ThinkVantage

Rescue and Recovery 4.21 Deployment Guide

Updated: December 10, 2009

A ThinkVantage Technology publication

ThinkVantage

Rescue and Recovery 4.21 Deployment Guide

Updated: December 10, 2009

Fourth Edition (December 2009)

Contents

Preface

This guide is intended for IT administrators, or those responsible for deploying the Rescue and Recovery program to computers throughout their organizations. The goal of Rescue and Recovery is to reduce costs by avoiding helpdesk calls, desk-side visits, and improve user productivity. Rescue and Recovery 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 apply patches to a system when a restore is performed. This guide provides the information required for installing the Rescue and Recovery application on one or more computers, provided that licenses for the software are available for each target computer. It also provides information on the many aspects of the tool that can be customized to support IT or corporate policies.

This deployment guide is developed for IT professionals and the unique challenges that they encounter. If you have suggestions or comments, communicate with your Lenovo authorized representative. Periodically, these guides are updated, so check the Lenovo Web site for future publications.

Information presented in this guide supports ThinkVantage programs and does not support Lenovo 3000 technology. For information regarding Lenovo 3000 technology, refer to the Lenovo Web site located at:
http://www.lenovo.com

Rescue and Recovery provides function and application help. For questions and information about using the various components included in the Rescue and Recovery workspace, refer to the online help system for the components located at:
http://www.lenovo.com/thinkvantage

Chapter 1. Overview

Rescue and Recovery 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.

Rescue and Recovery has the following features:
- The Rescue and Recovery Predesktop Area that starts even if the Windows operating system will not boot.
- The Rescue and Recovery Windows environment that allows for backing up files, file rescue, and recovery of the operating system and files.
- Antidote Delivery Manager

Rescue and Recovery 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 31.

Note: Some features of Rescue and Recovery run under the Windows operating system. In some instances, system information used in the Rescue and Recovery environment are gathered while Windows is running. If the Windows operating system malfunctions, that malfunction alone will not prevent the Rescue and Recovery environment from operating normally. 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 Rescue and Recovery.
- **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 Rescue and Recovery 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 viewer provides a readable way to view activity and asset log entries.

  Note: The event log viewing is supported on selected machine types of Lenovo-branded personal computers only.
- **Warranty status**

Rescue and Recovery 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 Rescue and Recovery 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. Rescue and Recovery 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 and migrating

With Rescue and Recovery, you can migrate a user's work environment from one system to another upon rejuvenating from a backup. A user's work environment includes the following items:

- Operating-system preferences, such as desktop and network connectivity settings.
- Files and folders
- Customized application settings, such as bookmarks in a Web browser or editing preferences in Microsoft Word.
- User accounts

For more information, see Chapter 4, “Rejuvenation and migration,” on page 53.

Hints and Tips

For hints and tips on using Rescue and Recovery 4.2, see the *Rescue and Recovery v4.2 Considerations* document located at:
http://www.lenovo.com/support

Antidote Delivery Manager

Antidote Delivery Manager is an antivirus, anti-worm infrastructure included in Rescue and Recovery. The objects are easy to implement, and allow an administrator to initiate network blocking and recovery within minutes of a reported problem. Antidote Delivery Manager can be launched by one administrator and it functions on systems that are both network and non-network attached. Antidote Delivery Manager compliments existing antivirus tools rather than replacing them, so maintaining virus scanning tools and obtaining patches are still required. Antidote Delivery Manager provides the infrastructure to halt destruction and apply the patches.

Note: Antidote Delivery Manager is disabled by default. For more information, see Appendix B, “Antidote Delivery Manager,” on page 119.

Chapter 2. Installation

Prior to installing Rescue and Recovery, you can customize the Rescue and Recovery XML file for your enterprise and then deploy it to client systems. The XML file packaged with Rescue and Recovery is named rnrdeploy.xml. Once the XML file is customized and installed, settings for Rescue and Recovery 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#tvsu

Installation considerations

Rescue and Recovery has two main interfaces. The primary interface operates in the Windows XP, Windows 2000 or Windows Vista® environment. The secondary interface (the Rescue and Recovery Predesktop Area) operates independently of either Windows XP or Windows 2000 operating system, in the Windows PE environment.

Notes:

1. Rescue and Recovery only works with the non-BIOS version of Computrace if Rescue and Recovery is installed first, and then Computrace is installed.
2. If you attempt to install Storage Management Subsystem on a computer with Rescue and Recovery 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 Rescue and Recovery 4.21 as a type 12 partition. See “Scenario 4 - Installing with WIM files and Windows Vista” on page 81 for instructions.
3. A possible security risk may be created when the Microsoft Recovery Console is installed on a system with Rescue and Recovery. 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.

Overinstall considerations

A new backup must be taken after installation of Rescue and Recovery 4.21 because old backups from previous versions will be deleted during installation. This backup can be done by using either a script or the user interface.

Notes:

1. If installing Rescue and Recovery 4.21 over versions, 1.0, 2.0, or 3.0 you will have to take a backup first. If you are installing Rescue and Recovery 4.21 over version 3.1 you don’t need to take a backup, but it is recommended.
2. Backup files captured by previous versions of Rescue and Recovery 1.0, 2.0, and 3.0 cannot be recovered by Rescue and Recovery 4.21.

Installing Rescue and Recovery

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?lndocid=MIGR-4Q2QAKThe 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. A number of legacy computers from IBM® can support Rescue and Recovery provided that they meet the requirements specified. For best results, make sure that you have the latest version of the software installed. To obtain the latest version of Rescue and Recoveryand information about IBM-branded computers that support Rescue and Recovery, see the following Lenovo Web site:
http://www.lenovo.com/thinkvantage

Requirements for IBM and Lenovo computers

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

- Operating system: Windows Vista, Microsoft Windows XP with Service Pack 1 or Windows 2000 with Service Pack 3 or greater.
- Memory: 128 MB for Windows 2000 and Windows XP, 512 MB for Windows Vista
  - 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.

    Note: If a computer has less than 200 MB of non-shared memory, Rescue and Recovery 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 greater must be installed.
- 2.4 GB of free space on your hard drive.

  Note: If you are installing Rescue and Recovery on the service partition, see “Scenario 3 - Installing on Type 12 service partition” on page 80 for more information on installation requirements.
- 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 installing non-IBM or non-Lenovo computers

Installation on non-IBM or 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 Rescue and Recovery.

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

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 78.

Support for booting from external media (CD/DVD and USB): Non-IBM or 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 software. For additional information see the Lenovo Web site at: http://www.lenovo.com/thinkvantage

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

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 Rescue and Recovery.

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.

or using msiexec.exe,

- For installation target directory paths that do NOT contain spaces:

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

- For installation target directory paths that contain spaces:

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

Once and administrative installation has been completed, the administrative user can make customizations to the source files, such as adding settings to the registry. To install from the unpacked source after customizations are made, the user calls msiexec.exe from the command line, passing the name of the unpacked MSI file.

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

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

Note: Enter the 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 rrinstall40.txt is created in the %temp% directory if the setup is launched by the setup.exe file (double click the main install.exe file and then run the main executable without parameters, or extract msi and run the setup.exe file). This file contains log messages that can be used to debug installation problems. This log file is not created when running the setup directly from the MSI package; this includes any actions performed from Add/Remove Programs. To create a log file for all MSI actions, you can enable the logging policy in the registry. To do this, create the value:

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

Installation examples

The following table shows installation examples using setup.exe:

Table 1.

Description	Example
Silent installation with no reboot.	`setup.exe /s /v"/qn REBOOT="R""`
Administrative installation.	`setup.exe /a`
Silent administrative installation specifying the extract location for Rescue and Recovery.	`setup.exe /a /s /v"/qn TARGETDIR="F:\TVTRR""`
Silent uninstallation setup.exe /s /x /v/qn.	`setup.exe /s /x /v/qn`
Installation with no reboot. Create an installation log in temp directory for Rescue and Recovery.	`setup.exe /v"REBOOT="R" /L*v %temp%\rrinstall40.log"`
Installation without installing the Predesktop Area setup.exe /vPDA=0.	`setup.exe /vPDA=0`

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

Table 2.

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

Installing Rescue and Recovery 4.21 with existing versions

If you are installing Rescue and Recovery 4.21 on a machine with Rescue and Recovery 3.1 installed, you can use the over-install feature. If you are installing Rescue and Recovery 4.21 over versions 1, 2 or 3.0, uninstall the previous version through Windows Add/Remove programs and then install Rescue and Recovery 4.21. See "Overinstall considerations" on page 5 for more information.

Rescue and Recovery installation

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

1. The main installation executable for Rescue and Recovery is:
   - Z652ZISXXXXUS00.EXE for Windows XP and 2000
   - Z633ZISXXXXUS00.EXE for Windows Vista

   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.

   Note: Windows Vista uses a different package than Windows XP and 2000.
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 format
   - Z652ZABXXXXUS00.TVT for Windows XP and 2000
   - Z633ZABXXXXUS00.TVT for Windows Vista

   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 installation executable contains a file pdaversion.txt that contains the minimum version of the Predesktop Area that can work with that version of Windows. The installation executable installer will look for a Predesktop Area file using the following logic:
   - **Old Predesktop Area (Rescue and Recovery 1.0 or 2.X) exists or no Predesktop Area exists:**

     The 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.
   - **New (Rescue and Recovery 3.0 or greater) Predesktop Area exists:**

     The 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 installer presents a message that the current environment is not compatible with this version of Rescue and Recovery.
     - **Current code = Minimum code:**

The 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 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 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 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.

- Predesktop Area language packs (approximately 5 – 30 MB each): There are 16 language packs for Windows PE that are supported in Rescue and Recovery 4.21. Each language pack is named in the format z652ZABXXXXCC00.tvt where *XXXX* is the build ID and *CC* represents the language. One of these files is required if the Predesktop Area is being installed on a non-English system or a system with a non-supported language and must be in the same directory as the main installation and the US Predesktop Area .tvt file. If the Predesktop Area is being installed or updated and a language pack is required, the installation looks for the minimum level of language pack required in a version file contained within the installation executable. The installation also looks for a language pack .tvt file that is greater than any current language pack that is already installed and greater or equal than the minimum version required.

  Following is a list of languages supported in Rescue and Recovery 4.21:

  – 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 CIMPROIVIDER=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 Rescue and Recovery in a disk image

You can use your tool of choice to create a disk image that includes Rescue and Recovery. This deployment guide provides basic information regarding PowerQuest and Ghost as it applies to this application and installation.

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 Rescue and Recovery 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 12 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 Vista

Windows Vista 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 scenario in "Scenario 4 - Installing with WIM files and Windows Vista" on page 81 when installing and deploying Rescue and Recovery on Windows Vista.

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 which are created when Rescue and Recovery 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 to the Rescue and Recovery folder from a command prompt, type "CD %rr%" and press enter.

Table 8.

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 Rescue and Recovery installed.

Compatibility with Vista BitLocker

To achieve compatibility with Windows Vista 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.

If you have installed Windows Vista without using BitLocker Drive Preparation Tool, you must have two partitions on your system when installing Windows Vista. 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 Vista is installed, it will detect this and should install only the boot files to the smaller partition. Both partitions should be type 0x07.

If you have to install the Rescue and Recovery program on a system with BitLocker and without a service partition, run the following two commands to prevent the Windows Vista operating system from asking for the BitLocker key every time it boots. The two commands are:

- `bcdedit -deletevalue {globalsettings} extendedinput`
- `bcdedit -set {bootmgr} extendedinput 1`

To have the Rescue and Recovery program work correctly with BitLocker in Windows Vista, 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 drive to encrypt.

   Note: It is recommended to encrypt the system partition drive only.
5. Click **Turn on Bitlocker**, and follow the instruction on the screen to encrypt the chosen drive. After that, a recovery key is automatically created.
6. Save the recovery key to a USB storage device.
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 Vista, the BitLocker partition should be after the operating system partition for best results. If it is placed before the 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 Vista and BitLocker, a message will display, indicating that there was an error at shutdown. The message can be ignored and everything should operate normally.

Chapter 3. Configurations

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

XML and ADM file configurations

Configurations for Rescue and Recovery are done with the XML file, through the registry, and with Active Directory. Once the XML file is customized and installed, settings for Rescue and Recovery 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?lndocid=TVAN-ADMIN#tvsu

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:

Notes:

1. Rescue and Recovery cannot capture cached credentials for a domain user after a restore.
2. Rescue and Recovery cannot restore partitions that is created and placed physically before the system drive.

Single file restore

Single file restore prompts the user for the Backup Storage location, and then the user selects a backup. Rescue and Recovery 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. Rescue and Recovery 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 or after a restore. 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.

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 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. Rescue and Recovery 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.
/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 adminitrator 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

Table 12. Return codes (continued)

Return code	Return message
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

Express Repair

Also known as Fast Restore, Express Repair monitors and fixes operating system files from an alternate boot environment if they have changed or been corrupted outside of normal operating system by file corruption, or a virus. After Rescue and Recovery is installed and after a Windows operating system update, Express Repair stores the latest copy of each critical file including the *checksum* behind the Rescue and Recovery filter driver in its own database. Monitored files are listed in KernelFile.xml. The Express Repair database is located in the following path:

```
C:\RRBackups\FR
```

Express Repair supports the following operating systems:

- Windows XP
- Windows Vista 32 bit
- Windows Vista 64 bit

During restore operations launched from Windows or the preboot environment such as Quick Restore, Rejuvenation, or Full Restore, Express Repair files and checksums are deleted to avoid mismatching of operating system files. As a result, Express Repair stores all critical files and associated checksums after the next boot into the operating system. When a user boots to Windows PE, checksum compares critical operating system files. If a difference is detected, the user is prompted update files based on the latest version in the database, or boot to Windows. If a difference is not found, or if database not found, Express Repair exits and continue boot into Windows PE.

You can turn on or turn off Express Repair by setting the following policy in Group Policy:

```
ThinkVantage\Rescue and Recovery\Settings\Fast Restore
```

If this value is **Enabled** or not set, then Express Repair will run normally in the operating system and the Predesktop Area. If this value is **Disabled**, then Express Repair will not run in the operating system or in the Predesktop Area.

Note: The default value is **Enabled** for Windows XP, and **Disabled** for Windows Vista.
For more information on Group Policy and ADM files, 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#tvsu

Note: The XML and ADM file refer to Express Repair as Fast Restore.

Factory content/Image Ultra Builder

Factory content/Image Ultra Builder erases the hard disk and reinstalls all of the factory preinstalled software.

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 Rescue and Recovery; however, the configuration is stored in the registry. When Rescue and Recovery is installed, it will populate the scheduler with the appropriate settings.

Here is a description of the structure for the scheduler:

- Location: Install folder.

  Notes:

  1. Rescue and Recovery synchronizes backups from the primary backup location to the secondary backup location (a USB hard disk drive, second hard disk drive, or network drive). The previous backups on the secondary backup location will be overwritten after the synchronization.
  2. When creating a backup to a USB hard disk drive for the first time through the simplified user interface, the backing up operation will be cancelled automatically. The backing up to the USB hard disk drive will be successful from the second time.
- 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 Rescue and Recovery, 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.

Mapping a network drive for backups

The map 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=116226064151192077230149185054220105210064012092037082020 15...
Pwd=116226064151000000000149185054220105210064012092037082020 15...
```

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 Rescue and Recovery 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: *Large Enterprise individual language* files that you can download from the Lenovo Web site:
http://www.lenovo.com/support

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 z652zisxxxxus.exe /a /s /v"/qn TARGETDIR
   (Where XXXX is the build ID.)
   ="C:\TVTRR" REBOOT="R"" /w
   ```

2. Install Rescue and Recovery using the MSIEXE file:
   a. For all MSI files, add the following installation-log generation code:

      ```
      /L*v %temp%\rrinstall.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 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"
```

3. 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 sysprepbackup 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 Rescue and Recovery. 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 z652zisus00xxxx.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 rnrdeploy.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 rnrdeploy.xml file:

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

   For additional information on how to use the rnrdeploy.xml file, refer to the ThinkVantage Technologies XML/ADM Supplement. This supplement can be downloaded from the Lenovo Web site at: http://www.lenovo.com/support/site.wss/document.do?lndocid=TVAN-ADMIN#tvsu Navigate to Support and Downloads and User's Guides and

Manuals. Select the brand name of ThinkVantage Technologies, select the family name of Rescue and Recovery and then click Continue.

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 28.
4. Install Rescue and Recovery 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 sysprepbackup 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 Rescue and Recovery. 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.

Sysprep Backup/Restore

Password Persistence will not work with Sysprep Backup/Restore, because in a Sysprep Backup image, the Password Persistence information does not exist. Turn off and then start the system after completing a Sysprep Backup. To restore from the Sysprep Backup, switch to the advanced interface of Rescue and Recovery and select the **DO NOT PRESERVE my Windows User ID and password** option. Do *not* perform the restore in the simplified interface which is enabled to use the Password Persistence by default. Only a full restore can be performed with base backups that were taken using Sysprep. Rejuvenate, or operating system and application restore will not work with a Sysprep base 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.	• 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.	• 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.	• 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.	• 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 Rescue and Recovery, all other files will retain their original date and time.

Battery power settings for backups

With the corresponding ADM file installed for Rescue and Recovery, 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 Rescue and Recovery 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?lndocid=TVAN-ADMIN#tvsu

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 a restore from an incremental backup. That is how Rescue and Recovery 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 Rescue and Recovery 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 Rescue and Recovery in the Windows environment and in the Predesktop Area.

Using Rescue and Recovery 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 Rescue and Recovery.

Include and exclude backup files with registry settings

Rescue and Recovery can include and exclude an individual file, a folder, or an entire partition. With Rescue and Recovery 4.21, 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 Rescue and Recovery. This GUI exclude list is managed through the registry at: HKLM\SOFTWARE\Lenovo\Rescue and Recovery\Settings\ExcludeList.

OSAppsList: Rescue and Recovery 4.21 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 Rescue and Recovery 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 Rescue and Recovery is started unless the setting is disabled.

If the Simple User Interface setting is disabled, the advanced user interface will be displayed each time Rescue and Recovery 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 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#tvsu

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 Rescue and Recovery, 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.

Table 14. RRUTIL.exe files and customization options (continued)

File or Directory	Customization options
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.

Vista considerations

The \minint directory does not exist on the Vista version of Rescue and Recovery. The new folder in Vista is called *tvtos* and the entire preinstallation environment operating system is contained in a *.wim* file.

To edit the .wim file, you need to obtain the imagex.exe file in the Microsoft OPK for Vista.

Working with WIM files and ImageX

Windows Vista 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 scenario in "Scenario 4 - Installing with WIM files and Windows Vista" on page 81 when installing and deploying Rescue and Recovery on Windows Vista.

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 12 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 Download Rescue and Recovery and Client Security Solution Web site located at:

http://www.lenovo.com/support/site.wss/document.do?sitestyle=lenovo&lndocid=TVAN-ADMIN

The RRUTIL program works with the Rescue and Recovery filter driver on virtual partitions, and mounts type 12 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 4.21 is not backwards compatible with earlier versions of Rescue and Recovery.

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 12:

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
   ```
3. An optional command line input will be a text file to capture the output of this option.
4. 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 12 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 12:

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 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.
3. 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 12:

1. 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".
2. 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-12:

1. Delete the file(s) of \preboot. \minint, or root of the PE partition either virtual or type 12 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 Rescue and Recovery is not installed on the system, or 0 if Rescue and Recovery 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:\RRTemp. In c:\RRTemp would be a mirror image of the \RRbackups directory structure where the files are to go.

```
C:\RRTemp\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.
2. Sample command: RRUTIL /bs would display the backup space on the console.

As previously stated in this chapter, the rrutil.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 rrutil.exe, do the following:

1. Copy rrutil.exe to the root of the C drive.
2. Create getlist.txt file with the following syntax:

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

   Save the file as c:\temp\getlist.txt.
3. At a command prompt, type the rrutil.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-12 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`* `RRUTIL -r \temp\rr\test.txt test2.txt` the file is in the preboot\rr directory	Rename a file in the Predesktop Area.
`RRUTIL -bp c:\temp`	Update or replace files in RRBACKUPS virtual partition.

Table 15. Command and switch options (continued)

Command and switch options	Result
`RRUTIL -bl` *`path`* RRUTIL -bl lists to `c:\rr-list.txt` `rrutil -bl c:\rrtemp`	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.

4. 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 pdagui*xx*.ini, which is a configuration file where you can customize elements of the Rescue and Recovery environment (see "Customizing the preboot environment" on page 38).

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\systme32\drivers.
3. Update \minint\system32\winpeoem.sif to include the subdirectory containing the driver (for an example, examine this file from 4.21 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 pdagui*xx*.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 pdaguien.ini file, see "Example: pdaguixx.ini" on page 37.

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 pdagui*xx*.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 Rescue and Recovery to present the desired background.

Note: To get, edit, and replace the mainbk.bmp file, see "Using RRUTIL.EXE" on page 32.

Editing pdagui.ini

Changing the left-panel entries requires editing the pdagui*xx*.ini (where *xx* is the language designation) file. For information about getting pdagui*xx*.ini from the Rescue and Recovery environment and replacing the file, see "Using RRUTIL.EXE" on page 32.

Rescue and Recovery 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 40). 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.

Table 17. Left-panel entries and customization options (continued)

Entry	Customization options
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
Create migration file	WIZRR.EXE
Open browser	OPERA.EXE
Map a network drive	MAPDRV.EXE
Diagnose hardware	PCDR.CMD; launches the PC Doctor application, IBM, 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 pdagui*xx*.ini (where *xx* is the language designation) file. For information regarding getting pdagui*xx*.ini from the Rescue and Recovery environment and replacing the file, see "Example: pdaguixx.ini" on page 37.

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 pdagui*xx*.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 32 for a complete list of executables that can be started from the title bar.

Modifying user messages and window status: pdagui*xx*.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 pdagui*xx*.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**
  %tvtdrive%Preboot\Helps\en\f_welcom.htm
- **Command1**
  %tvtdrive%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 pdagui*xx*.ini (where *xx* is the language designation) file, you can modify the values in the following lines:

```
NoShowChk=
RebootText=
```

The two values for "NoShowChk" are `0` and `1`. 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 pdagui*xx*.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 Rescue and Recovery 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 32.
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 Rescue and Recovery under Microsoft Vista 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

Rescue and Recovery 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 32.
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 32. 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 Rescue and Recovery 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 32.
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 32.

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 32.
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 32.

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 32.
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 32.

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 32.
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 Rescue and Recovery 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 32.

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 32.
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 Rescue and Recovery 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 32.

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 Rescue and Recovery, 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 32.
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/mgpeg=8,,,,mpeg,mpg,mpe,m2v,m1v,mpa,|
        ```

        to

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

     b. Scroll up to the [File Types Extension] section of the norm1.ini file, and then search for the mime type of the file. For example, find the following: VIDEO/MPEG=,8
     c. Change the ,8 value to the following:

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

        Note: If the 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 Rescue and Recovery for the changes to be effective.
   - If the extension is not present and files of the desired type do not work correctly, do the following:
     a. In the [File Types Extension] section of norm1.ini, locate the temporary mime entry. The following is an example: temporary=1,,,,lwp,prz,mwp,mas,smc,dgm,|
     b. Add the file type extension to the list. For example, if you want to add .CAB as a recognized extension, add it according to the following sample entry:

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

        Note: The trailing comma and pipe symbol are essential for this setting to work. If either is omitted, all file extensions in the list might be disabled.
     c. Save the file to the directory path C:\TEMP\.
     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 32.
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 32.
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 32.
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 32.
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 32.

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 32.
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 32.

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?lndocid=TVAN-ADMIN#tvsu
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 Rescue and Recovery 4.21 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 Rescue and Recovery graphical user interface or the Rescue and Recovery command-line interface (RRCMD) with specified parameters. Once the password is set, it will be used to protect all backups unless the password is disabled or changed.

You can set, change, disable, or enable a backup password according to the following examples.

- **Using the Rescue and Recovery graphical user interface**

  The password can be set through the **Set schedule and preferences** option.

  – Setting a new password

    Select the **Protect your backups with a password** check box and type your password.

  – Changing the password

    Click **Set Password** and type both the old and new password.

  – Disabling the password

    Clear the **Protect your backups with a password** check box. The backup password will be disabled and all future backup data will have no password protected.

    Note: If you have old backups that are made with a previous password, you will still be required to type the previous backup password in the PDA when restoring those backups. When new backups have been created to merge all old backups, the backup password will no longer be required for restoring incremental backups. However, because the base backup is password protected, restoring the base backup will still require the previous password.

  – Enabling the password

    Select the **Protect your backups with a password** check box. It will keep using the previous password if no new password is set.

- **Using the RRCMD command-line interface**

  All commands related to backup password setting are provided below.

  – Setting a new password

    You can create a password using the following syntax:

    ```
    rrcmd createpassword password=xxx
    ```

    xxx is the password you set for the backup.

    You can also set the backup password following a backup operation. The backup, basebackup, and sysprepbackup options in the following syntax support using the `password` parameter to create a backup password, for example:

    ```
    rrcmd [backup | basebackup | sysprepbackup] location=L name=mybackup
    password=xxx
    ```

    xxx is the password you set for the backup.

    Note: The backup password information will be created after performing the commands above and you will use this password for future backups. Once a backup password is created, the above `password=xxx` command cannot be used. The command `changepassword=xxx` must be used subsequently.

  – Changing the password

    You can change the old password to a new password using the syntax:

    ```
    rrcmd changepassword password=xxx new_password=yyy
    ```

    xxx is the old password, and yyy is the new password you set for the backup.

  – Disabling the password

    You can disable the backup password from being used in future backups using the following syntax:

```
rrcmd disablepassword password=xxx
```

– Enabling the password

  Currently no parameter in the RRCMD can be used to enable the backup password. To enable the backup password, you need to use the Rescue and Recovery advanced graphical user interface by selecting the **Protect your backups with a password** check box or using Group Policy.

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

Here are log files located in the c:\swshare directory:

- Engine.log

  Logs all functions by the engine and the main backup service.
- rr.log

  Logs functions by the main Rescue and Recovery GUI interface.
- Restore.log

  Logs restore operations like full restore, rejuvenation, and single file restores.
- tvtsched.log

  Log for the scheduler service that call Rescue and Recovery and InvAgent.
- Rescue.log

  Log for antidote, specifically for the mailman.exe function.

Chapter 4. Rejuvenation and migration

As part of the Rescue and Recovery program, rejuvenation and migration tools are utilized to help you rejuvenate and migrate your data and settings. Migration methods are managed with System Migration Assistant. For additional information about System Migration Assistant, see the deployment guide or the users guide at: http://www.lenovo.com/supportTo assist you with rejuvenation and migration, this chapter provides the following information:

Creating a command file

During the capture phase, System Migration Assistant reads the contents of the command file and archives settings. This section contains information about command files and the statements that they can contain.

System Migration Assistant provides a default command file (command.xml), that you can use as a template to create a customized command file. If you installed System Migration Assistant in the default location, this file is located in the c:\%RR%\migration\bin directory.

Note: XML technology is used to describe command file commands.

Consider the following points concerning command files:

- XML Command file must be saved in Unicode (UTF-16) format.
- The command file follows XML version 1.0 syntax, and is case-sensitive.
- Each command and parameter section must start with <TagName>and end with </TagName>, and its value must be described between those tags.
- Syntax errors might cause an error when you run System Migration Assistant. If System Migration Assistant encounters an error, it writes the error to the log file and continues the operation. Depending on the severity of the error, the end results may be corrupted.

File commands

The following table contains information about the commands, with the exception of those concerning file migration or the registry, that can be used in a command file:

Table 22.

Command	Parameters	Parameter Values and Examples

<Desktop>	• <accessibility>
	• <active_desktop>
	• <colors>
	• <desktop_icons>
	• <display>
	• <icon_metrics>
	• <keyboard>
	• <mouse>
	• <pattern>
	• <screen_saver>
	• <sento_menu>
	• <shell>
	• <sound>
	• <start_menu>
	• <taskbar>
	• <wallpaper>
	• <window_metrics>
	• <desktop_settings>
	• <time_zone>
		To select a desktop setting, set the parameter to True. Otherwise, set the parameter to False or leave it unspecified.
		
		For example:
		`<Desktop>`
		`<colors>`
		`true`
		`</colors>`
		`<desktop_icons>`
		`true`
		`</desktop_icons>`
		`<screen_saver>`
		`true`
		`</screen_saver>`
		`<start_menu>`
		`false`
		`</start_menu>`
		`<time_zone>`
		`true`
		`</time_zone>`
		`</Desktop>`

<Network>	• <ip_subnet_gateway _configuration>
	• <dns_configuration>
	• <wins_configuration>
	• <computer_name>
	• <computer_description>
	• <domain_workgroup>
	• <mapped_drives>
	• <shared_folders_drives>
	• <dialup_networking>
	• <odbc_datasources>
		To select a desktop setting, set the parameter to True. Otherwise, set the parameter to False or leave it unspecified.
		
		For example:
		`<Network>`
		`<computer_name>`
		`true`
		`<computer_name>`
		`<mapped_drives>`
		`false`
		`</mapped_drives>`
		`</Network>`

Table 22. (continued)

Command	Parameters	Parameter Values and Examples

<Applications>	<Application>
	
	For a list of all the applications that are supported, see the *ThinkVantage System Migration Assistant User's Guide* located at:
	`http://www.lenovo.com /thinkvantage`
		For example: To capture all applications supported, set $(all).
		`<Applications>`
		`<Application>`
		`Lotus Notes`
		`</Application>`
		`<Application>`
		`Microsoft Office`
		`</Application>`
		`</Applications>`
		
		or
		`<Applications>`
		`<Application>`
		`$(all)`
		`</Application>`
		`</Applications>`

<Registries>	• <Registry> • <hive> • <keyname> • <value>	To capture or apply the registry settings, specify the hive, keyname and value as the parameters in the command file. For example: <HKEY_CURRENT_USER><Control Panel><Colors><Menu Bar><236.233.218>.

<IncUsers>	<UserName>	To capture all user profiles, set $(all) or use ** as a wild card for all users. Otherwise, specify users individually.
		
		The following wild cards are available.
		• ** for a variable length wild card
		• % for a fixed length wild card (1 character)
		
		For example:
		`<IncUsers>`
		`<UserName>`
		`Administrator`
		`</UserName>`
		`<UserName>`
		`domain\Kelli`
		`</UserName>`
		`</IncUsers>`

<ExcUsers>	<UserName>	To exclude users from the migration process, specify the domain and user name of the user. The following wild cards are available. • * for a variable length wild card • % for a fixed length wild card (1 character)

Table 22. (continued)

Command	Parameters	Parameter Values and Examples

<Printers>	<Printer>
	
	<PrinterName>
		This control statement is effective for both the source and the target computer.
		
		To capture all printers, set the parameter to *$(all)*. Specify each printer individually to capture the default printer only. Set the parameter to *$(DefaultPrinter)*.
		
		For example:
		`<Printers>`
		`  <Printer>`
		`  $(all)`
		`  </Printer>`
		`</Printers>`
		
		`or`
		
		`<Printers>`
		`  <Printer>`
		`  <PrinterName>`
		`  Lenovo 5589-L36`
		`  </PrinterName>`
		`  </Printer>`
		`</Printers>`
		
		`or`
		
		`<Printers>`
		`  <Printer>`
		`  $(DefaultPrinter)`
		`  </Printer>`
		`</Printers>`

Table 22. (continued)

Command	Parameters	Parameter Values and Examples
<MISC>	<bypass_registry>	To deselect all registry settings, set to True. Otherwise, set to False or leave it unspecified.
	<overwrite existing files>	To overwrite existing files, set to True. Otherwise, set to False or leave it unspecified.
	<log_file_location>	To specify the directory to where log files are written, enter a fully qualified directory name. You can specify a shared directory on another system. If you do not set this parameter, the log files write to d:/InstDir/, where c is the drive letter of the hard disk drive and /InstDir/ is the directory where the applications are installed.
	<temp_file_location>	To specify the directory to where temporary files are written, enter a fully qualified directory name. You can specify a shared directory on another system. If you do not set this parameter, temporary files are written to c:/InstDir/etc/data, where c is the drive letter of the hard disk drive and /InstDir/ is the directory where the applications are installed.
	<resolve_icon_links>	To copy only those icons that have active links, set to True. Otherwise, set the parameter to False or leave it unspecified.

File-migration commands

System Migration Assistant processes file-migration commands in the following order: file inclusion commands are performed first, then file exclusion commands are performed from the inclusion files.

System Migration Assistant selects and unselects files on the basis of the original location of files and folders on the source computer. File redirection statements are stored in the profile and are interpreted during the apply phase. File migration is recursive into sub-directories.

The processing of file and directory names is not case sensitive.

The following table contains information about the file-migration commands. All file migration commands are optional.

Table 23.

Command	Parameter	Description	Example

<FilesAndFolders>	<run>	Starts the process of a command. The </run> parameter ends the process of a command.	To capture or apply file migration, set the parameter to True. Otherwise, set the parameter to False or leave it unspecified.
			
			For example:
			`<FilesAndFolders>`
			`<run>true</run>`
			`</FilesAndFolders>`

<Exclude_drives>	<Drive>	Specifies the drive letter to exclude drives from being scanned.	For example:
			`<ExcludeDrives>`
			`<Drive>D</Drive>`
			`<Drive>E</Drive>`
			`</ExcludeDrive>`

<Inclusions>	<IncDescription>
	
	<Description>
	
	<DateCompare>
	
	<Operand>
	
	<Date>
		• <Description> is the fully-qualified filename. You can use wildcard character for both filename and folder name.
		• <DateCompare> is an optional parameter that you can use to select files based on the date when they were created.
		– <Operand> is either NEWER or OLDER.
		– <Date> is the baseline date in mm/dd/yyyy format.
			To search for matching files in the specified directories.
			
			For example:
			
			Example 1
			`<Inclusions>`
			`<IncDescription>`
			`<Description>`
			`c:\MyWorkFolder\ls`
			`</Description>`
			`</IncDescription>`
			`</Inclusions>`
			
			Note: To specify the folder name, add .\. at the end of the description.

Table 23. (continued)

Command	Parameter	Description	Example

<Inclusions>	<SizeCompare>
	
	<Operand>
	
	<Size>
	
	<Dest>
	
	<Operation>
	where
		• <SizeCompare> is the optional parameter to select files based on their size.
		– <Operand> is either LARGER or SMALLER.
		– <Size> is the file size in MB.
		• <Dest> is an optional parameter that specifies the name of the destination folder on the target system where the files will be written.
		• <Operation> is an optional parameter that specifies how the file path is to be handled. Specify either of the following:
		– P - preserves the path of the file and recreates the file on the target system starting at the location specified by the <Dest> parameter.
		– R - removes the path of the file and places the file directly in the location specified by the <Dest> parameter.
		
		Note: If the P or R command is not used in the <Operation> tag, the default is to leave the <Operation> empty, for example, <Operation></Operation>.
			Example 2
			`<Inclusions>`
			`<IncDescription>`
			`<Descriptin>`
			`C:\MyWorkFolder\*.*`
			`</Decsription>`
			`<DateCompare>`
			`<Operand>`
			`NEWER`
			`</Operand>`
			`<Date>07/31/2005</Date>`
			`</DateCompare>`
			`</IncDescription>`
			`</Inclusions>`
			
			Example 3
			`<Inclusions>`
			`<IncDescription>`
			`<Description>`
			`C:\MyWorkFolder/*.*`
			`</Description>`
			`<SizeCompare>`
			`<Operand>`
			`SMALLER`
			`</Operand>`
			`<Size>200</Size>`
			`</SizeCompare>`
			`</IncDescription>`
			`</Inclusions>`
			
			Example 4
			`<Inclusions>`
			`<IncDescription>`
			`<Description>`
			`C:\MyWorkFolder\*.*`
			`</Description>`
			`<Dest>`
			`D:\MyNewWorkFolder`
			`</Dest>`
			`<Operation>`
			`</Operation>`
			`<IncDescription>`
			`</Inclusions>`

Table 23. (continued)

Command	Parameter	Description	Example

<Exclusions>	<ExcDescription>
	
	<Description>
	
	<DateCompare>
	
	<Operand>
	
	<Date>
	
	<SizeCompare>
	
	<Operand>
	
	<Size> where
		• <Source> is a fully qualified file name or folder name. You can use the wild card character for both file name and folder name.
		• <DateCompare> is an optional command that you can use to select files based on the date when they were created.
		– <Operand> is either NEWER or OLDER.
		– <Date> is the baseline date in mm/dd/yyyy format.
		• <SizeCompare> Optional parameter to select files based on their size.
		– <Operand> is either LARGER or SMALLER.
		– <Size> is the file size in MB.
			To unselect all matching files in a specified directory
			
			For example:
			
			Example 1
			`<Exclusions>`
			`<ExcDescription>`
			`<Description>`
			`C:\YourWorkFolder`
			`</Description>`
			`</ExDescription>`
			`</Exclusions>`
			
			Example 2
			`<Exclusions>`
			`<ExcDescription>`
			`<Description>`
			`C:\YourWorkFolder`
			`</Description>`
			`<DateCompare>`
			`<Operand>`
			`OLDER`
			`</Operand>`
			`<Date>07/31/2005</Date>`
			`</DateCompare>`
			`</ExcDescription>`
			`</Exclusions>`
			
			Example 3
			`<Exclusions>`
			`<ExcDescription>`
			`<Description>`
			`C:\YourWorkFolder`
			`</Description>`
			`<SizeCompare>`
			`<Operand>`
			`LARGER`
			`</Operand>`
			`<Size>200`
			`</Size>`
			`</SizeCompare>`
			`</ExcDescription>`
			`</Exclusions>`

Examples of file-migration commands

This section contains examples of file-migration commands. These examples demonstrate how to combine file-inclusion and file-exclusion commands to refine your file selection. Only the file-handling sections of the command file are shown.

Selecting files during the capture phase

This section contains three examples of code used to select files during the capture phase.

Example 1

The following code example selects all files with a .doc extension (Microsoft Word documents) and relocates them in the "d:\My Documents" directory. It then excludes all files that are in the d:\No_Longer_Used directory.

