ThinkVantage Technologies Deployment Guide

Updated: May 31, 2006

Includes:

- Rescue and Recovery Version 3.0
- Client Security Solution Version 6.0
- Fingerprint Software Version 4.6

ThinkVantage

ThinkVantage Technologies Deployment Guide

Updated: May 31, 2006

First Edition (September 2005)

Contents

Preface

This guide is intended for IT administrators, or those who are 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 and deskside visits and improve user productivity. It is an essential tool that enables users and administrators to restore backups, access files, diagnose problems, and make Ethernet connections in case the Microsoft® Windows® operating 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 system when a restore is performed. This guide provides the information required for installing the Rescue and Recovery application on one or many computers, provided that licenses for the software are available for each target computer, and information on the many aspects of the tool that can be customized to support IT or corporate policies. 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.

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.

This deployment guide is developed with IT professionals and the unique challenges that they encounter. If you have suggestions or comments, communicate with your Lenovo authorized representative. We will periodically update these guides, so check this Web site for later versions:

www.lenovo.com/ThinkVantage

Chapter 1. Overview

The audience of this guide is IT Security, Administration and other personnel who are responsible for the implementation and deployment of security technology within a corporation. ThinkVantage™ 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.

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

Major components

The major components of this guide are:

- ThinkVantage Rescue and Recovery
- ThinkVantage Client Security Solution
- ThinkVantage Fingerprint Software

A discussion of each is presented below.

Rescue and Recovery

Rescue and Recovery has two major components:

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

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

The Rescue and Recovery Pre Desktop environment

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

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

- **Rescue and Restore**

  - **Recovery overview:** Links users to help topics about the various recovery options that 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 that cover configuration.
  - **Recover password/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**
  - **Map network drive:** Helps end users access network drives for software downloads or file transfer.
- **Troubleshoot**
  - **Diagnostic overview:** Links to Rescue and Recovery diagnostics help topics.
  - **Diagnose hardware:** Opens the PC Doctor application that can perform hardware tests and report results.
  - **Create diagnostic disks**
  - **Boot from another device**
  - **System information:** Provides details regarding the computer and its hardware components.
  - **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.
  - **Warranty status**

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

Appendix B, “TVT.TXT settings and values,” on page 131 addresses configuring the Rescue and Recovery environment for deployment. Although installing Rescue and Recovery includes the installation of Rapid Restore™ Ultra, this guide treats them as individual components in descriptions of customization, configuration, and deployment.

The Rescue and Recovery Windows environment

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

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

Antidote Delivery Manager

Antidote Delivery Manager is an anti-virus, anti-worm infrastructure included in ThinkVantage Rescue and Recovery. The objects are easy to implement, efficient, and allow an administrator to initiate blocking and recovery within minutes of a reported problem. It can be launched by one administrator and it functions on systems that are not network attached. Antidote Delivery Manager complements existing antivirus tools rather than replacing them, so maintaining virus scanning tools and obtaining patches is still required. Antidote Delivery Manager provides the infrastructure to halt destruction and apply the patches.

Encrypting backups

Backups are encrypted by default with the 256 AES key. If you choose to install Client Security Solution Version 6.0, you have the ability to encrypt using Client Security Software Gina.

Client Security Solution 6.0

The primary purpose of the Client Security Solution software is to help a customer protect the PC as an asset, protect confidential data on the PC and to protect network connections accessed by the PC. For IBM® and Lenovo-branded systems that contain a Trusted Computing Group (TCG) compliant Trusted Platform Module (TPM), Client Security Solution (CSS) software will leverage the hardware as the root of trust for the system. If the system doesn't contain an embedded security chip, Client Security Solution will leverage software based cryptographic keys as the root of trust for the system. Features of Client Security Solution 6.0 include:

- **Secure User Authentication**

  Require a hardware protected Client Security passphrase for users to access Client Security Solution protected functions
- **Fingerprint User Authentication**

  Leverage the integrated and USB attached fingerprint technology to authenticate users to password protected applications
- **Client Security Passphrase / Fingerprint Based Windows Logon**

  Require users to logon to Windows using their hardware protected Client Security passphrase or fingerprint
- **Protect Data**

  Encrypt sensitive files by storing them in a secure location on the hard drive which requires valid user authentication and a properly configured security chip
- **Manage Logon Passwords**

  Securely manage and store sensitive logon information such as user IDs and passwords
- **End User Password/Passphrase Recovery**

  Enable users to self-recover from a forgotten Windows password/ Client Security passphrase by answering preconfigured questions
- **Audit Security Settings**

  Allow users to view a detailed list of workstation security settings and make changes to comply to defined standards.
- **Transfer Digital Certificates**

  Hardware protect the private key of User and Machine certificates

Client Security passphrase

The Client Security passphrase is an optional additional form of user authentication that will provide enhanced security to Client Security Solution applications. The Client Security passphrase has the following requirements:

- Be at least eight characters long
- Contain at least one digit
- Be different from the last three passphrases
- Contain no more than two repeating characters
- Not begin with a digit
- Not end with a digit
- Not contain the user ID
- Not be changed if the current passphrase is less than three days old
- Not contain three or more identical consecutive characters as the current passphrase in any position
- Not be the same as the Windows password.

The Client Security passphrase is not acceptable to the same type of attacks that the Windows password is. It is important to note, a Client Security passphrase is only known by the individual user and the only way to recover from a forgotten Client Security passphrase is to leverage the Client Security password recovery function. If the user has forgotten the answers to their recovery questions, then there is no way to recover the data protected by the Client Security passphrase.

Client Security password recovery

This optional setting allows enrolled users to recover a forgotten Windows password or Client Security passphrase by answering three questions correctly. If this feature is enabled, during end user Client Security enrollment, each user will get to select three answers to 10 pre-chosen questions. If the user ever forgets their Windows password or Client Security passphrase, they will have the option to answer these three questions to reset their password or passphrase by themselves.

Notes:

1. When using the Client Security passphrase, this is the only option for recovery of a forgotten passphrase. If the user forgets the answer to their three questions, then a user will be forced to re-run the enrollment wizard and lose all previous Client Security protected data.
2. When using Client Security to protect the Rescue and Recovery Pre Desktop environment, the Password Recovery option will actually display the user's Client Security passphrase and/or Windows Password. This is because the Pre Desktop environment does not have the ability to automatically perform a Windows password change. This comment is also true when a non-network attached locally cached domain user performs this function at the Windows logon.

