

Rescue and Recovery 4.3 Deployment Guide

Updated: September 28, 2009

Rescue and Recovery 4.3 Deployment Guide

Updated: September 28, 2009

Third Edition (October 2009)

© Copyright Lenovo 2008, 2009.

LENOVO products, data, computer software, and services have been developed exclusively at private expense and are sold to governmental entities as commercial items as defined by 48 C.F.R. 2.101 with limited and restricted rights to use, reproduction and disclosure.

LIMITED AND RESTRICTED RIGHTS NOTICE: If products, data, computer software, or services are delivered pursuant a General Services Administration "GSA" contract, use, reproduction, or disclosure is subject to restrictions set forth in Contract No. GS-35F-05925.

Contents

Preface	v	Log files	49
Chapter 1. Overview	1	Create Rescue Media	49
Predesktop Area	1	Chapter 4. Best practices.	51
Windows environment	2	Scenario 1 - New rollouts.	51
Rejuvenating	2	Preparing the hard disk drive	51
Hints and Tips.	3	Installing	51
Chapter 2. Installation.	5	Updating	53
Installation considerations	5	Enabling the Rescue and Recovery desktop.	53
Installing the Rescue and Recovery program.	6	Scenario 2 - Installing on OEM systems	54
Installation requirements	6	Best practices for hard drive setup: Option 1	55
Installation components.	7	Best practices for hard drive setup: Option 2	55
Installation log files	8	Scenario 3 - Installing with WIM files and Windows	7
Rescue and Recovery installation	9	7	56
Rescue and Recovery environmental variables.	13	Scenario 4 - Standalone install for CD or script files	57
Compatibility with BitLocker	13	Scenario 5 - Working with Active Directory and	ADM files
Chapter 3. Configurations	15	Corporate Active Directory Rollout	58
XML and ADM file configurations.	15	Scenario 6 - Performing a Bare Metal Restore from	an Admin Backup
Recovery methods	15	Scenario 7 - Manually creating the Service Partition	of S drive
Single file restore	16		58
File rescue.	16	Appendix A. Administrative tools	61
Operating system and applications	16	Command line support	61
Restore system drive only	16	Mailman	61
Rejuvenation	16	AWizard.exe	61
Full restore	17	SETPASSWORD	61
Custom recovery	17	RELOADSCHED	61
Backups	20	RRCMD command-line interface	61
Scheduling backups and associated tasks	20	CLEANDRV.EXE	64
Sysprep Backup/Restore	21	CONVDATE	64
Mapping a network drive for backups	22	CREATSP	64
Password Persistence	25	InvAgent	65
EFS file limitation	25	MapDrv	66
Battery power settings for backups	25	Rescue and Recovery Boot manager control	(BMGR32).
Completing a backup	26	BMGR CLEAN	70
Microsoft Message Queuing (MSMQ).	26	Active Directory Support.	71
Rescue and Recovery in the Windows environment	26	Administrative (ADM) template files	71
Using the Rescue and Recovery program in the	Windows environment	Group Policy settings	72
26		Appendix B. User tasks	83
Working with the Predesktop Area	29	Windows 7	83
Working with WIM files and ImageX.	30	Create rescue media	83
Using RRUTIL.EXE.	30	Rescue and Recovery user interface switching.	84
Customizing the preboot environment	36	Appendix C. Notices	85
Configuring the Opera browser.	41	Trademarks	86
Changing the video resolution	47		
Startup applications	47		
Passwords.	48		
Password access.	48		

Preface

Information presented in this guide is to support Lenovo computers installed with the ThinkVantage® Rescue and Recovery® program.

The Rescue and Recovery program is an essential tool that enables users and administrators to restore backups, access files, diagnose problems, and make Ethernet connections if the Microsoft® Windows® operating system will not open or run correctly. It also enables deployment of critical updates to systems that are corrupted or off the network, as well as automatically applying patches to a system when a restore operation is performed. The Rescue and Recovery program helps reduce IT management costs by decreasing helpdesk calls and desk-side visits, as well as improving user productivity.

The *Rescue and Recovery Deployment Guide* provides the information required for installing the Rescue and Recovery program on one or more computers, and also provides instructions and scenarios on the administrative tools that can be customized to support IT or corporate policies.

This guide is intended for IT administrators, or those responsible for deploying the Rescue and Recovery program to computers throughout their organizations. If you have suggestions or comments, communicate with your Lenovo® authorized representative. This guide is updated periodically, and you can check the latest publication on the Lenovo Web site at:
<http://www.lenovo.com/support/site.wss/document.do?Indocid=TVAN-ADMIN>

For information about using various components included in the Rescue and Recovery workspace, refer to the online help system and user guides that come with the Rescue and Recovery program.

Chapter 1. Overview

The Rescue and Recovery program represents a unique combination of 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.

The Rescue and Recovery program has the following features:

- The Rescue and Recovery Predesktop Area provides an environment to start your computer when you fail to log in to the Windows operating system.
- The Rescue and Recovery Windows environment enables you to back up the operating system and files and restore the operating system and files in familiar interfaces.
- The Rescue and Recovery program enables you to store backup files on external USB storage devices, such as USB flash drives and USB hard disk drives.
- The Rescue and Recovery program enables you to store the backup data of multiple computers on one storage device.

The Rescue and Recovery program includes the option to switch to a simplified user interface with a few basic operations, or stay with the advanced user interface with extended options. For more information on interface switching, see “Rescue and Recovery interface switching” on page 28.

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 does not function correctly, this will not prevent the Rescue and Recovery environment from operating normally. Windows functions are not configured in the Rescue and Recovery environment.

Predesktop Area

The Rescue and Recovery Predesktop Area provides an emergency workspace for 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 users solve problems without consuming IT staff time.

The Rescue and Recovery Predesktop Area has four major categories of functions:

- **Rescue and Restore**
 - **Recovery overview:** Links users to help topics about the various recovery options that are provided.
 - **Rescue files:** Enables users to copy files created in Windows applications to removable media or to a network and to continue to work even with a disabled workstation.
 - **Restore from backup:** Enables users to restore files that have been backed up with the Rescue and Recovery program.
- **Configure**
 - **Configuration overview:** Links to Rescue and Recovery environment help topics about configuration.
 - **Recover password or passphrase:** Provides a user or an administrator with the ability to recover a password or passphrase in the Rescue and Recovery environment.

- **Access BIOS:** Opens the 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:** Allows you to download needed files to the partition in the \SWSHARE folder in the Windows partition.
 - **Map network drive:** Helps users access network drives for software downloads or file transfer.
- **Troubleshoot**
 - **Diagnostic overview:** Links to the Rescue and Recovery program diagnostics help topics.
 - **Diagnose hardware:** Opens the PC Doctor application that can perform hardware tests and report results.
 - **Create diagnostic disks:** Enables you to create a set of diagnostic diskettes.
 - **Boot from another device:** Enables you to boot from the Rescue and Recovery CD, a set of back up CD's, an internal drive or a detachable storage device such as a USB hard disk drive.

Note: To boot from a USB hard disk drive or a second hard disk drive, ensure that the hard disk drive is not compressed.

 - **System information:** Provides details about the computer and its hardware components.
 - **Event log:** Provides details of recent user activities and listings of computer hardware to aid in problem determination and resolution. The log files provide a readable way to view activities and a set of log entries.

Note: The feature of viewing the log files is supported on select machine types of Lenovo-branded personal computers only.

 - **Warranty status**

The Rescue and Recovery program is available on Lenovo-branded personal computers that come with preinstalled software. It is also available for purchase as a CD file so that organizations can benefit from the Rescue and Recovery program on non-Lenovo branded computers. You can then purchase separate licenses for individual computers.

Windows environment

The Rescue and Recovery Windows environment enables 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 users' computers, thereby limiting risk and downtime. the Rescue and Recovery program offers your clients an extra layer of support by pre-configuring automatic external backup to a server or external storage. Backups are encrypted by default with the 256 AES key.

Rejuvenating

The Rescue and Recovery program can optimize system performance by taking a new incremental backup and then defragment your hard drive. The rejuvenation process helps eliminate viruses, adware and spyware, while maintaining your current settings and data.

For more information, see “Rejuvenation” on page 16.

Hints and Tips

For hints and tips on using the Rescue and Recovery program, see the *Rescue and Recovery v4.3 Considerations* document located at:
<http://www.lenovo.com/support>

Chapter 2. Installation

Prior to installing the Rescue and Recovery program, you can customize the Rescue and Recovery XML file for your enterprise and then deploy it to client systems. The XML file packaged with the Rescue and Recovery program is named `rnrdploy.xml`. Once the XML file is customized and installed, settings for the Rescue and Recovery program are managed with the registry or Active Directory. For more information, see the accompanying XML/ADM Supplement for the deployment guide located on the ThinkVantage Technologies Administrator Tools page:

<http://www.lenovo.com/support/site.wss/document.do?lndocid=TVAN-ADMIN#rnr>

Installation considerations

The Rescue and Recovery program has two main interfaces. The primary interface operates in the Microsoft Windows environment. The secondary interface, the Rescue and Recovery Predesktop Area, operates independently of the Windows operating system, in the Windows PE environment.

The Rescue and Recovery program 4.3 is designed for the Windows 7 operating system. The earlier versions of the Rescue and Recovery program for Windows 2000, Windows XP or Windows Vista® cannot be installed on the Windows 7 operating system. Therefore, the Windows Installer program does not support the overinstall behavior from previous versions of the Rescue and Recovery program.

It is recommended to make a new backup after installing the Rescue and Recovery program 4.3 to your Windows 7 operating system. You can make the backup by using either a script or the user interface.

Notes:

1. The Rescue and Recovery program only works with the non-BIOS version of Computrace if the Rescue and Recovery program is installed first, and then Computrace is installed.
2. If you attempt to install Storage Management Subsystem on a computer with the Rescue and Recovery program installed with the Windows PE area already installed as a virtual partition, then Storage Management Subsystem will not install. Both Windows PE and Storage Management Subsystem use the `C:\minint` directory for its file system. The way to have both installed at the same time is to install the Rescue and Recovery program as a type `0x07` partition. See "Scenario 6 - Performing a Bare Metal Restore from an Admin Backup" on page 58 for instructions.
3. A possible security risk may be created when the Microsoft Recovery Console is installed on a system with the Rescue and Recovery program. Microsoft Recovery Console looks for all folders with the path `C:*\system32\config\` and if it finds that path it assumes it is an operating system. If the registry entries that require a Windows password are not present, then recovery console will allow a user to choose the operating system and then gain access to the entire hard drive without needing to enter a password.

Installing the Rescue and Recovery program

The Rescue and Recovery installation package was developed with InstallShield 10.5 Premier as a Basic MSI project. InstallShield Premier 10.5 uses the Windows Installer to install applications, which gives administrators many capabilities to customize installations, such as setting property values from the command line. This chapter describes ways to use and run the Rescue and Recovery setup package. For a better understanding, read the entire chapter before you begin to install this package.

Note: When installing this package, refer to the readme file that is posted on the Lenovo Web page at:

<http://www.lenovo.com/support/site.wss/document.do?Indocid=MIGR-4Q2QAK>
The Readme file contains up-to-the-minute information on software versions, supported systems, system requirements, and other considerations to help you with the installation process.

Installation requirements

This section addresses system requirements for installing the Rescue and Recovery package on Think branded systems. For best results, make sure that you have the latest version of the software installed. To obtain the latest version of the Rescue and Recovery program, see the Lenovo Web site:
<http://www.lenovo.com/thinkvantage>

Requirements for Lenovo computers

Lenovo-branded computers must meet or exceed the following requirements to install the Rescue and Recovery program:

- Operating system: Windows 7
- Memory: 1 GB
 - In shared memory configurations, the BIOS setting for maximum shared memory must be set to no less than 8 MB.
 - In non-shared memory configurations, 120 MB of non-shared memory is required.

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

- Internet Explorer® 5.5 or later must be installed.
- 2.4 GB of free space on your hard drive.
- VGA-compatible video that supports a resolution of 800 x 600 and 24-bit color.
- Supported Ethernet card.
- User must have administrative privileges.

Requirements for non-Lenovo computers

Installation on non-Lenovo computers have the following requirements:

Installation requirements: 2.4 GB of free hard disk space. The base install uses 930 MB.

Minimum system memory requirements: 256 MB system RAM to install the Rescue and Recovery program.

Hard disk drive configuration: The Rescue and Recovery program is not supported on the factory pre-loads for original equipment manufacturer (OEM) computers.

Note: For the Rescue and Recovery program, the OEM computers hard disk drive must be configured according to recommendations in "Scenario 2 - Installing on OEM systems" on page 54.

Support for booting from external media (CD/DVD and USB): Non-Lenovo 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 boot-ability

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 antivirus software) might not be compatible with the Rescue and Recovery software. For information regarding compatibility issues, refer to the Readme file and various utilities that accompany the Rescue and Recovery program. For additional information see the Lenovo Web site at: <http://www.lenovo.com/thinkvantage>

Network adapters for the Rescue and Recovery program: 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 operating system and are independent of the Windows operating system. For supported Lenovo computers, required drivers are included with the Rescue and Recovery program.

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

Installation components

This section contains installation components of the Rescue and Recovery program.

Administrative installation procedure

The 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.

You can obtain the setup package from:
<http://www.lenovo.com/support>

To perform an administrative installation, run 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:\. For example, other local drives or mapped network drives. 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.

- For installation target directory paths that do NOT contain spaces, use the following command line as an example:

```
setup.exe /a /s /v"/qn TARGETDIR=F:\TVTRR"
```
- For installation target directory paths that contain spaces, an escape character '/' must be placed preceding the double-quoted target directory:

```
setup.exe /a /s /v"/qn TARGETDIR=\"F:\TVTRR\Rescue and Recovery\""
```

Note: If your version of Windows Installer is not current, setup.exe is configured to update the Windows Installer engine to version 3.0. This update will cause the installation action to prompt for a reboot even with an administrative extract installation. Use the reboot properly to prevent a reboot in this situation. If the Windows Installer is at least version 3.0, setup.exe will not attempt to install.

Once an administrative installation has been completed, the administrative user can make customizations to the source files, such as adding settings to the registry.

Using msixec.exe

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

- For installation paths that do NOT contain spaces:

```
msixec.exe /a "Lenovo Rescue and Recovery.msi" /qn TARGERDIR=F:\TVTRR
```
- For installation paths that contain spaces:

```
msixec.exe /a "Lenovo Rescue and Recovery.msi" /qn TARGERDIR=\  
"F:\TVTRR\Rescue and Recovery\""
```

The following is an example to use msixec.exe.

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

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

For information on command line parameters and public properties, go to the Microsoft Web site at:
<http://www.microsoft.com>

Installation log files

The log file rinstall43w.log is created in the %temp% directory if the setup is launched by the setup.exe file (double-click the install.exe file to run it without parameters, or extract msi and run the setup.exe file). The log file contains log messages that can be used to debug installation problems. The log file includes any

