TXT settings and values

The default values identified below are suggested settings. The values might be different for different configurations (for example, Preload, Web Download, OEM version). The following installation configuration settings are available:

Setting	Values
AccessFile (see GUIGroup)	<*filename*>, where <*filename*> is the fully qualified path to a file that holds the names of Windows local groups (not domain groups) that are permitted to perform Rescue and Recovery operations. If blank or missing, all users who can log onto the computer can launch the GUI and perform command line operations. By default the file is blank.
BackupPartition	0 = First partition on a specified drive 1 = Second partition on a specified drive 2 = Third partition on a specified drive 3 = Fourth partition on a specified drive Drives are specified in the following sections: [BackupDisk] = local hard disk drive [SecondDisk] = second local hard disk drive [USBDisk] = USB hard disk drive **Note:** Partitions must already exist. If not set, the user will be prompted to establish the partition (if there is more than one partition on the destination drive when the destination drive is selected in the user interface).
BatteryPercentRequired	Range is from 0 to 100. the default is 100.
CPUPriority	*n* where *n* = 1 to 5; 1 is the lowest priority and 5 is highest priority. The default is 3.
DisableArchive	0 = enable archive 1 = hide archive The default is 0.

Setting	Values
DisableBackupLocation	0 = enable all destination 0x01 = disable Local destination 0x02 = disable Cd/DVD drive 0x08 = disable USB/ HDD 0x10 = disable Network 0x20 = disable second HDD 1 = hide archive These can be combined to grey out multiple locations. For example, a value of 0x0A would disable CD/DVD and USB HDD, value of 0x38 would disable USB HDD, Network, and 2nd HDD. To only enable backup to local hard drive, you can use 0x3A (or even 0xFE))
DisableBootDisc	0 = always create bootable CD when creating CD/DVD backups 1 = don't create bootable CD The Disable Boot Disc function is only for Backups not for Archive
DisablePreferences	0 = enable set preferences 1 = hide set preferences The default is 0.
DisableRestore	0 = enable restore 1 = hide restore The default is 0.
DisableSFR	0 = enable single file restore 1 = hide single file restore The default is 0
EncryptBackupData	0 = do not encrypt backup1 = encrypt backup (default)
Exclude (see Include)	0 = do not apply GUIEXCLD.TXT 1 = apply GUIEXCLD.TXT.txt **Notes:** 1. Exclude and select files can be defined prior to installation and be applied during the installation process. 2. Exclude and Include cannot both be 1
GUIGroup (see AccessFile)	*<group>*, where *<group>* is a Windows local group (not a domain group) that is permitted to perform Rescue and Recovery operations. The list of privileged groups is stored in a file that is defined by the AccessFile entry.

Setting	Values
HideAdminBackups	0 = Show administrator backups in list. 1 = Hide administrator backups. The default is 0.
HideBaseFromDelete	0 = Show base backup on Delete Backups dialog. 1 = Hide base backup on Delete Backups dialog. The default is 0.
HideDeleteButton	0 = Enable Delete button on Delete Backups dialog 1 = Disable Delete button on Delete Backups dialog The default is 0.
HideGUI	0 = show the GUI to authorized users 1 = hide the GUI from all users
HideLocationNotFoundMessage	0 = show dialog message 1 = hide dialog message The default is 0.
HideMissedBackupMessages	0 = hide dialog box 1 = show dialog box The default is 1.
HideNoBatteryMessage	0 = display message 1 = hide message The default is 1
HidePasswordPersistence	0 = hide GUI 1 = show GUI The default is 1.
HidePasswordProtect	0 = Show password protect checkbox. 1 = Hide password protect check box. The default is 0.
Include (see Exclude)	0 = do not apply GUIINCLD.TXT 1 = apply GUIINCLD.TXT and display the option to set include files and folders **Notes:** 1. Exclude and select files can be defined prior to installation and be applied during the installation process. 2. Exclude and Include cannot both be 1.

Setting	Values
LocalBackup2Location	*x*:*foldername* (where *x* = drive letter and *foldername* = any fully qualified folder name.) The default is this: <1st partition letter on the second drive>:\IBMBackupData **Notes:** 1. Because the drive letter can change over time, Rescue and Recovery will associate the drive letter to a partition at the time of install, and then use the partition information rather than the drive letter. 2. This is the location filed of TaskParameters entry.
MaxBackupSize	*x*, where *x* is the size in GB. This value will not prevent a backup from exceeding this threshold. If the threshold is exceeded, however, the user will be warned about the file size the next time an ″On Demand″ backup is taken.
MaxNumberOf IncrementalBackups	default = 5, min = 2, max = 32
NetworkUNCPath	network share using the format: \\<computername>\<share folder> There is no default. **Note:** This location will not be protected by the File Filter Driver.
NetworkUNCPath	<*server share name*>, for example, \\MYSERVER\SHARE\FOLDER
NumMinutes	*x*, where the task runs after *x* minutes have passed.
PasswordRequired	0 = no password required to open the Rescue and Recovery environment. 1 = password required to open the Rescue and Recovery environment.
PDAPreRestore	*cmd*, where *cmd* is a fully qualified path to the program to run in the Rescue and Recovery environment prior to a restore operation.
PDAPreRestore *n*	*cmd*, where *cmd* is a fully qualified path to the program to run in the Rescue and Recovery environment prior to a restore operation.
PDAPreRestoreParameters	Parameters to be used in the PDARestore program.
PDAPreRestoreParameters *n*	Parameters to be used in the PDARestore program.
PDAPreRestoreShow	0 = hide task 1 = show task
PDAPreRestoreShow *n*	0 = hide task 1 = show task
PDAPostRestore	*cmd*, where *cmd* is a fully qualified path to the program to run in the Rescue and Recovery environment prior to a restore operation.
PDAPostRestore *n*	*cmd*, where *cmd* is a fully qualified path to the program to run in the Rescue and Recovery environment prior to a restore operation.
PDAPostRestoreParameters	Parameters to be used in the PDARestore program.