ThinkVantage Fingerprint Software

The objective of biometric fingerprint technologies offered by Lenovo is to help customers reduce the costs associated with managing passwords, enhance the security of their systems and help address regulatory compliance. Together with our fingerprint readers, ThinkVantage Fingerprint Software enables fingerprint authentication to their PC and a network. The solution also integrates with Client Security Solution Version 6.0 offering expanded functionality. You can find out more about the Lenovo fingerprint technologies and download the software at:

www.thinkpad.com/fingerprint

ThinkVantage Fingerprint Software offers these functions:

- **Client Software Capabilities**
  - **Replace Microsoft Windows password**

    Replace with your fingerprint for easy, fast and secure system access.
  - **Replace BIOS (also known as power on password) and Hard Drive passwords**

    Replace these passwords with your fingerprint to enhance logon security and convenience.
  - **Single Swipe access to Windows:**

    A user can simple swipe their finger ONCE at start up to gain access to BIOS AND Windows, saving valuable time.
  - **Integration with Client Security Solution** for use with the CSS Password Manager and to leverage the Trusted Platform Module. Users can swipe their finger to access websites and select applications.
- **Administrator Features**
  - **Toggle Security Modes:**

    An administrator can toggle between secure and convenient modes to modify access rights of limited users.
  - **Management Console:**

    Helps administrators by enabling remote software customization of the Fingerprint Software through script-driven command line interface.
- **Security Capabilities**
  - **Software Security:**

    Protects user templates through strong encryption when stored on a system and when transferred from the reader to the software.
  - **Hardware Security:**

    Readers have a security co-processor which stores and protects fingerprint templates, BIOS passwords and encryption keys.

Password Manager

The Client Security Password Manager enables you to manage and remember all your sensitive and easy-to-forget application and Web site login information, such as user IDs, passwords, and other personal information. The Client Security Password Manager stores all information through the embedded security chip so that access to your applications and Web sites remain totally secure.

This means that rather than having to remember and provide a plethora of individual passwords-- all subject to different rules and expiration dates-- you only have to remember one password/passphrase, provide your fingerprint, or a combination of identification elements.

The Client Security Password Manager enables you to perform the following functions:

- **Encrypt all stored information through the embedded security chip**

  The Client Security Password Manager automatically encrypts all information through the embedded security chip. This ensures that all your sensitive password information is secured by the Client Security Solution encryption keys.

- **Transfer user IDs and passwords quickly and easily utilizing a simple type-and-transfer interface**

  The Client Security Password Manager type-and-transfer interface enables you to place information directly into the logon interface of your browser or application. This helps minimize typing errors and enables you to save all of your information securely through the embedded security chip.
- **Autokey user IDs and passwords**

  The Client Security Password Manager automates your login process, entering your login information automatically when you access an application or Web site whose logon information has been entered into the Client Security Password Manager.
- **Generate random passwords**

  The Client Security Password Manager enables you to generate random passwords for each application or Web site. This enables you to increase the security of your data because each application will have much more rigorous password protection enabled. Random passwords are far more secure than user-defined passwords because experience indicates that most users use easy-to-remember personal information for passwords that are often relatively easy to crack.
- **Edit entries using the Client Security Password Manager interface**

  The Client Security Password Manager enables you to edit all of your account entries and set up all optional password features in one easy-to-use interface. This makes managing your passwords and personal information quick and easy.
- **Access your logon information from the icon tray on the Microsoft(R) Windows(R) desktop or with a simple keyboard shortcut**

  The Password Manager icon grants you easy access to your logon information whenever you might need to add another application or Web site to the Password Manager. Each Client Security Password Manager function can also be easily accessed by a simple keyboard shortcut.
- **Export and import login information**

  The Client Security Password Manager enables you to export your sensitive login information so that you can securely carry it from computer to computer. When you export your login information from the Client Security Password Manager, a password-protected export file is created that can be stored on removable media. Use this file to access your user information and passwords anywhere you go, or to import your entries into another computer with Password Manager.

  Note: Import will only work with Client Security Solution Version 6.0. Client Security Software Version 5.4X and previous versions will not import into Client Security Solution 6.0 Password Manager.

SafeGuard PrivateDisk

Protect data using SafeGuard PrivateDisk. Almost everybody stores confidential data on the PC. SafeGuard PrivateDisk protects confidential data. It works like an ″electronic safe″ for confidential and valuable information on your computer, all disk drives and mobile media. Protected information cannot be accessed or read by unauthorized persons.

How does SafeGuard PrivateDisk work? SafeGuard PrivateDisk is based on the Virtual Disk Principle.

- A virtual disk can be created on any available drive

  - Mobile memory media (such as disk, USB sticks, CD-ROM, DVD, or Zip drive)
  - Hard disks, network drives
- The driver operates like a hard disk drive
  - The operating system sends write and read commands to the driver transparently.
  - The driver manages the encrypted storage.
  - All data and directory information is encrypted.
- SafeGuard PrivateDisk works with the Client Security Solution and the Trusted Platform Module to protect digital certificates generated by PrivateDisk
- SafeGuard PrivateDisk uses a symmetric cipher algorithm with a new random AES key for each virtual disk
  - AES, 128 Bit, CBC mode
  - New random key for each virtual disk
- Authentication through:
  - Password
  - Private Key (X.509 certificate), smartcard optional
  - Use of automatically generated EFS certificates is possible
- Password security:
  - PKCS#5
  - Time delay after wrong password presentation
  - Password dialog with ″interception protection″

Security Advisor

The Security Advisor tool allows you to view a summary of security settings currently set on your computer. You can review these settings to view your current security status or to enhance your system security. Some of the security topics included are hardware passwords, Windows users passwords, Windows password policy, protected screen saver, and file sharing. The categories default values displayed can be changed through the TVT.txt file.

Certificate Transfer Wizard

The Client Security Certificate Transfer Wizard guides you through the process of transferring the private keys associated with your certificates from the software-based Microsoft cryptographic service provider (CSP) to the hardware-based Client Security Solution CSP. After the transfer, operations using the certificates are more secure because the private keys are protected by the embedded security chip.

Hardware Password reset

This tool creates a secure environment that runs independently of Windows and helps you reset forgotten power-on and hard-disk-drive passwords. Your identity is established by answering a set of questions that you create. It is a good idea to create this secure environment as soon as possible, before a password is forgotten. You cannot reset a forgotten hardware password until this secure environment is created on your hard drive and after you have enrolled. This tool is available on select ThinkCentre® and ThinkPad computers only.

Support for systems without Trusted Platform Module

Client Security Solution 6.0 now supports IBM and Lenovo-branded systems that do not have a compliant embedded security chip. This will allow a standard installation across the entire enterprise in order to create a homogenous security environment. The systems that have the embedded security hardware will be more robust against attack; however, the software only machines will also benefit from the additional security and functionality.

System Migration Assistant

System Migration Assistant (SMA) is a software tool that system administrators can use to migrate a user's work environment from one system to another. 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

System administrators can use SMA to either set up a standard work environment for a company or to upgrade an individual user's computer. Individual users can use SMA either to backup a computer or to migrate settings and files from one computer system to another. For example, from a desktop computer to a mobile computer (laptop).

OEM differences

Client Security Solution 6.0 is not available for OEM systems at this time. Rescue and Recovery will not leverage any of the Client Security Solution applications on OEM machines.