actions performed by the **Add/Remove Programs** applet from Control Panel. The log file is not created when you are running the setup.exe file directly from the MSI package. To create a log file for all MSI actions, you can enable the logging policy in the registry. To do this, create the following value:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer]
"Logging"="voicewarmup"
```

The following table shows examples of installations using the setup.exe file.

Table 1. Examples of running Setup.exe

Description	Example
Perform silent installation with no reboot.	setup.exe /s /v"/qn REBOOT="R""
Perform administrative installation.	setup.exe /a
Perform silent administrative installation specifying the extract location for the Rescue and Recovery program.	setup.exe /a /s /v"/qn TARGETDIR="F:\TVTRR""
Perform silent uninstallation.	setup.exe /s /x /v/qn
Perform installation with no reboot. Create an installation log in temp directory for the Rescue and Recovery program.	setup.exe /v"REBOOT="R" /L*v %temp%\rinstall143w.log"
Perform installation without installing the Predesktop Area.	setup.exe /vPDA=0

The table below shows installation examples using Rescue and Recovery.msi:

Table 2.

Description	Example
Perform installation.	msiexec /i "C:\TVTRR\Rescue and Recovery.msi"
Perform silent installation with no reboot.	msiexec /i "C:\TVTRR\Rescue and Recovery.msi" /qn REBOOT="R"
Perform silent uninstallation.	msiexec /x "C:\TVTRR\Rescue and Recovery.msi" /qn
Perform installation without installing the Predesktop Area.	msiexec /i "C:\TVTRR\Rescue and Recovery.msi" PDA=0

Rescue and Recovery installation

The following instructions are for the files that can be downloaded separately from the *Individual language files for Large Enterprise* download page.

1. The main installation executables for the Rescue and Recovery program are:

- Z902ZISXXXUS00.exe
- Z902ZABXXXUS00.tvt

where XXXX is the build ID. This is a self-extracting installation package that extracts the installation source files and launches the installation using the Windows Installer. It contains the installation logic and the Windows application files. The package does not contain any of the Predesktop Area files.

2. Predesktop Area US Base (approximately 135 MB): This is the password protected zip file that contains the entire Predesktop Area US base. Its name is in the following formats:

- Z902ZISXXXUS00.exe

- Z902ZABXXXXUS00.tvt

where *AB* determines the compatibility of the Predesktop Area and *XXXX* is the build id. This file is required to install the Predesktop Area on all language systems. This file must be in the same directory as the main installation package (either installation executable or Rescue and Recovery.msi if extracted or OEM install). The exceptions to this are if the Predesktop Area is already installed and does not need to be upgraded or if the property PDA=0 is set on the command line when executing the installation and the Predesktop Area (any version) does not already exist.

The Windows Installer will compare the current Predesktop Area's compatibility code against the minimum version compatibility code and take the following actions based on the results:

- **Current code > Minimum code:**

The Windows Installer presents a message that the current environment is not compatible with this version of the Rescue and Recovery program.

- **Current code = Minimum code:**

The Windows Installer compares the current version level against the minimum version level. If the current level is greater than or equal to the minimum level, the Windows Installer looks for a .tvt file with a compatibility code (for example: AA, AB) that is equal to the minimum version compatibility code and a level that is greater than the current version level (all other version fields in the .tvt filename must match the minimum version exactly). If it does not find a file, the install process continues without updating the Predesktop Area. If the current level is less than the minimum level, the Windows Installer will look for a .tvt file with a compatibility code (AA or AB) that is equal to the minimum version compatibility code and a level that is greater than or equal to the minimum version level (all other version fields in the .tvt filename must match the minimum version exactly). If a file is not found meeting these criteria, the installation is halted.

- **Current code < Minimum code:**

The Windows Installer will look for a .tvt file with a compatibility code (for example: AA, AB) that is equal to the minimum version compatibility code and a level that is greater than or equal to the minimum version (all other version fields in the .tvt filename must match the minimum version exactly). If a file is not found meeting these criteria, the installation is halted.

The Rescue and Recovery program supports the following languages:

- Brazilian Portuguese
- Danish
- Dutch
- English
- Finnish
- French
- German
- Italian
- Japanese
- Korean
- Norwegian
- Portuguese

- Russian
- Spanish
- Swedish
- Simplified Chinese
- Traditional Chinese

Rescue and Recovery custom public properties

The installation package for the Rescue and Recovery program contains a set of custom public properties that can be set on the command line when running the installation. The available custom public properties are:

Table 3.

Property	Description
PDA	Specifies whether to install the Predesktop Area. Default value is 1. 1 = install Predesktop Area. 0 = do not install Predesktop Area. NOTE: This setting is not used if any version of the Predesktop Area already exists.
CIMPROVIDER	Specifies whether to install the Common Information Model (CIM) Provider component. Default is to not install the component. Specify CIMPROVIDER=1 on the command line to install the component.
EMULATIONMODE	Specifies to force the installation in Emulation mode even if a Trusted Platform Module (TPM) exists. Set EMULATIONMODE=1 on the command line to install in Emulation mode.
HALTIFTPMDISABLED	If the TPM is in a disabled state and the installation is running in silent mode, the default is for the installation to proceed in emulation mode. Use the HALTIFTPMDISABLED=1 property when running the installation in silent mode to halt the installation if the TPM is disabled.
ENABLETPM	Set ENABLETPM=0 on the command line to prevent the installation from enabling the TPM
SUPERVISORPW	Set SUPERVISORPW="password" on the command line to supply the supervisor password to enable the chip in silent or non-silent installation mode. If the chip is disabled and the installation is running in silent mode, the correct supervisor password must be supplied to enable the chip, otherwise the chip is not enabled.

Including the Rescue and Recovery program in a disk image

You can create a disk image that includes the Rescue and Recovery program. This deployment guide takes PowerQuest and Ghost as examples.

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 with Rescue and Recovery

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

Minimum script files:

Table 4. X:\PQ\RRUSAVE.TXT

Script language	Result
SELECT DRIVE 1	Selects the first hard disk drive.
SELECT PARTITION ALL (Needed if you have a type 0x07 partition or if you have multiple partitions in your image.)	Selects all partitions.
Store with compression high	Stores the image.

Table 5. X:\PQ\RRDEPLY.TXT

Script language	Result
SELECT DRIVE 1	Selects the first hard disk drive.
DELETE ALL	Deletes all partitions.
SELECT FREESPACE FIRST	Selects first free space.
SELECT IMAGE ALL	Selects all partitions in image.
RESTORE	Restores the image.

Image creation:

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

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

Image deployment:

Table 7. X:\PQ\PQIMGCTR / CMD=X:\PQ\RRDEPLY.TXT /MBI=1 / IMG=X:\IMAGE.PQI

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

Using WIM files, ImageX, and Windows 7

Windows 7 deployment is based on disk imaging using ImageX. ImageX utilizes file-based imaging with WIM files instead of sector-based image formats. Considering this formatting development, use the scenario in “Scenario 6 - Performing a Bare Metal Restore from an Admin Backup” on page 58 when installing and deploying the Rescue and Recovery program on Windows 7.

Using Symantec Ghost-based tools with Rescue and Recovery

When you create the Ghost image, you must use the command line switch `-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.

Rescue and Recovery environmental variables

The following table contains environmental variables that are created when the Rescue and Recovery program is installed. These variables can be used when creating scripts or when changing to a desired directory from a command prompt. For example, to change the `c:\Program Files\Lenovo\Rescue and Recovery` directory from a command prompt, type `CD %rr%` and press Enter.

Table 8. Rescue and Recovery environmental variables

Environmental variable	Directory
%rr%	c:\Program Files\Lenovo\Rescue and Recovery
%SWSHARE%	c:\SWSHARE
%TVT%	c:\Program Files\Lenovo
%TVTCOMMON%	c:\Program Files\Common Files\Lenovo

Note: For a complete list of variables, run the `set` command on a computer that has the Rescue and Recovery program installed.

Compatibility with BitLocker

To achieve compatibility with BitLocker Drive Encryption, it is recommended to install the Rescue and Recovery program to your operating system after the partitions are properly set up with the Microsoft BitLocker Drive Preparation Tool.

When setting up the BitLocker partition, it is recommended to use the Microsoft BitLocker Drive Preparation Tool. The boot partition should be at least 2 GB in size.

If you do not use the BitLocker Drive Preparation Tool to prepare the BitLocker partition, you must have two partitions on your system when installing Windows 7. One partition should be 2 GB and marked as active; this is where the boot files reside. The other is where your operating system is installed and where your data will reside. When Windows 7 is installed, it will detect the two partitions and should install only the boot files to the smaller partition. Both partitions should be type 0x07.

Compatibility with BitLocker without TPM

If the security chip (TPM) is not activated in the BIOS Setup Utility, to achieve compatibility with BitLocker without TPM, do the following:

1. Run `gpedit.msc` from the **Start** menu. The Group Policy Editor window opens.

2. Click **Computer Configuration** → **Windows Components** → **BitLocker Drive Encryption** → **Operating System Drives**.
3. Enable the **Require additional authentication at startup** option
4. Select the option **Allow BitLocker without a compatible TPM**.

Best practice of BitLocker encryption on a system with the Rescue and Recovery program

To have the Rescue and Recovery program work correctly with BitLocker in Windows 7, the best practice is:

1. Uninstall the Rescue and Recovery program if it has been installed.
2. Restart the computer and use the BitLocker Drive Preparation Tool to prepare the system for BitLocker Drive Encryption.
3. Install the Rescue and Recovery program and restart the computer.
4. Start BitLocker from Control Panel and choose the partition to encrypt.

Note: It is recommended to encrypt the Windows operating system partition (usually drive C) only.

5. Click **Turn on BitLocker**, and follow the instruction on the screen to encrypt the chosen partition. After that, a recovery key is automatically created.
6. Save the recovery key to a USB storage device.

Note: Keep the USB storage device in a secured place. The recovery key is needed when booting to Windows 7 or the Rescue and Recovery workspace. The BitLocker encryption will be lost if the hard disk drive is cleared by the Diskpart commands or other hard disk tools.

7. Wait until the encryption process completes. After that, you can use the Rescue and Recovery program to perform backup and restore operations.

For more information about BitLocker, go to the Microsoft Web site at: <http://support.microsoft.com/kb/933246/>

Notes:

1. When setting up BitLocker in Windows 7, the BitLocker partition should be after the Windows operating system partition for best results. If it is placed before the Windows operating system partition, the partition number will need to be updated in the Rescue and Recovery ADM settings.
2. When restoring a system that is using Windows 7 and BitLocker, a message will display, indicating that there was an error at shutdown. The message can be ignored and everything should operate normally.
3. For OEM or non-Lenovo standard preload systems, you need to suspend the encryption of the Windows operating system partition when performing any backup or restore operations using the Rescue and Recovery program, otherwise the Rescue and Recovery program will not enter PDA.
4. You might need to clear the TPM and encrypt the partitions again after restoring the system from a backup with BitLocker encryption.

Chapter 3. Configurations

This chapter provides information that you will need to configure the Rescue and Recovery program for your enterprise. Within this chapter, you will find the following topics:

- “XML and ADM file configurations”
- “Recovery methods”
- “Backups” on page 20
- “Rescue and Recovery in the Windows environment” on page 26
- “Working with the Predesktop Area” on page 29
- “Log files” on page 49
- “Create Rescue Media” on page 49

XML and ADM file configurations

Configurations for the Rescue and Recovery program are done with the XML file, through the registry, and with Active Directory. Once the XML file is customized and installed, settings for the Rescue and Recovery program are managed with the registry or Active Directory. For more information, see the accompanying *ThinkVantage Technologies XML/ADM Supplement* for the deployment guide located on the ThinkVantage Technologies Administrator Tools page: <http://www.lenovo.com/support/site.wss/document.do?Indocid=TVAN-ADMIN#rnr>

Recovery methods

Within this section, you will find information for restore types and recovery methods such as rejuvenation, custom recovery, and express repair. The following methods are used for restoring files:

- “Single file restore” on page 16
- “File rescue” on page 16
- “Operating system and applications” on page 16
- “Restore system drive only” on page 16
- “Rejuvenation” on page 16
- “Full restore” on page 17
- “Custom recovery” on page 17

Notes:

1. The Rescue and Recovery program cannot capture cached credentials for a domain user after a restore operation.
2. The Rescue and Recovery program cannot restore partitions that are created and placed physically before the system drive.
3. The Rescue and Recovery program do not support a full restore operation if you boot your system from another external media. For example, if you perform a full restore operation from your USB hard disk drive, make sure that you boot your system from this USB hard disk drive as well.

Single file restore

Single file restore prompts the user for the Backup Storage location, and then the user selects a backup. The Rescue and Recovery program will display files that the user is authorized to access. The user then selects the files, folders, or both to be restored and the system will restore them to their original locations.

File rescue

File rescue used before restore, prompts the user for the backup storage location and then the user selects a backup. The Rescue and Recovery program will display the files that the current user is authorized to access. The user then selects the files, folders, or both to be rescued. Excluding the local hard disk, the system will display available file locations where the files can be rescued. The user will need to choose a destination with sufficient space for the rescued files and the system restore files.

Operating system and applications

Operating system and Applications gives the user the option to select a backup before the system deletes files. Files designated to be deleted are defined by the rules in the registry. When a backup has been selected, the system will restore the files defined by the registry from the selected backup. There are options in the registry file that can specify a program to run before a restore operation or after a restore operation. See the *ThinkVantage Technologies XML/ADM Supplement* for more information about registry settings and values.

Notes:

1. Operating system and Applications always use Password Persistence.
2. Operating system and Applications restore is not available from CD/DVD backup.

You can add custom tasks to run before and after both Backups and Restores. See *ThinkVantage Technologies XML/ADM Supplement* for the backup and restore settings.

Restore system drive only

This function enables you to restore only the system drive to the state when you make the latest backup of the system drive. If you have multiple partitions on your hard disk drive, you have the option to restore only the system drive and leave the other partitions intact.

Rejuvenation

When you need to rejuvenate your system, the Rescue and Recovery program will optimize system performance by taking a new incremental backup and then defragment your hard drive. The rejuvenation process helps eliminate viruses, adware and spyware, while maintaining your current settings and data.

To rejuvenate your system, complete the following steps:

1. From the Rescue and Recovery interface, click the **Restore your system from a backup** icon. The Restore your system screen is displayed.
2. On the Restore your system screen, select **Rejuvenate your system**.
3. Choose the drive and backup that you want to use to rejuvenate your system by completing the following procedure:

- a. Select the appropriate drive from the drop-down menu of available drives. Backup files on the selected drive are displayed by the Rescue and Recovery interface.
- b. Select the backup file that you want to use to rejuvenate your system.
- c. Click **Next**.
- d. Confirm that the selected backup is the one that you want to use to rejuvenate your system, and then click **Next** to begin the restoration process.

Note: Do not power off your computer during this operation.

- e. Click **OK**. A progress bar is displayed.

You can add custom tasks to run either before or after a rejuvenation. See the *ThinkVantage Technologies XML/ADM Supplement* for the rejuvenation settings.

Note: Some operating system settings are stored in the registry. Considering rejuvenation restores your registry from a backup and restores certain registry keys captured from the current system settings, you may find some inconsistencies after the rejuvenation process. For example, if you have a shared folder in a backup and not at the time of the rejuvenation process, it will be shared again after completing a rejuvenation from that backup. Also, if you have a shared folder at the time of the rejuvenation process but it was not in the backup, the folder will still be shared after rejuvenation finishes.

Full restore

Full restore deletes all files on the local drive, and then restores the files from the selected backup. If password persistence is selected, the most recent password available will be restored.

Custom recovery

As an extension of the Rescue and Recovery program, custom recovery technology has been added to the recovery process. Users will interact with this custom recovery method through the Rescue and Recovery program and the Lenovo Base Software Selector programs. By performing a custom recovery, users have the option of including and excluding individual components such as applications, device drivers or operating systems as part of the recovery process. Administrators will define what options a user will have during a custom recovery process with the ThinkVantage Base Software Administrator program.

The Base Software Administrator program is a versatile software utility that you can use to accomplish custom recovery and preinstallation related tasks. With the Base Software Administrator program, you can customize the recovery process for users and you can create personalization files used to automate the preinstallation setup for Windows.

Customizing the recovery process

In today's electronic environment, computer systems are threatened by malicious activity with the distribution of viruses, worms, and Trojan horses. Technology and anti-virus software has improved in the fight against malicious activity; however, there are times when the software on a computer will need to be renewed by removing malicious files and starting over. The Rescue and Recovery program is a valuable tool in the renewal process by providing methods to restore a computer in the event the computer is sold, recycled, transferred to another area or needs to be put in an operational state after all other methods of recovery has failed.

Various types of recovery methods can be used to renew computer systems. The Base Software Administrator program utilizes the full factory recovery method and the custom factory recovery method. The full factory recovery method restores the factory contents of the hard drive that consists of components such as applications, device drivers, and the operating system. Factory components are installed at the factory prior to the purchase of a computer. Using the Base Software Administrator program, you can control the recovery options that are available to the user during the recovery process. The following list provides the recovery methods you can designate a user to perform:

- Full factory recovery only
- Custom factory recovery only
- Either a full factory recovery or a custom factory recovery

Components consist of applications, device drivers, and operating systems. These components are in a custom packaged format and are contained in the service partition of the computer. From a recovery standpoint, components are categorized as follows:

- Required components are always installed upon recovery.
- Optional components are displayed for the user on the Base Software Selector menu.
- Restricted components are not installed upon recovery, and are not displayed to the end user.

Manifest files: Customizing the recovery process is controlled with manifest files. The Base Software Administrator program can create custom manifest files. Manifest files have the extension `.cfi`, and contain information about the components within the service partition where it resides. Manifest files also control the selections available to the user during a custom recovery. The information contained in a manifest file includes component categorization such as required, optional, and restricted. In addition, manifest files contain meta-data, such as descriptions and comments.

Preinstallation setup

To accomplish preinstallation setup, you can use the Base Software Administrator program to create personalization files. A personalization file has the file extension of `.per` and contains information needed to automate the preinstallation setup for Windows. The recovery process reads the personalization file, extracts the data from the personalization file and places the data in the correct Windows control files. You can save time and effort by using the Base Software Administrator program to customize personalization files and then deploying those personalization files onto user computers. For example, you can create a personalization file to set the Time Zone for Windows and then deploy that personalization file to a users computer; therefore, a user will not have to manually validate the Time Zone settings.

Personalization files: Personalization files are customized by defining the settings with the Base Software Administrator program. The following tables provide a description of each type of setting that can be defined.

The General settings table provides the settings used to define the user name, organization and time zone for a computer:

Table 9. General settings

Setting	Windows control file keyword	Description
Name	FullName=	Sets the user name for the computer.
Organization	OrgName=	Sets the organization the computer belongs to, such as a specific department or location.
Time zone	TimeZone=	Sets the time zone for the computer.

The Network settings table provides the settings used to assign the computer name, administrator password and the workgroup or domain of the destination computer:

Table 10. Network settings

Setting	Windows control file keyword	Description
Computer name	ComputerName=	Sets the name for the computer.
Administrator password	AdminPassword=	Sets the administrator password.
Encrypted administrator password	EncryptedAdminPassword=	Sets the encrypted administrator password.
Workgroup	JoinWorkgroup=	Sets the workgroup for the computer.
Domain	JoinDomain=	Sets the domain for the computer.
Domain administrator	DomainAdmin=	Sets the domain administrator for the computer.
Domain administrator password	DomainAdminPassword=	Sets the domain administrator password for the computer.

Advanced settings are used to define one or more commands that can be run the first time a user logs on to his or her system.

Command line interface: The following executable supports a command line interface for the Base Software Administrator program and is supported under WinPE and the Windows environment:

```
TBSADMIN.EXE [/DEPLOY [/SILENT] [/BOOTSP=YES|NO]
[/MANIFEST="<path>"] [/PERSONALIZATION="<path>"]]
```

The following table provides the switches for the Base Software Administrator program.

Table 11. Switches

Switch	Description
/DEPLOY	Required to trigger a deploy. If /BOOTSP, /MAN or /PER is also specified, the deploy wizard is not displayed.

Table 11. Switches (continued)

Switch	Description
/SILENT	Suppresses any message boxes for error or successful completion. (For return codes, the following table.)
/BOOTSP	Takes an explicit Y or N value to indicate whether the service partition should be set active. For example, /BOOTSP=Y. A value of N allows the administrator to reset the C: partition active again, so recovery doesn't automatically occur on next reboot.

The executable returns the following codes:

Table 12. Return codes

Return code	Return message
0	Success
1	Unable to access service partition.
2	Error copying manifest file into service partition
3	Error copying personalization file into service partition
4	Error deleting file from service partition
5	Error writing AUTO.TAG file in service partition
6	Error setting service partition active

Backups

The following sections provide customization information for Rescue and Recovery backups.

Scheduling backups and associated tasks

The scheduler is not designed to be specific to the Rescue and Recovery program; however, the configuration is stored in the registry. When the Rescue and Recovery program 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 task.
- Script to run.
- Named pipe to be used for progress notifications. This is an optional setting.
- Schedule information monthly, weekly, daily, weekday, or weekend - multiple schedules. Tuesdays and Fridays for example, can be supported by creating two schedules.
- Parameters to pass to tasks.

For the Rescue and Recovery program, perform incremental backups on schedule, with callbacks before and after the backup.

In the Rescue and Recovery ADM file, there is an option to configure the Schedule Task 1 and Schedule Task 2 settings. The following registry keys must be added for the scheduled tasks:

- For Schedule Task 1, this key is HKLM\Software\Lenovo\Scheduler\tasks\task1
- For Schedule Task 2, this key is HKLM\Software\Lenovo\Scheduler\tasks\task2

Note: If the task needs to be shown, add the DWORD value name TaskShow and set the value to 1 in this key. By default, tasks are hidden.

Sysprep Backup/Restore

Sysprep Backup/Restore is performed by using the RRCMD parameter. For instructions on RRCMD, see “RRCMD command-line interface” on page 61.

Sysprep backup changes in Windows 7

The Sysprep backup operation in Windows 7 is different from that in Windows XP or Windows Vista. This is due to the new version Windows RE built from Windows 7. You can download the accessory package from the Lenovo Support Web site at <http://www.lenovo.com/support/site.wss/document.do?Indocid=MIGR-4Q2QAK>, and follow the steps to perform the correct Sysprep backup operation through **Generalize** option.

Overview of Windows RE (Recovery Environment) installation process in Windows 7

Unlike Windows Vista, Windows RE has been installed to the Windows 7 operating system. On a system installed using the setup.exe file, prior to OOBE (Out-Of-Box Experience), the default Windows RE image (winre.wim) is located in the \Windows\System32\Recovery subdirectory. However, once the user completes OOBE, the following will happen:

1. A Recovery folder is created on the system partition (C partition).
2. The WinRE.wim file is moved to C:\Recovery\Subdirectory).
3. An **OS Loader** entry is created for Windows RE in the BCD (Boot Configuration Data).
4. The **RecoverySequence** setting is created in the Windows 7 object in the BCD.
5. Other (undocumented) configuration files are updated.

These steps enable Windows RE on the Windows 7 operating system. Conversely, when using the System Preparation Tool with the **Generalize** option, a sysprep plug-in disables Windows RE by undoing these steps. The key point here is that, unlike Windows Vista, Windows 7 is responsible for managing various moving parts (for example, .wim, BCD, and so on) that allow Windows RE to work correctly. For more information about Windows RE in Windows 7, read the document provided on the Microsoft Web site at:

[http://technet.microsoft.com/en-us/library/dd744388\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd744388(WS.10).aspx)

Restore a Sysprep Backup

Password Persistence cannot work with Sysprep Backup/Restore, because the Password Persistence information does not exist in a Sysprep Backup image. Restart the system after completing a Sysprep Backup.

To restore from the Sysprep Backup, see “RRCMD command-line interface” on page 61. Only a full restore operation can be performed with base backups that

were taken using Sysprep. Rejuvenating or restoring the operating system and applications will not work with a Sysprep base backup.

Mapping a network drive for backups

The mapping network drive function relies on the registry settings located at HKLM\Software\Lenovo\MND.

The Universal Naming Convention entry contains the computer name and share of the location you are attempting to attach.

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

User and Pwd entries are the username and password entries. They are encrypted.

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

```
UNC=\\server\share
NetPath=\\9.88.77.66\share
User=11622606415119207723014918505422010521006401209203708202015...
Pwd=11622606415100000000014918505422010521006401209203708202015...
```

For deployment, this file can be copied onto multiple computers that will use the same user name and password. The UNC entry is overwritten by the Rescue and Recovery program based on a value in the rnrdeploy.xml file.

Setting up user accounts for network backups

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

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, such as the administrator, the merge process will fail.

Capturing a Sysprep utility image in the base backup

These instructions are for the files that can be downloaded separately for the *Individual language files for large enterprise* that you can download from the Lenovo Web site:

<http://www.lenovo.com/support/site.wss/document.do?Indocid=MIGR-4Q2QAK>

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

1. Perform an administrative installation:

```
:: Extract the WWW EXE to the directory C:\TVTRR
start /WAIT z902zisxxxxus.exe /a /s /v"/qn TARGETDIR
(Where XXXX is the build ID.)
="C:\TVTRR" REBOOT="R" /w
```
2. Install the Rescue and Recovery program using the MSIEXE file:
 - a. For all MSI files, add the following installation-log generation code:

```
/L*v %temp%\rinstall.txt
```
 - b. To install the setup files using the MSIEXE file, enter the following command:

```
: Perform the install of Rescue and Recovery

msiexec /i "C:\TVTRR\Rescue and Recovery.msi"
```
 - c. To silently install the setup files using MSIEXE:

With reboot at the end, enter the following command:

: Silent install using the MSI with a reboot
: Type the following command on one line

```
start /WAIT msixexec /i "C:\TVTRR\Rescue and Recovery.msi" /qn
```

With reboot suppressed, enter the following command:

: Silent install using the MSI without a reboot
: Type the following command on one line

```
start /WAIT msixexec /i "C:\TVTRR\Rescue and Recovery.msi" /qn REBOOT="R"
```

3. Enter the following commands:

```
net start "TVT Backup Service"
```

: Create Sysprep Base Backup to Local Hard Drive
: Type the following command on one line

```
cd "\Program Files\Lenovo\Rescue and Recovery"  
rrcmd sysprepbbackup location=l name="Sysprep Backup"
```

If you want to use a password, add the syntax `password=pass`.

4. Run 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.    **  
*****
```

5. Shut down and reboot the machine when Sysprep is complete.

Note: The operating system will reboot into the Predesktop Area of the Rescue and Recovery program. The status bar with **System Restore in Progress** will appear.

6. When complete, the message **Sysprep Backup is Complete** will appear.

7. Power off the system using the power button.

8. Capture the image for deployment.

Capturing a multiple partition machine and excluding files in a Sysprep backup

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

1. Perform an administrative installation action:

```
:: Extract the WWW EXE to the directory C:\TVTRR  
start /WAIT z902zibus00xxxx.exe /a /s /v"/qn TARGETDIR  
(where XXXX is the build ID)  
="C:\TVTRR" REBOOT="R" /w
```

2. Add the following command to the end of the `nrdeploy.xml` file in `C:\tvtrr\Program Files\Lenovo\Rescue and Recovery`:

```
<Rescue__and__Recovery..Settings..Backup path  
="Rescue and Recovery\Settings\Backup">
```

To EXCLUDE a partition, add the following to the `nrdeploy.xml` file:

```
<BackupPartitions dword="20" />  
</Rescue__and__Recovery..Settings..Backup>
```

For additional information on how to use the `nrdeploy.xml` file, refer to the ThinkVantage Technologies XML/ADM supplement on the Lenovo Web site

at:
<http://www.lenovo.com/support/site.wss/document.do?Indocid=TVAN-ADMIN#rnr>

3. If you want to exclude .mpg and .jpg files from the backups, set the registry entry to include them at: HKLM\SOFTWARE\Lenovo\Rescue and Recovery\Settings\BackupList. For more information on including and excluding backups with the registry see Include and exclude backup files with Registry settings“Include and exclude backup files with registry settings” on page 26.
4. Install the Rescue and Recovery program using MSIEXE:
 - a. For all MSI files, add the following installation-log generation code:
`/L*v %temp%\rrinstall.txt`
 - b. To install the setup files using MSIEXE, type the following command:
: Perform the install of Rescue and Recovery

`msiexec /i "C:\TVTRR\Rescue and Recovery.msi"`
 - c. To silently install the setup files using MSIEXE:
With reboot at the end, enter the following command:
: Silent install using the MSI with a reboot

: Type the following command on one line
`start /WAIT msiexec /i "C:\TVTRR\Rescue and Recovery.msi" /qn`
With reboot suppressed, enter the following command:
: Silent install using the MSI without a reboot

: Type the following command on one line
`start /WAIT msiexec /i "C:\TVTRR\Rescue and Recovery.msi" /qn REBOOT="R"`
5. Enter the following commands:
:Start the Rescue and Recovery Service
`net start "TVT Backup Service"`

:Create Sysprep Base Backup to Local Hard Drive

: Type the following command on one line

`cd "\Program Files\Lenovo\Rescue and Recovery"`
`rrcmd sysprepbakup location=L name="Sysprep Base Backup"`
If you want to use a password, add the syntax `password=pass`.
6. Run 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. **  
*****
```
7. Shut down and reboot the machine when Sysprep is complete.

Note: The operating system will reboot into the Predesktop Area of the Rescue and Recovery program. The status bar with **System Restore in Progress** will appear.
8. When complete, the message **Sysprep Backup is Complete** will appear.
9. Power off the system using the power button.
10. Capture the image for deployment.

Supported Sysprep multiple drive configurations

Windows PE drive enumeration may be different than the Windows main operating system enumeration for Primary partitions. If you wish to backup to a partition other than C:\ Primary, you must set the Backup partition type to Extended.

Note: Backups will fail when doing a Sysprep backup if the drive letters of the partitions are changed after running the Sysprep backup.

Password Persistence

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

Table 13. Password Persistence considerations

Issue	Impact if Password Persistence is enabled
If a user logs into an 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 current account and password.	<ul style="list-style-type: none">• User will lose Encrypted File System data• You cannot use Encrypted File System and Password Persistence together.
If the user did not exist on backup, then the user will not have any of their user folders or files. All Internet Explorer favorites and application data do not exist.	<ul style="list-style-type: none">• The User ID documents settings are not set.• Potential data loss
Deleting the user ID in the current accounts and passwords will remove the user ID authentication information from all the backups.	<ul style="list-style-type: none">• User does not have access to data.
If a manager or a network administrator wanted to delete the access of several ex-employees and wanted to restore to the base backup to reset the system to remove all of the employees authentication accounts, the ex-employees would still have access with Password Persistence.	<ul style="list-style-type: none">• Is not a standard of the Microsoft User ID maintenance practices and recommendations.

When restoring from a local hard drive, the current password will be used when Password Persistence is selected. When restoring from USB or the network, the password of the most recent backup will be used.

EFS file limitation

The date and time stamp attributes are not preserved for EFS files restored by the Rescue and Recovery program, all other files will retain their original date and time.

Battery power settings for backups

With the corresponding ADM file installed for the Rescue and Recovery program, if you have the Battery Percent Requirement set in Group Policy at 1% in the following ADM path: *ThinkVantage\Rescue and Recovery\Settings\Backup*, and the system that you are attempting to backup has 1% remaining battery power, set the following policy to **Hide** the **No Battery** user message:
ThinkVantage\Rescue and Recovery\Settings\User Messages

For more information on Active Directory configurations for the Rescue and Recovery program using Group Policy, see the accompanying XML/ADM Supplement for the deployment guide located on the ThinkVantage Technologies Administrator Tools page:

<http://www.lenovo.com/support/site.wss/document.do?Indocid=TVAN-ADMIN#rnr>

Completing a backup

Applications installed or uninstalled after the selected backup is created might need to be installed again to function correctly. Make sure that the system is connected to an AC power supply before initiating a backup, restore, rejuvenation, or archive procedure. Failure to do so can result in data loss or an irretrievable system failure.

Microsoft Message Queuing (MSMQ)

If you are using MSMQ, you might have problems starting the service after from an incremental backup. That is how the Rescue and Recovery program knows what files have changed so it can back them up. So, if all those files aren't backed up on an incremental, then the files could get out of synch and cause the service to fail. Here are some registry settings that run a command before the Rescue and Recovery program takes a backup that sets the Archive bit on all files in the MSMQ directory. This means the entire directory will be backed up every incremental.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Lenovo\Rescue and Recovery\Settings\Backup
\PreBackup]
"Pre"="cmd"
"PreParameters"="/c attrib +A \"%windir%\system32\msmq\*.*)" /S /D"
"PreShow"=dword:00000000
```

Rescue and Recovery in the Windows environment

The following sections provide information on using the Rescue and Recovery program in the Windows environment and in the Predesktop Area.

Using the Rescue and Recovery program in the Windows environment

The Rescue and Recovery program in the Windows environment enables you to perform numerous types of backups. The following information instructs you on how to use backup files with the Rescue and Recovery program.

Include and exclude backup files with registry settings

The Rescue and Recovery program can include and exclude an individual file, a folder, or an entire partition. With Rescue and Recovery 4.3, these capabilities are controlled by the following registry entries which are the type REG_MULTI_SZ:

- HKLM\SOFTWARE\Lenovo\Rescue and Recovery\Settings\BackupList
- HKLM\SOFTWARE\Lenovo\Rescue and Recovery\Settings\ExcludeList
- HKLM\SOFTWARE\Lenovo\Rescue and Recovery\Settings\OSAppsList

Setting the base backup location: The following registry entry will set a base backup as soon as an installation is complete:

```
HKLM\Software\Lenovo\Rescue and Recovery\runbasebackuplocation
DWord = location value
```

BackupList: The registry entry format is:

HKLM\SOFTWARE\Lenovo\Rescue and Recovery\Settings\BackupList

- One line per include/exclude rule entry.
- If more than one setting applies to a file or folder, the last setting applied is used. Entries at the bottom of the registry entry take precedence.
- Entries must start with either:
 - ;
for a comment
 - I
for include files or folders that match the entry
 - X
for exclude files or folder that match the entry
 - S
for include Single Instance Storage on a file or a folder
 - i
for files or folder that you can choose to include
 - x
for files or folders that you can choose to exclude
 - s
for files or folders that the user can choose to add to Single Storage

The following are examples of entries:

```
S=*
X=*
i=*
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=?:\Program Files\*
I=?:\msapps\*
X=?:\Recycled
X=?:\RECYCLER
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\*
  s=?:\Documents and Settings\*\Desktop\*
  s=?:\Documents and Settings\*\My Documents\*
x=*.vol
s=*.vol

```

ExcludeList: Within this section of the registry, you can choose to exclude software applications from the recovery process initiated by the Rescue and Recovery program. This GUI exclude list is managed through the registry at: HKLM\SOFTWARE\Lenovo\Rescue and Recovery\Settings\ExcludeList.

OSAppsList: The Rescue and Recovery program 4.3 provides the ability to selectively restore particular files and folders when doing an OS & Apps restore through the registry key settings:

HKLM\SOFTWARE\Lenovo\Rescue and Recovery\Settings\OSAppsList

The OSAppsList setting will define what files, folders, or file types comprise the operating system and applications. This file can be customized by the administrator and a default external file will be provided. When the user chooses to recover the operating system, they will see a menu that allows them to choose Restore.

Only with the following Windows options: Only files that match the rules contained in this external file will be restored. The administrator can customize the contents of this external file.

Trouble ticket

Because there is no way to transmit information through file transfer or e-mail from the Rescue and Recovery environment, the end user is directed to use the e-mail function integrated in the browser. The logging function packages the log events into a file, and directs the end user to e-mail the file after he or she completes the recovery process and logs onto Windows. The file received from the end user creates the *Req 115 Trouble Ticket* XML file, which combines (Current, HW, InvAgent, and PCDR diagnostic log information), and will be placed in a location which can be easily found and accessible from both the Rescue and Recovery environment and operating system – C:\SWSHARE.

The Diagnostics tool available in the Predesktop Area of the Rescue and Recovery program aids in problem determination. Output from tests performed by the Diagnostics tool are stored in a manner which can be viewed or transmitted to a help desk.

Rescue and Recovery interface switching

The Rescue and Recovery user interface provides the option to switch between the simplified user interface and the advanced user interface. The simplified user interface has a few basic options, while the advanced user interface has extended options. By default, you will see the simplified user interface each time the Rescue and Recovery program is started unless the setting is disabled.

If the **Simplified User Interface** setting is disabled, the advanced user interface will be displayed each time the Rescue and Recovery program starts. You can disable the simplified user interface at the following Active Directory policy:

ThinkVantage\Rescue and Recovery\User Interface\Simple User Interface

You can disable interface switching so that a user will not be able to switch between the two interfaces. To disable the interface switching, set the following Active Directory policy to **Disabled**:

ThinkVantage\Rescue and Recovery\User Interface\Interface Switching

For additional information about Rescue and Recovery settings and working with Active Directory and Group Policy, see the accompanying XML/ADM Supplement for the deployment guide located on the ThinkVantage Technologies Administrator Tools page:

<http://www.lenovo.com/support/site.wss/document.do?Indocid=TVAN-ADMIN#rnr>

Working with the Predesktop Area

To customize parts of the Rescue and Recovery Predesktop Area, use the `rrutil.exe` utility program to GET and PUT files from the Predesktop Area or the protected backups folder.

Note: The Predesktop Area can be manually started if the operating system does not start.

These files or directories along with their customization options are listed in the following table:

Table 14. RRUTIL.exe files and customization options

File or Directory	Customization options
\MININT\SYSTEM32 WINBOM.INI	Add a static IP address, change video resolution. Note: If you customize the winbom.ini file for the Rescue and Recovery program, you must customize all winbom.ini files.
\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 or change behavior of files with specific extensions.
OPERA_010.CMD	Exclude Window user's favorites.
OPERA6.INI	Configure the Opera browser or disable the address bar.
PDAGUIxx.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.

The `\minint` subdirectory does not exist on the Windows Vista version of the Rescue and Recovery program. The new subdirectory in Windows Vista is `\vtos` and the entire preinstallation environment of the operating system is contained in a WIM file.