Setting	Values
PDAPostRestoreParameters *n*	Parameters to be used in the PDARestore program.
PDAPostRestoreShow	0 = hide task 1 = show task
PDAPostRestoreShow *n*	0 = hide task 1 = show task
Post (see PostParameters)	*cmd*, where *cmd* is a fully qualified path to an executable file to run after to the primary task.
Post (see PostParameters) *n*	*cmd*, where *cmd* is a fully qualified path to an executable file to run after to the primary task. **Note:** This is for Backup only
PostParameters (see Post)	*cmd*, where *cmd* is a fully qualified path to an executable file to run after to the primary task. This is for Backup only.
PostParameters *n* (see Post)	*parms*, where *parms* are parameters to be used in the post-task
	parms, where *parms* are parameters to be used in the post-task. **Note:** This is for Backup only
PostRestore	*cmd*, where *cmd* is a fully qualified path to the program to run in Windows after a restore operation has been completed
PostRestore *n*	*cmd*, where *cmd* is a fully qualified path to the program to run in Windows after a restore operation has been completed
PostRestoreParameters	Parameters to be used in the PostRestore program
PostRestoreParameters *n*	Parameters to be used in the PostRestore program
PostRestoreShow	0 = hide restore-task 1 = show restore-task
PostRestoreShow *n*	0 = hide restore-task 1 = show restore-task
PostShow	0 = hide post-task 1 = show post-task The default is 0.
PostShow *n*	0 = hide post-task 1 = show post-task The default is 0. **Note:** This is for Backup only
Pre (see PreParameters)	*cmd*, where *cmd* is a fully qualified path to an executable file to run prior to the primary task.
PreParameters (see Pre)	parms, where *parms* are parameters to be used in the pre-task

Setting	Values
PreShow	0 = hide pre-task 1 = show pre-task The default is 1.
PreWinRestore	cmd, where cmd is a fully qualified path to theprogram to run in Windows prior to a restore operation.
PreWinRestore *n*	cmd, where cmd is a fully qualified path to theprogram to run in Windows prior to a restore operation.
PreWinRestoreParameters	Parameters to be used in the PreWinRestore program
PreWinRestoreParameters *n*	Parameters to be used in the PreWinRestore program
PreWinRestoreShow	0 = hide post-task 1 = show post-task
PreWinRestoreShow *n*	0 = hide post-task 1 = show post-task
RunBaseBackup	0 = don't perform the base backup 1 = perform base backup The default is 0.
ScheduleDayOfThe-Month	*x*, where *x* = 1 to 28 or 35 for monthly backups only. 35 = the last day of the month
ScheduleDayOfTheWeek	For weekly backups only 0 = Sunday 1 = Monday 2 = Tuesday 3 = Wednesday 4 = Thursday 5 = Friday 6 = Saturday The default is 0 (Sunday).
ScheduleFrequency	0 = not scheduled 1 = daily 2 = weekly 3 = monthly The default is 2 (weekly).
ScheduleHour	*x*, where *x* = 0 to 23 and 0 is 12:00 AM, 12 is noon, and 23 is 11:00 PM. The default is 0.

Setting	Values
ScheduleMinute	*x*, where *x* = 0 to 59 (which increments) represent the minute within the hour to start the incremental backup. The default is 0.
ScheduleWakeFor-Backup	0 = do not wake the computer for scheduled backups 1 = wake the computer, if it is a desktop for scheduled backups, but do not wake notebook computers 2 = wake the computer regardless of whether it is a desktop or notebook The default is 2. **Note:** If a notebook wakes for a backup, but ac power is not detected, it will return to suspend/hibernate before a backup operation starts.
ScheduleMode	*x*, where *x* is a bit mask with a value of: • 0 = no schedule • 0x01 = every minute • 0x04 = every week • 0x08 = every month • 0x10 = every time the service starts (normally every machine boot) • 0x20 = the machine wakes from suspend/hibernate • 0x40 = USB HDD becomes attached • 0x80 = network becomes attached This parameter is automatically updated when the user changes values in the GUI. If the ScheduleFrequency value is changed by either manual changes to the TVT.TXT file or scripting, reloadsched will update this parameter. **Note:** The `USB HDD becomes attached` or `network becomes attached` bits do not need to be set for automatic synchronization of backups from local hard drive to USB HDD or network.)
SkipLockedFiles	0 = display dialog box when a corrupt file is encountered 1 = always skip corrupt files
Task	*cmd*, where *cmd* is a fully qualified path to the program to run as the primary task.
TaskParameter	*parms* are parameters to be used in the task.
TaskShow	0 = hide task 1 = show task The default is 1.
UUIDMatchRequired	0 = Computer UUID match is not required. 1 = Computer UUID match is required. **Note:** Backups that have been captured when the UUIDMatchRequired was set to 1 will continue to require a UUID match, even if this setting is changed later.