Chapter 2. Install considerations

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

Rescue and Recovery

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

Notes:

1. Rescue and Recovery will only work with the Non-BIOS version of Computrace if Rescue and Recovery is installed first, and then Computrace is installed. See Chapter 8, “Best Practices,” on page 107
2. If you attempt to install SMS on a system with Rescue and Recovery installed with the Windows PE area already installed as a virtual partition, then SMS will not install. Both Windows PE and SMS 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 2.0 as a Type 12 partition. See “Installing Rescue and Recovery into a type 12 service partition” on page 120 for instructions for installing to type 12.
3. A possible security risk may be created when 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

Rescue and Recovery Version 3.0 supports an over-install operation of Rescue and Recovery 2.0.

It is recommended that a new backup be taken after installation of Rescue and Recovery 3.0. This can be done by using either a script or the user interface.

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

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

The following script will copy backups to a USB HDD, delete the current backups, and then perform a base backup.

```
@echo off

::Change directories to \Program Files\IBM\IBM Rescue and Recovery
cd %rr%

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

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

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

Client Security Solution

When deploying Client Security Solution 6.0, the following aspects must be taken into account.

Client Security Solution has included in the code the necessary drivers and software support to enable the security hardware (Trusted Platform Module) of the machine that is to receive Client Security Solution 6.0. Enablement of the hardware requires at least one reboot since the chip is actually controlled through BIOS and requires successful BIOS authentication in order to complete the procedure. In other words, if a BIOS Administrator/Supervisor password is set, it will be required to enable/disable the Trusted Platform Module.

Before any functions can be carried out by the Trusted Platform Module, "Ownership" must first be initialized. Each system will have one and only one Client Security Solution Administrator that will control the Client Security Solution options. This administrator must have Windows administrator privileges. The administrator can be initialized using XML deployment scripts.

After Ownership of the system is configured, each additional Windows user that logs into the system will automatically be prompted with the Client Security Setup Wizard in order to enroll and initialize the user's security keys and credentials.

Software emulation for Trusted Platform Module

The Client Security Solution has the option to run without a Trusted Platform Module on qualified systems. The functionality will be exactly the same except it will use software based keys instead of using hardware protected keys. The software can also be installed with a switch to force it to always use software based keys instead of leveraging the Trusted Platform Module. This is an install time decision and can not be reversed without uninstalling and reinstalling the software.

The syntax to force a software emulation of the Trusted Platform Module:

```
InstallFile.exe "/v EMULATIONMODE=1"
```

Upgrade scenarios

See "Installed Software scenarios" on page 96 for information about upgrading from previous levels of Client Security Solution.

Chapter 3. Rescue and Recovery customization

This chapter provides information that can be used to customize ThinkVantage Rescue and Recovery.

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

Before starting this procedure, make sure that the TVT file or files, such as z062zaa1025us00.tvt, is located in same directory as the executable or MSI file, or install will fail. If your file is named setup_tvtrnr3_1027**c**.exe, then you downloaded the combined package. These instructions are for the files that can be downloaded separately off of the *Large Enterprise individual language files* download page

To perform a simple deployment that places a backup icon on the desktop for the user, do the following:

1. Extract the SETUP_TVTRNR*XXXX*.EXE (where *XXXX* is the build ID) to a temporary directory:

   ```
   start /WAIT setup.exe /a /s /v"/qn TARGETDIR="C:\TVTRR" REBOOT="R"" /w
   ```

2. Customize the TVT.TXT file, as required. For example, you might want to schedule a weekly backup at 3:00 pm every Tuesday. Add the following entries in the [Rescue and Recovery] section of TVT.TXT to accomplish this. (See Appendix B, “TVT.TXT settings and values,” on page 131 for additional setting information.)

   ```
   ScheduleHour=15

   ScheduleMinute=00

   ScheduleDayOfTheWeek=2
   ```

3. Copy Z062ZAA1025US00.TVT file to C:\tvtrr as well. The TVT file must to be in same folder as the MSI file.
4. Initiate the MSI installation, deferring the reboot:

   ```
   start /WAIT msiexec /i "C:\TVTRR\Rescue and Recovery - client security
   solution.msi" /qn REBOOT="R" /L*v %temp%\rrinstall.txt
   ```

   Note: The above command was modified to fit on this page. Enter this command as one string.

5. Customize the Rescue and Recovery environment. (See “Predesktop area” on page 17 for detailed information.)
6. Delete the temporary files in the C:\TVTRR directory. (Refer to “Windows environment” on page 14).
7. Write a command file with the following commands:

   ```
   del "c:\Documents and Settings\All Users\Desktop\Create Base Backup.lnk
   "%RR%rrcmd.exe" backup location=L name=Base level=0
   ```

   Note: The above command was modified to fit on this page. Enter this command as one string.

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

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

Capturing a Sysprep image in the base backup

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

1. Perform an administrative install:

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

2. Add the following section to the end of the TVT.TXT file in C:\TVTRR\Program Files\IBM ThinkVantage\:

   ```
   [Backup0]
   BackupVersion=3.0
   ```

3. Install Rescue and Recovery using the MSIEXE file:

   a. For all MSIs, add the following install-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 - Client
      Security Solution.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 - Client
      Security Solution.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 - Client
      Security Solution.msi" /qn REBOOT="R"
      ```

4. 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"\"IBM ThinkVantage\Rescue and Recovery"
   rrcmd sysprepbackup location=l name=Sysprep Backup"
   ```

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

5. 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.     **
***************************************************
```

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

   Note: The operating system will reboot into the PreDesktop area of Rescue and Recovery. You will see a status bar that says **System Restore in Progress**
7. When complete, you will see a message that says **Sysprep Backup is Complete**.
8. Power off the system using the power button.
9. 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 install:

   ```
   :: Extract the WWW EXE to the directory C:\TVTRR
   start /WAIT setup_tvtrrXXXX.exe /a /s /v"/qn TARGETDIR="C:\TVTRR" REBOOT="R"" /w
   ```

2. Add the following section to the end of the TVT.TXT file in C:\\″tvtrr\Program Files″\″IBM ThinkVantage\Rescue and Recovery″:

   ```
   [Backup0]
   BackupVersion=3.0

   [BackupDisk]
   CustomPartitions=0
   ```

   To EXCLUDE a partition, add the following to the TVT.TXT file:

   ```
   [BackupDisk]
   CustomPartitions=1

   [PartitionX].
   IncludeInBackup=0
   ```

   where **X** is the Partition Number
3. If you want to exclude .MPG and JPG files from the backups add them to IBMFILTER.TXT as in the following example:

   ```
   X=*.JPG
   X=*.MPG
   ```

4. Install Rescue and Recovery using MSIEXE:
   a. For all MSI’s , add the following install-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 - Client Security Solutiion.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 - Client
      Security Solutiion.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 -
   Client Security Solutiion.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"\IBM ThinkVantage\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. You will see a status bar that says **System Restore in Progress**
8. When complete, you will see a message that says **Sysprep Backup is Complete**.
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.

Windows environment

Including and excluding files in backups

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

The files that control the include and exclude functions, listed in order of precedence, are as follows. All files are located in the C:\program files\ibm thinkvantage\rescue and recovery directory.
1. IBMFILTER.TXT
2. GUIEXCLD.TXT

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

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

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

The following are always excluded from any backup:
- PAGEFILE.SYS
- HIBERFILE.SYS
- C:\SYSTEM VOLUME INFORMATION

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

IBMFILTER.TXT

The file format is:

- One line per include/exclude rule entry.
- If more than one rule applies to a file or folder, the last rule applies. Entries at the bottom of the file take precedence.
- Entries must start with either:
  - **;**

    for a comment
  - **I**

    must include files or folders that match the entry
  - **X**

    must exclude files or folder that match the entry
  - **S**

    must 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**

    optionally used to identify a file or folder as Single Instance Storage that would normally be included.