To edit the WIM file, you need to obtain the `imagex.exe` file in the Microsoft OEM Preinstallation Kit (OPK) for Windows Vista.

Working with WIM files and ImageX

Windows 7 deployment is based on disk imaging using ImageX. ImageX utilizes file-based imaging with WIM files instead of sector-based image formats. Considering this formatting development, use the scenario in “Scenario 6 - Performing a Bare Metal Restore from an Admin Backup” on page 58 when installing and deploying the Rescue and Recovery program on Windows 7.

Using RRUTIL.EXE

The RRUTIL program is designed to access the Rescue and Recovery service partition and virtual partition data. This utility will work with both virtual partitions and type 0x07 partitions. This utility allows customization of the Predesktop Area (PDA) by administrators. Only an Administrator user can use this tool by default.

You can obtain rrutil.exe from the ThinkVantage Technologies Administrator Tools Web page located at:
<http://www.lenovo.com/support/site.wss/document.do?Indocid=TVAN-ADMIN#rnr>

The RRUTIL program works with the Rescue and Recovery filter driver on virtual partitions, and mounts type 0x07 partitions as a drive in order gain access. The opening of these partitions is only done long enough to perform the requested commands then closed again.

Note: The RRUTIL program for version 4.3 is not backwards compatible with earlier versions of the Rescue and Recovery program.

This program allows administrators to perform the following functions:

- View directories in the Predesktop Area.
- Add or update files in the Predesktop Area.
- Delete files from the Predesktop Area.
- Rename files in the Predesktop Area.
- View the files in \RRbackups directories.
- Add backups to \RRbackups directories.
- Get files from \RRbackups directories.
- Display the disk space usage of \RRbackups directories.

Predesktop Area directory list

```
RRUTIL /lx [<path>dirlist.txt]
```

Create a list of the contents of the \preboot, \minint, or root directories of the Predesktop Area partition either virtual or type 0x07:

1. The data is written as a text stream of all the files in each sub directory to a file named dirlist.txt in a directory name supplied by the user, or to the root of drive c:\ if not path is given.
2. This would be the equivalent of the following DOS style command (“dir * /s > c:\temp\dirlist.txt”) in the directory of interest. Listing of the contents of the root of the PE partition would be “dir * > c:\temp\dirlist.txt” only. Example output:

```
Directory of \
```

```
10/20/03 00:00:00 AM          42  AUTOEXEC.ICR
03/12/04 00:00:00 AM          42  AUTOEXEC.bat
```

03/10/04 00:00:00 AM	165	BOOT.INI
08/16/02 00:00:00 AM	53786	COMMAND.COM
12/16/03 00:00:00 AM	222	CONFIG.ICR
12/16/03 00:00:00 AM	222	CONFIG.SYS
04/06/00 00:00:00 AM	655	FINDDRV.BAT
09/17/03 00:00:00 AM	14320	HIMEM.SYS

- An optional command line input will be a text file to capture the output of this option.
- Sample command: RRUTIL /lx [<path>dirlist.txt] Note: Enablement of the optional entry may be deferred to a later release.

The following list provides the values for x:

- 1 \preboot
- 2 \minint
- 4 <root of c:\ or root of type 0x07 partition>

Multiple listings would be simple addition of each x. So \preboot and \minint would be a value of 3. dirlist.txt contents:

```
\minint\system32\drivers*.sys
\preboot\startup\*.*
```

Get files from Predesktop Area directories

```
RRUTIL /g <path>getlist.txt <copy to location>
```

Copy individual files from the \preboot, \minint, or root of the PE partition either virtual or type 0x07:

- A text file identifies the files that should be copied to a location specified in the command line.
- The <copy to location> must be an existing directory that will receive the files from the Predesktop Area. The files will be copied in this directory in same tree structure as they are found in the Predesktop Area. This will avoid same name files from copying over each other.
- Sample command: RRUTIL /g <path> getlist.txt <copy to location> getlist.txt contents:

```
\PELDR
\preboot\startup\Restore.cmd
\preboot\usrintfc\PDAGUI.ini
```

Note: Wildcards are not supported in this function. You must understand the Predesktop Area environment before attempting any modifications.

Put files in the Predesktop Area directories

```
RRUTIL /p <path>
```

Update (add/replace) files in \preboot, \minint, or root of the PE partition either virtual or type 0x07:

- Place all the files in a temp folder on drive c:\. Based on location in the temp directory, the files will be copied into the PE partitions in the same locations. For example, to add/replace a file.cmd file in \preboot\startup, the user would place the file.cmd file in c:\tempdir\preboot\startup and then run the command "RRUTIL /p c:\tempdir".
- Sample Command: RRUTIL /p c:\PDATemp contained in c:\PDATemp would be a mirror image of the directory structure of \preboot, \minint, or root of Predesktop Area. The files in the root of c:\PDATemp would put the files in the root of the PE partition.

Delete files from the Predesktop Area directories

```
RRUTIL /d C:\temp\dellist.txt
```

Delete a file in the \preboot, \minint, or root of the Rescue and Recovery partition either virtual or type 0x07:

1. Delete the file(s) of \preboot, \minint, or root of the PE partition either virtual or type 0x07 based on the contents of a text file.
2. Dellist.txt must contain a tree structure of the files to be deleted from the PDA.
3. Sample Command: RRUTIL /d <path> dellist.txt dellist.txt contents:

```
\preboot\startup\custom.cmd Sample file name only  
\preboot\usrintfc\test.txt Sample file name only
```

Rename a file in the Predesktop Area

```
RRUTIL /r \<PDA-path>\oldfilename.ext newfilename.ext
```

Rename a file located in the Predesktop Area. This function only works on files in the Predesktop Area. The path to the file to be renamed must be included without the drive letter. The new name of the file should only include the name without any path information.

Example:

```
RRUTIL -r \preboot\usrintfc\peaccessibmen.ini peaccessibmen.old
```

Test for Rescue and Recovery being installed

```
RRUTIL /bq
```

This command can be used in a batch file to help in automated processing. If the Rescue and Recovery code is not installed on the system only, the functions that access the Predesktop Area will be available.

Example:

```
RRUTIL -bq
```

Results in the environment variable %errorlevel% being set to -2, if the Rescue and Recovery program is not installed on the system, or 0 if the Rescue and Recovery program is installed. Type echo %errorlevel% to see the results of the command.

Backup directory list

```
RRUTIL /bl <path>
```

List all of the contents of the \RRbackups directories. Display the file size and date of each file in the backup as well as its location. The list below is an example of a backup directory with a base backup and one incremental backup.

```
Directory of \RRbackups\C\0\
```

```
03/11/04 08:02:44 AM 50003968 Data0  
03/11/04 08:04:05 AM 50003968 Data1  
03/11/04 08:07:10 AM 50003968 Data10  
03/11/04 09:09:03 AM 50003968 Data100  
03/11/04 09:10:39 AM 50003968 Data101  
03/11/04 09:12:07 AM 50003968 Data102  
03/11/04 09:13:24 AM 50003968 Data103  
03/11/04 08:01:31 AM EFSFile  
03/15/04 22:22:47 PM 338772 HashFile  
03/11/04 09:17:44 AM 748 Info  
03/15/04 22:22:47 PM 34443040 TOCFile
```

Directory of \RRbackups\C\1\

```
03/15/04 22:29:29 PM 50003968 Data0
03/15/04 22:29:45 PM 50003968 Data1
03/15/04 22:44:50 PM 50003968 Data10
03/15/04 22:51:56 PM 50003968 Data11
03/15/04 22:56:39 PM 50003968 Data12
03/15/04 23:00:27 PM 43480478 Data13
03/15/04 22:30:00 PM 50003968 Data2
03/15/04 22:30:19 PM 50003968 Data3
03/15/04 22:30:34 PM 50003968 Data4
03/15/04 22:30:57 PM 50003968 Data5
03/15/04 22:32:25 PM 50003968 Data6
03/15/04 22:33:42 PM 50003968 Data7
03/15/04 22:34:40 PM 50003968 Data8
03/15/04 22:42:57 PM 50003968 Data9
03/15/04 22:22:47 PM EFSFile
03/15/04 23:00:27 PM 374742 HashFile
03/15/04 23:00:27 PM 748 Info
03/15/04 23:00:27 PM 38099990 TOCFile
```

Get files from \RRBackups directories

```
RRUTIL /bg <path>getlist.txt <copy to location>
```

Copy individual files from the \RRbackups directories:

1. A text file identifies the files that should be copied to a location specified in the command line.
2. The <copy to location> must be an existing directory that will receive the files from the \RRbackups directory. The files will be copied in this directory in the same tree structure as they are found in the \RRbackups directory.
3. Sample command: RRUTIL /bg <path> getlist.txt <copy to location> getlist.txt contents:

Note: Wildcards are not supported in this function. You must understand the \RRbackups directories environment before attempting modifications.

Put files in the \RRBackups directories

```
RRUTIL /bp <path>
```

Update (add/replace) files in \RRbackups virtual partition:

1. Place all the files in a temp folder on drive c:\, then based on location in the temp directory, files will be copied into the \RRbackups directories in the same location.
2. Sample command: RRUTIL /bp c:\SWTOOLS. In c:\SWTOOLS would be a mirror image of the \RRbackups directory structure where the files are to go.

```
c:\SWTOOLS\C\0 Data0 Data1
EFSFile HashFile Info TOCFile
```

to

```
C:\RRbackups\C\0 Data0 Data1
EFSFile HashFile Info TOCFile
```

Determine \RRBackups space consumed

```
RRUTIL /bs
```

Determine the amount of space that is consumed by \RRbackups

1. Ability to determine how much space is consumed by backups. Listing by backup, for example, base and each incremental how much space is consumed.

- Sample command: RRUTIL /bs would display the backup space on the console.

As previously stated in this chapter, the rutil.exe file enables you to GET files from and PUT files into the Rescue and Recovery environment, it also allows listing of files in the Rescue and Recovery environment and in the backups folder. These procedures are used for all file customizations of the Rescue and Recovery environment. The following procedures provide another example of how to utilize the GET and PUT function with the Rescue and Recovery environment.

To use rutil.exe, do the following:

- Copy rutil.exe to the root of the C drive.
- Create getlist.txt file with the following syntax:

```
\preboot\usrintfc\file name
```

Save the file as c:\temp\getlist.txt.

- At a command prompt, type the rutil.exe command and one of the switches defined in the following table. Then, complete the command with the appropriate parameters, as shown in the following table.

Table 15. Command and switch options

Command and switch options	Result
RRUTIL -l1	List the contents of preboot directory.
RRUTIL -l2	List the contents of minint directory.
RRUTIL -l4	List the contents of the root of the C drive or root of type 0x07 partition.
RRUTIL -g c:\temp\getlist.txt C:\temp	Get files from preboot partition.
RRUTIL -d c:\temp\ dellist.txt	Delete files from the preboot partition.
RRUTIL -p c:\temp	Add or replace files in the preboot partition.
RRUTIL -r path \oldname.ext newname.ext	Rename a file in the Predesktop Area.
RRUTIL -r \temp\rr\test.txt test2.txt the file is in the preboot\rr directory	
RRUTIL -bp c:\temp	Update or replace files in RRBACKUPS virtual partition.
RRUTIL -bl path RRUTIL -bl lists to c:\rr-list.txt rrutil -bl c:\SWTOOLS	List the RRBACKUPS directory.
RRUTIL -bg c:\temp\bgetlist.txt C:\temp	Copy individual files from the \RRBACKUPS.
RRUTIL -bs	Display space used by RRBackups directory.

- After you have performed the GET routine, you can then edit the file using a standard text editor.

Example: pdaguixx.ini

This example refers to pdaguixx.ini, which is a configuration file where you can customize elements of the Rescue and Recovery environment (see “Customizing the preboot environment” on page 36).

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

Table 16. Language codes

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 `pdaguien.ini` from the Rescue and Recovery environment

1. Create `getlist.txt` file with the following parameters:

```
\preboot\usrintfc\pdaguien.ini
```
2. Save the file as `c:\temp\getlist.txt`.
3. At a command prompt, type the following command:

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

Putting the file `pdaguien.ini` back into the Rescue and Recovery environment

From a command line, issue the following command:

```
C:\RRUTIL.EXE -p c:\temp
```

Note: The PUT (-p) routine uses 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 as the `getlist.txt` file, as follows:

```
c:\temp\preboot\usrintfc\pdaguien.ini
```

Example 1: Adding device drivers (such as ethernet) to the Predesktop Area

The following example provides instruction on adding device drivers to the Predesktop 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, the `E100B325.din` or `INTELNIC.dll` files must be in the `\MININT\SYSTEM32\DRIVERS` directory.)

Notes:

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

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

Example 2 : Adding mass-storage controller drivers (such as SATA) to the Predesktop Area

1. Create a subdirectory under \minint\system32\ to contain the driver.
2. Copy *.sys into \minint\system32\drivers.
3. Update \minint\system32\winpeoem.sif to include the subdirectory containing the driver (for an example, examine this file from 4.3 build 37).
4. Ensure the iastor file and folder are in the subdirectory you created..
5. Make sure the subdirectory you created containing the iastor driver has a valid txtsetup.oem file.

Customizing the preboot environment

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

- Changing the main GUI fonts
- Changing 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 obtain, edit, and replace the pdaguixx.ini file, see “Example: pdaguixx.ini” on page 34.

Changing the main GUI fonts

You can change the font of the main graphical user interface (GUI). The default settings might not display all characters correctly, depending on the language and characters required. In pdaguixx.ini (where *xx* is the language designation) the [Fonts] section contains the default settings for the character style that is 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 and tested with the Rescue and Recovery environment:

- Courier
- Times New Roman
- Comic Sans MS

Other fonts might be compatible, but have not been tested.

Changing the environment background

The background of the right panel is a bitmap graphic and is named mainbk.bmp. The file mainbk.bmp 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 high

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

Note: To get, edit, and replace the mainbk.bmp file, see “Using RRUTIL.EXE” on page 30.

Editing pdagui.ini

Changing the left-panel entries requires editing the pdaguixx.ini (where xx is the language designation) file. For information about getting pdaguixx.ini from the Rescue and Recovery environment and replacing the file, see “Using RRUTIL.EXE” on page 30.

The Rescue and Recovery program has twenty-two 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, %tvtdrive%\Preboot\Opera\ENum3.exe,
```

Table 17. Left-panel entries and customization options

Entry	Customization options
00-01	Fully customizable.
02	Must remain a button type 1 (see Table 18 on page 38). Text can be changed. An application or help function can be defined. No icon can be added.
03-06	Fully customizable.
07	Must remain a button type 1. Text can be changed. An application or help function can be defined. No icon can be added.
08-10	Fully customizable.
11	Must remain a button type 1. Text can be changed. An application or help function can be defined. No icon can be added.
16	Must remain a button type 1. Text can be changed. An application or help function can be defined. No icon can be added.
17-22	Fully customizable.

Defining entry types: **Button00** must be a unique identifier. The number determines the order by which the buttons are 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:

Table 18. Entry type parameters

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. 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. Define a help topic to be launched using the Opera browser.
4	Display a restart message window before launching. Change the value to direct the GUI to present a message to the user that the computer must be restarted before the specified function is performed.
5	Reserved.
6	Reserved.
7	Launch and wait. Use this value to force 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. The GUI retrieves 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.
9	Reserved.
10	Reserved.

Defining entry fields:

Button00=[0-10], "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 is cut and ellipsis points indicate that more characters follow. The full title text is displayed when using hover help.

Button00=[0-10], "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=[0-10], "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 entry.

Button00=[0-10], "title", file.bmp, [0 or 1], 1

This is a reserved function and must always be set to 1.

Button00=[0-10], "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 is required before a specified application is started.

Button00=[0-10], "title", file.bmp, [0 or 1], 1, [0 or 1], %tvtdrive%[pathname\executable]

The value of %tvtdrive% 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=[0-10], "title", file.bmp, [0 or 1], 1, [0 or 1], %tvtdrive %[pathname\executable], [parameters]

Provide the 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, 07, 11 and 16 must remain type 0 (or header) entries, and they 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-three.

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

Table 19. Left-panel functions and executables

Function	Executable
Recover files	WIZRR.EXE
Restore from backup	WIZRR.EXE
Open browser	OPERA.EXE
Map a network drive	MAPDRV.EXE
Diagnose hardware	PCDR.CMD; launches the PC Doctor application, and Lenovo-branded preinstallation models only
Create diagnostic diskettes	DDIAGS.CMD

Changing entries and functions in the right panel

Changing the right-panel entries require editing the pdaguixx.ini (where xx is the language designation) file. For information regarding getting pdaguixx.ini from the Rescue and Recovery environment and replacing the file, see "Example: pdaguixx.ini" on page 34.

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 pdaguixx.ini (where xx is the language designation). These links operate the same way as the left-panel entries. The button number values are 00 through 04. The same applications that can be started from the left panel can be started from the [TitleBar] entries. See "Using RRUTIL.EXE" on page 30 for a complete list of executables that can be started from the title bar.

Modifying user messages and window status: pdaguixx.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 pdaguixx.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 12. You can set the font that the title, head and bold is displayed in.

The following settings are an example for the [Welcome] section:

```
[Welcome]
Title = "Welcome to Rescue and Recovery"
Line01 = "The 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 your files, folder or backups using Rescue and
Recovery(TM)"
Line05 = "*Configure your system settings and passwords"
Line06 = "your system settings and passwords"
Line07 = "*Communicate using the Internet and link to the Lenovo support site"
Line08 = "use the Internet and link to the Lenovo support site"
Line09 = "*Troubleshoot problems using diagnostics"
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**
Lenovo License Agreement HTML page.
- **HELP**
Help
- **LICENSE**
License
- **CANCEL**
Cancel
- **Command0**
%vttdrive%\Preboot\Helps\en\f_welcom.htm
- **Command1**
%vttdrive%\Preboot\Helps\en\C_ILA.htm

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

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

In the [REBOOT] section of the pdaguixx.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. To hide the message, mark the check box. When the check box is marked, 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 pdaguixx.ini (where xx is the language designation) are available in the file, but cannot be customized: [Messages], [EXITMSG], and [HelpDlg].