Setting	Values
Yield	*n* where *n* = 0 to 8; 0 means that Rescue and Recovery does not yield and 8 means that Rescue and Recovery produces the maximum yield value. **Note:** A higher yield will incrementally slow down backup performance and provide better interactive performance. The default is 0.

After Rescue and Recovery is installed, the following configurations can be altered in the TVT.TXT file that is located in the installed directory. They will be initialized with the values assigned during installation. See previous section for descriptions of these parameters.

TVT.txt Backup and Restore

In order to support silent installation, the Rescue and Recovery Backup and Restore configuration is defined by an external file (*tvt.txt*) that is edited before installation. The tvt.txt file will follow the standard Windows .ini file format, with the data organized by sections denoted by [] and an entry per line of the format "setting=value". IBM Rescue and Recovery will use the product name for the section header (such as Rapid Restore Ultra). In addition, the include/exclude filter file can be defined before installation and be applied during the installation process.

If the IT administrator would like to customize their backups with settings, they should edit the txt.txt file in the install directory. The best time to do this is either before installing Rescue and Recovery or after it is installed and before the first backup. A tvt.txt file is included in every backup location. Before the first backup, there is only one tvt.txt file. If this approach is used, all the backups will have all of the changes without having any tvt.txt version and synchronization problems. Sometimes the tvt.txt file must be edited after a backup. In this case there are two ways to update all the tvt.txt files with the latest changes. The IT administrator can either copy the install directory tvt.txt file to all of the backup folders or start another backup and the process will automatically synchronize all of the tvt.txt versions with the install directory version. The second method is preferable.

Scheduling backups and associated tasks

The scheduler is not designed to be specific to Rescue and Recovery. However, the configuration is stored in the same TVT.TXT file. When Rescue and Recovery is installed, it will populate the scheduler with the appropriate settings.

Here is a description of the structure for the scheduler:
- Location: Install folder
- Entry for each scheduled ″job″
- Script to run
- Named pipe to be used for progress notifications (optional)
- Schedule information (monthly, weekly, daily, (weekday, weekend - multiple schedules (e.g. Tuesdays and Fridays) can be supported by creating two schedules))
- Variables to pass to functions

Consider the following example: For the case of Rescue and Recovery performing incremental backup on schedule, with callbacks before and after the backup, the following entry instructs the application accordingly:

```
[SCHEDULER]
Task1=RapidRestoreUltra
[RapidRestoreUltra]
Task="c:\program files\ibm\rapid restore ultra\
rrucmd.exebackup.bat"
TaskParameters=BACKUP location=L name="Scheduled"
ScheduleFrequency=2
ScheduleDayOfTheMonth=31
ScheduleDayOfTheWeek=2
ScheduleHour=20
ScheduleMinute=0
ScheduleWakeForBackup=0
Pre="c:\program files\antivirus\scan.exe"
Post="c:\program files\logger\log.bat"
```

Managing Different TVT.txt files

Since hard disk drives can have multiple partitions, the backup and restore program needs to know which partition will store the backup data. If a particular destination has multiple partitions,and backup operations will be scripted, the following setting needs to be configured prior to the backup operation. If the backup operation can be initiated by the user, you can ignore this section. For backups to the local hard drive, the configuration setting is found in the TVT.txt file in the [BackupDisk] section. (Backups to the second local hard drive use section [SecondDisk] and backups to the USB HDD would use section [USBDisk]: BackupPartition=x (in the range of 0 - 3, where 0 represents the first partition on the appropriate drive) Note: partitions must already exist. If not set, the user will be prompted, if there's more than one partition, when the appropriate destination is selected in the GUI For example: if it was desired to backup to the second partition on the USB HDD, then the TVT.TXT file entry would look like this: [USBDisk] BackupPartition=1

```
[USBDisk]
BackupPartition=1
```

Mapping a network drive for backups

The Map Network Drive function relies on the MAPDRV.INI file which is located in the C:\IBMTOOLS\UTILS\MND directory. All information is stored in the DriveInfo section.

The UNC entry contains the computername and share of the location you are attempting to attach to.

The NetPath entry is output from the mapdrv.exe contains the actual name which was used when making the connection.

User and Pwd entries - The username and password entries are encrypted.

The following is an example entry for mapping a network drive:

```
[DriveInfo]
```

```
UNC=\\server\share
NetPath=\\9.88.77.66\share
User=116226064151192077230149185054220105210064012092037082020 15...
Pwd=116226064151000000000149185054220105210064012092037082020 15...
```

For deployment, this file can be copied onto multiple computers that will use the same username and password. The UNC entry is overwritten by Rapid Restore Ultra based on a value in the TVT.TXT.

Setting up user accounts for network backups

When the RRUBACKUPS directory is created on the network share, the service makes it a read-only folder, and assigns it access rights so that *only* the account that created the folder has full control over the folder.

In order to complete a merge operation, MOVE permissions exist for the User account. If logged in with an account other than the account that created the folder initially (i.e., administrator), the merge process will fail.