```
<Inclusions>
<IncDescription>
<Description>*:\*.doc/s</Description>
<Dest>d:\My Documents</Dest>
<Operation>r</Operation>
</IncDescription>
</Inclusions>
<Exclusions>
<ExcDescription>
<Description>d:\No_Longer_Used\</Description>
</ExcDescription>
</Exclusions>
```

Example 2

The following code example selects the contents of the drive, excluding all files located in the root of the d drive and all files with a .tmp extension.

```
<Inclusions>
<IncDescription>
<Description<d:\*.*/s<\Description>
</IncDescription>
</Inclusions>
<Exclusions>
<ExcDescription>
<Description>d:\*.*</Description>
</ExcDescription>
<ExcDescription>
<Description>*:\*.tmp/s</Description>
</ExcDescription>
</Exclusions>
```

Example 3

The following code example selects the entire contents of the c drive, excluding all files located in the directory: %windir%. The %windir% directory specifies the Windows directory.

```
<Inclusions>
<IncDescription>C:\*.*/s</Description>
</Inclusion>
<Exclusions>
<ExcDescription>
<Description>%windir%\</Description>
</ExcDescription>
</Exclusions>
```

Example 4

The following code example selects the entire contents of the %USERPROFILE% folder that is the User Profile Path of the current logon user, excluding all files with a .dat extension and “Local Settings” subfolder.

```
<Inclusions>
<IncDescription>
<Description>%USERPROFILE%\</Description>
</IncDescription>
</Inclusions>
<Exclusions>
```

Migrating additional application settings

To create custom application files, you must have a thorough knowledge of the application, including the storage locations of customized settings. By default, System Migration Assistant is pre-configured to migrate settings for several applications. You can also create a custom application file to migrate settings for additional applications. This file must be named application.xml or application.smaapp and located in the c:\%RR%\Migration\bin\Apps, where *Apps* specifies the application and c is the drive letter of the hard disk drive. Priority is given to the application.smaapp file when both the application.smaapp file and application.xml custom applications file of the same application exist.

To support a new application, you can copy an existing application file and make the necessary changes. For example, Microsoft_Access.xml is an existing application file.

Consider the following points about application files:

- *application*.xml
  - By default, only application.xml exists.
  - The <tag> enclosed with ″<!--″ and ″-->″ is treated as comments. For example:

    ```
    <!--Files_From_Folders>
    <!-Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi\*.* /s
    </Files_From_Folder>
     <Files_From_Folder>%Personal Directory%\*.pdf</Files_from_Folder>
    </Files_From_folders-->
    ```
  - Each command must be described in a separate section.
  - Each section begins with a command enclosed by tags, for example, <AppInfo> or <Install_Directories>. You can enter one or more fields in a section; each field must be on a separate line.
  - If the application file contains syntax errors, the operation continues and writes the errors to the log file.

Table 24 shows information about application files:

Table 24.

Section	Command	Value	What it does
<Applications>			
<Family>		A text string. Leading spaces are ignored; do not enclose the text string in quotation marks.	Specifies the non-version-specific name of the application. When you run in batch mode, you use this string in the applications section of the command file. For example: `<Family>Adobe Acrobat Reader</Family>`
<SMA_Version>		A numeric value.	Specifies the System Migration Assistant version number. For example, `<SMA_Version>SMA 5.0</SMA_Version>`
<App>		*ShortName* where ShortName is a version-specific short name for an application.	Specifies a version-specific short name for one or more applications. For example, `<APP>Acrobat_Reader_50</APP>`
<Application ShortName=*ShortName*> where *ShortName* is the short name for an application that you specified in the "Applications" section.			
<Name>		A text string	Specifies the name of the application.
<Version>		A numeric value	Specifies the version of the application.

<Detects>
 	
<Detect>
		Root, PathAndKey	Specifies a registry key. System Migration Assistant detects an application by searching for the specified registry key.
			
			For example,
			`<Detects>`
			`<Detect>`
			`<hive>HKLM</hive>`
			`<keyname>`
			`Software\Adobe\Acrobat Reader\5.0\`
			`</keyname>`
			`</Detect>`
			`</Detects>`

<Install_Directories>
 	
For example:
`<Install_Directories>`
`<Install_Directory>`
`<OS>WinXP</OS>`
`<Registry>`
`<hive>HKLM</hive>`
`<keyname>Software\Adobe\Acrobat Reader\5.0\InstallPath</keyname>`
`<value>(Default)</value>`
`</Registry>`
`</Install_Directory>`
`<Install_Directory>`
`<OS>Win2000</OS>`
`<Registry>`
`<hive>HKLM</hive>`
`<keyname>Software\adobe\Acrobat Reader\5.0\InstallPath</keyname>`
`<value>(Default)</value>`
`</Registry>`
`</Install_Directory>`
`</Install_Directories>`

<OS>	A text string	Specifies the operating system, and can be one of the following: • Windows Vista • Windows XP • Windows 2000 • Windows NT • Windows 98
<Registry>	*hive* is either HKLM or HKCU. *keyname* is the keyname. *value* is an optional command that specifies the registry value that is migrated.	Specifies the installation directory as it appears in the registry.

SMAVariable\Location[|File][/s]
 	
where
• SMAvariable is one of the following variables that specify the location of the customization files:
– %Windows Directory% (location of operating-system files)
– %Install Directory% (location of the application as defined in the Install_Directories section)
– %Appdata Directory% (the Application Data directory, which is a subdirectory of the user profile directory)
– %LocalAppdata Directory% (the Application Data directory in the Local Settings folder, which is a subdirectory of the user profile directory)
– %Cookies Directory% (the Cookies directory, which is a subdirectory of the user profile directory)
– %Favorites Directory% (the Favorites directory, which is a subdirectory of the user profile directory)
– %Personal Directory% (the Personal directory, which is a subdirectory (My Documents) of the user profile directory. This environment variable cannot be used by Windows NT4.)
	Specifies the customization files that you want to migrate.
	
	For example:
	`<Files_From_Folder>`
	`%AppData Directory%\Adobe\Acrobat\Whapi`
	`</Files_And_Folders>`
	
	System Migration Assistant captures the files in %AppData Directory%\Adobe\Acrobat\Whapi folder. The files in the subdirectories are not included.
	`<Files_From_Folder>`
	`%AppData Directory%\Adobe\Acrobat\Whapi\ /s`
	`</Files_From_Folder>`
	
	System Migration Assistant captures the files in %AppData Directory%\Adobe\Acrobat\Whapi folder. The files in the subdirectories are included.
	`<Files_From_Folder>`
	`%AppData Directory%\Adobe\Acrobat\Whapi\*.*`
	`</Files_From_Folder>`
	
	System Migration Assistant captures the files in %AppData Directory%\Adobe\Acrobat\Whapi folder. The files in the subdirectories are not included.
	`<Files_From_Folder>`
	`%AppData Directory%\Adobe\Acrobat\Whapi\*.* /s`
	`</Files_From_Folder>`
	
	System Migration Assistant captures the files in %AppData Directory%\Adobe\Acrobat\Whapi folder. The files in the subdirectories are included.
	`<Files_From_Folder>`
	`%AppData Directory%\Adobe\Acrobat\Whapi`
	`</Files_From_Folder>`
	
	When "\" does not follow "Whapi", System Migration Assistant treats "Whapi" not as a folder but as a file.

• *Location* specifies a fully qualified file or directory. You can use wildcard characters in the file name but not the path. If you specify a directory, all files are copied. • *[File]* is an optional parameter that can be used only if Location specifies a directory, and File is the file to be copied. You can use wildcard characters in the file name but not the path. • *[/s]* is an optional parameter. If you use [/s], all files in subdirectories are copied. • SMA5.0 user can use Windows environment variable. The environment variable of the user who started SMA is used as the value of a Windows environment variable.	
<Registries> Optional	

hive is either HKLM or HKCU.
 	
keyname is the keyname. Value is an optional command that specifies the registry value that is migrated.
	Specifies the registry entries that you want to migrate.
	
	For example:
	`<Registries>`
	`<Registry>`
	`<hive>HKCU</hive>`
	`<keyname>`
	`Software\Adobe\Acrobat`
	`</keyname>`
	`<value></value>`
	`</Registry>`
	`</Registries>`

<Registry_Excludes> Optional	

hive is either HKLM or HKCU.
 	
keyname is the keyname. Value is an optional command that specifies the registry value that is migrated.
	Specifies registry keys and values that you want to exclude from the selected registry entries.
	
	For example:
	`<Registry_Excludes>`
	`<Registry>`
	`<hive>HKCU</hive>`
	`<keyname>`
	`Software\Adobe\Acrobat Reader\5.0\AdobeViewer`
	`</keyname>`
	`<value>xRes</value>`
	`</Registry>`
	`</Registry_Excludes>`

<Files_Through_Registry>	

<OS>
 	
specifies the operating system and is one of the following values:
• Windows Vista
• WinXP
• Win2000
• WinNT
• Win98
 	
<Registry> specifies the registry entry and is in the format hive, keyname, value, where:
• hive is either HKLM or HKCU.
• keyname is the keyname.
• value is an optional command that specifies the registry value the is migrated. File is the file name. You can use wildcard characters.
 	
File is the file name. You can use wildcard characters.
	Specifies customization files to be migrated
	
	For example:
	`<Files_Through_Registries>`
	`<Files_Through_Registry>`
	`<OS>WinXP</OS>`
	`<Registry>`
	`<hive>HKCU</hive>`
	`<keyname>`
	`Software\Lotus\Organizer\99.0\Paths`
	`</keyname>`
	`<value>Backup</value>`
	`</Registry>`
	`<File>*.*/s</File>`
	`</Files_Through_Registry>`
	`</Files_Through_Registries>`

<Files_From_Folders> Optional	
<PreTargetBatchProcessing>	

`<PreTargetBatchProcessing>`
`<!CDAT[batch commands]]`
`<PreTargetBatchProcessing>`
	<PreTargetBatchProcessing> performs Batch processing before <Registries> processing by Apply.
	
	For example:
	`<PreTargetBatchProcessing>`
	`<!CDATA[copy /y c:\temp\*.* c:\migration`
	`del c:\migration\*.mp3`
	`</PreTargetBatchProcessing>`

<TargetBatchProcessing>	

`<TargetBatchProcessing>`
`<!CDAT[batch commands]]`
`<TargetBatchProcessing>`
	<TargetBatchProcessing> performs Batch processing after <Registries> processing by Apply.
	
	For example:
	`<TargetBatchProcessing>`
	`<!CDATA[copy /y c:\temp\*.* c:\migration`
	`del c:\migration\*.mp3`
	`<TargetBatchProcessing>`

Creating an application file

To determine which application settings must be migrated for custom application files, you must carefully test the applications.

Complete the following steps to create an application file:

1. Use a text editor that can handle Unicode to open an existing application.xml file. If you installed SMA in the default location, the application.xml files are located in the c:\%RR%\Migration\bin\Apps directory, where d is the drive letter of the hard disk drive.

2. Modify this application.xml file for the application and applications settings that you want to migrate.
3. Modify the information in the <Applications> section.
4. Modify the <Name> and <Verison> commands in the <Application Shortname=*Shortname*> section.
5. Determine the registry keys that must be migrated:
   a. Click **Start**, and then click **Run**. The Run window opens. In the Open field, type regedit and click **OK**. The Registry Editor window opens.
   b. In the left pane, expand the **HKEY_LOCAL_MACHINE** node.
   c. Expand the **Software** node.
   d. Expand the vendor-specific node, for example, **Adobe**.
   e. Continue navigating until you have located the registry key for the application. In this example, the registry key is SOFTWARE\Adobe\Acrobat Reader\6.0.
   f. Set the value of theDetect field. For example:

```
<Detects>
<Detect
<hive>HKLM</hive>
<keyname>Software\Adobe|acrobat Reader\6.0<keyname>
</Detect
</Detects
```

6. Modify the name and version commands in the Install_Directories section.
7. Determine the path to the installation directories for the application.
   a. From the Registry Editor window, navigate to the HKLM\SOFTWARE\Adobe\Acrobat Reader\6.0\InstallPath node.
   b. Add the appropriate command to the Install_Directories section of the application file. For example:

```
<Install_Directory>
<OS>WinXP</OS>
<Registry>
<hive>HKLM</hive
<keyname>Software\Adobe\Acrobat Reader\6.0\InstallPath</keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>
```

   Note: If you do not find an application-specific directory in the HKLM\Software\Microsoft\Windows\CurrentVersion\AppPaths directory, you must locate a directory that contains the installation path elsewhere in the HKLM\Software tree. Then, use that key in the<Install_Directories> section
8. In the <Files_From Folders> section, specify the customization files you want to migrate.
   a. Since many applications by default save files in the Documents and settings subdirectory, check the Application data directory for directories that pertain to the application. If one exists, you can use the following command to migrate the directory and files:

```
<Files_From_Folder>SMAvariable\Location\[File] [/s] </Files_From_Folder>
```

   where Location\ is a fully qualified file or directory, and [File] is an optional parameter that can be used only if Location\ specifies a directory. In the Adobe Reader example, the customization files are in the Preferences directory.

b. Check all related directories for personal settings that might be stored there.
c. Check the Local Settings directory.

9. Determine registry entries that you want to migrate. They will be in HKCU (HKEY_CURRENT_USER). In the <Registries> section of the application file, add the appropriate commands.
10. Save the application.xml file in the c:\program files\lenovo\System Migration Assistant\Migration\bin\apps directory, where c is the drive letter of the hard disk drive.
11. Test the new application file.

Example of an application.xml file for Adobe Reader

This section contains an application file for Adobe Reader.