Removing Factory Restore

To hide the Restore to Factory Contents option in Windows PE, rename the file \preboot\recovery\Recover.cmd to another name and that option will not appear on the wizard. That renamed .cmd file can later be run to restore from factory contents. If the service partition has been removed, then this step is not necessary.

Configuring the Opera browser

The Opera browser has two configuration files: the default configuration file, and the active configuration file. An user can make changes to the active configuration file, but loses changes made when the Rescue and Recovery program is restarted.

To make permanent changes to the browser, edit the copies of both the opera6.ini and the 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, see "Using RRUTIL.EXE" on page 30.
2. The Opera workspace has been modified to provide enhanced security. Some browser functions have been deleted.

Opera will not save settings after it is closed

If you are using the Rescue and Recovery program under Windows 7 and want to have the Opera browser remember its preferences during the current boot to the Predesktop Area, modify the opera.exe file. Specify the full path to the settings file on the fifth line of the \preboot\opera\opera_web.cmd from

```
start opera.exe /Settings opera_default.ini %1
```

to

```
start opera.exe /Settings %tvtdrive%\preboot\opera\opera_default.ini %1
```

Note: If you reboot, your changed preferences will be lost even with this change.

E-mail

The Rescue and Recovery program provides support for Web-based e-mail through the Opera browser. Opera provides IMAP-based e-mail which can be enabled through the large enterprise configuration, but is not supported. To get the reference information on how to enable, read the *System Administrator's Handbook* at:

<http://www.opera.com/support/mastering/sysadmin/>

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 RRUTIL process described in "Using RRUTIL.EXE" on page 30.
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 disables the Opera toolbar, but leaves 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 RRUTIL process as described in "Using RRUTIL.EXE" on page 30. The address bar is disabled when Opera runs.

Customizing bookmarks

The Opera browser is configured to read the bookmarks established in this ramdrive file: Z:\OPERADEF6.ADR. This file is generated when the Rescue and Recovery program is started from code in the startup routine. The startup routine automatically imports Windows Internet Explorer bookmarks and adds some additional bookmarks. Because the ramdrive file that is generated on startup is not permanent, it adds bookmarks to Internet Explorer, which is 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 RRUTIL process described in "Using RRUTIL.EXE" on page 30.
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, enter the following:
python.exe favs.pyc z:\operadef6.adr "All Users, Administrator"
5. Save the file.
6. Put the file back by using the RRUTIL process described in "Using RRUTIL.EXE" on page 30.

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

1. Get the C:\PREBOOT\STARTUP\OPERA_010.CMD for editing by using the RRUTIL process as described in "Using RRUTIL.EXE" on page 30.
2. Open the file for editing.
3. Locate the following line in the .CMD file: PYTHON.EXE.FAVS.PYC
Z:\OPERADEF6.ADR
4. Complete 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.
5. Save the file.
6. Put the file back by using the RRUTIL process described in "Using RRUTIL.EXE" on page 30.

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 by using the RRUTIL process described in "Using RRUTIL.EXE" on page 30.
2. Open the file for editing.
3. 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>

4. Save the file.
5. Put the file back by using the RRUTIL process described in "Using RRUTIL.EXE" on page 30.

To add an HTTP, HTTPS, FTP, Gopher, or WAIS proxy server, 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 is true 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 follows:

1. Get the C:\PREBOOT\OPERA\DEFAULTS\STANDARD_menu.ini file by using the RRUTIL process described in "Using RRUTIL.EXE" on page 30.
2. Locate the following string:
;;Item, 50761
3. Open the file for editing.
4. Locate the [Link Popup Menu].
5. Remove the two semicolons, and then save the file. When the Rescue and Recovery program is closed and reopened, a user is able to right-click a link and the "Save Target As" option is displayed. This results in display of the "Save As" window.

Note: Straight links (not redirected links) work with the preceding procedure. For example, if a link targets a .php script, Opera saves the script only, not the file to which the script points.

6. Put the file back by using the RRUTIL process described in "Using RRUTIL.EXE" on page 30.

To specify a fixed download directory, do the following:

1. Get the C:\PREBOOT\OPERA\norm1.ini file by using the RRUTIL process described in "Using RRUTIL.EXE" on page 30.
2. Open the file for editing.
3. In the file, locate this line:
Download Directory=%OpShare%
4. Change %OpShare% to the full path of the directory to which you want downloaded files to be saved.
5. Save the norm1.ini file. When the Rescue and Recovery program is closed and reopened, Opera saves downloaded files to the specified directory.
6. Put the file back by using the RRUTIL process described in "Using RRUTIL.EXE" on page 30.

Notes:

1. Customizing the full path for downloading does not enable users to save the target file, even if the link is redirected.
2. The Opera browser is configured to download only the .zip, .exe, and .txt file types, and customizing only changes Opera behavior for these file types. Internet access is provided to help users get up and running. For the purposes of the Rescue and Recovery program, the number of recognized file types is limited. If another file type needs to be transferred, create a .zip file, which can then be extracted.)
3. File types are recognized by MIME (Multipurpose Internet Mail Extensions) type rather than by file extension. For example, if a .txt file is named with .euy as an extension, the file is 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 RRUTIL process described in "Using RRUTIL.EXE" on page 30.
3. Open the file for editing.
4. Locate the [File Types] section of the file.

5. Use the search function find the desired file, 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/mpeg=8,, ,mpeg,mpg,mpe,m2v,m1v,mpa,|`

`to`
`video/mpeg=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 specified value is already set , do not change the value.
 - d. Save the file, and then copy the file to opera6.ini, and then restart the Rescue and Recovery program 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\.
 - d. Copy the file to opera6.ini.
 - e. Restart the 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 help files.
2. Get the preboot\opera\norm1.ini file by using the RRUTIL process described in "Using RRUTIL.EXE" on page 30.
3. Open the file for editing.
4. Locate the [File Types] section of the file. Search for the extension you want to work with. For example, you want all .txt files to be saved to the SWSHARE folder.
5. 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 SWSHARE folder.

6. Continuing with the .txt example, change the line to read as follows:
`TEXT/PLAIN=1,,,,TXT,|`
7. Save the file.

8. Put the file back by using the RRUTIL process as described in “Using RRUTIL.EXE” on page 30.
9. Restart the Rescue and Recovery workspace for changes to be effective.

Adding a static IP address

To add a Static IP address, complete the following steps:

1. Get the \MININT\SYSTEM32 winbom.ini file by using the RRUTIL process described in “Using RRUTIL.EXE” on page 30.
2. Open the file for editing.
3. 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
```

4. Get the \PREBOOT\SWWORK NETSTART.TBI file by using the RRUTIL process described in “Using RRUTIL.EXE” on page 30.
5. Change


```
factory -minint
```

 to


```
factory -winpe
```
6. Comment out the following lines:


```
regsvr32 /s netcfgx.dll
netcfg -v -winpe
net start dhcp
net start nla
```
7. Put the \SWWORK\ NETSTART.TBI and \MININT\SYSTEM32 winbom.ini files back by using the RRUTIL process described in “Using RRUTIL.EXE” on page 30.

Note: The default environment supports only the DHCP environment.

The following table provides the entry and description for IP configurations:

Table 20. Static IP address entries

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

Changing the video resolution

You can change the video resolution by changing the default Predesktop Area resolution settings of 800 × 600 × 16-bit. To change the settings, complete the following procedures:

1. Get the \MININT\SYSTEM32\WINBOM.INI file by using the RRUTIL process described in “Using RRUTIL.EXE” on page 30.
2. Open the file for editing.
3. Add the following entries:

```
[ComputerSettings]
DisplayResolution=800x600x16 or 1024x768x16
```

When the Rescue and Recovery environment starts, you see an additional window during startup that is titled “Factory preinstallation”. The colors are reduced from thousands to 256.

4. Put back the \MININT\SYSTEM32\WINBOM.INI file by using the RRUTIL process described in “Using RRUTIL.EXE” on page 30.

Startup applications

The Rescue and Recovery Windows PE environment has the ability to support a startup scripts, programs, or customized programs. These scripts or programs will be processed before the Rescue and Recovery Windows PE environment reaches the main PE interface page.

The directory to place the scripts or programs is \Preboot\Startup. Scripts or programs in this directory are processed alphanumerically. For example, a script called a.bat would be processed before 1.exe.

To place a script or program in this directory, complete the following steps:

1. Get the RRUTIL from the Lenovo Rescue and Recovery Administration Tools site at:
<http://www.lenovo.com/support/site.wss/document.do?lnocid=TVAN-ADMIN#rnr>
2. Create a Temp directory.
3. In the \Temp directory create the following directory tree: \preboot\startup.

4. Put the script or program into the \Temp\preboot\startup path.
5. From a command line, type in RRUTIL -p \Temp.
6. To verify that the script or program was copied successfully, type in RRUTIL -g from a command line. This will generate a file named getlist.txt.
7. Examine the contents of getlist.txt for the \preboot\startup directory. The script or program should be listed under this tree.

Passwords

The following are four password options available in the Predesktop Area:

- Predesktop Area or Master password
- User ID and password or passphrase
- Backup password
- No password

Predesktop Area or master password

You can set an independent Predesktop Area password. This password is set through the command line interface, and is the only password option available if the Rescue and Recovery program 4.3 only is installed on the system.

You can create this Predesktop Area password using the following command: C:\Program Files\Lenovo\Rescue and Recovery\pe_masterpw_app.exe. The parameters for this command are:

Table 21.

Parameter	Description
pe_masterpw_app.exe -create	Creates the actual password.
pe_masterpw_app.exe -verify	Verifies that the password is valid and that it can be used.
pe_masterpw_app.exe -remove	Removes the password
pe_masterpw_app.exe -exists	Checks to see if the password exists.
pe_masterpw_app.exe -silent	Hides all the messages.

Backup password

The backup password can be set through the GUI Set Password or command line interface RRCMD with backup specified. Following are some examples:

```
rrcmd backup location=L name=mybackup password=pass
```

```
rrcmd basebackup location=L name=basebackup password=pass
```

```
rrcmd sysprepbackup location=L name=Sysprep Backup password=pass
```

No password

This option uses no authentication and allows the user to enter the Predesktop Area without using a password.

Password access

There are three options for password access:

- Master password
- User ID and password or passphrase
- No password

Master password

The master password is a single password that allows you access to the Predesktop Area and backups. This is set by using the command line interface, and is the only password option if Client Security Solution is not installed.

User ID and password or passphrase

This option uses the Client Security Solution code for password or passphrase management. The Client Security Solution GINA will prompt the user for this password or passphrase on startup of the Predesktop Area. This provides better security for a multi-user environment. If a user logs on using the GINA, that user is allowed access to that user's files only, and no one else's.

This option can be set through the command line interface or the GUI.

No password

This option uses no authentication.

Log files

The following are log files located in the C:\swshare directory:

- Engine.log
Logs all activities of the engine and the main backup service.
- rr.log
Logs all activities of the main Rescue and Recovery user interface.
- Restore.log
Logs restore operations like full restore, rejuvenate, and single file restore operations.
- tvtsched.log
Logs the scheduler service that calls the Rescue and Recovery program and/or InvAgent.
- Rescue.log
Logs the activities of the mailman.exe program.
- patch.log
Logs the activities of the Rescue and Recovery patches applied to the system.
- sft.log
Logs single file restore operations.

Create Rescue Media

The Create Recovery Disc function has been separated from the Create Rescue Media application in the Windows 7 version of the Rescue and Recovery program, and this makes the Create Rescue Media a unique function to create the bootable rescue media for virtual Predesktop Area. To enhance user experience, we provide the following entries to launch the Create Rescue Media program in the Rescue and Recovery program 4.3:

1. An additional menu button for accessing the Create Rescue Media program is available in the advanced mode of the Rescue and Recovery program.
2. A shortcut to the Create Rescue Media program is available on the **Advanced** tab in the advanced mode of the Rescue and Recovery program.
3. The Create Rescue Media function is embedded in the Lenovo ThinkVantage Tools application.

4. A message prompts to create the rescue media when performing a backup, if the Rescue and Recovery program detects that no rescue medium has been created before.

For more information about the Create Rescue Media function, consult its Help information system by pressing F1 after launching the Rescue and Recovery 4.3 program.

Chapter 4. Best practices

This chapter provides best practice scenarios to install and configure the Rescue and Recovery program for your enterprise. Within this chapter, you will find the following topics:

- “Scenario 1 - New rollouts”
- “Scenario 2 - Installing on OEM systems” on page 54
- “Scenario 3 - Installing with WIM files and Windows 7” on page 56
- “Scenario 4 - Standalone install for CD or script files” on page 57
- “Scenario 5 - Working with Active Directory and ADM files” on page 57
- “Scenario 6 - Performing a Bare Metal Restore from an Admin Backup” on page 58
- “Scenario 7 - Manually creating the Service Partition of S drive” on page 58

Scenario 1 - New rollouts

This section describes installing the Rescue and Recovery program in a new rollout on Lenovo-branded computers.

Preparing the hard disk drive

The first step to consider when deploying a system is preparing the hard disk drive of your donor system. In order to make sure you are starting with a clean hard disk drive, you must clean out the Master Boot Record on the primary hard disk drive.

1. Remove all storage devices, such as second hard disk drives, USB hard disk drives, USB memory keys and PC Card Memory 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 cleandrv.exe file 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 the Rescue and Recovery program. The last step in the process is to install the Rescue and Recovery program.

Installing

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

1. Assuming that the installation file is located in the root of the C drive, create a file EXE_EXTRACT.cmd, which will extract the file z902zisXXXXus00.exe for Windows 7 (where XXXX is the build ID) to the C:\SWTOOLS\APPS\rnr directory:

```
:: This package will extract the WWW EXE to the directory c:\SWTOOLS for an  
:: administrative installation.
```

```

@ECHO OFF
:: This is the name of the EXE (Without the .EXE)
set BUILDID=z902zisXXXus00.exe
:: This is the drive letter for the z902zisXXXus00.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 EXMD c:\SWTOOLS
:: Explode the WWW EXE to the directory c:\SWTOOLS
start /WAIT %SOURCEDRIVE%\%BUILDID% /a /s /v"/qn TARGETDIR=c:\SWTOOLS"
Copy z902ZAB10YYUS00.tvt and Z333ZAA10ZZUS00.tvt to c:\SWTOOLS\
(where YY and ZZ are build IDs)
copy z902ZAB10YYUS00.tvt to c:\SWTOOLS
copy Z333ZAA10ZZUS00.tvt C: to c:\SWTOOLS
If you want installation for supported languages besides US,
copy z902ZAB10YYUS00.tvt to c:\SWTOOLS
(where YY is the build ID and CC is the country code).
copy z902ZAB10YYUS00.tvt to c:\SWTOOLS

```

2. You can make many customizations before the installation of the Rescue and Recovery program. Some examples in this scenario are:
 - Change maximum number of incremental backups to 4.
 - Set the Rescue and Recovery program to perform an incremental backup every day at 1:59 p.m. to the local hard disk drive and call it Scheduled.
 - Hide the Rescue and Recovery user interface to all users not in the local Administrators Group.
3. Customize the default rnrdeploy.xml file. Some parameters can be modified. See the *ThinkVantage Technologies XML/ADM Supplement* for more information.
4. In the same directory as the install MSI file, create an install.cmd file, which will perform several actions:
 - Copy the custom rnrdeploy.xml file into the installation package created in the c:\SWTOOLS directory:
 - Perform a silent installation of the Rescue and Recovery program without a reboot at the end.
 - Start the Rescue and Recovery program so that a base backup can be performed.
 - After the service is started, set up the environment to create an ISO image of the Rescue and Recovery 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 rnrdeploy.xml here
copy rnrdeploy.xml "c:\SWTOOLS\Program Files\Lenovo\Rescue and Recovery"
:: Install using the MSI with no reboot (Remove "REBOOT="R"" to force a reboot)
start /WAIT msiexec /i "c:\SWTOOLS\Rescue and Recovery.msi" /qn REBOOT="R"
:: Start the service. This is needed to create a base backup.
start /WAIT net start "Rescue and Recovery Service"
:: Make an ISO file here - ISO will reside in c:\Program Files\Lenovo\Rescue and Recovery\rrcd

```

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

```

:: Set up the environment
set PATH=%SystemDrive%\Program Files\Common Files\Lenovo\Python24
set PATHEXT=%PATHEXT%;.PYW;.PYO;.PYC;.PY

```

```

set TCL_LIBRARY=%SystemDrive%\Program Files\Common Files\Lenovo\Python24
\tcl\tc18.4
set TK_LIBRARY=%SystemDrive%\Program Files\Common Files\Lenovo\Python24
\tcl\tk8.4
set PYTHONCASEOK=1
set RR=C:\Program Files\Lenovo\Rescue and Recovery\
set PYTHONPATH="C:\Program Files\Common Files\Lenovo\Python24"
:: The next line will create the ISO silently and not burn it
C:\Program Files\Common Files\Lenovo\Python24\python
C:\Program Files\Common Files\Lenovo\spi\mkspiim.pyc
:: Take the base backup... service must be started
c:
cd "C:\Program Files\Lenovo\Rescue and Recovery"
RRcmd.exe backup location=L name=Base level=0
:: Reboot the system
C:\Program Files\Common Files\Lenovo\BMGR"/bmgr32.exe /R

```

Updating

You may need to make a major change to your system, such as a service pack update to Windows. Before you install the service pack, you force an incremental backup on the system and identify that backup by name by performing the following steps:

1. Create a FORCE_BU.CMD file and push it down to your target systems.
2. Launch the FORCE_BU.CMD file once it is on the target systems.