Appendix C. Command line tools for IBM Rescue and Recovery

Rescue and Recovery features can also be invoked locally or remotely by corporate IT administrators through the command line interface. Configuration settings can be maintained via remote text file settings.

Rescue and Recovery Boot Manager control (BMGR32)

The boot manager interface command-line interface is BMGR32. It resides in the directory C:\IBMTOOLS\UTILS. The following table presents the switches and their results for BMGR32.

bmgr32 switch	Result
/B0	Boot to partition 0 (based on the order in the partition table)
/B1	Boot to partition 1
/B2	Boot to partition 2
/B3	Boot to partition 3
/BS	Boot to the IBM Service Partition
/BW	Boot to the Rescue and Recovery protected partition
/CFG<file>	Apply the configuration file parameters. (See the following section for details regarding the configuration file.)
/D<n>	Apply changes to disk n, where n is 0-based, (default: n=0)
/H0	Hide partition 0
/H1	Hide partition 1
/H2	Hide partition 2
/H3	Hide partition 3
/HS	Hide the IBM Service Partition
/P12	Hide the IBM Service Partition by setting partition type to 12
/INFO	Display HDD information
/M0	Rescue and Recovery environment is located in the Service Partition
/M1	Rescue and Recovery environment is located in the C:\PARTITION (dual boot Windows and Windows PE)
/M2	Rescue and Recovery environment is located in the Service Partition with DOS (dual boot Windows PE and DOS; IBM Preload Only)
/OEM	Computer is not an IBM Computer. This forces a second check for the F11 (default) key press after POST. This may be required for older IBM systems. This is also the default setting for the OEM version of Rescue and Recovery.
/IBM	System is an IBM Computer
/Q	silent
/V	verbose
/R	Reboot computer

bmgr32 switch	Result
/U0	Unhide partition 0
/U1	Unhide partition 1
/U2	Unhide partition 2
/U3	Unhide partition 3
/US	Unhide IBM service partition
/F<mbr>	Load the RRE master boot record program.
/U	Unload RRE master boot record program.
/?	List command line options.

RRUCMD

The primary Rescue and Recovery command line interface is RRUCMD. The command is located in the C:\PROGRAM FILES\IBM\IBM RAPID RESTORE ULTRA\ subdirectory. Refer to the following information to use the command line interface for Rescue and Recovery.

Syntax:

```
RRUcmd <command> <filter=filterfile> <location=<c>> [name=<abc> | level=<x>] [silent]
```

Command	Result
Backup	To initiate a normal backup operation (must include location and name parameters)
Restore	To initiate a normal restore operation (must include location and level)
List	To list files that are included in the backup level (must include location and level)
Basebackup	To initiate an alternative base backup (not to be used as a basis for incremental backups) (must include location, name, & level) (level must be > 99) (if another base backup with the same level already exists, it will be overwritten)
Sysprepbackup	Stages a backup operation in the PDA after the computer is rebooted. The primary use for this feature is to capture a sysprep'd backup.
Copy	Copy backups from one location to another (also known as archive) (must include location)
Delete	Delete backups (must include location)
filter=<filterfile>	Used only with **restore** command. It identifies what files and folders will be restored and does not alter other files.
Location=<c>	One or more of the following can be selected with the associated result. L for primary local hard drive U for USB HDD S for second local hard drive N for network C for CD/DVD Restore
name=<abc>	Where *abc* is the name of the backup

Command	Result
`level=<x>`	Where *x* is a number from 0 (for the base) to max number of incremental backups (only used with the restore option. For backup commands, the level=<x> command is only required if performing an administrator backup (equal to or greater than 100, for example). **Notes:** 1. To restore from the latest backup, do not provide this parameter. 2. All backup and restore features are routed through the service so that the appropriate sequencing can be maintained (e.g. callbacks are performed). The backup command is replaced with the command line options.)
`SFR /h /b /u /vsr`	File transfer and Rescue utility. / `/sr` launches to the Single File Restore view to get individual files from backups. `/h` displays list of command line options `/b` launches and sets backup as the source `/u` launches and sets "unbacked up files" as the source `/v` verbose debugging
`Reloadsched`	Applies schedule changes made to the tvt.txt file. If modifications to the schedule are performed, this command (or a reboot) must be performed to load the new schedule into the scheduler.

cfgmod *tvt.txt mod file* [/D]	Provides a method of updating the tvt.txt file using a script. The format of the mod file is one line per entry. Each entry includes a section number (delimited by [and]), (optionally) followed by a parameter name, (optionally) followed by "=", (optionally) followed by the value. For example, to adjust the backup schedule, the mod file entries could be:
	`[RapidRestoreUltra]ScheduleFrequency=1`
	`[RapidRestoreUltra]ScheduleHour=8`
	`[RapidRestoreUltra]ScheduleMinute=0`
	
	The optional /D parameter defines if the modification is to add or delete the entry. If /D is not provided, the entry is added. In this case, all fields in each entry must be provided for the update to be made. If the /D parameter is provided, the corresponding entry/section is deleted. The "=value" is not required to delete an entry. To delete an entire section, provide only the section number.
	
	The format of the boot manager configuration file is backward compatible with the previous version of boot manager. Any switch not shown below, is not supported. The file format is a text file with each entry is on one line.
	