```
<?xml version="1.0"?>
<Applications>
<Family>Adobe Acrobat Reader</Family>
<SMA_Version>SMA 5.0</SMA_Version>
<APP>Acrobat_Reader_70</APP>
<APP>Acrobat_Reader_60</APP>
<APP>Acrobat_Reader_50</APP>
<Application ShortName="Acrobat_Reader_50">
<AppInfo>
<Name>Acrobat_Reader_50</Name>
<Version>5.0</Version>
<Detects>
<Detect>
<hive>HKLM</hive>
<keyname>Software\Adobe\Acrobat Reader\5.0</keyanme>
</Detect>
</Detects>
</AppInfo>

<Install_Directories>
<Install_Directory>
<OS>WinXP</OS>
<Registry>
<hive>HKLM</hive>
<keyname>Software\Adobe\Acrobat Reader\5.0\InstallPath</keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>

<Install_Direcotry>
<OS>Win2000</OS>
<Registry>
<hive>HKLM</hive>
<keyname>Software\Adobe\Acrobat Reader\5.0\InstallPath</keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>

<Install_Directory>
<OS>Win98</OS>
<Registry>
<hive>HKLM</hive>
<keyname>Software\Adobe\Acrobat Reader\5.0\InstallPath<keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>

<Install_Directory>
<OS>WinNT</OS>
```

```
<Registry>
<hive>HKLM</hive>
<keyname>Software\Adobe\Acrobat Reader\5.0\InstallPath</keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>
</Install_Directories>

<Files_From_Folders>
<Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi\*.* /s
</Files_From_Folder>
<Files_From_Folder>%Personal Directory%\*.pdf
</Files_From_Folder>
</Files_From_Folders>
<Files_Through_Registries>
</Files_Through_Registries>

<Registries>
<Registry>
<hive>HKCU</hive>
<keyname>Software\Adobe\Acrobat</keyname>
</Registry>
<Registry>
<hive>HKCU</hive>
<keyname>Software\Adobe\Acrobat Reader</keyname>
</Registry>

<Registry>
<hive>HKCU</hive>
<keyname>Software\Adobe\Persistent Data</keyname>
</Registry>
</Registries>

<Registry_Excludes>
<Registry>
<hive>HKCU</hive>
<keyname>Software\Adobe\Acrobat Reader\5.0\AdobeViewer</keyname>
<value>xRes</value></Registry>

<Registry>
<hive>HKCU</hive>
<keyname>Software\Adobe\Acrobat Reader\5.0\Adobe\Viewer</keyname>
<value>yRes</value>
</Registry>

<Registry_Excludes>
<SourceBatchProcessing>
</SourceBatchProcessing>

<PreTargetBatchProcessing>
</PreTargetBatchProcessing>

<TargetBatchProcessing>
</TargetBatchProcessing>
</Application>

<Application ShortName="Acrobat_Reader_6.0">
<AppInfo>
<Name>Adobe Acrobat Readr 6.0<\Name>
<Version>6.0</Version>
<Detects>
<Detect>
<hive>HKLM</hive>
<keyname>Software\Adobe\Acrobat Reader\6.0</keyname>
</Detect>
</Detects>
<\AppInfo>
```

```
<Install_Directories>
<Install_Directory>
<OS>WinXP</OS>
<Registry>
<hive>HKLM</hive>
<keyname>Software\Adobe\Acrobat Reader\6.0\InstallPath</keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>

<Install_Directory>
<OS>Win2000</OS>
<Registry>
<hive>HKLM</hive>
<keyname>Software\Adobe\Acrobat Reader\6.0\InstallPath</keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>

<Install_Directory>
<OS>Win98</OS>
<Registry>
<hive>HKLM</hive>
<keyname>Software\Adobe\Acrobat Reader\6.0\InstallPath </keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>

<Install_Directory>
<OS>WinNT</OS>
<Registry>
<hive>HKLM</hive>
<keyname>Software\Adobe\Acrobat Reader\6.0\InstallPath</keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>
</Install_Directories>

<Files_From_Folders>
<Files_From_Folder>%AppData Directory%\Adobe\Acrobat\6.0\*.* /s
</Files_From_Folder>
<Files_From_Folder>%Personal Directory%\*.pdf
</Files_From_Folder>
</Files_From_Folders>
<Files_Trough_Registries>
</Files_Trough_Registries>

<Registries>
<Registry>
<hive>HKCU</hive>
<keyname>Software\Adobe\Acrobat</keyname>
</Registry>

<Registry>
<hive>HKCU</hive>
<keyname>Software\Adobe\Acrobat Reader</keyname>
</Registry>
</Registries>

<Registry_Excludes>
<Registry>
<hive>HKCU</hive>
<keyname>Software\Adobe\Acrobat Reader\6.0\AdobeViewer</keyname>
<value>xRes</value>
</Registry>
```

```
<Registry>
<hive>HKCU</hive>
<keyname>Software\Adobe\Acrobat Reader\6.0\Adobe\Viewer</keyname>
<value>yRes</value>
</Registry>

<Registry_Excludes>

<SourceBatchProcessing>
</SourceBatchProcessing>

<PreTargetBatchProcessing>
</PreTargetBatchhProcessing>

<TargetBatchProcessing>
<![CDATA[if /i "%SourceApp%" == "Acrobat_Reader_50" goto Update50
goto Done:Update50
regfix
"HKCU\Software\Adobe\Acrobat Reader\5.0"
"HKCU\Software\Adobe\Acrobat Reader\6.0"
regfix
"HKLM\Software\Adobe\Acrobat Reader\5.0\AdobeViewer"
"HKLM\Software\Adobe\Acrobat Reader\6.0\AdobeViewer"
:Done]] >
</TargetBatchProcessing>
</Application>

<Application ShortName="Acrobat_Reader_7.0">
<AppInfo>
<Name>Adobe Acrobat Reader 7.0<\Name>
<Version>6.0</Version>
<Detects>
<Detect>
<hive>HKLM</hive>
<keyname>Software\Adobe\Acrobat Reader\7.0</keyname>
</Detect>
</Detects>
<\AppInfo>

<Install_Directories>
<Install_Directory>
<OS>WinXP</OS>
<Registry>
<hive>HKLM</hive>
<keyname>Software\Adobe\Acrobat Reader\7.0\InstallPath</keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>

<Install_Directory>
<OS>Win2000</OS>
<Registry>
<hive>HKLM</hive>
<keyname>Software\Adobe\Acrobat Reader\7.0\InstallPath</keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>

<Install_Directory>
<OS>Win98</OS>
<Registry>
<hive>HKLM</hive>
<keyname>Software\Adobe\Acrobat Reader\7.0\InstallPath</keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>
```

```
<Install_Directory>
<OS>WinNT</OS>
<Registry>
<hive>HKLM</hive>
<keyname>Software\Adobe\Acrobat Reader\7.0\InstallPath</keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>
</Install_Directories>

<Files_From_Folders>
<Files_From_Folder>%AppData Directory%\Adobe\Acrobat\7.0\*.* /s
</Files_From_Folder>
<Files_From_Folder>%Personal Directory%\*.pdf
</Files_From_Folder>
</Files_From_Folders>

<Files_Through_Registries>
</Files_Through_Registries>

<Registries>
<Registry>
<hive>HKCU</hive>
<keyname>Software\Adobe\Acrobat</keyname>
</Registry>
<Registry>
<hive>HKCU</hive>
<keyname>Software\Adobe\Acrobat Reader</keyname>
</Registry>
</Registries>

<Registry_Excludes>
<Registry>
<hive>HKCU</hive>
<keyname>Software\Adobe\Acrobat Reader\7.0\AdobeViewer</keyname>
<value>xRes</value>
</Registry>

<Registry>
<hive>HKCU</hive>
<keyname>Software\Adobe\Acrobat Reader\7.0\Adobe\Viewer</keyname>
<value>yRes</value>
</Registry>

<Registry_Excludes>
<SourceBatchProcessing>
</SourceBatchProcessing>

<PreTargetBatchProcessing>
</PreTargetBatchProcessing>

<TargetBatchProcessing>
<![CDATA[
if /i "%SourceApp%" == "Acrobat_Reader_50" goto Update50
if /i "%SourceApp%" == "Acrobat_Reader_60" goto Update60
goto Done:Update50
regfix
"HKCU\Software\Adobe\Acrobat Reader\5.0"
"HKCU\Software\Adobe\Acrobat Reader\7.0"
regfix
"HKLM\Software\Adobe\Acrobat Reader\5.0\AdobeViewer"
"HKLM\Software\Adobe\Acrobat Reader\7.0\AdobeViewer"
goto Done:Update60
regfix
"HKCU\Software\Adobe\Acrobat Reader\6.0"
"HKCU\Software\Adobe\Acrobat Reader\7.0"
regfix
```

```
"HKLM\Software\Adobe\Acrobat Reader\6.0\AdobeViewer"
"HKLM\Software\Adobe\Acrobat Reader\7.0\AdobeViewer"
:Done]] >
</TargetBatchProcessing>
</Application>
</Applications>
```

Chapter 5. Best practices

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

Scenario 1 - New rollouts

This section describes installing Rescue and Recovery in a new rollout on Lenovo-branded and IBM-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 Rescue and Recovery. The last step in the process is to install Rescue and Recovery.

Installing

This first step in the installation process is the extraction of the InstallShield executable to the C:\RRTEMP directory. If you are going to install Rescue and Recovery 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 z652zisXXXXus00.exe for Windows XP or the file z633zisXXXXus00.exe for Windows Vista (where *XXXX* is the build ID) to the C:\RRTEMP directory:

   ```
   :: This package will extract the WWW EXE to the directory c:\RRTemp for an
   ```

```
:: administrative installation.
@ECHO OFF
:: This is the name of the EXE (Without the .EXE)
set BUILDID=z652zisXXXXus00.exe
:: This is the drive letter for the z652zisXXXXus00.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:\RRTemp
:: Explode the WWW EXE to the directory c:\RRTemp
start /WAIT %SOURCEDRIVE%\%BUILDID% /a /s /v"/qn TARGETDIR=c:\RRTemp"
Copy Z652ZAB10YYUS00.tvt and Z333ZAA10ZZUS00.tvt to C:\rrtemp\
(where YY and ZZ are build IDs)
copy Z652ZAB10YYUS00.tvt to C:\RRTemp
copy Z333ZAA10ZZUS00.tvt C: to C:\RRTemp
If you want installation for supported languages besides US,
copy Z652ZAB10YYUS00.tvt to C:\RRTemp
(where YY is the build ID and CC is the country code).
copy Z652ZAB10YYUS00.tvt to C:\RRTemp
```

2. You can make many customizations before the installation of Rescue and Recovery. Some examples in this scenario are:
   - Change maximum number of incremental backups to 4.
   - Set Rescue and Recovery to perform an incremental backup every day at 1:59 p.m. to the local hard disk 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:\RRTemp directory:
   - Perform a silent installation of Rescue and Recovery without a reboot at the end.
   - Start Rescue and Recovery so that a base backup can be performed.
   - After the service is started, set up the environment to create an ISO image of the 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:\RRTemp\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:\RRTemp\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\tcl8.4
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 Rescue and Recovery 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 32 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,
```

```
%tvtdrive%\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,
%tvtdrive%\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 32.
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 25. 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 Rescue and Recovery on OEM computers. To install Rescue and Recovery, eight free sectors must be available in the Master Boot Record on the hard disk drive. Rescue and Recovery 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 Rescue and Recovery provides the desired functions and features:

Best practices for hard drive setup: Option 1

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

1. Set up a test client with the image that contains the OEM product recovery code.
2. Install Rescue and Recovery. If eight free sectors in the 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 Rescue and Recovery at: http://www.lenovo.com/support/site.wss/document.do?lndocid=TVAN-ADMIN#tvsu 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

Rescue and Recovery builds and burns the rescue media CD from the current service area contents, rather than from a pre-assembled ISO image. However, if an appropriate ISO (.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
\tcl\tcl8.4
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\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 on Type 12 service partition

This section describes installing Rescue and Recovery on a Type 12 service partition. You must have the following in order to install Rescue and Recovery into a type 12 service partition:
- The SP.PQI file. This file includes base bootable files to create a service partition.
- PowerQuest PQDeploy
- Latest installer for Rescue and Recovery

There are several options related to installing the Rescue and Recovery environment in a service partition.

Note: The type 12 partition must reside in the last used entry in the partition table on the same drive that contains Windows. You can use the information on BMGR32 to determine where the type 12 partition resides on the hard disk drive. For more information, see "Rescue and Recovery Boot manager control (BMGR32)" on page 90.

To perform the installation, complete the following procedure:
1. Leave at least 700 MB of unallocated free space at the end of the drive.

2. Using PowerQuest PQDeploy, restore the SP.pqi file to the unallocated free-space. If you need additional assistance with PowerQuest PQDeploy, reference documentation from PowerQuest.
3. Delete the primary partitions created in step 1 (except the C drive), and then reboot.

   Note: System volume information may be on the newly created service partition. The system volume information needs to be deleted through Windows System Restore.

4. Install Rescue and Recovery and reboot, when prompted.

Scenario 4 - Installing with WIM files and Windows Vista

Windows Vista 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 Rescue and Recovery on Windows Vista:

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 Vista, WIM files, or ImageX, see the following Web site:
http://www.microsoft.com

Scenario 5 - 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 Rescue and Recovery.
2. Configure BIOS password recovery silently.

Scenario 6 - 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 Rescue and Recovery 4.21 on an image machine.
2. From the Windows Start menu, run gpedit.msc.
3. Right click on Administrative Templates under Computer Configuration.

4. Select Add/Remove Templates.
5. Press the Add button and then select the rnr.adm file. The rnr.adm file can be obtained from the Administrative tools package located at: http://www.lenovo.com/support/site.wss/document.do?lndocid=TVAN-ADMIN#tvsu
6. Press 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 present. 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 dropdown box labeled Advanced Menu.
11. Click OK on the Advanced Menu Properties dialog box.
12. From the Windows Start menu, run regedit.
13. Navigate to and 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. Press the Save button.

Now, you can create an installation package that will install Rescue and Recovery 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 7 - 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 85.
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 8 - Manually creating the Service Partition of S drive

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

1. Boot from the Windows Vista 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>clean`
5. Restart the computer.
6. Boot from the Windows Vista 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="SERVICEV003" quick`
13. Install Windows Vista 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 Vista 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 4.21 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?lndocid=TVAN-ADMIN#tvsu

Command line support

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

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 Rescue and Recovery:

Syntax:

`RRcmd` *`command filter=filterfile location=c`* `[name=`*`abc`*` | level=`*`x`*`] [silent]`

Table 26. 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).
`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. If you are setting a password when creating a Sysprep backup to the network then the password file will not be written to the backup location until an incremental backup is taken. The following information provides two work alternate methods: a. Create a local Sysprep backup and copy the backups to either the network or the USB. b. Create an incremental backup to the network or the USB after the Sysprep backup and either keep or delete the incremental backup.

Table 26. RRcmd parameters (continued)

Command	Result
`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
`Migrate`	Create migration file from a backup.
`Filter=`*`filterfile`*	Files and folders that will be restored. This command is used only with the **Restore** command.
`Location=`*`c`*	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=`*`abc`*	Where *abc*, is the name of the backup.
`level=`*`x`*	Where *x* 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=*x* command is only required if performing an administrator backup (equal to or greater than 100, for example). **Notes:** 1. To restore from the latest backup, do not provide this parameter. 2. All backup and restore features are routed through the service so that the appropriate sequencing can be maintained, callbacks are performed, for example. The backup command is replaced with the command-line options.)

Boot manager Configuration File Format	The format of the boot manager configuration file is backward compatible with the previous version of boot manager. Any switch not show below is not supported. The file format is a text file with each entry is on a separate line.
	`<PROMPT1=this is the text that will appear on F11 prompt>`
	`<KEY1=F11>`
	`<WAIT=40>`

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.

How to replace files in a base backup

To replace a file in your backups:

1. Modify a file or files that exist in the backups, for example: c:\install.log
2. Create a file in the root of c:\, called file.txt.
3. Edit file.txt 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 this file.txt closed.
4. Run RRCMD Changebase filename=c:\file.txt drive=c: destination="c:\RRBACKUPS"

   Note: Check single file restore with the user interface to notice change in size.

CLEANDRV.EXE

The cleandrv.exe file cleans the drive of all files. There will be no operating system after running this command. See "Scenario 4 - Installing with WIM files and Windows Vista" on page 81 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 Rescue and Recovery Administration tools from: http://www.lenovo.com/support/site.wss/document.do?lndocid=TVAN-ADMIN#tvsu
2. Open a CMD windows
3. Type in Convdate
4. To convert DWORD Values, type the date and time in the Select date and time fields.

   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 27.

Parameters	Description
size=*x*	Size of service partition to create, in megabytes.
drive=*x*	The drive number to create the service partition on. If not specified, the first non-USB drive is used. This parameter is optional.
/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 sectiont2 ...**

  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 map 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 28. 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.

Table 28. MapDrv parameters (continued)

Parameter	Result
/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.
/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 29. 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.

Table 29. BMGR32 parameters (continued)

Parameter	Result
/BW	Boot to the Rescue and Recovery protected partition.
/BWIN	Reset request to boot to Predesktop Area. This must be called prior to booting.
/CFG*file*	Apply the configuration file parameters. See "RRCMD command-line interface" on page 85 for details regarding the configuration file.
/DS	Return the Master boot record (MBR) data sector (0-based).
/D*n*	Apply changes to disk n, where n is 0-based, (default: disk containing environment variable "SystemDrive" or "C:\" if "SystemDrive" is not defined.)
/H0	Hide partition 0.
/H1	Hide partition 1.
/H2	Hide partition 2.
/H3	Hide partition 3.
/HS	Hide the service partition.
/P12	Hide the service partition by setting partition type to 12.
/INFO	Display hard disk drive information (checks for 8 free sectors).
/INFOP	Display hard disk drive information (checks for 16 free sectors).
/M0	Rescue and Recovery environment is located in the service partition.
/M1	Rescue and Recovery environment is located in the C:\PARTITION (dual boot Windows and Windows PE).
/M2	Rescue and Recovery environment is located in the service partition with DOS (dual boot Windows PE and DOS; Lenovo-branded or IBM-branded preload Only).
/OEM	Computer is not an IBM branded or Lenovo-branded computer. This forces a second check for the F11 (default) key press after POST. This may be required for older IBM-branded systems. This is also the default setting for the OEM version of Rescue and Recovery.
/Patch*n*	Used for installation program only to set a variable that the Master boot record patch program can access.
Patchfile*filename*	Used for installation program only to install the Master boot record patch.
/PRTC	Used for installation program only, to retrieve patch return code.
/IBM	System is an IBM branded or Lenovo-branded computer.
/Q	Silent.
/V	Verbose.
/R	Reboot computer.
/REFRESH	Reset partition table entries in data sector.
/THINK	Configure the boot manager to use the blue button on the keyboard to enter the Predesktop Area.

Table 29. BMGR32 parameters (continued)

Parameter	Result
`/TOC tocvalue`	Set the BIOS TOC location (16 characters that represent 8 bytes of data).
`/U0`	Show partition 0.
`/U1`	Show partition 1.
`/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 ¼ 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 Rescue and Recovery.
- **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 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 30. 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 Rescue and Recovery 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 Rescue and Recovery.
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 31.

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

SP.PQI

This file can be used to create a type 12 service partition. See "Scenario 3 - Installing on Type 12 service partition" on page 80 for more information.

Note: This function is not available in Windows Vista.

Active Update

Active Update is an eSupport technology that utilizes the update clients on the local system to deliver the desired packages on the Web without any user interaction. Active Update queries the available update clients and uses the updated client to install the desired package. Active Update will launch ThinkVantage System Update or Software Installer on the system.

To determine if the Active Update Launcher is installed, check for the existence of the following registry key:

```
HKLM\SOFTWARE\Thinkvantage\ActiveUpdate
```

To determine if the registry is configured to allow Active Update, the ThinkVantage Technology program should check within its own registry key for the value of the EnableActiveUpdate attribute. If EnableActiveUpdate=1, the ThinkVantage Technology program should add the Active Update menu item under the Help menu.

To call Active Update, the calling ThinkVantage Technology program should launch the Active Update Launcher program and pass a parameter file. (See the Active Update Parameter File for a description of the parameter file).

To disable Active Update Launcher menu item from help menu for all ThinkVantage Technology programs:

1. Go to the HKLM\Software\ThinkVantage\ActiveUpdate registry key

2. Rename or delete the Active Update key

To disable Active Update Launcher menu item from help menu for individual ThinkVantage Technology program:

1. Go to the registry key:
   - For Rescue and Recovery - HKLM\Software\Lenovo\Rescue and Recovery
2. Add the DWORD value *EnableActiveUpdate* and set value to 0

To enable the Active Update Launcher menu item from the help menu if it is not available under the help menu for the individual TVT:

1. Go to the registry key:
   - For Rescue and Recovery - HKLM\Software\Lenovo\Rescue and Recovery
2. Add the DWORD value *EnableActiveUpdate* and set value to 1

Active Update Parameter File

The Active Update parameter file contains the settings to be passed to Active Update. The TargetApp parameter is passed as shown in this example:

```
<root>
       <TargetApp>ACCESSLENOVO</TargetApp>
</root>
```

```
<root>
       <TargetApp>1EA5A8D5-7E33-11D2-B802-00104B21678D</TargetApp>
</root>
```

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 Rescue and Recovery, 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 administrators policy setting will override the preference set by the user.

When Rescue and Recovery 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.

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 32. 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\

Table 32. Registry locations (continued)

Header	Header
Default user preferences	HKLM\Software\Lenovo\Rescue and Recovery\User defaults

Group Policy settings

The tables in this section provide policy settings for the Computer Configuration and the User Configuration for Rescue and Recovery and Client Security Solution.

Rescue and Recovery

The tables in this section provide policy settings for Rescue and Recovery.

User Configuration: The following table provides the policy for the User Configuration Settings tab:

Table 33. User configuration>Rescue and Recovery>Settings

Policy	Description
Analyze FileSize Threshold	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: 20MB.
Sort Filter Files	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 34. User Configuration>Rescue and Recovery>User interface

Policy	Setting	Description
Menus	Backup Menu	Show, gray or hide the Backup menu. Default: Show.
Menus	Restore Menu	Show, gray or hide the Restore menu in the main user interface. Default: Show.
Menus	Advanced Menu	Show, gray or hide the Advanced menu in the main user interface. Default: Show.
Menus	Help Menu	Show, gray or hide the Help menu in the main user interface. Default: Show.
Menu Items	Backup Now	Show, gray or hide the Backup Now menu item and buttons in the main user interface. Default: Show.
Menu Items	Schedule Preferences	Show, gray or hide the Schedule Preferences menu item and buttons in the main user interface. Default: Show.
Menu Items	Optimize	Show, gray or hide the Optimize menu item and button in the main user interface. Default: Show.
Menu Items	View Backups	Show, gray or hide the View Backups' menu item and buttons in the main user interface. Default: Show.
Menu Items	Restore	Show, gray or hide the 'Restore' menu item and button in the main user interface. Default: Show.

Table 34. User Configuration>Rescue and Recovery>User interface (continued)

Policy	Setting	Description
Menu Items	Rescue Files	Show, gray or hide the Rescue Files menu item and button in the main user interface. Default: Show.
Menu Items	Copy Backups	Show, gray or hide the Copy Backups menu item in the main user interface. Default: Show.
Menu Items	Delete Backups	Show, gray or hide the Delete Backups menu item in the main user interface. Default: Show.
Menu Items	Exclude	Show, gray or hide the Exclude menu item in the main user interface. Default: Show.
Menu Items	Include	Show, gray or hide the Include menu item in the main user interface. Default: Show.
Menu Items	Single Storage	Show, gray or hide the Single Storage menu item in the main user interface. Default: Show.
Menu Items	Create Migration File	Show, gray or hide the Create Migration File menu item in the main user interface. Default: Show.
Menu Items	Sysprep Backup	Show, gray or hide the Sysprep Backup menu item in the main user interface. Default: Hide.
Menu Items	Help	Show, gray or hide the Help menu item in the main user interface. Default: Show.
Menu Items	Context Help	Show, gray or hide the Context Help menu item in the main user interface. Default: Show.
Menu Items	Active Update	Show, gray or hide the Active Update menu item in the main user interface. Default: Show.
Menu Items	Users Guide	Show, gray or hide the Users Guide menu item in the main user interface. Default: Show.
Menu Items	About	Show, gray or hide the About menu item in the main user interface. Default: Show.
Backup	Configured Backup Location	Show, gray or hide the radio button to back up your data. Default: Show.
Backup	Optical Backup Location	Show, gray or hide the radio button to create a backup to optical media. Default: Show.
Backup	Max Incrementals Exceeded	Show or hide the Max Incrementals Exceeded dialog. Default: Hide.
Restore	Full Restore	Show, gray or hide the Full Restore radio button.
Restore	Rejuvenate	Show, gray or hide the Rejuvenate radio button in the restore options. Default: Show.
Restore	Restore OSApps	Show, gray or hide the Restore OS/Apps radio button in the restore options. Default: Show.
Restore	SFR Restore NTFS To Fat32	Show or hide the Fat32 partitions when restoring files from NTFS. Default: Show.
Restore	Rescue File Search	Show, gray or hide the Rescue File Search button. Default: Show.
Restore	Password Persist	Show, gray or hide the Password Persist radio buttons. Default: Show.
Restore	Base Backup	Show or hide the Base Backup from being restored via the User Interface. Default: Show.
Restore	Admin Backups	Show or hide the 'Admin Backups' from being restored through the User Interface. Default: Show.

Table 34. User Configuration>Rescue and Recovery>User interface (continued)

Policy	Setting	Description
Schedule and Preferences	Primary Backup Location	Show, gray or hide the 'Primary Backup Location' in the Schedule and Preference dialog. Default: Show.
Schedule and Preferences	Alternate Backup Location	Show, gray or hide the Alternate Backup Location in the Schedule and Preference dialog. Default: Show.
Schedule and Preferences	Schedule Settings	Show, gray or hide 'Schedule Settings' in the Schedule and Preference dialog. Default: Show.
Schedule and Preferences	Schedule Frequency	Show, gray or hide Schedule Frequency in the Schedule and Preference dialog. Default: Show.
Schedule and Preferences	Schedule Time	Show, gray or hide Schedule Time' in the Schedule and Preference dialog. Default: Show.
Schedule and Preferences	Suspend Check	Show, gray or hide the Suspend checkbox in the Schedule and Preferences dialog. Default: Hide.
Schedule and Preferences	Backup Partitions	Show, gray or hide the Backup Partitions checkboxes in the Schedule and Preferences dialog. Default: Show.
Schedule and Preferences	Backup Storage Warning	Show, gray or hide the Backup Storage Warning item in the Schedule and Preferences dialog. Default: Show.
Schedule and Preferences	Password Protect	Show, gray or hide the Password Protect item in the Schedule and Preferences dialog. Default: Show.
Schedule and Preferences	CSS Encrypt	Show, gray or hide the CSS Encrypt item in the Schedule and Preferences dialog. Default: Show.
Schedule and Preferences	Lock Hard Disk	Show, gray or hide the Lock Hard Disk item in the Schedule and Preferences dialog. Default: Show.
Copy Backups	Copy To Optical	Show, gray or hide the Copy To Optical radio button. Default: Show.
Copy Backups	Copy To USB	Show, gray or hide the Copy To USB radio button. Default: Show.
Copy Backups	Copy To Second	Show, gray or hide the Copy To Second radio button. Default: Show.
Copy Backups	Copy To Network	Show, gray or hide the Copy To Network radio button. Default: Show.
Delete	Base Backup	Show or hide the Base Backup from delete page. Default: Show.
Migrate	Migrate Delete Files	Show, gray or hide the Migrate Delete Files item on the Migration page. Default: Show.
Migrate	Migration Password	Show, gray or hide the Migration Password item on the Migration page. Default: Show.
User Interface		Enable or disable the main user interface. Default: Enabled.
Restore Interface		Enable or disable the 'Restore' interface. Default: Enabled.
Simple User Interface		Enable or disable the simple user interface. Default: Enabled
Interface Switching		Enable or disable the ability to switch between advanced and simple user interfaces. Default: Enabled

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

Computer Configuration: The following table provides the policy for the Computer Configuration for Rescue and Recovery under the Settings tab.

Table 35. Computer Configuration>Rescue and Recovery>Settings

Policy	Setting	Sub-Setting	Description
Backup	PreBackup	Pre	Command to run prior to backup. Include the full path to the file, if that path is not in the environment variable. Default: None.
Backup	PreBackup	PreParameters	The parameter that passes the command that is run prior to backup. Default: None.
Backup	PreBackup	PreShow	Show or hide the command that is run prior to backup. Default: Show.
Backup	PreBackup	Pre0	Command to run prior to the base backup. Include the full path to the file, if that path is not in the environment variable. Default: None.
Backup	PreBackup	PreParameters0	The parameter that passes the command that is run prior to the base backup. Default: None.
Backup	PreBackup	PreShow0	Show or hide the command that is run prior to the base backup. Default: Show.
Backup	PreBackup	Pre1	Command to run prior to incremental backup number 1. Include the full path to the file, if that path is not in the environment variable. Default: None.
Backup	PreBackup	PreParameters1	The parameter that passes the command that is run prior to incremental backup number 1. Default: None.
Backup	PreBackup	PreShow1	Show or hide the command that is run prior to incremental backup number 1. Default: Show.
Backup	PreBackup	Pre2	Command to run prior to incremental backup number 2. Include the full path to the file, if that path is not in the environment variable. Default: None.
Backup	PreBackup	PreParameters2	The parameter that passes the command that is run prior to incremental backup number 2. Default: None.
Backup	PreBackup	PreShow2	Show or hide the command that is run prior to incremental backup number 2. Default: Show.

Table 35. Computer Configuration>Rescue and Recovery>Settings (continued)

Policy	Setting	Sub-Setting	Description
Backup	PreBackup	Pre3	Command to run prior to incremental backup number 3. Include the full path to the file, if that path is not in the environment variable. Default: None.
Backup	PreBackup	PreParameters3	The parameter that passes the command that is run prior to incremental backup number 3. Default: None.
Backup	PreBackup	PreShow3	Show or hide the command that is run prior to incremental backup number 3. Default: Show.
Backup	PreBackup	Pre4	Command to run prior to incremental backup number 4. Include the full path to the file, if that path is not in the environment variable. Default: None.
Backup	PreBackup	PreParameters4	The parameter that passes the command that is run prior to incremental backup number 4. Default: None.
Backup	PreBackup	PreShow4	Show or hide the command that is run prior to incremental backup number 4. Default: Show.
Backup	PreBackup	Pre5	Command to run prior to incremental backup number 5. Include the full path to the file, if that path is not in the environment variable. Default: None.
Backup	PreBackup	PreParameters5	The parameter that passes the command that is run prior to incremental backup number 5. Default: None.
Backup	PreBackup	PreShow5	Show or hide the command that is run prior to incremental backup number 5. Default: Show.
Backup	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.
Backup	PostBackup	PostParameters	The parameter that passes the command that is run following the conclusion of a backup. Default: None.
Backup	PostBackup	PostShow	Show or hide the command that is run following a backup. Default: Show.

Table 35. Computer Configuration>Rescue and Recovery>Settings (continued)

Policy	Setting	Sub-Setting	Description
Backup	PostBackup	Post0	Command to run after the base backup concludes. Include the full path to the file, if that path is not in the environment variable. Default: None.
Backup	PostBackup	PostParameters0	The parameter that passes the command that is run following the conclusion of the base backup. Default: None.
Backup	PostBackup	PostShow0	Show or hide the command that is run following the base backup. Default: Show.
Backup	PostBackup	Post1	Command to run after incremental backup number 1 concludes. Include the full path to the file, if that path is not in the environment variable. Default: None.
Backup	PostBackup	PostParameters1	The parameter that passes the command that is run following the conclusion of incremental backup number 1. Default: None.
Backup	PostBackup	PostShow1	Show or hide the command that is run following incremental backup number 1. Default: Show.
Backup	PostBackup	Post2	Command to run after incremental backup number 2 concludes. Include the full path to the file, if that path is not in the environment variable. Default: None.
Backup	PostBackup	PostParameters2	The parameter that passes the command that is run following the conclusion of incremental backup number 2. Default: None.
Backup	PostBackup	PostShow2	Show or hide the command that is run following incremental backup number 2. Default: Show.
Backup	PostBackup	Post3	Command to run after incremental backup number 3 concludes. Include the full path to the file, if that path is not in the environment variable. Default: None.
Backup	PostBackup	PostParameters3	The parameter that passes the command that is run following the conclusion of incremental backup number 3. Default: None.
Backup	PostBackup	PostShow3	Show or hide the command that is run following incremental backup number 3. Default: Show.

Table 35. Computer Configuration>Rescue and Recovery>Settings (continued)

Policy	Setting	Sub-Setting	Description
Backup	PostBackup	Post4	Command to run after incremental backup number 4 concludes. Include the full path to the file, if that path is not in the environment variable. Default: None.
Backup	PostBackup	PostParameters4	The parameter that passes the command that is run following the conclusion of incremental backup number 4. Default: None.
Backup	PostBackup	PostShow4	Show or hide the command that is run following incremental backup number 4. Default: Show.
Backup	PostBackup	Post5	Command to run after incremental backup number 5 concludes. Include the full path to the file, if that path is not in the environment variable. Default: None.
Backup	PostBackup	PostParameters5	The parameter that passes the command that is run following the conclusion of incremental backup number 5. Default: None.
Backup	PostBackup	PostShow5	Show or hide the command that is run following incremental backup number 5. Default: Show.
Backup	Backup Local		Enable or disable 'Backup Local' as a selected destination for backup. Default: Enabled.
Backup	Backup Second		Enable or disable 'Backup Second' as a selected destination for backup. Default: Disabled. **Notes:** 1. If a service partition backup fails due to insufficient space, manually delete partial backups before attempting another backup or restoring from the failed backup. 2. When backing up the service partition to external media, set the following registry key before restoring your system with Rescue and Recovery: `HKLM\Software\Lenovo\Rescue and Recovery\Settings\Backup\BackupSPNetwork=1`

Table 35. Computer Configuration>Rescue and Recovery>Settings (continued)

Policy	Setting	Sub-Setting	Description
Backup	Backup USB		Enable or disable 'Backup USB' as a selected destination for backup. Default: Disabled. **Notes:** 1. If a service partition backup fails due to insufficient space, manually delete partial backups before attempting another backup or restoring from the failed backup. 2. When backing up the service partition to external media, set the following registry key before restoring your system with Rescue and Recovery: `HKLM\Software\Lenovo\Rescue and Recovery\Settings\Backup\BackupSPNetwork=1`
Backup	Backup Network		Enable or disable 'Backup Network' as selected destination for backup. Default: Disabled. **Notes:** 1. If a service partition backup fails due to insufficient space, manually delete partial backups before attempting another backup or restoring from the failed backup. 2. When backing up the service partition to external media, set the following registry key before restoring your system with Rescue and Recovery: `HKLM\Software\Lenovo\Rescue and Recovery\Settings\Backup\BackupSPNetwork=1`
Backup	Local Partition Number		Set the partition number for backups on the local drive. Valid values: 1-100. Default: 1.
Backup	USB Partition Number		Set the partition number for backups on the USB drive. Valid values: 1-100. Default: 1.
Backup	Second HDD Partition Number		Set the partition number for backups on the Second hard disk drive. Valid values: 1-100. Default: 1.

Table 35. Computer Configuration>Rescue and Recovery>Settings (continued)

Policy	Setting	Sub-Setting	Description
Backup	Backup Partitions		Select the partitions that should be backed up. This DWORD is a bitmap of logical drive letters that should be included in the backup. 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. Example: If you back up drive c: and e: only, you will get the binary value 00010100. The hexadecimal value for it: 0x00000014 and the decimal value for it: 20. **Note:** Convert your hexadecimal number to decimal before entering. Default: 0xFFFFFFFF. Entering a zero has a meaning similar to the default, which means finding all available partitions and back them up.
Backup	Max Backup Size		The maximum backup size (in GB). Valid values are 1-1000. Default: available free space.
Backup	Max Number Incrementals		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: *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.* This message is to let you know that the oldest incremental backup will not be deleted, but merged to the next incremental backup.
Backup	Encrypt With CSS		Enable or disable 'Encrypt With Client Security Solution' as a backup option. This option permits hardware or static-key encryption. Default: Disabled.
Backup	Resume After Power Loss		Enable or disable 'Resume After Power Loss' as a backup option. Default: Enabled.

Table 35. Computer Configuration>Rescue and Recovery>Settings (continued)

Policy	Setting	Sub-Setting	Description
Backup	Capture Migration Info		Enable or disable 'Capture Migration Info' as a backup option. When enabled, with each backup, data is collected that permits the System Migration Assistant to transfer current system settings to another machine, should the need arise. Default: Enabled.
Backup	Backup SP Second		Enable or disable 'Backup SP Second' as an option. When enabled, the system service partition can be backed up to the second system drive. Default: Disabled.
Backup	Backup SP USB		Enable or disable 'Backup SP USB' as an option. When enabled, the system service partition can be backed up to the USB drive. Default: Disabled.
Backup	Backup SP Network		Enable or disable 'Backup SP Network' as an option. When enabled, the system service partition can be backed up to the network. Default: Disabled.
Backup	CPU Priority		CPU Priority of backups. Values: 1-5 (1=Lowest Priority, 5=Highest Priority). Default: 3.
Backup	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.
Backup	Boot Disc		Enable or disable the creation of a 'Boot Disc' when backing up to CD/DVD or creating an archive to those media. Default: Enabled.
Backup	VerifyDisc		Enable or disable 'Verify Disc' when backing up to a CD/DVD or creating an archive to those media. Default: Enabled.
Backup	Battery Percent Required		'Battery Percent Required' before commencing a scheduled backup. This policy ensures there is enough battery power left to complete a backup. Values: 0-100. Default: 0.
Backup	Skip Locked Files		Enable or disable 'Skip Locked Files' when backing up. If enabled, locked files will be not be backed up. Default: Disabled.
Backup	Min Percent Free Space		The minimum percent of free space on the destination drive required for backup. Values: 0-100. Default: 0.

Table 35. Computer Configuration>Rescue and Recovery>Settings (continued)

Policy	Setting	Sub-Setting	Description
Backup	Protect With UUID		Enable or disable the 'Protect With UUID' option. If enabled, this will prevent the backups taken on one machine from being restored on another. Default: Disabled.
Backup	Protect With Password		Enable or disable the 'Protect With Password' option, if enabled, backups may be protected with a password. Default: Disabled.
Backup	User Message		Show or Hide the User Interface message for 'No Battery'. **Note:** If you have the Battery Power Requirement set at 1%, and the system that you are attempting to backup has 1% remaining battery power, set this policy to **Hide** to proceed with the backup.
Restore	PreRestore	PreWinRestore	Command to run prior to a restore from Windows. Include the full path to the file, if that path is not in the environment variable. Default: None.
Restore	PreRestore	PreWinRestoreParameters	The parameter that passes the command that is run prior to a restore from Windows. Default: None.
Restore	PreRestore	PreWinRestoreShow	Show or hide the command that is run prior to a restore from Windows. Default: Show.
Restore	PreRestore	PreWinRestore0	Command to run prior to a restore of the base backup from Windows. Include the full path to the file, if that path is not in the environment variable. Default: None.
Restore	PreRestore	PreWinRestoreParameters0	The parameter that passes the command that is run prior to a restore of the base backup from Windows. Default: None.
Restore	PreRestore	PreWinRestoreShow0	Show or hide the command that is run prior to a restore of the base backup from Windows. Default: Show.
Restore	PreRestore	PreWinRestore1	Command to run prior to a restore of incremental backup number 1 from Windows. Include the full path to the file, if that path is not in the environment variable. Default: None.
Restore	PreRestore	PreWinRestoreParameters1	The parameter that passes the command that is run prior to a restore of incremental backup number 1 from Windows. Default: None.

Table 35. Computer Configuration>Rescue and Recovery>Settings (continued)

Policy	Setting	Sub-Setting	Description
Restore	PreRestore	PreWinRestoreShow1	Show or hide the command that is run prior to a restore of incremental backup number 1 from Windows. Default: Show.
Restore	PreRestore	PreWinRestore2	Command to run prior to a restore of incremental backup number 2 from Windows. Include the full path to the file, if that path is not in the environment variable. Default: None.
Restore	PreRestore	PreWinRestoreParameters2	The parameter that passes the command that is run prior to a restore of incremental backup number 2 from Windows. Default: None.
Restore	PreRestore	PreWinRestoreShow2	Show or hide the command that is run prior to a restore of incremental backup number 2 from Windows. Default: Show.
Restore	PreRestore	PreWinRestore3	Command to run prior to a restore of incremental backup number 3 from Windows. Include the full path to the file, if that path is not in the environment variable. Default: None.
Restore	PreRestore	PreWinRestoreParameters3	The parameter that passes the command that is run prior to a restore of incremental backup number 3 from Windows. Default: None.
Restore	PreRestore	PreWinRestoreShow3	Show or hide the command that is run prior to a restore of incremental backup number 3 from Windows. Default: Show.
Restore	PreRestore	PreWinRestore4	Command to run prior to a restore of incremental backup number 4 from Windows. Include the full path to the file, if that path is not in the environment variable. Default: None.
Restore	PreRestore	PreWinRestoreParameters4	The parameter that passes the command that is run prior to a restore of incremental backup number 4 from Windows. Default: None.
Restore	PreRestore	PreWinRestoreShow4	Show or hide the command that is run prior to a restore of incremental backup number 4 from Windows. Default: Show.

Table 35. Computer Configuration>Rescue and Recovery>Settings (continued)

Policy	Setting	Sub-Setting	Description
Restore	PreRestore	PreWinRestore5	Command to run prior to a restore of incremental backup number 5 from Windows. Include the full path to the file, if that path is not in the environment variable. Default: None.
Restore	PreRestore	PreWinRestoreParameters5	The parameter that passes the command that is run prior to a restore of incremental backup number 5 from Windows. Default: None.
Restore	PreRestore	PreWinRestoreShow5	Show or hide the command that is run prior to a restore of incremental backup number 5 from Windows. Default: Show.
Restore	PreRestore	PrePDARestore	Command to run prior to a restore from the Rescue and Recovery workspace. Include the full path to the file, if that path is not in the environment variable. Default: None.
Restore	PreRestore	PrePDARestoreParameters	The parameter that passes the command that is run prior to a restore from the Rescue and Recovery workspace. Default: None.
Restore	PreRestore	PrePDARestoreShow	Show or hide the command that is run prior to a restore from the Rescue and Recovery workspace. Default: Show.
Restore	PreRestore	PrePDARestore0	Command to run prior to a restore of the base backup from the Rescue and Recovery workspace. Include the full path to the file, if that path is not in the environment variable. Default: None.
Restore	PreRestore	PrePDARestoreParameters0	The parameter that passes the command that is run prior to a restore of the base backup from the Rescue and Recovery workspace. Default: None.
Restore	PreRestore	PrePDARestoreShow0	Show or hide the command that is run prior to a restore of the base backup from the Rescue and Recovery workspace. Default: Show.
Restore	PreRestore	PrePDARestore1	Command to run prior to a restore of incremental backup number 1 from the Rescue and Recovery workspace. Include the full path to the file, if that path is not in the environment variable. Default: None.

Table 35. Computer Configuration>Rescue and Recovery>Settings (continued)

Policy	Setting	Sub-Setting	Description
Restore	PreRestore	PrePDARestoreParameters1	The parameter that passes the command that is run prior to a restore of incremental backup number 1 from the Rescue and Recovery workspace. Default: None.
Restore	PreRestore	PrePDARestoreShow1	Show or hide the command that is run prior to a restore of incremental backup number 1 from the Rescue and Recovery workspace. Default: Show.
Restore	PreRestore	PrePDARestore2	Command to run prior to a restore of incremental backup number 2 from the Rescue and Recovery workspace. Include the full path to the file, if that path is not in the environment variable. Default: None.
Restore	PreRestore	PrePDARestoreParameters2	The parameter that passes the command that is run prior to a restore of incremental backup number 2 from the Rescue and Recovery workspace. Default: None.
Restore	PreRestore	PrePDARestoreShow2	Show or hide the command that is run prior to a restore of incremental backup number 2 from the Rescue and Recovery workspace. Default: Show.
Restore	PreRestore	PrePDARestore3	Command to run prior to a restore of incremental backup number 3 from the Rescue and Recovery workspace. Include the full path to the file, if that path is not in the environment variable. Default: None.
Restore	PreRestore	PrePDARestoreParameters3	The parameter that passes the command that is run prior to a restore of incremental backup number 3 from the Rescue and Recovery workspace. Default: None.
Restore	PreRestore	PrePDARestoreShow3	Show or hide the command that is run prior to a restore of incremental backup number 3 from the Rescue and Recovery workspace. Default: Show.
Restore	PreRestore	PrePDARestore4	Command to run prior to a restore of incremental backup number 4 from the Rescue and Recovery workspace. Include the full path to the file, if that path is not in the environment variable. Default: None.

Table 35. Computer Configuration>Rescue and Recovery>Settings (continued)

Policy	Setting	Sub-Setting	Description
Restore	PreRestore	PrePDARestoreParameters4	The parameter that passes the command that is run prior to a restore of incremental backup number 4 from the Rescue and Recovery workspace. Default: None.