The contents of the FORCE_BU.CMD file are:

```

:: Force a backup now
"%RR%rrcmd" backup location=L name="Backup Before XP-SP2 Update"

```

Enabling the Rescue and Recovery desktop

After realizing the benefits of the Rescue and Recovery program for a period of time, you may 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 rrutil.exe. See "Using RRUTIL.EXE" on page 30 for more information.

To modify the Predesktop Area, the UPDATE_RRE.CMD script demonstrates several processes:

- Use rrutil.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 in file getlist.txt.
- Create a directory structure to put files back into the Predesktop Area after editing the appropriate file.
- 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 the **Open Browser** button in the Rescue and Recovery environment. The Web page <http://www.lenovo.com/thinkvantage> opens.

To make the change, when Notepad opens with the pdaguien.ini file:

1. Change the line:

```
button13 = 8, "Open browser", Internet.bmp, 1, 1, 0,
```

```
%vtddrive%\Preboot\Opera\Opera.EXE, http://www.pc.lenovo.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,
```

```
%vtddrive%\Preboot\Opera\Opera.EXE,
```

```
http://www.lenovo.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 RRUTIL.EXE" on page 30.
3. Reboot the system into the Rescue and Recovery environment.
4. After you analyze the system and determine that there are files that you must back up, update the registry key at HKLM\SOFTWARE\Lenovo\Rescue and Recovery\Settings\BackupList.

Table 22. UPDATE_RR.CMD script

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

File will open automatically

pause
:: Make a copy of original file
copy
c:\RRDeployGuide\GuideExample\RROriginal\preboot\usrintfc\PDAGUIen.ini
c:\RRDeployGuide\GuideExample\RROriginal\preboot\usrintfc\
PDAGUIen.original.ini
notepad
c:\RRDeployGuide\GuideExample\RROriginal\preboot\usrintfc\PDAGUIen.ini
pause
copy c:\RRDeployGuide\GuideExample\RROriginal\preboot\usrintfc\
PDAGUIen.ini c:\RRDeployGuide\GuideExample\put\preboot\usrintfc
:: Place the updated version of the PDAGUIen into the RR
c:\RRDeployGuide\RRUTIL\RRUTIL -p c:\RRDeployGuide\GuideExample\put
ECHO.
ECHO Reboot to the RR to see the change
pause
c:\Program Files\Lenovo\Common\BMGR\bmgr32.exe /bw /r

Create getlist.txt:
\preboot\usrintfc\pdaguien.ini
```

Scenario 2 - Installing on OEM systems

This section describes installing the Rescue and Recovery program on OEM computers. To install the Rescue and Recovery program, eight free sectors must be available in the Master Boot Record on the hard disk drive. The Rescue and Recovery program uses a custom Boot Manager in order to enter into the Recovery area.

Some OEMs 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 the Rescue and Recovery program provides the desired functions and features:

Best practices for hard drive setup: Option 1

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

1. Set up a test client with the image that contains the OEM product recovery code.
2. Install the Rescue and Recovery program. If eight free sectors in the Master Boot Record (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 operating system, 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 the cleandrv.exe available from the Lenovo ThinkVantage Technologies Administrator Tools Web page at: <http://www.lenovo.com/support/site.wss/document.do?lnocid=TVAN-ADMIN#rnr> to ensure all sectors are cleared from the Master Boot Record 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: Option 2

Deploying the Rescue and Recovery program on existing clients requires some effort and planning. This scenario provides another option for a hard drive setup.

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

Creating a bootable Rescue and Recovery CD

The Rescue and Recovery program 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 (.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. These files and directories are included on the recovery CD:

- minint
- preboot
- win51
- win51ip
- win51ip.sp2

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 this much data around is a hard disk drive-intensive task, and might take fifteen or more minutes on some computers.

Creating the recovery ISO file and burning to a CD sample script file

To create the recovery ISO file and burn it to a CD sample script file, prepare the following code.

```
:: Make an ISO file here - ISO will reside in c:\SWTOOLS\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%\Program Files\Common Files\Lenovo\Python24
set PATHEXT=%PATHEXT%;.PYW;.PYO;.PYC;.PY
set TCL_LIBRARY=%SystemDrive%\Program Files\Common Files\Lenovo\Python24
\tc1\tc18.4
set TK_LIBRARY=%SystemDrive%\Program Files\Common Files\Lenovo\Python24
\tc1\tk8.4
set PYTHONCASEOK=1
set RR=c:\Program Files\Lenovo\Rescue and Recovery\
set PYTHONPATH=C:\Program Files\Common Files\Lenovo\logger
:: The next line will create the ISO silently and not burn it
c:\Program Files\Common Files\Lenovo\Python24\python c:\Program Files\
\Common Files\Lenovo\spi\mkspiim.pyc /scripted
:: The next line will create the ISO with user interaction and not burn it
:: c:\Program Files\Common Files\Lenovo\Python24\python c:\Program Files\
\Common Files\Lenovo\spi\mkspiim.pyc /scripted /noburn
```

Scenario 3 - Installing with WIM files and Windows 7

Windows 7 deployment is based on disk imaging with ImageX. ImageX utilizes file based imaging with WIM files instead of sector-based image formats. Considering this formatting development, use the following steps when installing and deploying the Rescue and Recovery program on Windows 7:

1. Boot to Windows PE 2.0
2. Launch Diskpart
3. Select Disk
4. Clean Disk
5. Create desired primary partition of size desired
6. Make the partition active

7. Assign the drive letter (C)
8. Exit Diskpart
9. Format disk such as c: /fs:ntfs /q /y /v:WinXP
10. Run bootsect /nt52
11. Run BMGR32.EXE /Fbootmgr.bin /M1 /IBM /THINK
12. Use Imagex.exe to apply your WIM file to C:
13. Reboot

For more information about Windows 7, WIM files, or ImageX, see the following Web site:

<http://www.microsoft.com>

Scenario 4 - Standalone install for CD or script files

For a standalone install for CD or script file, complete the following steps:

1. Use one batch file to silently install the Rescue and Recovery program.
2. Configure BIOS password recovery silently.

Scenario 5 - Working with Active Directory and ADM files

The following example illustrates how the Administrative Template file (.adm) can be used locally and how the settings can be exported through a registry file and then imported to all intended machines. This example documents how to hide the Advanced menu in the main user interface.

1. Install the Rescue and Recovery program on an image machine.
2. From the Windows Start menu, run gpedit.msc.
3. Right-click **Administrative Templates** under **Computer Configuration**.
4. Select **Add/Remove Templates**.
5. Click the **Add** button and then select the rnr.adm file. The rnr.adm file can be obtained from the Lenovo ThinkVantage Technologies Administrator Tools Web page at:
<http://www.lenovo.com/support/site.wss/document.do?Indocid=TVAN-ADMIN#rnr>
6. Click the **Close** button on the **Add/Remove Template** dialog box.
7. Click the **Administrative Templates** tab under the **Computer Configuration**. A new tab named **ThinkVantage** is presented. Under the **ThinkVantage** tab there will be a **Rescue and Recovery** tab. All the available setting can be configured now for this machine.
8. Go to **ThinkVantage** → **Rescue and Recovery** → **User Interface** → **Menus**, and double click on the **Advanced Menu** tab.
9. Select **Enabled** on the **Settings** tab of the **Advanced Menu Properties** dialog box.
10. Select **Hide** from the **Advanced Menu** dropdown box.
11. Click **OK** on the **Advanced Menu Properties** dialog box.
12. From the Windows **Start** menu, run regedit.
13. Right-click on the following registry key: HKLM\Software\Policies\Lenovo\Rescue and Recovery.
14. Click **Export**.
15. Type the file name in the **File Name** field on the **Export Registry File** dialog box.

16. Navigate to your intended path in the **Save As** field on the **Export Registry File** dialog box.
17. Click the **Save** button.

Now, you can create an installation package that will install the Rescue and Recovery program silently and have the package import this new registry key so that all machines will have the advanced menu hidden. This can be used for any of the settings in the ADM file.

Corporate Active Directory Rollout

For a corporate Active Directory rollout, complete the following steps:

1. Install either through Active Directory or LANDesk.
 - a. Take backups and get reports through Active Directory and LANDesk of who and when they were taken.
 - b. Give certain groups abilities to take backups, delete backups, schedule options, and password restrictions, then change groups and see if settings persists.
 - c. Through Active Directory, enable Antidote Delivery Manager. Place packages to be run and make sure reporting is captured.

Scenario 6 - Performing a Bare Metal Restore from an Admin Backup

This section describes how to perform a Bare Metal Restore from an admin backup created by using a command-line such as below:

```
rrcmd basebackup location=U level=100 name="admin backup on USB HDD"
```

Note: You can change the value of the name parameter to create backups to other locations. For modifying the RRCMD parameters, see "RRCMD command-line interface" on page 61.

Select either of the following methods to perform the Bare Metal Restore:

- Method A: restore the system by using the following command-line:

```
rrcmd restore location=U level=100
```
- Method B: complete the procedure as follows:
 1. Launch the advanced user interface from PDA.
 2. Click **Restore your system**.
 3. Make sure to select **Do not preserve windows passwords** during the following restoring process.

Scenario 7 - Manually creating the Service Partition of S drive

To manually create the Service Partition (SP) of S drive in the Windows 7 operating system, do the following:

1. Boot from the Windows 7 installation disc and proceed to the drive selection menu.
2. Press **Shift + F10** to access the command line.
3. Type `diskpart`, then press **Enter**.
4. To clean the hard disk drive, follow the commands below:
Note: The commands are case sensitive.
 - a. `Diskpart>sel disk 0`
 - b. `Diskpart>sel par 1`
5. Restart the computer.

6. Boot from the Windows 7 installation disc again and proceed to the drive selection menu.
7. Create Partition 1 with a 1GB size for the service partition.
8. Create Partition 2 for the operating system.
9. Format Partition 2 and leave Partition 1 unformatted.
10. Press **Shift + F10** to access the command line.
11. Type `diskpart`, then press **Enter**.
12. Follow the commands below:
Note: The commands are case sensitive.
 - a. `Diskpart>sel disk 0`
 - b. `Diskpart>sel par 1`
 - c. `Diskpart>format fs=ntfs label="SYSTEM_DRV" quick`
13. Install Windows 7 operating system on Partition 2.
14. When installation completes, log in to Windows.
15. Change the drive letter of the Partition 1 to *S*.
16. Activate Partition 1.
17. Copy `C:\boot*.*` to `S:\`, and restart the computer.
18. Boot from the Windows 7 installation DVD, and click **Repair your computer** to repair the operating system.
19. Restart and log in to Windows.

When you complete the above procedure, the Service Partition will be created and the RNR 4.3 and PDA files will be copied to the *S* drive instead of the virtual Service Partition.

Appendix A. Administrative tools

ThinkVantage technologies offers tools that can be implemented by corporate IT administrators. These tools can be downloaded from the Lenovo Web site at: <http://www.lenovo.com/support/site.wss/document.do?Indocid=TVAN-ADMIN#rnr>

Command line support

The following sections provide command line support for the Rescue and Recovery program in addition to Antidote Delivery Manager.

Mailman

Antidote Delivery Manager uses the command `C:\Program Files\Lenovo\Rescue and Recovery\ADM\mailman.exe`. This procedure will check the Antidote repository for tasks to be run. There are no command-line arguments.

AWizard.exe

The Antidote wizard executable (`AWizard.exe`) is located where the administrator installs it. There are no command-line arguments.

SETPASSWORD

The `SETPASSWORD` command sets the user password. For a discussion about passwords, see “Passwords” on page 48.

RELOADSCHED

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

Example:

```
C:\Program Files\Common Files\Lenovo\Scheduler
```

RRCMD command-line interface

The primary Rescue and Recovery command-line interface is `RRCMD`. The command is located in the `C:\Program Files\Lenovo\Rescue and Recovery\` subdirectory. The following table provides information to use the command-line interface for the Rescue and Recovery program:

Syntax:

```
RRCmd <command> <location=x> [<uuid=abc> | <index=x>] [level=x]<silent>
```

Table 23. *RRCmd* parameters

Command	Result
Backup	Initiate a normal backup operation (must include location and name parameters).
Restore	Initiate a normal restore operation (must include location and level).

Table 23. RRcmd parameters (continued)

Command	Result
List	List files that are included in the backup level (must include location and level).
Basebackup	Initiate an alternative base backup. This is not to be used as a basis for incremental backups, and must include the location, name and level. The level must be less than 99. If another base backup with the same level already exists, it will be overwritten.
Sysprepbackup	Stage a backup operation in the Pre Desktop Area after the computer is rebooted. The primary use for this feature is to capture a Sysprep backup. Notes: 1. In some cases, the progress bar does not move. If this occurs, you can verify the backup is occurring by listening to the hard disk drive. When the backup is complete, you will receive a message that the backup is complete. 2. Sysprepbackup in Windows 7 is not allowed to be copied after it is made; otherwise, it will cause problems when restoring the backup because the related REGISTRY values have not been set. It is recommended to create the Sysprepbackup directly to the external media location.
Copy	Copy backups from one location to another. This command is also known as archive and must include the location.
Rejuvenate	Rejuvenate operating system to the specified backup.
Delete	Delete backups. This command must include the location.
Changebase	Change files in all backups based on file.txt contents. Options in file.txt are: A Add D Delete R Replace
Filter= <i>filterfile</i>	Files and folders that will be restored. This command is used only with the Restore command.
Location= <i>c</i>	One or more of the following can be selected with the associated result: L For primary local hard drive U For USB hard drive S For second local hard drive N For network C For CD/DVD Restore
name= <i>abc</i>	Where <i>abc</i> , is the name of the backup.

Table 23. RRCmd parameters (continued)

Command	Result
level=x	Where <i>x</i> is a number from 0 (for the base) to maximum number of incremental backups (only used with the restore option. For backup commands, the level= <i>x</i> 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, callbacks are performed, for example. The backup command is replaced with the command-line options.)
Osfilter	This command is used only with the restore command. It uses the registry settings for OsAppsList to filter files being restored. This command line entry can be used to do an OsApps restore.
uuid & index	The uuid command is the identifier of system with backups, and there is a one-to-one correspondence between index and uuid. The value is retrieved by using the listsystem parameter.
listsystem	List the value of uuid and index of stored backups in the backup location. For example: rrcmd listsystem location=U
listbackup	The listbackup command must be used with listsystem. It displays more detailed backup information. For example: rrcmd listsystem location=U listbackup

How to replace a file in a base backup

To replace a file in a base backup, do the following:

1. Modify the file you want to replace in the base backup, for example, C:\install.log.
2. Create a file named file.txt in the root of the C:\ directory.
3. Edit the file.txt file and add the following path for the file you modified: R=<full path to the file you modified>. The following provides an example:
R=c:\install.log

Note: You must have the file.txt file closed.

4. Run
RRCMD Changebase filename=c:\file.txt drive=c: destination="c:\RRBACKUPS"

Note: You can check the size change of the single file restore operation in the user interface.

How to restore a backup from specific system

The Rescue and Recovery program now supports to store the backup data of multiple computers on one storage device. The various backups are differentiated by the unique uuid command. If you want to restore a specific backup, do the following:

Note: Suppose the backups are stored in a USB storage device.

1. Retrieve value of UUID and Index. You can get the value of UUID and Index of the backups stored in the USB storage device, by executing either of the following commands:
 - `rrcmd listsystem location=U`
 - `rrcmd listsystem location=U listbackup`
2. Select your backup to restore. For example, the command below is to restore the first backup (index=1) that is level=2:


```
rrcmd restore location=U index=1 level=2
```

CLEANDRV.EXE

The `cleandrv.exe` file cleans all files on the drive. There will be no operating system after running this command. See “Scenario 6 - Performing a Bare Metal Restore from an Admin Backup” on page 58 for more information.

CONVDATE

The CONVDATE utility is provided as part of the Rescue and Recovery Administration tools. This utility is used to determine the HEX values of date and time and to convert date and time values into HEX values, and can be used to set a custom date and time in a backup field of the registry.

```
[Backup0]
StartTimeLow=0xD5D53A20
StartTimeHigh=0x01C51F46
```

To run the CONVDATE utility, complete the following steps:

1. Extract the Rescue and Recovery Administration tools from:


```
http://www.lenovo.com/support/site.wss/document.do?Indocid=TVAN-ADMIN#rnr
```
2. Open a CMD window.
3. Type in `Convdate`.
4. Set the date and time in the `convdate` window.

Note: The corresponding registry file values are:

- High DWORD=StartTimeHigh
- Low DWORD=StartTimeLow

CREATSP

This command creates a partition for Service Partition by desired megabytes. The drive letter is optional.

The syntax is:

```
createsp size=x drive=x /y
```

The parameters for CREATSP are:

Table 24.

Parameters	Description
<code>size=x</code>	Size of service partition to create, in megabytes.
<code>drive=x</code>	The drive number to create the service partition on. If not specified, the first non-USB drive is used. This parameter is optional.

Table 24. (continued)

Parameters	Description
/y	Suppresses confirmation of the drive being cleaned. This parameter is optional.

Note: The bmgr32.exe file must be in the same directory as the createsp.exe file, and should be run from WinPE.

InvAgent

The InvAgent command can be found in C:\Program Files\Common Files\Lenovo\InvAgent\IA.exe.

The IA.exe creates a local XML output file that it stores in the same folder.

One XML file will be created. The name of the XML file is created by combining manufacturer, model-type, and serial number, for example, Lenovo-2373Q1U-99MA4L7.XML.