	The entries are:
	• <PROMPT1> - This is the text that will appear on the F11 prompt
	• <KEY1=F11
	• <WAIT=40>

Command	Result
Boot Manager Utility	The boot manager command line interface is as follows: /B0 - Boot to partition 0 (based on the order in the partition table) /B1 - Boot to partition 1 /B2 - Boot to partition 2 /B3 - Boot to partition 3 /BS - Boot to the IBM Service Partition /BW - Boot to the PDA partition /BWIN – Reset request to boot to WinPE. Must be called prior to booting /CFG<file> - apply the config file parameters /D<n> - apply changes to disk n, where n is 0-based, (default: n=0)/H0 - Hide partition 0 /H1 - Hide partition 1 /H2 - Hide partition 2 /H3 - Hide partition 3 /HS - Hide the IBM Service Partition /P12 - Hide the IBM Service Partition by setting partition type to 12 /IBM - System is an IBM Computer /INFO - Display HDD information and verifies there's 8 free sectors /INFOP – Displays HDD information and verifies there's 16 free sectors /M0 - PDA is located in the Service Partition /M1 - PDA is located in the C:\ partition (dual boot Windows & WinPE) /M2 - PDA is located in the Service Partition with DOS (dual boot WinPE & DOS) /OEM - System is not an IBM Computer /PATCH<n> - Used for installation program only to set a variable that an MBR patch program can access /PATCHFILE<filename> - Used for installation program only – to install an MBR patch /PRTC – Used for installation program only - used to retrieve patch return code /Q - silent /V - verbose /R - reboot system /U0 - Unhide partition 0 /U1 - Unhide partition 1 /U2 - Unhide partition 2 /U3 - Unhide partition 3 /US - Unhide IBM Service Partition /F<mbr> - load PDA master boot record program /? - List command line options
Boot Manager Configuration File Format	The format of the boot manager configuration file is backward compatible with the previous version of boot manager. Any switch not show below is not supported. The file format is a text file with each entry is on a separate line. <PROMPT1=this is the text that will appear on F11 prompt> <KEY1=F11> <WAIT=40>

MAPDRV

The mapdrv command will invoke the GUI to map a network drive. The MAPDRV.EXE command can be found in the C:\IBMTOOLS\UTILS\MND directory. The map network drive interface supports the following switches:

Syntax:

```
mapdrv [switches]
```

Switch	Result
/rru	Reads and saves, UNC, encrypted UserID and encrypted Password in C:\IBMTOOLS\UTILS\MND\MAPDRV.INI file, prompts user if connection can not be made (unless /s is also specified)
/nodrive	Make network connection without assigning drive letter to the connection
/s	Silent. Do not prompt the user regardless of whether connection is made--only effective if used in conjunction with /rru Return codes: 0 = success, > 0 = failed

Sample Command:

```
C:\IBMTOOLS\UTILS\MND\mapdrv /rru
```

CFGMOD

CFGMOD provides a method of updating the TVT.TXT file via a script. The CFGMOD command can be found in the C:\PROGRAM FILES\IBM\IBM RAPID RESTORE ULTRA\ directory. If you modify the backup schedule this command must be followed by RELOADSCHED. This utility must be run with administrator privileges.

Syntax:

```
cfgmod <TVT.TXT> <mod file>
```

The format of the mod file requires one line per entry. Each entry includes a section number (delimited by [and]), followed by a parameter name, followed by ″=″, followed by the value. For example, to adjust the backup schedule, the mod file entries could be as follow:

```
[RapidRestoreUltra]ScheduleFrequency=1
[RapidRestoreUltra]ScheduleHour=8
[RapidRestoreUltra]ScheduleMinute=0
```

RELOADSCHED

Sample Command:

```
C:\Program Files\IBM\IBM Rapid Restore Ultra\reloadsched
```

This command reloads the scheduled settings that are defined in TVT.TXT. If you make changes to TVT.TXT for scheduling, you must perform this command to activate the changes.

Appendix D. User Tasks

Users may not be able to perform certain tasks, based upon user rights. The following tables outline basic task capability with the Limited User/User, Power User, and Administrator default OS user ID permissions. The tasks and capabilities differ by Windows operating system.

Windows XP

The following table presents the tasks that ″limited,″ ″power,″ and ″administrative″ users can perform in Rescue and Recovery.

Windows XP users can perform the following:	**Limited User**	**Power User**	**Administrator**
Create Rescue Media ISO	No	No	Yes (with command line provided below)
Create bootable CD media	Yes	Yes	Yes
Create USB HDD bootable media	No	No	Yes
Initiate backup	Yes	Yes	Yes
Initialize restore in Rescue and Recovery Environment (RRE)	Yes	Yes	Yes
Perform single-file restore in RRE	No (Windows) Yes (RRE)	No (Windows) Yes (RRE)	Yes
Set include and exclude in the Rescue and Recovery interface	Yes	Yes	Yes
Backup to a network drive	Yes	Yes	Yes
Schedule backups	Yes	Yes	Yes

Windows 2000

The following table presents the tasks that ″limited,″ ″power,″ and ″administrative″ users can perform in Rescue and Recovery.