```
  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=?:\IBMTOOLS\*
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
```

Customizing other aspects of Rescue and Recovery

You can customize numerous aspects of Rescue and Recovery using an external file named TVT.TXT that is defined prior to the installation process. The TVT.TXT file is located in the C:\Program Files\IBM ThinkVantage\ subdirectory.

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

```
setting=value
```

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

```
[Rescue and Recovery]
EncryptBackupData=0
```

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

A complete list of setting strings, parameters, and default settings for the [Rescue and Recovery] section of TVT.TXT are presented in Appendix B, “TVT.TXT settings and values,” on page 131.

Trouble Ticket

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

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

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

OSFILTER.TXT

This file recovers the user's operating system and applications without impacting their data. Rescue and Recovery provides the ability to selectively restore particular files and folders (including subfolders) by using explicit enumeration and wild card filtering without deleting any other data. An external file will define what files, folders, or file types (leveraging wild cards) comprise OS and Applications. This file can be customized by the administrator and a default external file will be provided. When the user 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.

To view the OSFILTER.TXT file, use this path: `cd %RR%`. See "IBMFILTER.TXT" on page 15 for information on the file format.

Predesktop area

To customize parts of the Rescue and Recovery PreDesktop Area, which starts even if the operating system does not open, use the RRUTIL.exe utility program to GET and PUT files. These files and their customization options are listed in the following table:

Table 1. RRUTIL.exe files and customization options

File / Directory	Customization Options
\MININT\SYSTEM32 WINBOM.INI	Add a static IP address, change video resolution
\MININT\INF \MININT\SYSTEM32\DRIVERS	Add device drivers
MAINBK.BMP	Modify environment background
MINIMAL_TOOLBAR(1).INI	Disable address bar
NORM1.INI	Configure the Opera browser, disable the Opera address bar, change Opera proxy settings, specify fixed download directory, add specific file extension to the downloadable files list, change behavior of files with specific extensions
OPERA_010.CMD	Exclude Window user's favorites

Table 1. RRUTIL.exe files and customization options (continued)

File / Directory	**Customization Options**
OPERA6.INI	Configure the Opera browser, disable the address bar
PEACCESS*xx*.INI (where *xx* is the language designation)	Preboot environment: main GUI fonts, environment background, left and right panel entries and functions, HTML-based help system
STANDARD_MENU.INI	Enable display of ″Save As″ window

Using RRUTIL.EXE

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

The following procedure lists the steps to GET files from, and PUT files into, the Rescue and Recovery environment. These procedures are used for all file customizations of 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 2. 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.

`RRUTIL -bl` *`path`*
RRUTIL -bl lists to `C:\rr-list.txt`
`rrutil -bl c:\rrtemp`
	Lists the RRBACKUPS directory

`RRUTIL -br RRbackups\C\n` where n is the backup number	Delete the content of backup.
`RRUTIL -bg C:\temp\bgetlist.txt C:\temp`	Copy individual files from the \RRBACKUPS.

Table 2. Command and switch options (continued)

Command and switch options	Result
`RRUTIL -s`	Space consumed by RRBACKUPS.

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

Example: PEACCESSIBMxx.INI

This example refers to PEACCESSIBM*xx*.INI, which is a configuration file where you can customize elements of the Rescue and Recovery environment (see "Customizing the Preboot environment" on page 20).

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

Table 3. 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 PEACCESSIBMEN.INI from the Rescue and Recovery environment:

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

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

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

Putting the file PEACCESSIBMEN.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 that is established in the GETLIST.TXT file, as in the example below:

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

Example: Adding device drivers to the 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 previous instructions apply to any device driver that might be required to configure the computer.
   b. Due to the limitation of Windows Professional Edition, 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
```

Customizing the Preboot environment

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

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

Note: To get, edit, and replace the PEACCESSIBMEN.INI file, see “Example: PEACCESSIBMxx.INI” on page 19.

Changing the main GUI font

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 PEACCESSIBM*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 with the Rescue and Recovery environment. Other fonts might be compatible, but have not been tested:

- Courier
- Times New Roman
- Comic Sans MS

Changing the environment background

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

- 620 pixels wide
- 506 pixels deep

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

Note: To get, edit, and replace the MAINBK.BMP file, see "Using RRUTIL.EXE" on page 18.

Changing entries and functions in the left panel

Changing the left-panel entries requires editing the PEACCESSIBM*xx*.INI (where *xx* is the language designation) file. For information about getting PEACCESSIBM*xx*.INI from the Rescue and Recovery environment and replacing the file, see "Using RRUTIL.EXE" on page 18.

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

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

Table 4. Left-panel entries and customization options

Entry	Customization options
00-01	Fully customizable.
02	Must remain a button type 1 (see Table 5). 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 type 1. Text can be changed. An application or help function can be defined. No icon can be added.
08-10	Fully customizable.
11	Must remain a button type 1 Text can be changed. An application or help function can be defined. No icon can be added.
16	Must remain a 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 5. Entry type parameters

Parameter	Button type
`0`	Empty field. Use this value when you want to leave a row blank and unused.

Table 5. Entry type parameters (continued)

Parameter	Button type
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. Use these values to direct the GUI to present a message to the user that the computer must be restarted before the specified function is executed.
5	Reserved for Lenovo Group Ltd
6	Reserved for Lenovo Group Ltd
7	Launch and wait. The fields that follow this specification 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 for Lenovo Group Ltd
10	Reserved for Lenovo Group Ltd

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], %sysdrive%[pathname\executable]`
: The value of `%sysdrive@` must be the boot drive letter. Following the boot drive letter, you must provide a fully qualified path to an application or command file.

`Button00=[0-10], "title", file.bmp, [0 or 1], 1, [0 or 1],%sysdrive %[pathname\executable], [parameters]`
: Provide any number of parameters required by the target application that is being started.

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

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

Entries 02, 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 executables that you can start from the left-panel entries:

Table 6. 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	RDIAGS.CMD; launches the PC Dr 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 requires editing the PEACCESSIBM*xx*.INI (where *xx* is the language designation) file. For information regarding getting PEACCESSIBM*xx*.INI from the Rescue and Recovery environment and replacing the file, see “Example: PEACCESSIBMxx.INI” on page 19.