The scanner can be run from a command-line by using the following command-line syntax:

- **-help**
Show a short help message.
- **-listsections**
List all of the available sections of system information.
- **-listtables**
List all of the sections and the tables of system information.
- **-silent**
Run with no output to the screen.
- **-section section1 section2 ...**
Return in the XML output file only the data from the specified section(s).
- **-vpd**
Only collect the vital product data.
- **-leveln**
Sections are grouped into levels; n=1 is the least amount of information, n=5 is the most information.
- **-query data.element.str**
Returns the value of the specified data element.
- **-register filename.ccd**
Registers a custom collector DLL with the agent.
- **-unregister filename.ccd**
Removes a custom collector DLL from the registered list.
- **-delete filename.ccd**
Deletes the custom collector DLL and any associated files.
- **-install**
Run by an admin account to install any drivers needed for data collection.

MapDrv

MapDrv provides network share functions for ThinkVantage Technology products. MapDrv is used to connect and disconnect ThinkVantage Technology products with network shares. The network share information is contained in the registry and includes the network share name as an encrypted string. Network share information is stored in the registry at HKLM\Software\Lenovo\MND\<app id>.

If an Active Directory policy is used, these values are stored at: HKLM\Software\Policies\Lenovo\MND\<app id>.

MapDrv allows you to use the encryption engine to generate an encrypted username and password, which can be used to pre-populate network share information on multiple systems. By using the encryption engine, it does not update the registry in the system it's running on.

The command-line interface to MapDrv is as follows:

```
mapdrv /<function><app id> /unc <sharename> /user <username> /pwd  
<password> [/timeout <seconds>] [/s]
```

The MapDrv command will implement the user interface to map a network drive. The mapdrv.exe command can be found in the C:\Program Files\Common Files\Lenovo\MND directory. The mapping network drive interface supports the following parameters:

Syntax:

```
mapdrv [switches]
```

Entering the command with no parameters launches the application and the information must be entered manually.

The return codes for all parameters are:

- 0 = success
- > 0 = failed

When MapDrv is launched with no parameters, the user is prompted for the network share, user name, and password. It then attempts to connect to the specified network share using the specified credentials.

The following table provides information about the parameters and the result of each parameter for MapDrv:

Table 25. MapDrv parameters

Parameter	Result
/view	Allows a view of the network share.
/pwd	Provides the encrypted password for this share.
/store	Stores application ID, share name, user name, password and timeout values.
/s	Set to Silent. Do not prompt the user regardless of whether connection is made.
/timeout	Sets the timeout value.
/unc	The stored network share.

Table 25. MapDrv parameters (continued)

Parameter	Result
/user	Sets the stored encrypted user name for this share.
/NetPath	Sets the value output from MapDrv to indicate the actual connection path.

Using MapDrv

The following examples provide instruction on how to use MapDrv:

To Store network share information for a ThinkVantage Technology product:

This function stores the network share information in the registry to define the subkey from the main MapDrv registry key. The following command sets the Unc, User and Pwd values in the registry:

```
mapdrv /store <app id> /unc <sharename> /user <username> /pwd <password>
[/timeout <seconds>]
```

To connect a network share and a ThinkVantage Technology product: The following command connects to the share using the Unc, User, and Pwd values in the registry:

```
mapdrv /connect <app id> [/s]
```

To disconnect a network share and a ThinkVantage Technology product: The following command disconnects the network share for the specified ThinkVantage Technology if currently connected:

```
mapdrv /disconnect <app id>
```

To display encrypted user name and password strings: The following command is used to display the network share information saved in the registry key:

```
mapdrv /view <app id> /user <username> /pwd <password>
```

Rescue and Recovery Boot manager control (BMGR32)

The boot manager interface command-line interface is BMGR32. It resides in the directory C:\Program Files\Common Files\Lenovo\BMGR. The following table presents the switches and their results for BMGR32.

Table 26. BMGR32 parameters

Parameter	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 service partition.
/BW	Boot to the Rescue and Recovery protected partition.
/BWIN	Reset request to boot to Predesktop Area. This must be called prior to booting.

Table 26. BMGR32 parameters (continued)

Parameter	Result
<i>/CFGfile</i>	Apply the configuration file parameters. See “RRCMD command-line interface” on page 61 for details regarding the configuration file.
<i>/DS</i>	Return the Master boot record (MBR) data sector (0-based).
<i>/Dn</i>	Apply changes to disk n, where n is 0-based, (default: disk containing environment variable “SystemDrive” or “C:\” if “SystemDrive” is not defined.)
<i>/H0</i>	Hide partition 0.
<i>/H1</i>	Hide partition 1.
<i>/H2</i>	Hide partition 2.
<i>/H3</i>	Hide partition 3.
<i>/HS</i>	Hide the service partition.
<i>/P12</i>	Hide the service partition by setting partition type to 12.
<i>/INFO</i>	Display hard disk drive information (checks for 8 free sectors).
<i>/INFOP</i>	Display hard disk drive information (checks for 16 free sectors).
<i>/M0</i>	The Rescue and Recovery environment is located in the service partition.
<i>/M1</i>	The Rescue and Recovery environment is located in the C:\PARTITION (dual boot Windows and Windows PE).
<i>/M2</i>	The Rescue and Recovery environment is located in the service partition with DOS (dual boot Windows PE and DOS; Lenovo-branded preload Only).
<i>/OEM</i>	Computer is not a Lenovo-branded computer. This forces a second check for the F11 (default) key press after POST. This may be required for older systems. This is also the default setting for the OEM version of the Rescue and Recovery program.
<i>/Patchn</i>	Used for installation program only to set a variable that the Master boot record patch program can access.
<i>Patchfilename</i>	Used for installation program only to install the Master boot record patch.
<i>/PRTC</i>	Used for installation program only, to retrieve patch return code.
<i>/IBM</i>	System is an IBM branded or Lenovo-branded computer.
<i>/Q</i>	Silent.
<i>/V</i>	Verbose.
<i>/R</i>	Reboot computer.
<i>/REFRESH</i>	Reset partition table entries in data sector.
<i>/THINK</i>	Configure the boot manager to use the blue button on the keyboard to enter the Predesktop Area.
<i>/TOC tocvalue</i>	Set the BIOS TOC location (16 characters that represent 8 bytes of data).
<i>/U0</i>	Show partition 0.
<i>/U1</i>	Show partition 1.

Table 26. BMGR32 parameters (continued)

Parameter	Result
/U2	Show partition 2.
/U3	Show partition 3.
/US	Show service partition.
/Fmbr	Load the Rescue and Recovery environment (RRE) Master boot record program.
/U	Unload the Rescue and Recovery environment (RRE) Master boot record program.
/UF	Force installation or uninstallation of the Master boot record program
/?	List command-line options.

When calling bmgr.exe with a /info attribute, the following information is dumped:

- **Additional master boot records**
Sector numbers containing the master boot record, other than the first sector.
- **Data**
Sector number of the data sector used by the master boot record.
- **Patch indices**
Sector numbers of any patches applied using the master boot record.
- **Checksum return**
0 if there are no checksum errors.
- **Boot Partition**
The 1-based partition table index of the service partition.
- **Alt Partition**
Partition table index pointing to the DOS bootable area, if one exists.
- **Original MBR**
Sector number where the machine's original master boot record is stored.
- **IBM Flag**
Value from the data sector (1 if IBM branded or Lenovo-branded system, 0 if not)
- **Boot Config**
Displays the installation option used to describe the machine layout. Whether a service partition was used, or a virtual partition.
- **Signature**
Signature value found within the data sector and the first sector, should contain "NP".
- **Pause Duration**
Displays the number of $\frac{1}{4}$ seconds to wait if the F11 message is displayed to the screen.
- **Scan Code**
The key used when booting to the service area. The scan code for the F11 key is 85.
- **RR**
Not used by BMGR, this is set by the Rescue and Recovery program.

- **Prev Active Part**
Displays the partition table index of the previously active partition when booted to the service area.
- **Boot State**
Determines the current state of the machine:
 - 0 – Boot normal to operating system.
 - 1 – Boot to the service operating system
 - 2 – Boot back to the normal operating system from the service operating system.
- **Alt Boot Flag**
Boot to alternate operating system; DOS for example.
- **Previous Partition type**
Displays the partition type that the service partition was set to prior to booting to it, when booted to the service area.
- **Prior IBM MBR Index**
Used by Windows Installer.
- **Patch IN: OUT**
Input and output values from the patch code if used.
- **F11 Msg**
Message to display to user if proper BIOS calls not supported.

The following table provides error codes and error descriptions for BMGR32:

Table 27. BMGR32 Error codes

Error code	Error Description
5	Error applying selected options to master boot record.
6	Error installing the master boot record.
7	Error uninstalling the master boot record.
10	Error setting system type.
11	Error setting the master boot record mode.
13	Error installing compatibility patch.
14	Error setting compatibility patch parameters.
96	Error accessing sectors.
97	Error accessing sectors.

BMGR CLEAN

CleanMBR cleans the Master Boot Record. This program can be used when you encounter a Rescue and Recovery installation failure, such as not being able to install the Rescue and Recovery program with less than the required sectors free for the boot manager to install.

Notes:

1. After running this tool, the applications that are using MBR will be useless. For example: SafeGuard Easy, SafeBoot, and MBR version of Computrace.
2. Run before installing the Rescue and Recovery program.
3. Use the cleanmbr.exe for DOS and the cleanmbr32.exe for Windows.
4. After running DOS CleanMBR, run FDISK /MBR; it will put on the MBR.

The parameters for cleanmbr32.exe are:

Table 28.

Parameter (Required):	Description
/A	Clear MBR and install PC DOS MBR
Parameter (Optional):	
/Dn	Apply changes to drive. Use $n=0$ for the first drive.
/Y	Yes to all
/?	Display Help
/H	Display Help

Active Directory Support

Active Directory is a directory service. The directory is where information about users and resources is stored. The directory service allows access so you can manipulate those resources.

Active Directory provides a mechanism that gives administrators the ability to manage computers, groups, users, domains, security policies, and any type of user-defined objects. The mechanism used by Active Directory to accomplish this is known as Group Policy. With Group Policy, administrators define settings that can be applied to computers or users in the domain.

ThinkVantage Technology products currently use a variety of methods for gathering settings used to control program settings, including reading from specific application-defined registry entries.

For the Rescue and Recovery program, Active Directory can manage such settings as:

- Set back up locations.
- Set back up dates and times.

Administrative (ADM) template files

The ADM (Administrative) template file defines policy settings used by applications on the client computers. Policies are specific settings that govern the application behavior. Policy settings also define whether the user will be allowed to set specific settings through the application.

Settings defined by an administrator on the server are defined as policies. Settings defined by a user on the client computer for an application are defined as preferences. As defined by Microsoft, policy settings take precedence over preferences.

For example, a user may put a background image on his desktop. This is the user's preference setting. An administrator may define a setting on the server that dictates that a user must use a specific background image. The administrator's policy setting will override the preference set by the user.

When the Rescue and Recovery program checks for a setting, it will look for the setting in the following order:

- Computer policies

- User policies
- Default user policies
- Computer preferences
- User preferences
- Default user preferences

As described previously, computer and user policies are defined by the administrator. These settings can be initialized through the XML configuration file or through a Group Policy in the Active Directory. Computer and user preferences are set by the user on the client computer through options in the applications interface. Default user preferences are initialized by the XML configuration script. Users do not change the values directly. Changes made to these settings by a user will be updated in the user preferences.

Customers not using Active Directory can create a default set of policy settings to be deployed to client systems. Administrators can modify XML configuration scripts and specify that they be processed during the installation of the product.

Notes:

1. All schedule related settings are now set to delay for 1 hour, which means they will work one hour after it is set.
2. Do not launch the Rescue and Recovery program when configuring ADM settings using Group Policy.

Defining manageable settings

The following example shows settings in the Group Policy editor using the following hierarchy:

Computer Configuration>Administrative Templates>ThinkVantage>Rescue and Recovery>User Interface>Menus>Backup Menu

The ADM files indicate where in the registry the settings will be reflected. These settings will be in the following registry locations:

Table 29. Registry locations

Header	Header
Computer policies	HKLM\Software\Policies\Lenovo\Rescue and Recovery\
User policies	HKCU\Software\Policies\Lenovo\Rescue and Recovery\
Default user policies	HKLM\Software\Policies\Lenovo\Rescue and Recovery\User defaults
Computer preferences	HKLM\Software\Lenovo\Rescue and Recovery\
User preferences	HKCU\Software\Lenovo\Rescue and Recovery\
Default user preferences	HKLM\Software\Lenovo\Rescue and Recovery\User defaults

Group Policy settings

The tables in this section provides settings for the group policies in the Rescue and Recovery program.

Rescue and Recovery

The following table provides the policies for the Rescue and Recovery program.

Table 30. \Rescue and Recovery

Policy	Description
ConfigureSecurityGUIOption	Show, gray, or hide the Configure security settings button in the main user interface.
PDALogonGUIOption	Show, gray, or hide the GUI option to use a password to protect the Rescue and Recovery workspace.
PDALogonMode	Select the authentication mode for logging in to the PDA.
WindowsPasswordRecoveryOptioninGUI	Show, gray, or hide the GUI option to configure password recovery.

Settings

The following table provides the policies for the **Settings** tab:

Table 31. \Rescue and Recovery\Settings

Policy	Description
LockHardDisk	Enable or disable the Lock Hard Disk setting. Default: Disabled.
ParseEnvironmentVariables	Enable or disable the Parse Environment Variables setting. Default: Enabled.
SetPPArchiveBeforeBackup	Enable or disable the Set PP Archive Before Backup setting. Default: Enabled.
MaxSilentRetries	Set the maximum number of Silent Retries to network share. Default: 3.
Exclude	Enable or disable the Exclude setting. Default: Enabled.
Include	Enable or disable the Include setting. Default: Disabled.
SIS	Enable or disable the SIS setting. Default: Disabled.
AnalyzeFileSizeThreshold	Displays the threshold value used by the analyze function to determine if a file should be displayed or not. Values: 0-10 000 MB. Default: 20 MB.
SortFilterFiles	Displays the type of file sorting to show in the Exclude, Include, and SIS pages. Values: 1-4 (name asc, name desc, size asc, size desc). Default: 0 (no sorting).

User interface

The following table provides the policy settings for the user interface:

Table 32. \Rescue and Recovery\Settings\User interface

Policy	Setting	Description
UserInterface		Enable or disable the main user interface. Default: Enabled.
RestoreInterface		Enable or disable the Restore interface. Default: Enabled.
SimpleUserInterface		Enable or disable the simplified user interface. Default: Enabled.
AllowInterfaceSwitching		Enable or disable switching between advanced and simplified user interfaces. Default: Enabled.
Menus	BackupMenu	Show, gray, or hide the Backup menu. Default: Show.
Menus	RestoreMenu	Show, gray, or hide the Restore menu in the main user interface. Default: Show.

Table 32. \Rescue and Recovery\Settings\User interface (continued)

Policy	Setting	Description
Menus	AdvancedMenu	Show, gray, or hide the Advanced menu in the main user interface. Default: Show.
Menus	HelpMenu	Show, gray, or hide the Help menu in the main user interface. Default: Show.
MenuItems	BackupNow	Show, gray, or hide the Backup Now menu item in the main user interface. Default: Show.
MenuItems	SchedulePreferences	Show, gray, or hide the Schedule Preferences menu item in the main user interface. Default: Show.
MenuItems	Optimize	Show, gray, or hide the Optimize menu item in the main user interface. Default: Show.
MenuItems	ViewBackups	Show, gray, or hide the View Backups menu item in the main user interface. Default: Show.
MenuItems	Restore	Show, gray, or hide the Restore menu item in the main user interface. Default: Show.
MenuItems	RescueFiles	Show, gray, or hide the Rescue Files menu item in the main user interface. Default: Show.
MenuItems	CopyBackups	Show, gray, or hide the Copy Backups menu item in the main user interface. Default: Show.
MenuItems	DeleteBackups	Show, gray, or hide the Delete Backups menu item in the main user interface. Default: Show.
MenuItems	Exclude	Show, gray, or hide the Exclude menu item in the main user interface. Default: Show.
MenuItems	CreateRescueMedia	Show, gray, or hide the Create Rescue Media menu item in the main user interface. Default: Show.
MenuItems	Include	Show, gray, or hide the Include menu item in the main user interface. Default: Show.
MenuItems	SingleStorage	Show, gray, or hide the Single Storage menu item in the main user interface. Default: Show.
MenuItems	SysprepBackup	Show, gray, or hide the Sysprep Backup menu item in the main user interface. Default: Hide.
MenuItems	Help	Show, gray, or hide the Help menu item in the main user interface. Default: Show.
MenuItems	ContextHelp	Show, gray, or hide the Context Help menu item in the main user interface. Default: Show.
MenuItems	UsersGuide	Show, gray, or hide the Users Guide menu item in the main user interface. Default: Show.
MenuItems	About	Show, gray, or hide the About menu item in the main user interface. Default: Show.
Backup	ConfiguredBackupLocation	Show, gray, or hide the radio button to back up your data. Default: Show.
Backup	OpticalBackupLocation	Show, gray, or hide the radio button to create a backup to optical media. Default: Show.
Backup	MaxIncrementalsExceeded	Show or hide the Max Incrementals Exceeded dialog box. Default: Hide.
Restore	FullRestore	Show, gray, or hide the Full Restore radio button.