Windows 2000 users can perform the following:	**Limited User**	**Power User**	**Administrator**
Create Rescue Media ISO	No	No	Yes (with command line provided below)
Create bootable CD media	Yes	Yes	Yes
Create USB HDD bootable media	No	No	Yes
Initiate backup	Yes	Yes	Yes
Initialize restore in Rescue and Recovery Environment (RRE)	Yes	Yes	Yes
Perform single-file restore in RRE	No (Windows) Yes (RRE)	No	Yes

Windows 2000 users can perform the following:	Limited User	Power User	Administrator
Set include and exclude in the Rescue and Recovery interface	Yes	Yes	Yes
Backup to a network drive	No	No	Yes
Schedule backups	Yes	Yes	Yes

Administrators can use the following command lines to create the Rescue Media ISO. These command lines will enable you to make the required ISO file and it will be automatically be placed in the C:\IBMTOOLS\RRCD directory:

```
:: This line will create the ISO silently and not burn it
c:\IBMTOOLS\Python22\python c:\IBMTOOLS\utils\spi\mkspiim.pyc
 /scripted
:: This line will create the ISO with user interaction and not burn it
c:\IBMTOOLS\Python22\python c:\IBMTOOLS\utils\spi\mkspiim.pyc
 /noburn
```

Appendix E. Antidote Delivery Manager Command Reference and Examples

A command line packaging tool is provide for the administrator to create messages, Also, Antidote Delivery Manager provides some special command functions to be used in the messages.

Antidote Delivery Manager Command Guide

The boot manager interface command-line interface is BMGR32. It resides in the directory c:\IBMTOOLS\UTILS. The following table presents the switches and their results for BMGR32.

Commands	Description
APKGMES [/KEY *keyfile*|/NEWKEY *keyfile*|/NOSIG] *message_directory message_name*	For APKGMES /KEY a message file will be created from the contents of *message_directory*. The directory must contain a file named GO.RRS. If the /KEY parameter is used, a signing key will be retrieved from keyfile.prv and the key in keyfile.pub must have been distributed to all clients that will process the message. By default, the key file "KEYFILE.PRV" will be used. The /NEWKEY parameter can be used to create a key. If signing is not desired, specifying /NOSIG will prevent signing. A date stamp will be appended to the end of the message name – e.g. *message_name*YYMMDDHHmm.zap.
REBOOT [/*RR*|/Win] [/wait | /f]	Reboot the machine. With no parameters, reboot with the normal boot sequence. The parameter RR means reboot to Rescue and Recovery, and WIN means reboot to the normal operating system. The reboot will not occur until the script exits, so this should normally be the last command in a script. The optional WAIT command forces the system to boot to the specified environment on next reboot (manual or caused by other mechanism). The /f parameter forces the system to reboot now, and does not allow the user to save information from open applications. If no parameters are specified, the program defaults to /win (/wait and /f are not specified).
RETRYONERROR [ON|OFF] *retries*	By default, a script will only be tried once. However, if it is important to keep trying a script until it works, the RETRYONERROR command can be used to notify the mailbox function to keep trying to execute this script a finite number of times as specified by the retries parameter. If no number is specified, the default value is 3. A global default value can be set in the TVT.TXT file in the [rescue] section "retries = *retries*". Retries can also be set to FOREVER which could cause an infinite loop to occur.

Commands	Description
MSGBOX /msg *message text* [/head *header_text*] [/OK] [/CANCEL]| [/TIMER *timeout*] /B3	The MSGBOX command will display a message to the End User (if logged on). The message will remain displayed and the script will block until time out occurs, the cancel button is pressed or the **OK** button is pushed (if /OK is specified). A cancel button will not be on the panel if /CANCEL is not specified, and it will not be easy to get rid of the display. The command will return: • 0=OK was pressed • 1 = CANCEL • 2 = Timer expired The text in the message can be formatted using " \n " and " \t " to represent newline and tab respectively.
NETWK [/D|/E|/A [/IP *ip_address* | /DN *domain_name*] [/NM *netmask*]	NETWK /D (disable) will stop all network traffic by disabling all network adapters. Networking will be disabled until a NETWK /E (enable) command is run. NETWK /A restricts networking to the IP address specified by either the /IP switch (dotted decimal) or /DN (DNS name). The /NM switch provides the network mask. If /NM is not provided, then only the single machine specified by /IP or /DN will be accessible. The state of this command persists over reboots, so networking must be explicitly enabled.
APUBKEY [/ADD|/DELETE] *asn_1_encoded_public_key*	The APASSWD command allows an administrator to remotely manage the Antidote Delivery Manager message signing keys on each PC. More than one key can be stored on each PC. If a signed message is processed, each key will be tried until a successful one is found. Keys are not separately named, so must be referenced by the content. A new key can be added using the ADD parameter and deleted with the DELETE parameter. Be aware that if there are any keys specified in the TVT.TXT, unsigned messages (those built with /NOSIG) can no longer be used.
AUNCPW [/Add|/CHANGE|/DELETE] *unc* [/USER *userid*] [/PWD *password*] [/REF *ref_name*]	This command allows you to add, change or delete a password for a network drive The reference name can be used as a shortcut in a message instead of using the UNC. Return values are: • 0 = successful • 1 = unable to set with the information provided • 2 = successful, but a different UNC which has the same reference name has already been defined.