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

Customizing the function links in the right panel: To change the functions of the links that span the top of the right panel, modify the [TitleBar] section of PEACCESSIBM*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 18 for a complete list of executables that can be started from the title bar.

Modifying user messages and window status: PEACCESSIBM*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 PEACCESSIBM*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:

```
[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 IBM 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
%sysdrive%Preboot\Helps\en\f_welcom.htm

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

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

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

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

```
NoShowChk=
RebootText=
```

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

```
RebootText = "Arial"
```

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

Configuring the Opera browser

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

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

Notes:

1. To get, edit, and place the OPERA6.INI and NORM1.INI files, see “Using RRUTIL.EXE” on page 18.
2. The Opera workspace has been modified to provide enhanced security. As a result, some browser functions have been deleted.

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 18.
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 18. 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 impermanent, add 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 18.
2. Open the file for editing.
3. Locate the following line in the .CMD file: PYTHON.EXE.FAVS.PYC Z:\OPERADEF6.ADR
4. At the end of this line of code type in quotations the names of the Windows users whose favorites you want to exclude. For example, if you want to exclude the favorites for All Users and Administrator, the code line reads as follows:

   ```
   python.exe favs.pyc z:\Operadef6.adr "All Users, Administrator"
   ```
5. Save the file.
6. Put the file by using the RRUTIL process described in “Using RRUTIL.EXE” on page 18.

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

1. Get the C:\PREBOOT\STARTUP\OPERA_010.CMD for editing by using the RRUTIL process as described in “Using RRUTIL.EXE” on page 18.
2. Locate the following line in the .CMD file: PYTHON.EXE.FAVS.PYC Z:\OPERADEF6.ADR
3. Do one of the following:
   a. Type `REM` at the beginning of the line, as follows:

      ```
      REM python.exe favs.pyc z:\Operadef6.adr
      ```
   b. Delete the line of code from the file.
4. Save the file.
5. Put the file back by using the RRUTIL process described in “Using RRUTIL.EXE” on page 18.

Changing proxy settings

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

1. Get the file C:\PREBOOT\OPERA\PROFILE\NORM1.INI for editing by using the RRUTIL process described in “Using RRUTIL.EXE” on page 18.
2. Add the following section to the bottom of the NORM1.INI file:

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

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

3. Save the file.
4. Put the file back by using the RRUTIL process described in “Using RRUTIL.EXE” on page 18.

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

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

To add the port to the entry, place a colon after the address and type the port number. The same 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 18.
2. In the `[Link Popup Menu]` section, locate this string:

   ```
   ;;Item, 50761
   ```
3. Remove the two semicolons, and then save the file. When Rescue and Recovery is closed and reopened, an end user 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.
4. Put the file back to the directory structure by using the RRUTIL process described in “Using RRUTIL.EXE” on page 18.

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 18.
2. In the file, locate this line:

   ```
   Download Directory=%OpShare%
   ```

3. Change `%OpShare%` to the full path of the directory to which you want downloaded files to be saved.
4. Save the NORM1.INI file. When Rescue and Recovery is closed and reopened, Opera saves downloaded files to the specified directory.
5. Put the file back by using the RRUTIL process described in "Using RRUTIL.EXE" on page 18.

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 only changes Opera behavior for these file types. (There are potentially thousands of file types using a three-letter file extension. Just as the Rescue and Recovery environment is not intended to be a replacement for the Windows environment, the Opera browser is not intended to replace a full-service browser. Internet access is provided to help users get up and running. The number of recognized file types is necessarily limited. For the purposes of rescue and recovery, .ZIP, .EXE, and .TXT files should be sufficient. If another file type needs to be transferred, best results are realized by creating a .ZIP file, which can then be extracted.)
3. File types are recognized by mime type rather than by file extension. For example, if a .TXT file is named with .EUY as an extension, the file 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 18.
3. Locate the `[File Types]` section of the file.
4. Use the search function to discover whether the file extension you want is listed, but does not work; then do one of the following:
   - If the extension is found, but files with that extension do not work correctly, complete the following steps:
     a. Change the value following the extension from 8 to 1. (A value of 8 tells the browser to ignore the file. A value of 1 instructs the browser to save the file.) For example, change the following:

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

        to

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

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

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

        Note: If the 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. Open the PREBOOT\OPERA\NORM1.INI file for editing by using the RRUTIL process described in “Using RRUTIL.EXE” on page 18.
3. Locate the [File Types] section of the file, and then search for the extension you want to work with. For example, you want all .TXT files to be saved to the IBMSHARE folder.
4. Find the following entry: TEXT/PLAIN=2,,,,TXT,|

   Note: A value of 2 instructs the browser to display the text in Opera. A value of 1 instructs the browser to save the target file in the IBMSHARE folder.
5. Continuing with the .TXT example, change the line to read as follows:
   ```
   TEXT/PLAIN=1,,,,TXT,|
   ```
6. Save the file and put it back by using the RRUTIL process as described in “Using RRUTIL.EXE” on page 18.
7. Restart the Rescue and Recovery workspace for changes to be effective.

Adding a Static IP address

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

1. Get the \MININT\SYSTEM32 WINBOM.INI file by using the RRUTIL process described in “Using RRUTIL.EXE” on page 18.
2. Add `[WinPE.Net]` section before `[PnPDriverUpdate]` in WINBOM.INI file. For example, consider the following file: WINBOM.INI
   ```
   [Factory]
   WinBOMType=WinPE
   Reseal=No
   [WinPE]
   Restart=No
   [PnPDriverUpdate]
   [PnPDrivers]
   [NetCards]
   [UpdateInis]
   [FactoryRunOnce]
   [Branding]
   [AppPreInstall]
   ```

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

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

Table 7. 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*

3. Get the PREBOOT\IBMWORK NETSTART.TBI file by using the RRUTIL process described in “Using RRUTIL.EXE” on page 18.
4. Change

   ```
   factory -minint
   ```

   to

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

   ```
   regsvr32 /s netcfgx.dll
   netcfg -v -winpe
   net start dhcp
   net start nla
   ```
6. Put the \IBMWORK NETSTART.TBI and \MININT\SYSTEM32 WINBOM.INI files back by using the RRUTIL process described in “Using RRUTIL.EXE” on page 18.

Changing the video resolution

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

1. Get the MININT\SYSTEM32\WINBOM.INI file by using the RRUTIL process described in “Using RRUTIL.EXE” on page 18.
2. In the file WINBOM.INI, add the following entries:

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

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

3. Put back the MININT\SYSTEM32\WINBOM.INI file by using the RRUTIL process described in “Using RRUTIL.EXE” on page 18.

Startup applications

The Rescue and Recovery Windows PE environment has the ability to support a startup script, 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 script or programs is Preboot\Startup. Scripts or programs in this directory are processed alpha numerically. So, a script called A.BAT would be processed before 1.EXE.

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

1. Obtain RRUTIL from the Lenovo Rescue and Recovery Administration Tools site at:

   www.lenovo.com/ThinkVantage
2. Create a temp directory
3. In the \Temp directory create the following directory tree, \preboot\startup
4. Place the script or program into the \temp\preboot\startup path
5. From a CMD line type in RRUTIL –p \Temp
6. To verify that the script or program was copied successfully, type in RRUTIL –g from a CMD 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

There are four password options available in the PreDesktop area. They are:

- PreDesktop or Master Password
- User ID and password or passphrase
- Backup password
- No password

PreDesktop 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 Client Security Solution is not installed.

You can create this PreDesktop Area password using the following command: C:\Program Files\IBM ThinkVantage\Client Security Solution\pe_setupmasterpwd.exe.

The parameters for this command are:

Table 8.

Parameter	Description
create password	This parameter creates the actual password.
verify password	This parameter verifies that the password is valid and that it can be used.

Table 8. (continued)

Parameter	Description
change currentPassword *newPassword*	This parameter allows you to change the current password to another one.
exists	This parameter checks to see if the password exists
silent	This parameter hides all the messages
setmode values	0 = no authentication required 1 = user specific authentication required 2 = master password required

Note: A Limited user cannot change the password; an administrator can reset the password for a limited user.

User ID and password or passphrase

This option uses Client Security Solution code for password or passphrase management. The Client Security logon 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 logon, that user is allowed access to that user's files only, and no other user's files.

This option can be set by CSS GUI or through XML scripts.

Backup password

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