Restore	PreRestore	PrePDARestoreShow4	Show or hide the command that is run prior to a restore of incremental backup number 4 from the Rescue and Recovery workspace. Default: Show.
Restore	PreRestore	PrePDARestore5	Command to run prior to a restore of incremental backup number 5 from the Rescue and Recovery workspace. Include the full path to the file, if that path is not in the environment variable. Default: None.
Restore	PreRestore	PrePDARestoreParameters5	The parameter that passes the command that is run prior to a restore of incremental backup number 5 from the Rescue and Recovery workspace. Default: None.
Restore	PreRestore	PrePDARestoreShow5	Show or hide the command that is run prior to a restore of incremental backup number 5 from the Rescue and Recovery workspace. Default: Show.
Restore	PostRestore	PostWinRestore	Command to run following a restore from Windows. Include the full path to the file, if that path is not in the environment variable. Default: None.
Restore	PostRestore	PostWinRestoreParameters	The parameter that passes the command that is run following a restore from Windows. Default: None.
Restore	PostRestore	PostWinRestoreShow	Show or hide the command that is run following a restore from Windows. Default: Show.
Restore	PostRestore	PostWinRestore0	Command to run following a restore of the base backup from Windows. Include the full path to the file, if that path is not in the environment variable. Default: None.
Restore	PostRestore	PostWinRestoreParameters0	The parameter that passes the command that is run following a restore of the base backup from Windows. Default: None.
Restore	PostRestore	PostWinRestoreShow0	Show or hide the command that is run following a restore of the base backup from Windows. Default: Show.

Table 35. Computer Configuration>Rescue and Recovery>Settings (continued)

Policy	Setting	Sub-Setting	Description
Restore	PostRestore	PostWinRestore1	Command to run following a restore of incremental backup number 1 from Windows. Include the full path to the file, if that path is not in the environment variable. Default: None.
Restore	PostRestore	PostWinRestoreParameters1	The parameter that passes the command that is run following a restore of incremental backup number 1 from Windows. Default: None.
Restore	PostRestore	PostWinRestoreShow1	Show or hide the command that is run following a restore of incremental backup number 1 from Windows. Default: Show.
Restore	PostRestore	PostWinRestore2	Command to run following a restore of incremental backup number 2 from Windows. Include the full path to the file, if that path is not in the environment variable. Default: None.
Restore	PostRestore	PostWinRestoreParameters2	The parameter that passes the command that is run following a restore of incremental backup number 2 from Windows. Default: None.
Restore	PostRestore	PostWinRestoreShow2	Show or hide the command that is run following a restore of incremental backup number 2 from Windows. Default: Show.
Restore	PostRestore	PostWinRestore3	Command to run following a restore of incremental backup number 3 from Windows. Include the full path to the file, if that path is not in the environment variable. Default: None.
Restore	PostRestore	PostWinRestoreParameters3	The parameter that passes the command that is run following a restore of incremental backup number 3 from Windows. Default: None.
Restore	PostRestore	PostWinRestoreShow3	Show or hide the command that is run following a restore of incremental backup number 3 from Windows. Default: Show.
Restore	PostRestore	PostWinRestore4	Command to run following a restore of incremental backup number 4 from Windows. Include the full path to the file, if that path is not in the environment variable. Default: None.

Table 35. Computer Configuration>Rescue and Recovery>Settings (continued)

Policy	Setting	Sub-Setting	Description
Restore	PostRestore	PostWinRestoreParameters4	The parameter that passes the command that is run following a restore of incremental backup number 4 from Windows. Default: None.
Restore	PostRestore	PostWinRestoreShow4	Show or hide the command that is run following a restore of incremental backup number 4 from Windows. Default: Show.
Restore	PostRestore	PostWinRestore5	Command to run following a restore of incremental backup number 5 from Windows. Include the full path to the file, if that path is not in the environment variable. Default: None.
Restore	PostRestore	PostWinRestoreParameters5	The parameter that passes the command that is run following a restore of incremental backup number 5 from Windows. Default: None.
Restore	PostRestore	PostWinRestoreShow5	Show or hide the command that is run following a restore of incremental backup number 5 from Windows. Default: Show.
Restore	PostRestore	PostPDARestore	Command to run following a restore from the Rescue and Recovery workspace. Include the full path to the file, if that path is not in the environment variable. Default: None.
Restore	PostRestore	PostPDARestoreParameters	The parameter that passes the command that is run following a restore from the Rescue and Recovery workspace. Default: None.
Restore	PostRestore	PostPDARestoreShow	Show or hide the command that is run following a restore from the Rescue and Recovery workspace. Default: Show.
Restore	PostRestore	PostPDARestore0	Command to run following a restore of the base backup from the Rescue and Recovery workspace. Include the full path to the file, if that path is not in the environment variable. Default: None.
Restore	PostRestore	PostPDARestoreParameters0	The parameter that passes the command that is run following a restore of the base backup from the Rescue and Recovery workspace. Default: None.
Restore	PostRestore	PostPDARestoreShow0	Show or hide the command that is run following a restore of the base backup from the Rescue and Recovery workspace. Default: Show

Table 35. Computer Configuration>Rescue and Recovery>Settings (continued)

Policy	Setting	Sub-Setting	Description
Restore	PostRestore	PostPDARestore1	Command to run following a restore of incremental backup number 1 from the Rescue and Recovery workspace. Include the full path to the file, if that path is not in the environment variable. Default: None.
Restore	PostRestore	PostPDARestoreParameters1	The parameter that passes the command that is run following a restore of incremental backup number 1 from the Rescue and Recovery workspace. Default: None.
Restore	PostRestore	PostPDARestoreShow1	Show or hide the command that is run following a restore of incremental backup number 1 from the Rescue and Recovery workspace. Default: Show
Restore	PostRestore	PostPDARestore2	Command to run following a restore of incremental backup number 2 from the Rescue and Recovery workspace. Include the full path to the file, if that path is not in the environment variable. Default: None.
Restore	PostRestore	PostPDARestoreParameters2	The parameter that passes the command that is run following a restore of incremental backup number 2 from the Rescue and Recovery workspace. Default: None.
Restore	PostRestore	PostPDARestoreShow2	Show or hide the command that is run following a restore of incremental backup number 2 from the Rescue and Recovery workspace. Default: Show
Restore	PostRestore	PostPDARestore3	Command to run following a restore of incremental backup number 3 from the Rescue and Recovery workspace. Include the full path to the file, if that path is not in the environment variable. Default: None.
Restore	PostRestore	PostPDARestoreParameters3	The parameter that passes the command that is run following a restore of incremental backup number 3 from the Rescue and Recovery workspace. Default: None.
Restore	PostRestore	PostPDARestoreShow3	Show or hide the command that is run following a restore of incremental backup number 3 from the Rescue and Recovery workspace. Default: Show.

Table 35. Computer Configuration>Rescue and Recovery>Settings (continued)

Policy	Setting	Sub-Setting	Description
Restore	PostRestore	PostPDARestore4	Command to run following a restore of incremental backup number 4 from the Rescue and Recovery workspace. Include the full path to the file, if that path is not in the environment variable. Default: None.
Restore	PostRestore	PostPDARestoreParameters4	The parameter that passes the command that is run following a restore of incremental backup number 4 from the Rescue and Recovery workspace. Default: None.
Restore	PostRestore	PostPDARestoreShow4	Show or hide the command that is run following a restore of incremental backup number 4 from the Rescue and Recovery workspace. Default: Show.
Restore	PostRestore	PostPDARestore5	Command to run following a restore of incremental backup number 5 from the Rescue and Recovery workspace. Include the full path to the file, if that path is not in the environment variable. Default: None.
Restore	PostRestore	PostPDARestoreParameters5	The parameter that passes the command that is run following a restore of incremental backup number 5 from the Rescue and Recovery workspace. Default: None.
Restore	PostRestore	PostPDARestoreShow5	Show or hide the command that is run following a restore of incremental backup number 5 from the Rescue and Recovery workspace. Default: Show.
Restore	Password Persist		Show or hide the 'Password Persist' option in restore dialogs. Default: Show.
Rejuvenate	PreRejuvenate		Command to run prior to a rejuvenation restore. Include the full path to the file, if that path is not in the environment variable. Default: None.
Rejuvenate	PreRejuvenate Parameters		The parameter that passes the command that is run prior to a rejuvenation restore. Default: None.
Rejuvenate	PreRejuvenate Show		Show or hide the command that is run prior to a rejuvenation restore. Default: Show.
Rejuvenate	PostRejuvenate		Command to run following a rejuvenation restore. Include the full path to the file, if that path is not in the environment variable. Default: None.

Table 35. Computer Configuration>Rescue and Recovery>Settings (continued)

Policy	Setting	Sub-Setting	Description
Rejuvenate	PostRejuvenate Parameters		The parameter that passes the command that is run following a rejuvenation restore. Default: None.
Rejuvenate	PostRejuvenate Show		Show or hide the command that is run following a rejuvenation restore. Default: Show.
Rejuvenate	PostRejuvenate Reboot		Enable or disable a system reboot following a rejuvenation restore. Default: Enabled.
Mapped Network Drive	UNC		UNC location for the mapped network drive (format \\server\share). Default: None.
Mapped Network Drive	User		Use mapdrv.exe /view command to create an encrpyted value for this field. Default: None.
User Messages	Bootable Second		Show or hide the 'Bootable Second' message. Default: Hide.
User Messages	Bootable USB		Show or hide the 'Bootable USB' message. Default: Hide.
User Messages	Location Not Found		Show or hide the 'Location Not Found' message. Default: Show Note: If the location is a USB drive, this message will still be displayed.
User Messages	Missed Backup		Show or hide the 'Missed Backup' message. Default: Show.
User Messages	No Battery		Show or hide the 'No Battery' message. Default: Show.
User Messages	Scheduled Base		Show or hide the 'Scheduled Base' message. Default: Show.
User Messages	Power Loss Backup		Show or hide the 'Power Loss Backup' message. Default: Show.
User Messages	Post Rejuvenate Reboot		Show or hide the 'Post Rejuvenate Reboot' message. Default: Show.
Lock Hard Disk			Enable or disable the 'Lock Hard Disk' setting. Default: Disabled.
Parse Environment Variables			Enable or disable the 'Parse Environment Variables' setting. Default: Enabled.
Set PP Archive Before Backup			Enable or disable the 'Set PP Archive Before Backup' setting. Default: Enabled.
Max Silent Retries			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.

Table 35. Computer Configuration>Rescue and Recovery>Settings (continued)

Policy	Setting	Sub-Setting	Description
Fast Restore			Enable or disable the 'Fast Restore' feature. Default: Enabled
Analyze FileSize Threshold			The threshold used by the analyze function to determine if a file should be displayed or not. Values: 0-10,000 MB Default: 20MB.
Sort Filter Files			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).
Scheduled Tasks	Global Delay Start Minute		Set the global delay start minute of Scheduled Tasks. Default: Not configured.
Schedule eGatherer	Delay Start Minute		Set the delay start minute of eGatherer. Default: Not configured.
Schedule LogMon	Delay Start Minute		Set the delay start minute of LogMon. Default: Not configured.
Schedule Backup	Delay Start Minute		Set the delay start minute of scheduled backups. Default: Not configured.

Appendix B. Antidote Delivery Manager

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

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

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

Installing the Antidote network component

Rescue and Recovery 4.21 must be installed on all client systems. Configuration can be made before the installation or performed later.

Note: Antidote driver functionality will not be installed in the operating system by default because of potential conflicts with other drivers.

Windows Vista

Complete the following steps to install Antidote Delivery Manager on client systems with Windows Vista:

1. With administrative privileges, launch the MS DOS Command Prompt.
2. Change the directory to %rr%\adm.
3. Run iuservice -install.
4. Execute net start tvtnetwk.

Windows XP

Complete the following steps to install Antidote Delivery Manager on client systems with Windows XP:

1. With administrative privileges, launch the MS DOS Command Prompt.
2. Change the directory to %tvtcommon%\pfdinst.
3. Execute netsvcinst /install /inf:"c:\program files\common files\lenovo\pfdinst\netsf.inf" /cid:"lgl_tvtpktfilter".
4. Execute netsvcinst /install /inf:"c:\program files\common files\lenovo\pfdinst\netsf_m.inf" /cid:"lgl_tvtpktfiltermp".

Antidote with Windows Vista

For 64bit Windows Vista the registry location is HKLM\SOFTWARE\WOW6432Node\Lenovo\Rescue and Recovery\ADM Repository The repository path for the mailbox is set in the registry at the following location: HKLM\SOFTWARE\Lenovo\Rescue and Recovery\ADM

For 64-bit Windows Vista the installed folder location is C:\Program Files (x86)\Lenovo\Rescue and Recovery\ADM. Issue a CD command to C:\Program Files\Lenovo\Rescue and Recovery\ADM.

When running any of the Antidote commands in Windows Vista (32 or 64 bit) you must have elevated admin privileges, otherwise the values will go to an incorrect registry location.

Repository

The repository function runs on each system and periodically checks for new messages from the administrator. It checks at a scheduled time interval or at the occurrence of several interesting events (for example, boot, resume from suspend or hibernate, detection of a new network adapter, and assignment of a new IP address). The repository function looks for messages in a set of directories, in a Windows share location, such as \\machine\share\directory, at HTTP URLs, and at FTP URLs . If more than one message is found, it processes them in "directory sort by name" order. Only one message is processed at a time. A message is only processed successfully once. If processing a message fails, by default, it is not attempted again, but retrying on failure can be specified in the message itself.

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

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

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

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

Antidote Delivery Manager and Windows commands

The Antidote Delivery Manager system provides several commands to facilitate the operation of the system. In addition to the command to create messages and adjust settings, there are commands to control networking, determine and control operating system state, examine XML files from system inventories, and notify the user of progress of the Antidote Delivery Manager script on the client machine. The NETWK command enables or disables networking or restricts networking to a limited group of network addresses. The INRR command can be used to determine if the Windows 2000, Windows XP or Windows Vista is running or if the computer is in the Rescue and Recovery environment. The REBOOT command can be used to shut down the computer and specify that it should boot either to Windows 200, Windows XP or Windows Vista or to Rescue and Recovery. The MSGBOX application allows for communication with the user by displaying a message in a pop-up box. The message box can optionally contain OK and Cancel buttons so the message can act differently based on input from the user.

Certain Microsoft commands are also available to Antidote Delivery Manager. The permitted commands include all commands built into command shell, for example DIR or CD. Other useful commands, such as reg.exe to change the registry and chkdsk.exe to verify disk integrity, are available.

Antidote Delivery Manager utilization

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

- **Simple system test - Display notification**

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

  Write a go.rrs script on any machine where Antidote Delivery Manager has been installed. Include a line: `MSGBOX /MSG "Hello World" /OK`. Run the APKGMSG command on the directory containing go.rrs to create a message.
- **Script execution**

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

Major worm attack

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

1. **Lockdown phase**

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

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

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

3. **Patch and recovery phase**

   When the machine reboots in Windows XP, Antidote Delivery Manager begins processing again even before the user can log in. Patches should be installed at this time. The machine can be rebooted if the newly installed patches require it. Now that all cleanup and patching has been completed, the network can be enabled and the user is informed that normal operation is possible.

Minor application update

Not all maintenance requires the drastic measures previously described. If a patch is available, but a virus attack is not in progress, a more relaxed approach might be appropriate.

A single script can control the operation through the use of the RETRYONERROR command and tag files.

1. **Download Phase**

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

2. **Patch phase**

   The patch code is ready for installation and it is time to warn the user to start installation. If the user requests a delay, a tag file could be used to track the delay. Perhaps later requests to install the patch might be more urgent. Antidote Delivery Manager maintains this state even if the user powers off or reboots their system. When the user has completed all processing and is ready for a system reboot, the patch is installed and the system is rebooted, if required.

Attention: After a system has been restored and rebooted, reboot the system again in order for changes to take effect.

Accommodating VPNs and wireless security

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

The solution is to package all required files in the original message or download the needed files before rebooting. Place all necessary files in the directory with go.rrs. The script file must move the required files into their final positions before exiting the script (when the directory containing go.rrs on the client is deleted). Placing patches in the message file might not be practical if the patches are very large. In this case, the user should be informed, then networking is restricted to only the server containing the patch. Then the patch can then be downloaded while still in Windows XP. Although this can lengthen the exposure of Windows XP to a virus, the extra time is probably not significant.

Antidote Delivery Manager command guide

The boot manager command-line interface is Antidote Delivery Manager. It resides in the directory C:\Program Files\Lenovo\Rescue and Recovery\ADM. The following table presents the switches and their results for Antidote Delivery Manager.

Table 36. Antidote Delivery Manager commands

Commands	Description
`APKGMES [/KEY keyfile| /NEWKEY keyfile|/NOSIG] message_directory message_name [/NODATE]`	If the /KEY parameter is used, a signing key will be retrieved from keyfile.prv and the key in keyfile.pub must have been distributed to all clients that will process the message. By default, the key file "KEYFILE.PRV" will be used. The /NEWKEY parameter can be used to create a key. If signing is not desired, specifying /NOSIG will prevent signing. A date stamp will be appended to the end of the message name, such as *message_name*YYMMDDHHmm.zap.
`REBOOT [/RR|/Win] [/wait | /f]`	This command reboots the machine. With no parameters, reboot with the normal boot sequence. The parameter RR means reboot to Rescue and Recovery, and WIN means reboot to the normal operating system. The reboot will not occur until the script exits, so this should normally be the last command in a script. The optional WAIT command forces the system to boot to the specified environment on next reboot (manual or caused by other mechanism). The /f parameter forces the system to reboot now, and does not allow the user to save information from open applications. If no parameters are specified, the program defaults to /win (/wait and /f are not specified).
`RETRYONERROR [ON|OFF] retries`	By default, a script will only be tried once. However, if it is important to keep trying a script until it works, the RETRYONERROR command can be used to notify the mailbox function to keep trying to run this script a finite number of times as specified by the retries parameter. If no number is specified, the default value is 3.
`MSGBOX /msg message text [/head header_text] [/OK] [/CANCEL]| [/TIMER timeout]`	The MSGBOX command will display a message to the end user, if logged on. The message will remain displayed and the script will block until time out occurs, the cancel button is pressed or the **OK** button is pushed (if /OK is specified). A cancel button will not be on the panel if /CANCEL is not specified, and it will not be easy to get rid of the display. The command will return: • 0 = OK was pressed • 1 = CANCEL • 2 = Timer expired The text in the message can be formatted using \n and \t to represent newline and tab respectively.

Table 36. Antidote Delivery Manager commands (continued)

Commands	Description
`NETWK [/D|/E|/A [/IP ip_address | /DN domain_name] [/NM netmask]`	NETWK /D (disable) will stop all network traffic by disabling all network adapters. Networking will be disabled until a NETWK /E (enable) command is run. NETWK /A restricts networking to the IP address specified by either the /IP switch (dotted decimal) or /DN (DNS name). The /NM switch provides the network mask. If /NM is not provided, then only the single machine specified by /IP or /DN will be accessible. The state of this command does not persist over reboots, so networking must be explicitly enabled and disabled after every reboot.
`APUBKEY [/ADD|/DEL] asn_1_encoded_public_key`	The APASSWD command allows an administrator to remotely manage the Antidote Delivery Manager message signing keys on each PC. More than one key can be stored on each PC. If a signed message is processed, each key will be tried until a successful one is found. Keys are not separately named, so must be referenced by the content. A new key can be added using the ADD parameter and deleted with the DEL parameter.
`AUNCPW [/ADD|/CHANGE|/DEL] unc [/USER userid] [/PWD password] [/REF ref_name]`	This command allows you to add, change or delete a password for a network drive The reference name can be used as a shortcut in a message instead of using the UNC. Return values are: • 0 = Successful. • 1 = Unable to set with the information provided. • 2 = Successful, but a different UNC which has the same reference name has already been defined.

Table 36. Antidote Delivery Manager commands (continued)

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

Table 36. Antidote Delivery Manager commands (continued)

Commands	Description
`STATUS [/QUERY` *`location message_name`* `| /CLEAR` *`location`*`]`	The STATUS /QUERY command can be used to determine if a script has been run, or is queued to be run. The location value must be one of the following: • **FAIL** the message has already run and failed • **SUCCESS** The message has been completed successfully • **WORK** The message is currently being run, or will run next time Antidote Delivery Manager is run. • **CACHE** The message is queued to run. The STATUS/CLEAR command will clear the *location* specified. Return values are: • 0 = if the specified message found or the command completed successfully • 1 = if the specified message not found or the command failed
`MAILMAN [/RRU | RESET | /MB` *`mailbox`* `| /STATUS`	This command checks for mailbox locations and processes fixes found there. The following list provides the parameters: • **RRU** This parameter runs .ZAP which is stored in the Post Restore directory after each restore. • **RESET** This parameter halts processing of the currently running script. **Note:** This parameter should only be used in extenuating circumstances since usage is likely to cause errors. • **STATUS** This parameter returns a bitmask to indicate the current condition of the Antidote program. Return values are: – 0 = Antidote is configured properly – 1 = No mailbox defined – 2 = There are no keys defined, or NOSIG=1 is not defined

Supported Microsoft commands

The following table provides supported Microsoft commands.

Table 37. Supported Microsoft commands

Commands	Description
`ATTRIB.EXE`	Displays or changes file attributes.
`CACLS.EXE`	Displays or modifies access control list (ACLs) of files.
`CHKDSK.EXE`	Checks a disk and displays a status report.

Table 37. Supported Microsoft commands (continued)

Commands	Description
COMP.EXE	Compares the contents of two files or sets of files.
COMPACT.EXE	Displays or alters the compression of files on NTFS partitions.
CONVERT.EXE	Converts FAT volumes to NTFS. You cannot convert the current drive.
DISKPART.EXE	Partitions a drive.
FC.EXE	Compares two files or sets of files and displays the differences between them.
FIND.EXE	Searches for a text string in a file or files.
FINDSTR.EXE	Searches for strings in files.
FORMAT.COM	Formats a disk for use with Windows.
LABEL.EXE	Creates changes or deletes the volume label of a disk.
NET.EXE	Provides the networking commands.
PING.EXE	Checks to see if a network resource can be reached.
RECOVER.EXE	Recovers readable information from a bad or defective disk.
REG.EXE	Registry manipulation.
REPLACE.EXE	Replaces file.
RRCMD.EXE	Runs Backups from OS or restores from OS or Predesktop Area.
SORT.EXE	Sorts input.
SUBST.EXE	Associates a path with a drive letter.
XCOPY.EXE	Copies files and directory trees.

Note: Entering the PDA environment might fail after creating partitions using DISKPART.
When you create partitions using DISKPART, restart the system, and enter the PDA environment, the system might prompt the message "NTLDR is missing." Because Boot Manager is unable to locate the correct service partition, the system fails to load NTLDR.
If you encounter this problem, do the following:

1. Delete the partitions created using DISKPART.
2. Reinstall the Rescue and Recovery program.

Preparation and installation

The following procedures provide preparation and installation information for Antidote Delivery Manager, and Rescue and Recovery.

Preparation

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

Configuration

Several configuration items will be required. The items appear in the rnrdeploy.xml file.

Repository

The repository path for the mailbox is set in the registry at the following location:

```
HKLM\SOFTWARE\Lenovo\Rescue and Recovery\ADM
```

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

```
"mailbox"= c:\antidote
```

Schedule information

Schedule information is set in the registry at HKLM\SOFTWARE\Lenovo\Rescue and Recovery\ADM with the following setting:

- ″Task″=″C:\\Program Files\\Lenovo\\Rescue and Recovery\\ADM\\ mailman.exe″
- ″Mode″=dword:00000004 ″Hour″=dword:00000012
- ″Minute″=dword:00000000 ″DayOfWeek″=dword:00000003

The Schedule Mode is the frequency of checks.

Table 38. Schedule modes

Schedule Mode	
SCHED_NONE	0x000
SCHED_MINUTELY	0x001
SCHED_DAILY	0x002
SCHED_WEEKLY	0x004
SCHED_MONTHLY	0x008
SCHED_STARTUP	0x010
SCHED_WAKEUP	0x020
SCHED_USB_ATTACH	0x040
SCHED_NETWORK_ATTACH	0x080
SCHED_NETWORK_DETACH	0x100

Signing Key

If signing keys will be used, then they must be distributed to the client. The file keyfile.pub created by the APKGMES command contains the key. Each authorized public signing key appears in the registry. Use the APUBKEY function to set the following value: `nosig =` If it is set to 1, it will allow unsigned packages (packages built with the /NOSIG parameter) to be run. The following provides the registry location for the Signing Key:

```
HKLM\SOFTWARE\Lenovo\Rescue and Recovery\ADM
"NOSIG"=dword:00000001
```

Note: If it is not set to 1 or if public keys are present in the registry, unsigned packages will not run.

Network Drives

The following values are set by using the AUNCPW function `RscDrvY` and stored in the registry at HKLM\Software\Policies\Lenovo\MND\4.0\AD. The

/NEWKEY parameter can be used to create a key. If signing is not desired, specifying /NOSIG will prevent signing. Each `RscDrv` section contains information about one network share. Up to ten network shares can be defined for Antidote Delivery Manager.

- UNC = The UNC (Universal Naming Convention) of a drive that Antidote Delivery Manager connects to.
- User = Encrypted username.
- Pwd = Encrypted password.
- Ref = The reference name to be associated with this connection.

Installing the Antidote network component

Rescue and Recovery 4.21 must be installed on all client systems. Configuration can be made before the installation or performed later.

Windows Vista

Complete the following steps to install Antidote Delivery Manager on client systems with Windows Vista:

1. With administrative privileges, launch the MS DOS Command Prompt.
2. Change the directory to %rr%\adm.
3. Run iuservice -install.
4. Run net start tvtnetwk.

Windows XP

Complete the following steps to install Antidote Delivery Manager on client systems with Windows XP:

1. With administrative privileges, launch the MS DOS Command Prompt.
2. Change the directory to %tvtcommon%\pfdinst.
3. Run netsvcinst /install /inf:"c:\program files\common files\lenovo\pfdinst\netsf.inf" /cid:"lgl_tvtpktfilter".
4. Run netsvcinst /install /inf:"c:\program files\common files\lenovo\pfdinst\netsf_m.inf" /cid:"lgl_tvtpktfiltermp".

Server infrastructure

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

Simple system test – display notification

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

Deployment

Complete the following steps prior to deploying Antidote Delivery Manager:

1. Determine locations for the mailboxes:
   - *Mailboxes* are defined as directories on network shares, a local system on a harddrive, or removable media, or on a FTP or HTTP site.

- You might find it helpful to have multiple mailboxes in case one is not accessible. You can define up to ten mailbox locations.
- Network-based mailboxes should be read-only for clients and write access should be restricted.

2. Set up repositories in the registry:
   - On a donor system with Rescue and Recovery installed, edit the registry at HKLM\Software\Lenovo\Rescue and Recovery\ADM.
   - Change the following settings in the preceding key:

     ```
     "mailbox"=
     ```

     and then add your mailbox directory information. Mailboxes on the local drive, for example would look like this:

     ```
     "mailbox"=C:\ADM\Mailbox;\\Machine\Share\Directory
     ```

     Mailboxes on an FTP site would look like this:

     ```
     ftp://userid:password@ftpserver/mailbox
     ```

     Mailboxes on a shared network drive would look like this:

     ```
     \\Machine\Share\Directory
     ```

     Notes:

     a. HTTPS is not supported for mailbox functions.

     b. The HTTP Web server must be configured to deliver indexing turned on and list files capability.

     Drive letters may change between Windows Professional Edition and your normal operating system environment. The C: drive is most likely to change. To work around this, use the environment variable *CUSTOS* which always points to the drive containing the typical customer operating system. The preceding example would change to:

     ```
     mailbox=%CUSTOS%\ADM\Mailbox;ftp://userid:password@ftpserver/mailbox;
      \\Machine\Share\Director
     ```

     The string can be any length as long as it conforms to the standards of the device or protocol being used. For example, if using a local file, the path can not exceed 256 characters.
   - Multiple mailbox entries are separated by commas or semicolons.
   - Antidote Delivery Manager sequentially looks in the specified mailbox locations for packages.
3. If a user name and password are required for an FTP or HTTP connection, use this format:

   ```
   ftp//username:password@ftp.yourmailbox.com
   ```

4. For user name and password network shares mailboxes:

   User name and password entries are stored encrypted in the registry. To add an entry on the donor system:

   a. Open a DOS window

   b. Change directories to `C:\Program Files\Lenovo\Rescue and Recovery\ADM`

   c. Run this command:

      ```
      auncpw /add \\Machine\Share\Director /user username /pwd password /ref refID
      ```

      This command creates the following entry in the registry:

      ```
      HKLM\SOFTWARE\Policies\Lenovo\MND\ADM\RscDrvy
      or
      ```

```
HKLM\SOFTWARE\Lenovo\MND\ADM\RscDrvy UNC=\\Network\Share

and has the following settings:

"User"=01E23397A54D949427D5AF69BF407D5C
"Pwd"=04E22197B34D95943ED5A169A0407C5C
"Ref"=refID
```

Notes:

a. This entry can be used on any system to be used by Antidote Delivery Manager to gain access to the same share.

b. Up to ten network shares can be used by Antidote Delivery Manager.

c. In addition to the ten network shares, other mailbox entries can be added, such as FTP or local.

d. The auncpw.exe file has other functions which can be used for password management. Enter AUNCPW /? at command line or see Table 36 on page 124.

5. Create the Antidote Delivery Manager Public/Private key pair. For higher security, use the Public/Private key-pair capabilities of Antidote Delivery Manager. Antidote Delivery Manager utilizes a Public/Private key-pair to verify the authenticity of packages. The Private key should be closely guarded and not distributed. The matching Public key should be on every client managed through Antidote Delivery Manager. To create a Public/Private key pair on a non-donor system with Rescue and Recovery installed:

   a. Open a DOS window.

   b. Issue a CD command to C:\Program Files\Lenovo\Rescue and Recovery\ADM.

   c. Run this command:

   ```
   apkgmes.exe /newkey mykey
   ```

   This command creates two files, mykey.pub and mykey.prv; the public and private keys respectively.

   d. Copy the public key to the donor system's C:\Program Files\Lenovo\Rescue and Recovery\ADM directory.

   e. Open the file using a text editing program such as notepad.exe.

   f. Copy the contents of the file to the clipboard.

   g. On the command line, enter the following:

   ```
   apubkey.exe /add x
   ```

   where *x* is the contents of the clipboard.

   h. This will create an entry in the registry in the HKLM\Lenovo\Rescue and Recovery\ADM\ section: `"pubkey0"=906253...`.

   - Up to ten public keys can be stored in the registry.
   - The apubkey.exe file has other functions which can be used for Public key management. At the command line, enter `APUBKEY /?` or see Table 36 on page 124.

6. Create the Schedule Antidote Delivery Manager check (multiple schedules are allowed). Antidote Delivery Manager needs to run periodically on the system. To set up a schedule to run every twenty minutes, the following should be added to the registry on the donor system:

```
HKLM\Software\Lenovo\Scheduler\Rescue0
Mode=1
NumMinutes=20
TaskShow=1
Task=C:\Program Files\Lenovo\Rescue and Recovery\ADM\antidote
\mailman.exe
```

Notes:

a. The scheduler does not run in the Predesktop Area.

b. For more information, see "Scheduling backups and associated tasks" on page 23.

7. Create an Antidote Delivery Manager package.

   Note: If you would prefer to use a user interface to perform this step, download the Rescue and Recovery toolkit from http://www.lenovo.com/support/site.wss/document.do?sitestyle=lenovo&lndocid=TVAN-ADMIN .

   Having completed the previous steps, build and distribute your first package. On an administrator system (non-donor), perform the following:

   a. Create a directory such as *C:\ADM\Build*.

   b. In that directory, create a file called go.rrs and add the following:

   ```
   msgbox.exe /msg "Hello World!" /head "test" /ok /cancel
   ```

   c. Save and close the file.

   d. Issue a CD command to C:\Program Files\Lenovo\Rescue and Recovery\ADM

   e. Run this command:

   ```
   apkgmes.exe /key mykey.prv C:\adm\build HELLOPKG
   ```

   f. This will create a package called HELLOPKG*YYMMDDHHMM*.ZAP where *YYMMDDHHMM* are replaced with the current date/time.

8. Copy the HELLOPKGYY*MMDDHHMM*.ZAP to a mailbox location specified in step 2.

9. Implement Antidote Delivery Manager.

   a. When the timer has expired on the donor system, the package will run and a Hello World message box will appear.

   b. If you prefer not to wait, on the donor system, you can enter C:\Program Files\Lenovo\Rescue and Recovery\ADM\mailman.exe

Examples

Antidote Delivery Manager can be utilized in the following examples:

Example 1

This example shows using a package to fix a computer that is constantly displaying a blue screen because of a virus or bad entry in registry.

1. The virus is probably run through the Run Key in the registry. To fix the problem, a go.rrs file that runs *reg* needs to be created. See "Supported Microsoft commands" on page 127 for a list of Microsoft commands. *Reg* removes the registry value and deletes the executable from the system, if possible. The contents should look like this:

   ```
   reg delete HKLM\Software\Microsoft\Windows\Current Version\Run /v runvirusvalue
   /f del %custos%\windows\system32\virus.exe
   ```

2. Now place your go.rrs file in your *C:\ADM\BUILD* directory and run:

   ```
   apkgmes.exe /key mykey.prv C:\ADM\BUILD REMOVEVIRUS
   ```

3. Copy REMOVEVIRUS*YYDDHHMM*.ZAP to your mailbox.

4. Boot up each client and press the Access ThinkVantage button/F11 or the Enter key to enter the Predesktop Area where the mailman.exe file is run on startup and then run the REMOVEVIRUS package.

Example 2

This example pushes a Quick Fix Engineering update or patch down to client machines.

1. Create a directory to hold the script file and patch files, for example: *C:\ADM\PATCHBUILD*.
2. Place the QFE or patch executable in the C:\ADM\PATCHBUILD directory.
3. Create a file named go.rrs and place the following lines in it but customize the line that will run and install the Microsoft Quick Fix Engineering or patch. Since this patch can only be installed in a regular Windows operating system, this script prevents the install from attempting to run in Windows Professional Edition.

```
retryonerror /on 10
InRR.exe
if errorlevel 2 goto ERROR
if errorlevel 1 goto InOS
if errorlevel 0 goto InPE

:ERROR
exit 1

:InOS
REM DISABLE NETWORKING
Netwk.exe /d
patchinstall.exe
REM ENABLE NETWORKING
Netwk.exe /e
msgbox.exe /msg "Patch Installed" /head "Done" /ok
exit 0

:InPE
exit 1
```

4. Place go.rrs in C:\ADM\PATCHBUILD directory and run:

```
apkgmes.exe /key mykey.prv C:\ADM\PATCHBUILD PATCHBUILD
```

5. Copy PATCHBUILD*YYDDHHMM*.ZAP to your mailbox.
6. The patch will be installed either on next scheduled run of the mailman.exe file for the client machine or on reboot of the client machine.

Package completion logs

- **Fail log**

  This file is typically stored in the *C:\Program Files\Lenovo\Rescue and Recovery\ADM* directory. If a zap file exits with any non-zero value, it will be logged into this file.

- **Rescue.log**

  This file is typically located in the *C:\SWSHARE* directory. This file provides more detailed information that may help determine why a package may have failed, or to make sure a package worked. It has line by line logging of what occurs in a zap file.

- **Success Log**

  This file is typically stored in the *C:\Program Files\Lenovo\Rescue and Recovery\ADM* directory. If a zap file exited with value of zero then it is logged here.

Example 3

This example uses an FTP or HTTP site in the Predesktop Area:

1. Define an external Web site for packages:

   ```
   ftp.yourmailbox.com
   ```

2. Create public private keys See Step 5.
3. Add mailbox to registry.

   ```
   mailbox=ftp://username:password@ftp.yourmailbox.com
   ```

4. When the user presses F11 or the Enter key to enter the Predesktop area, the Antidote Delivery Manager package runs at boot time in the Predesktop area.

Example 4

This example uses the xmltool.exe file to target certain clients:

1. Distribute the XML file that has information in it that you would like compared to your client machines either through Active Directory, Systems Management Server, or some other management tool.

   ```
   <file>
   <activedirgroup>Marketing</activedirgroup>
   </file>
   ```

2. In the first line of your go.rrs file, place a line that uses the XML tool. This line is an example that would ONLY target machines in the Marketing group;

   ```
   xmltool.exe c:\mycompany\target.xml //file/activedirgroup /c EQU Marketing
   if errorlevel 0 goto RUNIT
   exit errorlevel

   :RUNIT
   #place code to  patch or whatever action
   ```

Example scripts

For example scripts download the Administrator Tools package located at: http://www.lenovo.com/support/site.wss/document.do?lndocid=TVAN-ADMIN#tvsu.

Virtualization Module for Antidote Delivery Manager

Virtualization Module for Antidote Delivery Manager assists in the protection of valuable data and computer systems against harmful viruses and worms. Virtualization Module for Antidote Delivery Manager is designed to improve the safety and manageability of computer systems.

With Virtualization Module for Antidote Delivery Manager, administrators will be able to remotely disconnect a terminal from the network, if a threat has been established. Administrators will also be able to remotely shut down the infected terminal. When all threats are non-existent, the system can then be rebooted into the Rescue and Recovery Predesktop Area to recover any files that may have been corrupted.

Requirements

The following requirements are essential to operate Virtualization Module for Antidote Delivery Manager:

- Internet Explorer 6.0 or higher.
- Windows XP Professional or Home Edition with Service Pack 2 on the customer operating system (terminals).
- Windows CE on the server operating system (server).

- Antidote Delivery Manager installed.
- Rescue and Recovery 3.1 or later installed.
- 512MB of memory.
- 30MB of free disk space.
- Installed on an NTFS partition.
- Intel processor that is compatible with virtualization technology (available on select Lenovo computers only).
- Intel virtualization technology processor enabled in BIOS.
- Logon with administrator privileges.

Note: The communication between the server operating system and the client operating system has been designed to be invisible. The administrator interacts with the customer operating system equipped with a Web browser. Virtualization Module for Antidote Delivery Manager will not open on the server operating system.

Installation

Ensure that the virtualization technology processor is enabled before installing the Virtualization Module for Antidote Delivery Manager program. To enable the virtualization technology processor, complete the following steps:

1. With the computer off, turn on the computer.
2. Press and release the F1 key until the logo appears or you hear a series of beeps.
3. If prompted, type your current password.
4. Navigate to the Intel Virtualization Technology line item located typically on the advanced screen.
5. Enable the Intel Virtualization Technology line item.
6. Press F10 to save and exit the Setup Utility.
7. Press Enter.

To install the Virtualization Module for Antidote Delivery Manager program, complete the following steps:

1. Start your computer.
2. Close any open programs.
3. Insert the Virtualization Module for Antidote Delivery Manager installation CD.

   Note: If the installation CD does not start automatically, complete the following steps:

   a. From the Windows desktop, click Start, and then click Run.
   b. Type d:\setup.exe (where *d* is the drive letter of the CD or DVD drive that contains the Rescue and Recovery Installation CD.)
   c. Follow the instructions on the screen.

   If your CD is damaged or cannot be read, contact your place of purchase.

Note: In order for the Virtualization Module for Antidote Delivery Manager installation to complete successfully you must enable the Intel Virtualization Technology option in BIOS. By default, this program is enabled. If it is not enabled, enter BIOS and set the option to enabled.

Overview

This section provides an overview of the Virtualization Module for Antidote Delivery Manager program.

The following table provides information for Network Status and Network Connections.

Table 39. Network Status and Connections

Module	Description
Network Status	Displays information in two different sections. First is the Windows IP configuration, such as: Host Name, WINs Proxy, Node Type, DNS Suffix, IP Routing, and Search List.
Network Status	Provides information such as: Connection-specific DNS Suffix, IP Address, Description, Subnet Mask, Physical Address, Default, Gateway, DHCP, and Auto-configuration.
Disable Network	Allows you to remotely disconnect a terminal from the network.
Enable Network	Allows you to re-enable the connection.
Repair Network	Allows you to make repairs to network connections.

The following table provides information for System status and Administration.

Table 40. System and Administration

Module	Description
System	Assists in recovery of corrupted files.
Administration	Allows you to manage server access and user accounts. You will see the following menu options: Server, and User Accounts.
Stop Windows XP Network	Allows you to stop network connections.
Restart	Allows you to remotely restart a terminal that has been threatened with a virus or worm.

The following table provides information for System Health and Help.

Table 41. System Health and Help

Module	Description
Health	Allows you to monitor system health, and provides health status.
Logs	Allows you to view log files.

Installing certificates

The user interface for the Virtualization Module for Antidote Delivery Manager program is Web-based and uses CA (Certificate Authority) Root certificates to communicate. A default certificate is installed. You can use this default certificate, customize the default certificate, or use your own custom certificate. These certificates must be installed to communicate with the Virtualization Module for Antidote Delivery Manager program. The following steps provide instructions on how to install certificates:

1. Open a Web browser such as Windows Internet Explorer.
2. Type the following IP address in the address field: 192.168.0.12.
3. On the Security Alert from Internet Explorer, click **View Certificate**.

4. On the General Tab, Click **Install Certificate**, or if you are working with an existing certificate, make a note of the Serial Number in the Value field on the Details tab.
5. Type your User ID and password in the User ID and password fields on the Authentication prompt.

   Note: If your User ID and password does not authenticate, you will be continuously prompted for your User ID and password. The User ID and password requested at the Authentication prompt will need to be set up on the server computer. This User ID and password is set up in User Accounts located on the Control Panel in Windows. Virtualization Module for Antidote Delivery Manager requires a password set for this User Account.
6. From the main menu in the Virtualization Module for Antidote Delivery Manager program, click **Manage and Configure**.
7. In the Upload field, click **Browse**, and browse to your certificate. Certificates will have the file extension of .pfx.
8. Type in your password.
9. Click **Submit**. A prompt will display letting you know the file was uploaded successfully.
10. From the Virtualization Module for Antidote Delivery Manager menu, click **Restart Target PC**. This reboots the server computer and engages the installed certificate.

Commands

The following commands are used to control the Virtualization Module for Antidote Delivery Manager program.

- /E - enables all networking (/ip and /nm ignored).
- /D - disables all networking (/ip and /nm ignored).
- /A - allows connection to defined IP address or domain name only.
- /IP - allows connection to specified ip_address only.
- /DN - allows connection to specified domain_name (DNS name) only.
- /NM - net_mask (optional) default = 255.255.255.255.

NETWK: The NETWK command controls the operation of all networks.

- NETWK /D disables all network traffic by disabling all network adapters.
- NETWK /E enables all network traffic. Networking will be disabled until a NETWK /E (enable) command is run.
- NETWK /A restricts networking to the IP address specified by either the /IP switch (dotted decimal) or /DN (DNS name).
- NETWK /NM provides the network mask. If /NM is not provided, then only the single machine specified by /IP or /DN will be accessible. The state of this command does not persist over reboots, so networking must be explicitly enabled and disabled after every reboot.

REBOOT: The REBOOT command allows scripts written by administrators to cause the computer to reboot. The syntax of this command is as follows:

reboot.exe [/rr | /win] [/wait | /f]

- /rr - boots to the Predesktop Area.
- /win - boots to the operating system immediately (default).

- /wait - boots to the Predesktop Area or operating system when the system is rebooted.
- /f - forces the system to reboot immediately and does not allow the user to close open applications.

Appendix C. User tasks

Users may not be able to perform certain tasks, based upon user rights. The following tables outline basic task capability with the limited user, power user, and administrator default operating system user ID permissions. The tasks and capabilities differ by Windows operating system.

Windows Vista

The following table presents the tasks that limited, power, and administrative users can perform in Rescue and Recovery in a Windows Vista environment.

Table 42. Windows Vista user tasks

Windows Vista users can perform the following:	**Limited user**	**Power user**	**Administrator**
Create rescue media ISO.	No	No	Yes (with command line provided below)
Create bootable CD media.	Yes	Yes	Yes
Create USB hard disk drive bootable media.	No	No	Yes
Initiate backup.	Yes	Yes	Yes
Initialize restore in Rescue and Recovery environment (RRE).	Yes	Yes	Yes
Perform single-file restore in Rescue and Recovery environment.	No (Windows) Yes (Windows Pre Boot Area)	No (Windows) Yes (Windows Pre Boot Area)	Yes
Set include and exclude in the Rescue and Recovery interface.	Yes	Yes	Yes
Backup to a network drive.	Yes	Yes	Yes
Schedule backups.	Yes	Yes	Yes
Predesktop Area login ID carry over **Note:** The last Windows administrator ID is the only ID that can automatically carry over from Windows to the Predesktop Area. Windows limited and power users will need to retype their user ID and passwords to logon to the Predesktop Area.	No	No	Yes

Windows XP

The following table presents the tasks that limited, power, and administrative users can perform in Rescue and Recovery in a Windows XP environment.

Table 43. Windows XP user tasks

Windows XP users can perform the following:	**Limited user**	**Power user**	**Administrator**
Create rescue media ISO.	No	No	Yes (with command line provided below)
Create bootable CD media.	Yes	Yes	Yes
Create USB hard disk drive bootable media.	No	No	Yes
Initiate backup.	Yes	Yes	Yes
Initialize restore in Rescue and Recovery environment (RRE).	Yes	Yes	Yes
Perform single-file restore in Rescue and Recovery environment.	No (Windows) Yes (Windows Pre Boot Area)	No (Windows) Yes (Windows Pre Boot Area)	Yes
Set include and exclude in the Rescue and Recovery interface.	Yes	Yes	Yes
Backup to a network drive.	Yes	Yes	Yes
Schedule backups.	Yes	Yes	Yes
Predesktop Area login ID carry over **Note:** The last Windows administrator ID is the only ID that can automatically carry over from Windows to the Predesktop Area. Windows limited and power users will need to retype their user ID and passwords to logon to the Predesktop Area.	No	No	Yes

Windows 2000

The following table presents the tasks that limited, power, and administrative users can perform in Rescue and Recovery in a Windows 2000 environment.

Table 44. Windows 2000 user tasks

Windows 2000 users can perform the following:	**Limited user**	**Power user**	**Administrator**
Create rescue media ISO.	No	No	Yes (with command line provided below)
Create bootable CD media.	Yes	Yes	Yes
Create USB hard disk drive bootable media.	No	No	Yes
Initiate backup.	Yes	Yes	Yes
Initialize restore in the Rescue and Recovery environment (RRE.	Yes	Yes	Yes

Table 44. Windows 2000 user tasks (continued)

Windows 2000 users can perform the following:	Limited user	Power user	Administrator
Perform single-file restore in the Rescue and Recovery environment (RRE).	No (Windows) Yes (Windows Pre Boot Area)	No	Yes
Set include and exclude in the Rescue and Recovery interface.	Yes	Yes	Yes
Backup to a network drive.	No	No	Yes
Schedule backups.	Yes	Yes	Yes

Create rescue media

Administrators can use the following command lines to create the Rescue Media ISO. These command lines enables 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 Rescue and Recovery 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 Rescue and Recovery 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 Rescue and Recovery settings and working with Active Directory and Group Policy, see the 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#tvsu

Appendix D. 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

Intel is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

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

- IBM
- Lotus
- Lotus Notes

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

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

ThinkVantage™

Printed in USA