Commands	Description
XMLtool for Conditionals	Conditionals (eGatherer, current HW information) • • **Usage:** xmltool.exe *filename xpath function comparator value* where: – **filename** The path and filename to the XML file – **xpath** The fully qualified xpath to value – **function** This must be one of the following values: - /C, compare the values (comparator and value must also be supplied) - /F , put the specified value into %IBMSHARE%\RET.TXT – **Comparator:** Must be one of the following: - LSS - LEQ - EQU - GTR - GEQ - NEW – **Value:** The value to compare the XML entry to. • Return Values: – **0** Comparison evaluates to true (/c) – **1** Comparison evaluates to false – **2** Incorrect command line paramaters – **3** Error opening XML file (not present or file has errors) – **4** Specified XPATH returned no value • **Example:** `xmltool.exe %ibmshare%\\ibmegath.xml //system_summary/bios_version GEQ 1UET36WW`
INRR	The INRR command can be used to determine if the script is running in the Rescue and Recovery environment. Return values are: • 0 = current OS PE • 1 = Current OS is not PE • >1 = Error

Commands	Description
STATUS [/QUERY *location message_name* | /CLEAR *location]*	The STATUS /QUERY command can be used to determine if a script has been run, or is queued to be run. The location value must be one of the following: • **FAIL** the message has already run and failed • **SUCCESS** The message has been completed successfully • **WORK** The message is currently being run, or will run next time Antidote Delivery Manager is run. • **CACHE** The message is queued to run. The STATUS/CLEAR command will clear the *location* specified. Return values are: • 0 = if the specified message found or the command completed successfully • 1 = if the specified message not found or the command failed

Supported Microsoft Commands

Commands	Description
ATTRIB.EXE	Displays or changes file attributes
CACLS.EXE	Displays or modifies access control liss (ACLs) of files
CHKDSK.EXE	Check a disk and displays a status report
COMP.EXE	Compares the contents of two files or sets of files
COMPACT.EXE	Displays or alters the compression of files on NTFS partitions
CONVERT.EXE	Converts FAT volumes to NTFS. You cannot convert the current drive
DISKPART.EXE	Partition a drive
FC.EXE	Compares two files or sets of files and displays the differences between them
FIND.EXE	Searches for a text string in a file or files
FINDSTR.EXE	Searches for strings in files
FORMAT.COM	Formats a disk for use with Windows
LABEL.EXE	Creates changes or deletes the volume label of a disk
NET.EXE	The networking commands
PING.EXE	Checks to see if a network resource can be reached
RECOVER.EXE	Recovers readable information from a bad or defective disk
REG.EXE	Registry manipulation
REPLACE.EXE	Replaces file
RRUCMD.EXE	Use to run Backups from OS or Restores from OS or RR Sorts input
SORT.EXE	Sorts input

Commands	Description
SUBST.EXE	Associates a path with a drive letter
XCOPY.EXE	Copies files and directory trees

Installation and Preparation

Preparation

If a signing key will be used, the administrator needs to run the packaging tool with the /NEWKEY parameter to generate a new signing key.

Configuration

Several configuration items will be required. The items appear in the TVT.TXT file:

Repository

Each client needs list of repositories. This should include floppy and C:\ as well as at least one network drive specified with a UNC. mailbox = [drive and path to mailbox locations, comma separated, in order of importance]. Example:

```
[rescue] mailbox = %y%\antidote, c:\antidote
```

Schedule Information

The Schedule Mode is the frequency of checks.

Schedule Mode	
SCHED_NONE	0x000
SCHED_MINUTELY	0x001
SCHED_DAILY	0x002
SCHED_WEEKLY	0x004
SCHED_MONTHLY	0x008
SCHED_STARTUP	0x010
SCHED_WAKEUP	0x020
SCHED_USB_ATTACH	0x040
SCHED_NETWORK_ATTACH	0x080

```
[Scheduler]
Task1=RapidRestoreUltra
Task2=Rescue

[rescue]
ScheduleFrequency=0
ScheduleMode=0x02
TaskShow=1
Task=c:\ibmtools\antidote\mailman.exe
ScheduleHour=11
ScheduleMinute=28
ScheduleDayOfTheWeek=3
ScheduleWakeForBackup=0
```

Signing Key

If signing keys will be used, they must be distributed to the client. The file keyfile.pub created by they APKGMES command contains the key. Each authorized

public signing key appears in the TVT.TXT file as: pubkeyX = ... where X is replaced by an integer, up to 9 public keys can be stored. Use APUBKEY function to set this value nosig = If set to 1, it will allow unsigned packages (packages built with the /NOSIG parameter) to be run.

Note: if not set to 1, or if public keys are present in the TVT.TXT file, unsigned packages will not run.

Network Drives

The following values are set by using the AUNCPW function [RscDrvY]. Each RscDrv section contains information about one network share. Up to 10 network shares can be defined for Antidote Delivery Manager.

- UNC = The UNC of a drive you need Antidote Delivery Manager to connect to.
- User = Encrypted username
- Pwd = Encrypted password
- Ref = The reference name to be associated with this connection

Installation on Clients

Rescue and Recovery 2.0 must be installed on all clients. Configuration prepared above may be included in the installation or performed later.

Server Infrastructure

The administrator must establish network shares for repository or provide an FTP or HTTP site. An additional repository may be needed for fixes and patches.