Table 32. \Rescue and Recovery\Settings\User interface (continued)

Policy	Setting	Description
Restore	Rejuvenate	Show, gray, or hide the Rejuvenate radio button in the restore options. Default: Show.
Restore	RestoreOSApps	Show, gray, or hide the Restore OS/Apps radio button in the restore options. Default: Show.
Restore	SFRRestoreNTFSToFat32	Show or hide the Fat32 partitions when restoring files from NTFS. Default: Show.
Restore	RescueFileSearch	Show, gray, or hide the Rescue File Search button. Default: Show.
Restore	PasswordPersist	Show, gray, or hide the Password Persist radio button. Default: Show.
Restore	BaseBackup	Show or hide the Base Backup from being restored through the user Interface. Default: Show.
Restore	AdminBackups	Show or hide the Admin Backups from being restored through the user Interface. Default: Show.
Schedule and Preferences	BackupLocation	Show, gray, or hide the Backup Location in the Schedule and Preference dialog box. Default: Show.
Schedule and Preferences	ScheduleSettings	Show, gray, or hide Schedule Settings in the Schedule and Preference dialog box. Default: Show.
Schedule and Preferences	ScheduleFrequency	Show, gray, or hide Schedule Frequency in the Schedule and Preference dialog box. Default: Show.
Schedule and Preferences	ScheduleTime	Show, gray, or hide Schedule Time in the Schedule and Preference dialog box. Default: Show.
Schedule and Preferences	SuspendCheck	Show, gray, or hide the Suspend check box in the Schedule and Preferences dialog box. Default: Hide.
Schedule and Preferences	BackupPartitions	Show, gray, or hide the Backup Partitions check box in the Schedule and Preferences dialog box. Default: Show.
Schedule and Preferences	BackupStorageWarning	Show, gray, or hide the Backup Storage Warning item in the Schedule and Preferences dialog box. Default: Show.
Schedule and Preferences	PasswordProtect	Show, gray, or hide the Password Protect item in the Schedule and Preferences dialog box. Default: Show.
Schedule and Preferences	LockHardDisk	Show, gray, or hide the Lock Hard Disk item in the Schedule and Preferences dialog box. Default: Show.
Schedule and Preferences	MaxIncrementalBackups	Show, gray or hide the Maximum number of incremental backups allowed control item in the Schedule and Preferences dialog box. Default: Show.
CopyBackups	CopyToOptical	Show, gray, or hide the Copy To Optical radio button. Default: Show.

Table 32. \Rescue and Recovery\Settings\User interface (continued)

Policy	Setting	Description
CopyBackups	CopyToUSB	Show, gray, or hide the Copy To USB radio button. Default: Show.
CopyBackups	CopyToSecond	Show, gray, or hide the Copy To Second radio button. Default: Show.
CopyBackups	CopyToNetwork	Show, gray, or hide the Copy To Network radio button. Default: Show.
Delete	BaseBackup	Show or hide the Base Backup from the Delete page. Default: Show.
Simplified	Backup	Show, gray, or hide the Backup button on the simplified user interface. Default: Show.
Simplified	Restore	Show, gray, or hide the Restore button on the simplified user interface. Default: Show.
Simplified	ChangeBackupOptions	Show, gray, or hide the Change Backup Options link on the simplified user interface. Default: Show.
Simplified	Help	Show, gray, or hide the Help button on the simplified user interface. Default: Show.
Simplified	QuickRestore	Show, gray, or hide the Quick Restore button on the simplified user interface. Default: Show.
Simplified	FullRestore	Show, gray, or hide the Full button on the simplified user interface. Default: Show.
Simplified	Delete Backups	Show, gray, or hide the Delete Backups option on the simplified user interface. Default: Show.
Simplified	Backup Name	Show, gray, or hide the Backup Name option on the simplified user interface. Default: Show.
Simplified	FactoryRecovery	Show, gray, or hide the Factory Recovery radio button on the simplified user interface if the Factory Recovery program is installed. Default: Show.
Simplified	RescueFiles	Show, gray, or hide the Rescue Files button on the simplified user interface. Default: Show.
Simplified	RescueFilesCleanup	Show, gray, or hide the Rescue Files Cleanup button on the simplified user interface. Default: Show.
Simplified	LaunchAntivirus	Show, gray, or hide the Launch Antivirus function on the simplified user interface. Default: Show.
Simplified	SystemInformation	Show, gray, or hide the System Information button on the simplified user interface. Default: Show.

Note: If you are attempting to remove an entire screen using an Active Directory template, disable the menu item instead of hiding each item on the screen.

Backup

The following table provides the policy settings for Backup.

Table 33. \Rescue and Recovery\Settings\Backup

Policy	Setting	Description
BackupLocal		Enable or disable Backup Local as a selected destination for backup. Default: Enabled.
BackupSecond		<p>Enable or disable Backup Second as a selected destination for backup. Default: Disabled.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. If a service partition backup fails due to insufficient space, manually delete the failed backup before making another backup or attempting to restore from the failed backup. 2. When backing up the service partition to external media, set the following registry key before restoring your system with the Rescue and Recovery program: HKLM\Software\Lenovo\ Rescue and Recovery\ Settings\Backup\ BackupSPNetwork=1
BackupUSB		<p>Enable or disable Backup USB as a selected destination for backup. Default: Disabled.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. If a service partition backup fails due to insufficient space, manually delete the failed backup before making another backup or attempting to restore from the failed backup. 2. When backing up the service partition to external media, set the following registry key before restoring your system with the Rescue and Recovery program: HKLM\Software\Lenovo\ Rescue and Recovery\ Settings\Backup\ BackupSPNetwork=1

Table 33. \Rescue and Recovery\Settings\Backup (continued)

Policy	Setting	Description
BackupNetwork		<p>Enable or disable Backup Network as a selected destination for backup. Default: Disabled.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. If a service partition backup fails due to insufficient space, manually delete the failed backup before making another backup or attempting to restore from the failed backup. 2. When backing up the service partition to external media, set the following registry key before restoring your system with the Rescue and Recovery program: HKLM\Software\Lenovo\ Rescue and Recovery\ Settings\Backup\ BackupSPNetwork=1
LocalPartitionNumber		Set the partition number for backups on the local drive. Valid values: 1-100. Default: 1.
USBPartitionNumber		Set the partition number for backups on the USB drive. Valid values: 1-100. Default: 1.
SecondHDDPartitionNumber		Set the partition number for backups on the Second hard disk drive. Valid values: 1-100. Default: 1.
Backup Partitions		<p>Select the partitions that should be backed up. A DWORD (double word) is a bitmap of logical drive letters that should be included in the backup.</p> <p>To get the right hexadecimal value for drive letters, lay out the drive letters from right to left (for example, ...HGFEDCBA), and put 1 for partitions that will be backed up.</p> <p>Example: If you back up drive C: and E: only, you will get the binary value 00010100. The hexadecimal value for it is 0x00000014 and the decimal value for it is 20.</p> <p>Note: Convert your hexadecimal number to decimal before entering a value. Default: 0xFFFFFFFF. Entering a zero has a meaning similar to the default, which means finding all available partitions and back them up.</p>
MaxBackupSize		The maximum backup size (in GB). Valid values are 1-1000. Default: available free space.

Table 33. \Rescue and Recovery\Settings\Backup (continued)

Policy	Setting	Description
MaxNumberIncrementals		The maximum number of allowable incremental backups. Valid values: 2-31. Default: 3. Note: If you have completed backup number 3 and proceed to complete backup number 4 and encounter a message that states: <i>You have reached your defined limit of 3 incremental backups. You may increase the maximum number of incremental backups allowed or the oldest incremental backup will be deleted.</i> This message is to let you know that the oldest incremental backup will be deleted, and will be merged to the next incremental backup.
ResumeAfterPowerLoss		Enable or disable Resume After Power Loss as a backup option. Default: Enabled.
CPUPriority		CPU Priority of backups. Values: 1-5 (1=Lowest Priority, 5= Highest Priority). Default: 3.
Yield		Yield indicates amount of delay to insert between disk writes during a backup. This permits system backups from hogging all of the disk i/o bandwidth. Values: 0-8 (0=off, 8=least disk activity). Default: 0.
BootDisc		Enable or disable the creation of a Boot Disc when backing up to a CD/DVD or creating an archive to those media. Default: Enabled.
VerifyDisc		Enable or disable Verify Disc when backing up to a CD/DVD or creating an archive to those media. Default: Enabled.
BatteryPercentRequired		Battery Percent Required is essential before commencing a scheduled backup. This policy ensures there is enough battery power left to complete a backup. Values: 0-100. Default: 0.
SkipLockedFiles		Enable or disable Skip Locked Files when backing up. If enabled, locked files will not be backed up. Default: Disabled.
MinPercentFreeSpace		The minimum percentage of free space on the destination drive required for backup. Values: 0-100. Default: 0.
ProtectWithPassword		Enable or disable the Protect With Password option. If enabled, backups will be protected with a password. Default: Disabled.
RequiredGBFreeSpace		Set the amount of free space in GB that is required for a backup to occur.
AutosyncRetryNetwork		Number of minutes before the user will be prompted again after the user chooses not to retry an auto-synchronization to Network.
Prebackup is used when the user wants to run any applications or script before the Rescue and Recovery program starting a backup.		

Table 33. \Rescue and Recovery\Settings\Backup (continued)

Policy	Setting	Description
PreBackup	Pre	Command to run prior to a backup operation. Include the full path to the file, if that path is not in the environment variable. Default: None.
PreBackup	PreParameters	The parameter that passes the command that is run prior to a backup operation. Default: None.
PreBackup	PreShow	Show or hide the command that is run prior to a backup operation. Default: Show.
Postbackup is used to run applications or script when a backup operation is finished. When in Windows Vista or Windows 7 operating system, make sure that the application or script is not interactive. Otherwise, all graphic user interfaces will pop up on the Windows service session, and this will not be focused to the user. This is the design of the Microsoft Windows operating system.		
PostBackup	Post	Command to run after a backup concludes. Include the full path to the file, if that path is not in the environment variable. Default: None.
PostBackup	PostParameters	The parameter that passes the command that is run following the conclusion of a backup. Default: None.
PostBackup	PostShow	Show or hide the command that is run following a backup operation. Default: Show.

Restore

The following table provides the policy settings for Restore.

Table 34. \Rescue and Recovery\Settings\Restore

Policy	Setting	Description
PasswordPersist		Show or hide the Password Persist option in Restore dialog boxes. Default: Show.
PreRestore	PreWinRestore	Command to run prior to a restore operation from Windows. Include the full path to the file, if that path is not in the environment variable. Default: None.
PreRestore	PreWinRestoreParameters	The parameter that passes the command that is run prior to a restore operation from Windows. Default: None.
PreRestore	PreWinRestoreShow	Show or hide the command that is run prior to a restore operation from Windows. Default: Show.
PreRestore	PrePDARestore	Command to run prior to a restore operation from the Rescue and Recovery workspace. Include the full path to the file, if that path is not in the environment variable. Default: None.
PreRestore	PrePDARestoreParameters	The parameter that passes the command that is run prior to a restore operation from the Rescue and Recovery workspace. Default: None.
PreRestore	PrePDARestoreShow	Show or hide the command that is run prior to a restore operation from the Rescue and Recovery workspace. Default: Show.
PostRestore	PostWinRestore	Command to run following a restore operation from Windows. Include the full path to the file, if that path is not in the environment variable. Default: None.

Table 34. \Rescue and Recovery\Settings\Restore (continued)

Policy	Setting	Description
PostRestore	PostWinRestoreParameters	The parameter that passes the command that is run following a restore operation from Windows. Default: None.
PostRestore	PostWinRestoreShow	Show or hide the command that is run following a restore operation from Windows. Default: Show.
PostRestore	PostPDARestore	Command to run following a restore operation from the Rescue and Recovery workspace. Include the full path to the file, if that path is not in the environment variable. Default: None.
PostRestore	PostPDARestoreParameters	The parameter that passes the command that is run following a restore operation from the Rescue and Recovery workspace. Default: None.
PostRestore	PostPDARestoreShow	Show or hide the command that is run following a restore operation from the Rescue and Recovery workspace. Default: Show.

Rejuvenate

The following table provides the policy settings for Rejuvenate.

Table 35. \Rescue and Recovery\Settings\Rejuvenate

Policy	Description
PreRejuvenate	Command to run prior to a rejuvenate operation. Include the full path to the file, if that path is not in the environment variable. Default: None.
PreRejuvenateParameters	The parameter that passes the command that is run prior to a rejuvenate operation. Default: None.
PreRejuvenateShow	Show or hide the command that is run prior to a rejuvenate operation. Default: Show.
PostRejuvenate	Command to run following a rejuvenate operation. Include the full path to the file, if that path is not in the environment variable. Default: None.
PostRejuvenateParameters	The parameter that passes the command that is run following a rejuvenate operation. Default: None.
PostRejuvenateShow	Show or hide the command that is run following a rejuvenate operation. Default: Show.
PostRejuvenateReboot	Enable or disable a system reboot following a rejuvenate operation. Default: Enabled.

User Messages

The following table provides the policy settings for User Messages.

Table 36. \Rescue and Recovery\Settings\User Messages

Policy	Description
BootableSecond	Show or hide the Bootable Second message. Default: Hide.
BootableUSB	Show or hide the Bootable USB message. Default: Hide.
MissedBackup	Show or hide the Missed Backup message. Default: Show.
NoBattery	Show or hide the No Battery message. Default: Show.
ScheduledBase	Show or hide the Scheduled Base message. Default: Show.
PowerLossBackup	Show or hide the Power Loss Backup message. Default: Show.

Mapping network drive

The following table provides the policy settings for the mapping network drive function.

Table 37. \mnd\Rescue and Recovery

Policy	Description
UNC	UNC location for the mapped network drive (format \\server\share). Default: None.
User	Use mapdrv.exe /view command to create an encrypted value for this field. Default: None.
PWD	Create default password for the mapped network drive. Default: none

Scheduler tasks

The following table provides the policy settings for the Scheduler tasks.

Table 38. \Scheduler\Tasks

Policy	Description
DayOfMonth	If the Scheduled Backup Mode is configured for Monthly, this allows selecting which day of the month when scheduled backups should occur. Default: none.
DayOfWeek	If the Scheduled Backup Mode is configured for Weekly, this allows selecting which day of the week when scheduled backups should occur. Default: none.
Hour	Select the hour when scheduled backups should occur. Valid values: 0–23. Default: none.
Minute	Select the minute when scheduled backups should occur. Valid values: 0–59. Default: none.
Pre	Command to run prior to the scheduled backup task. Include the full path to the file. Default: none.
PreParameters	The parameters that passes the command that is run prior to the scheduled backup task. Default: none.
Post	Command to run after the scheduled backup task. Include the full path to the file. Default: none.
PostParameters	The parameters that passes the command that is run after the scheduled backup task. Default: none.

Appendix B. User tasks

Users belonging to different user groups have different rights and abilities to perform various user tasks.

Windows 7

The following table presents the tasks that the limited users, power users, and administrators can perform with the Rescue and Recovery program in a Windows 7 environment.

Table 39. Windows 7 user tasks

Tasks	Limited user	Power user	Administrator
Create rescue media ISO.	No	No	Yes (with command lines provided below)
Create bootable CD media.	Yes	Yes	Yes
Create USB hard disk drive bootable media.	No	No	Yes
Initiate backup.	Yes	Yes	Yes
Initialize restore operation in the Rescue and Recovery environment (RRE).	Yes	Yes	Yes
Perform single-file restore operation in the Rescue and Recovery environment.	No (Windows) Yes (Windows Pre Boot Area)	No (Windows) Yes (Windows Pre Boot Area)	Yes
Set options to be included or excluded in the Rescue and Recovery interface.	Yes	Yes	Yes
Backup to a network drive.	Yes	Yes	Yes
Schedule backups.	Yes	Yes	Yes
Carry over Predesktop Area login ID Note: The last Windows administrator ID is the only ID that can automatically be carried over from Windows to the Predesktop Area. Windows limited users and power users will need to retype their user IDs and passwords to log on to the Predesktop Area.	No	No	Yes

Create rescue media

Administrators can use the following command lines to create the Rescue Media ISO. These command lines enable you to make the required ISO file and the file is automatically placed in the C:\Program Files\Lenovo\Rescue and Recovery\rrcd\ directory:

:: This line will create the ISO silently and not burn it

```
c:\Program Files\Common Files\Lenovo\Python24\python c:\Program Files\Common Files
\Lenovo\spi\mkspiim.pyc /scripted
:: This line will create the ISO with user interaction and not burn it
c:\Program Files\Common Files\Lenovo\Python24\python c:\Program Files\Common Files
\Lenovo\spi\mkspiim.pyc /scripted /noburn
```

Rescue and Recovery user interface switching

The Rescue and Recovery user interface provides the option to switch between a simplified user interface or an advanced user interface. The simplified interface has a few basic options, while the advanced interface has extended options. When the Rescue and Recovery program is started, you will see the simplified user interface by default. By disabling the simplified user interface, you can have advanced user interface displayed each time the Rescue and Recovery program starts.

You can disable interface switching so that a user will not be able to switch between the two interfaces. To disable the interface switching, set the following policy to **HIDE**:

AllowInterfaceSwitching

For additional information about the Rescue and Recovery settings and working with Active Directory and Group Policy, see the accompanying XML/ADM Supplement for the deployment guide located on the ThinkVantage Technologies Administrator Tools page:

<http://www.lenovo.com/support/site.wss/document.do?Indocid=TVAN-ADMIN#rnr>

Appendix C. Notices

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

Lenovo 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:

Lenovo (United States), Inc
1009 Think Place
Building One
Morrisville, NC 27560
USA
Attention: Lenovo Director of Licensing

LENOVO GROUP LTD. 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. Lenovo 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 Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo 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.

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

Any references in this publication to non-Lenovo 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 Lenovo product, and use of those Web sites is at your own risk

Any performance data contained herein was determined in a controlled environment. Therefore, the result in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Trademarks

The following terms are trademarks of Lenovo in the United States, other countries, or both:

- Lenovo
- Rescue and Recovery
- ThinkVantage

Microsoft, Internet Explorer, Windows, and Windows Vista are trademarks of the Microsoft group of companies.

Intel is a trademark of Intel Corporation in the U.S. and other countries.

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

ThinkVantage™

Printed in USA