```
rrcmd backup location=L name=mybackup password=pass
rrcmd basebackup location=L name=basebackup password=pass
rrcmd sysprepbackup location=L name="Sysprep Backup" password=pass
```

No password

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

ID 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 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.

Note: This also includes the information in the user's SecureDrive PrivateDisk encrypted volume file.

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

No password

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

Restore type

Following are the methods for restoring files:

- File rescue
- Single file restore
- Operating System and Appls
- Rejuvenation
- Full restore
- Factory content/Image Ultra Builder

Note: Rescue and Recovery cannot capture cached credentials for a domain user after a restore.

File rescue (before any restore)

This function prompts the user for the backup storage location, next the user selects a backup. ThinkVantage Rescue and Recovery should then display the files that the user logged in is authorized to access. The user then selects the files and/or folders to be rescued. The system then displays available locations for the files to be rescued to, excluding the local HDD. The user chooses a destination with sufficient space and the system restores the files.

Single file restore

This function prompts the user for the Backup Storage location, next the user selects a backup. ThinkVantage Rescue and Recovery should then display the files that the user logged in is authorized to access. The user then selects the files and/or folders to be restored and the system will restore them to their original locations.

Operating System and Apps

This function gives the user the option to select a backup then the system deletes files defined by the rules in osfilter.txt. It then restores the files defined by OSFILTER.TXT from the selected backup. There are also options in the tvt.txt file that can specify a program to run before a restore or after a restore, see TVT settings and valuesAppendix B, "TVT.TXT settings and values," on page 131.

Notes:

1. OS and Apps always use Password Persistence.
2. OS and Apps restore is not available from CD/DVD backup.

You can add custom tasks to run before and after both Backups and Restores. See Appendix B, "TVT.TXT settings and values," on page 131 for the backup and restore settings.

Rejuvenation

When you select to rejuvenate your system, the Rescue and Recovery program will optimize system performance by taking a new incremental backup and then defragmenting your hard drive and backups. It then restores selected settings and data from a backup of your choice. The rejuvenation operations helps eliminate viruses, adware and spyware while maintaining your current settings and data. This operations might take some time.

To rejuvenate your system, complete the following procedure:

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. You are reminded not to power off your computer during this operation.
   e. Click **OK** to proceed. A progress bar is displayed. This operation will take some time.

You can add custom tasks to run either before or after a Rejuvenation. See Appendix B, “TVT.TXT settings and values,” on page 131 for the rejuvenation settings

Note: Applications installed or uninstalled after the selected backup was created might need to be installed again to function correctly.
Attention: 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.

Full restore

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

Factory content/Image Ultra Builder (IUB)

This function erases the hard disk and reinstalls all of the factory pre-installed software.

Password persistence

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

Table 9. 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 persistent account and password.	• User will lose Encrypted File System data • You cannot use Encrypted File System and Password Persistence together.
If the user didn't exist on that particular backup, then they don't have any of their User Folders or files. All Internet Explorer Favorites and Application data will not exist.	• The User ID Documents Settings are gone • Potential data loss
Deleting user in the current accounts and passwords will remove their authentication information from all the backups.	• User will not have access to data
If a manager or a network administrator 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 employees would still have access with Password Persistence.	• Is against the recommendation of 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.

Hardware Password reset

The Hardware Password reset environment runs independently of Windows and will allow you to reset forgotten power-on and hard-disk-drive passwords. Your identity is established by answering a set of questions that you create when you enroll. It is a good idea to create, install and enroll this secure environment as soon as possible before a password is forgotten. You can not reset forgotten hardware passwords until after you have enrolled. This recovery media is supported on select ThinkCentre™ and ThinkPad computers only.

Creating this environment does not help you recover from forgotten Windows passwords, or password associated with the Rescue and Recovery workspace. By creating this environment, you are adding an additional bootable device to the Startup Device Menu, from which you can reset your forgotten hardware passwords. You access this menu by pressing F12 when you are prompted for your power-on password.

There are three stages involved in setting up password deployment:

1. Package building
2. Package deployment
3. Enrollment

Set an Administrator or Supervisor password in BIOS before beginning this procedure. If you do not have BIOS Administrator or Supervisor password set, your environment will not be as secure as possible. All systems you plan to deploy the password reset package must have Supervisor password. When you complete this procedure, your power-on password and hard-drive password will be the same. This procedure is designed to help you complete the task of creating the secure environment and to help you reset your forgotten passwords after the secure environment is created.

Package Building

To create a secure environment, do the following:

1. In the hardware password reset install application, mark the Create secure environment to reset hardware passwords radio button.
2. Click OK. The BIOS Supervisor Password window opens.
3. In the Enter Supervisor Password field, type your administrator or supervisor password. This is the Administrator or Supervisor password that you have previously set in BIOS to protect your hardware settings.
4. Click OK. The create key window opens.
5. In the key generation area, do one of the following:

   The first time you create this secure environment you have to create a new key. A key is a security feature used to authenticate your identity Any subsequent attempts to create a secure environment will give you the option to either use the same key that you created on your initial attempt if you choose to export it or create a different key. If you are creating this environment for one computer only, it is a good idea to generate a new key. You can opt to generate a key each time you build a new secure OS. This option however requires that you re-perform the enrollment procedure on each machine. If the same key is used, enrollment does not have to be re-performed. If you are creating this environment for several computers, you may want to use the same key. It is however recommended that if you are going to the same key, you must store the key in a secure location.