Simple System Test – Display Notification

Script Preparation and Packaging

Write a GO.RRS script on any machine where Antidote Delivery Manager has been installed. Include a line MSGBOX /MSG “Hello World” /OK. Execute the command directly from the command prompt to make sure it works as desired. Then run the APKGMSG command on the directory containing GO.RRS to make a message. Place the message file in one of the repository directories on your machine and observe correct operation.

Major Worm Attack

The following example demonstrates one possible approach to combating a major virus. The basic approach is to turn off networking, then reboot to Rescue and Recovery, repair the registry, copy a replacement file into place, the boot back to Windows XP and restore networking. For demonstration purposes, an application below needs to be updated for revised syntax.

Go.RRS

```
set tagfile=1.tag
set pingtarg=192.168.1.1
retryonerror /on 10
set custos
if errorlevel 1 set custos=%systemDrive%

cd %custos%\ibmtools\utils\rescue\dne\work

inRR.exe
```

```
|  if errorlevel 2 goto ERROR
|  if errorlevel 1 goto InOS
|  if errorlevel 0 goto inRR
|
|  :InOS
|  cd
|  if exist %tagfile% goto DONE
|
|  msgbox /msg "Antidote has detected a new message \n  \n ..... \n  \n Don't worry; be Happy!
|  Antidote will fix your system for you" /ok /timer 30
|  call nettest.cmd %pingtarg%
|  set el=%errorlevel%
|  if %el% == 0 msgbox /msg "Network is working" /timer 5 /head "Correct"
|  if not %el% == 0 msgbox /msg "Network is disabled" /timer 5 /head Failure
|  NetWk.exe /d
|  msgbox.exe /msg "Antidote Recovery Process is running. \n  \n Networking has been disabled." /head
|  "Networking" /timer 15
|  call nettest.cmd %pingtarg%
|  set el=%errorlevel%
|  if %el% == 0 msgbox /msg "Network is working" /timer 5 /head "Failure"
|  if not %el% == 0 msgbox /msg "Network is disabled" /timer 5 /head "Correct"
|  msgbox.exe /msg "System will reboot in 20 seconds \n  \n Press OK to reboot now, or Cancel to reboot later."
|  /head "Select Repair Urgency" /timer 20 /ok /cancel
|  if errorlevel 2 goto PENOW
|  if errorlevel 1 goto PELATER
|  if errorlevel 0 goto PENOW
|
|  :PENOW
|  reboot /rr
|  goto NOT_DONE
|
|
|  :PELATER
|  %custos%\ibmtools\utils\bmgr32.exe /bw
|  msgbox.exe /msg "System will apply fix next time you reboot" /head "Reboot" /ok
|  goto NOT_DONE
|
|  :inRR
|  REM DISABLE NETWORKING
|  msgbox.exe /msg "Networking will be disabled in 5 seconds. \n  \n  Network disable pending"
|  /head "Network shutdown" /timer 5
|  NetWk.exe /d
|
|  REM USE EGATHERER VALUES FOR CONDITIONAL BRANCH
|
|  msgbox /msg "Checking Registry" /timer 5
|  xmltool %ibmshare%\ibmegath.xml //EG_GATHERED_DATA/EG_INSTALLED_MICROSOFT_SOFTWARE/
|  EG_SOFTWARE_PACKAGE[@ID='DirectX']/EG_VERSION GEQ \"4.09.00.0901\"
|  if errorlevel 1 goto FILECOPY
|
|  msgbox.exe /msg "Applying Registry fix. \n  \n Press OK to continue..." /head "Registry Fixeroo" /ok
|  reg.exe load HKLM\tempSW %custos%\windows\system32\config\SOFTWARE
|  reg.exe add "HKLM\tempSW\IBM\eGatherer\Local Viewer\scans\banka" /v benke /d binki /f
|  reg.exe add "HKLM\tempSW\IBM\eGatherer\Local Viewer\scans\banka" /v bonko /d bunku /f
|  reg.exe delete "HKLM\tempSW\IBM\eGatherer\Local Viewer\scans\banka" /v bonko /f
|  reg.exe unload HKLM\tempSW
|
|  :FILECOPY
|  msgbox /msg "Registry Now OK \n  \n Applying Fix" /timer 5
|  copy payload.txt %custos%\
|
|  REM RE-ENABLE NETWORK
|  msgbox.exe /msg "Networking will be enabled in 5 seconds. \n  \n Network enable pending" /head
|  "Network shutup" /timer 5
|  NetWk.exe /e
|
|  REM TAG IT
```

```
echo 1 > %tagfile%

REM REBOOT
msgbox.exe /msg "System will reboot in 5 seconds..." /head "Reboot..." /timer 5
reboot.exe
goto NOT_DONE

:ERROR
:NOT_DONE
exit 1

:DONE
NetWk.exe /e
msgbox.exe /msg "Fix Applied \n  \n You may now continue normal operation."
/head "Done" /ok
exit 0
```

NETTEST.CMD

```
PING –n 1 %1 > nul 2>&
```

PAYLOAD.TXT

```
a test file
of a payload to deliver.
```

Appendix F. Notices

IBM may not offer the products, services, or features discussed in this document in all countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change IBM product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of IBM or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Non-IBM Web sites

Any references in this publication to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product, and use of those Web sites is at your own risk.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM
ImageUltra
ThinkPad
ThinkCentre
ThinkVantage
Lotus Notes
Rapid Restore
ScrollPoint

Lotus and Lotus Notes are trademarks

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.