   In the key generation area do one of the following:

   - If this is your first time creating a key and you plan to create the secure environment on this computer only, then make the Generate new key radio button.
   - If this is your first time creating a key and you want to create a secure environment that can be deployed to other computers, then mark the Generate new key radio button. Then mark the Export key to file checkbox. Use the Browse button to define where you want the key to be stored.
   - If you have already created a key and want to use the key to create a secure environment that can be deployed to other computers, then mark the Import Key from file radio button. Use the Browse button to define where the key you want to use is located. You will need the key created in the above option.

   Set up a donor system for each type of supported systems when deploying to Thinkpad, Thinkcentre and per language for example French, German, Japanese. The purpose is to secure the OS which is based on the Rescue and Recovery partition and would be different for each system.
6. In the install area, uncheck the Automatically install the hardware password reset after it is created check box.
7. Click **OK**.

8. Click **OK** to a dialog box informing you that the Hardware Password feature will not be enabled on this computer until the install package has been run.

   To find the path to the executable file type cd %rr%\rrcd\passwordreset\pwdreset.exe at the command line prompt.

Package deployment

Use your company's existing distribution medium to deploy the created package.

Enrollment

To enroll the password reset, do the following:

1. Run the pwdreset.exe
2. Click OK to restart your computer. Your computer will restart and prompt you to enter your BIOS passwords. Enter your BIOS passwords and then click **Enter**. Your computer will restart into the secure environment where the Welcome to Hardware Password reset window opens.
3. Mark the **Setup hardware reset** radio button if this is your first time creating the secure environment or if you would like to re-enroll your computer and hard disks.
4. Click **Next**. The hard disks setup window opens.
5. In the computer serial number area, mark the Setup check box besides the computer you want to setup.
6. Click **Nex**t. The Enter new power-on password window opens.
7. In the **New power-on password field**, type the power-on password you want to use. If you already have a power-on password it will be reset to the one you enter into the field. In addition, your hard-disk-drive password also will be set to the same password.
8. Click **Next**. The create security questions and answer window opens.
9. In each of the three question fields type the question you want to use.
10. In each of the three answer fields type the answer to each question. You will be required to know each answer in the event that you forget your power-on password and attempt to reset it.
11. Click **Next** and then click **Finish**. Your computer will restart in the Windows environment.

Here are the hardware password reset installer error messages. The first two are generic titles, used in combination with the remainder of the messages. It is recommended that you reinstall the product in both cases.

- **IDS_STRING_ERR** ″Error″
- **IDS_STRING_ERR_INT** ″Internal Error″
- **IDS_STRING_ERR_CMDLINE** ″The command line option that you typed was not recognized.\n\nUsage: scinstall [/postenroll | /biosreset | /newplanar]″
- **IDS_STRING_ERR_NOTSUPPORTED**

  Hardware password reset is not supported on this computer.
- **IDS_STRING_ERR_MEM**

  This computer does not have enough memory to run the hardware password reset feature.
- **IDS_STRING_ERR_ENVAR**

  A required environment variable is missing. Rescue and Recovery 3.0 (or higher) must be installed to use the hardware password reset feature.

- **IDS_STRING_ERR_MISSINGDLL**

  A required DLL is missing. Rescue and Recovery 3.0 (or higher) must be installed to use the hardware password reset feature.

- **IDS_STRING_ERR_BIOSMAILBOX**

  BIOS update to install the hardware password reset feature failed. Turn off your computer; then restart and retry the hardware password reset installation.

- **IDS_STRING_ERR_INSTALLRETRY**

  This operation did not complete successfully. To try again, turn off your computer, restart, and run the hardware password reset installation again.

- **IDS_STRING_ERR_INSTALLPUNT**

  This operation did not complete successfully. To troubleshoot the problem, consult your system administrator or the Rescue and Recovery documentation for details.

Chapter 4. Client Security Solution customization

This chapter uses terms defined by the Trusted Computing Group (TCG) regarding the Trusted Platform Module. For a more detailed explanation of these terms, refer to the following site for references and definitions:

http://www.trustedcomputinggroup.org/

Advantages of the embedded security chip/Trusted Platform Module

A Trusted Platform Module is an embedded security chip designed to provide security-related functions for the software utilizing it. The embedded security chip is installed on the motherboard of a system and communicates through a hardware bus. Systems that incorporate a Trusted Platform Module can create cryptographic keys and encrypt them so that they can only be decrypted by the same Trusted Platform Module. This process, often called *wrapping* a key, helps protect the key from disclosure. On a system with a Trusted Platform Module, the master wrapping key, called the Storage Root Key (SRK), is stored within the Trusted Platform Module itself, so the private portion of the key is never exposed. The embedded security chip can also store other storage keys, signing keys, passwords, and other small units of data. However, there is limited storage capacity in the Trusted Platform Module, so the SRK is used to encrypt other keys for off-chip storage. Because the SRK never leaves the embedded security chip, it forms the basis for protected storage.

When data protected by the Trusted Platform Module is needed, the protected data passes into the secure embedded hardware environment for processing. After successful authentication and decryption, the unprotected data can be used within the system.

Systems that incorporate a Trusted Platform Module are resistant to attack in the same ways that any hardware is more resistant to attack than software. This is especially important when leveraging cryptographic keys. Private portions of asymmetric key pairs are kept segregated from memory controlled by the operating system. The Trusted Platform Module uses its own internal firmware and logical circuits for processing instructions, does not rely upon the operating system, and is not subject to external software vulnerabilities.

No system can provide perfect security, including systems that use Trusted Platform Module technology. The embedded security chip is designed to resist tampering or electrical analysis. However, performing the kind of analysis needed to uncover Trusted Platform Module-protected secrets requires physical access to the machine and additional specialized hardware, making secrets on a embedded security chip-enabled platform much more secure than those on a software only system. Increasing the difficulty of stealing secrets from systems helps to raise the overall level of security for the individual or enterprise.

The embedded security chip use is an optional process and requires a Client Security Solution Administrator. Whether for individual user or a corporate IT department, the Trusted Platform Module must be initialized. Subsequent operations, such as the ability to recover from a hard drive failure or replaced system board, are also restricted to the Client Security Solution Administrator.

How Client Security Solution manages cryptographic keys

The inner workings of the Client Security Solution is described by the two main deployment activities; Take Ownership and Enroll User. While running the Client Security Setup Wizard for the first time, the Take Ownership and Enroll User processes are both performed during the initialization. The particular Windows user id that completed the Client Security Setup Wizard is the Client Security Solution Administrator and is enrolled as an active user. Every other user that logs into the system will be automatically requested to enroll into Client Security Solution.

- **Take Ownership - assign Client Security Solution administrator**

  A single Windows Administrator user id is assigned as the sole Client Security Solution Administrator for the system. Client Security Solution administrative functions must be performed through this user id. The Trusted Platform Module authorization is either this user's Windows password or Client Security passphrase.

  Note: The only way to recover from a forgotten Client Security Solution Administrators password or passphrase is to either uninstall the software with valid Windows permissions or to clear the security chip in BIOS. Either way, the data protected through the keys associated with the Trusted Platform Module will be lost. Client Security Solution also provides an optional mechanism that allows self-recovery of a forgotten password or passphrase based on a question and answer challenge response that is part of the Enroll User function. The Client Security Solution Administrator makes the decision whether to use the feature or not.
- **Enroll User**

  Once the Take Ownership process is completed and a Client Security Solution Administrator is created, a User Base Key can be created to securely store credentials for the currently logged on Windows user. This design allows for multiple users to enroll into Client Security Solution and leverage the single Trusted Platform Module. User keys are protected through the security chip, but actually stored off the chip on the hard drive. Unlike other security technologies, this design creates hard drive space as the limiting storage factor instead of actual memory built into the security chip. With this design, the number of users that can leverage the same secure hardware is vastly increased.

Take Ownership

The root of trust for Client Security Solution is the System Root Key (SRK). This non-migratable asymmetric key is generated within the secure environment of the Trusted Platform Module and never is exposed to the system. The authorization to leverage the key is derived through the Windows Administrator account during the "TPM_TakeOwnership" command. If the system is leveraging a Client Security passphrase, then the Client Security passphrase for the Client Security Solution administrator will be the Trusted Platform Module authorization, otherwise it will be the Client Security Solution Administrator's Windows password.

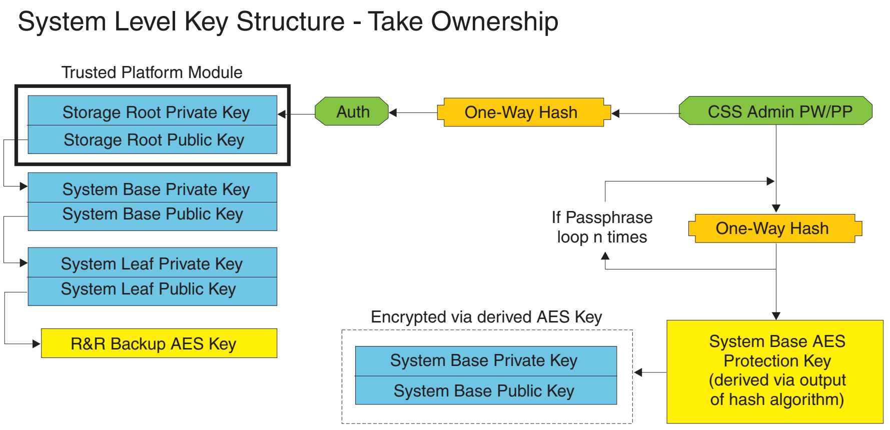


Figure 1.

With the SRK created for the system, other key pairs can be created and stored outside of the Trusted Platform Module, but wrapped or protected by the hardware-based keys. Since the Trusted Platform Module, which includes the SRK is hardware and hardware can be damaged, a recovery mechanism is needed to make sure damage to the system doesn't prevent data recovery.

In order to recover a system, a System Base Key is created. This migratable asymmetric storage key will allow the Client Security Solution Administrator to recovery from a system board swap or planned migration to another system.

In order to protect the System Base Key but allow it to be accessible during normal operation or recovery, two instances of the key is created and protected by two different methods. First, the System Base Key is encrypted with an AES symmetric key that is derived from knowing the Client Security Solution Administrator's password or Client Security passphrase. This copy of the Client Security Solution Recovery Key is solely for the purpose of recovering from a cleared Trusted Platform Module or replaced system board due to hardware failure.

The second instance of the Client Security Solution Recovery Key is wrapped by the SRK to import it to the key hierarchy. This double instance of the System Base Key allows the Trusted Platform Module to protect secrets bound to it below in normal usage and allows for a recovery of a failed system board through the System Base Key that is encrypted with an AES key unlocked by the Client Security Solution Administrator password or Client Security passphrase.

Next, a System Leaf Key is created. This legacy key is created to protect system level secrets such as the AES key used by Rescue and Recovery to protect backups.

Enroll User

In order to have each user's data protected by the same Trusted Platform Module, each user will have their own User Base Key created. This migratable asymmetric storage key is also created twice and protected by a symmetric AES key generated from each User's Windows password or Client Security passphrase. The second instance of the user base key is then imported into the Trusted Platform Module and protected by the system SRK. See Figure 2 on page 42.

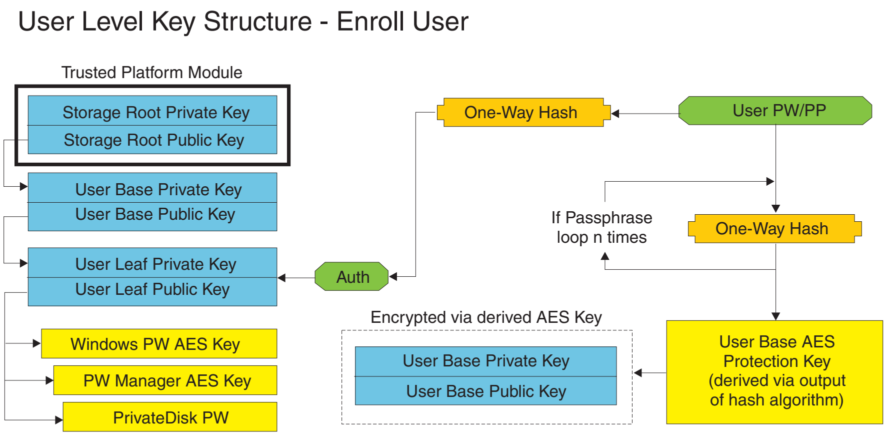


Figure 2.

With the User Base Key created, a secondary asymmetric key called the User Leaf Key is created in order to protect the individual secrets such as Password Manager AES key used to protect internet logon information, PrivateDisk Password used to protect data, and the Windows Password AES Key used to protect the access to the operating system. Access to the User Leaf Key is controlled by the User's Windows password or Client Security Solution passphrase and is automatically unlocked during logon.

Software emulation

If a system does not have a Trusted Platform Module, then a software based root of trust will be used. The same functionality will be available to the user, except they will have decreased security since the root of trust will be software based keys. The Trusted Platform Module's SRK is replaced with a Software-based RSA Key and AES Key to provide the protection that the Trusted Platform Module provided. The RSA key wraps the AES key and the AES Key is used to encrypt the next RSA key in the hierarchy.

System board swap

A system board swap infers that the old SRK to which keys were bound to is no longer valid, and another SRK is needed. This can also happen if the Trusted Platform Module is cleared through the BIOS.

The Client Security Solution Administrator is required to bind the system credentials to a new SRK. The System Base Key will need to be decrypted through the System Base AES Protection Key derived from the Client Security Solution Administrator's authorization credentials. See Figure 3 on page 43.

Note: If a Client Security Solution Administrator is a domain user ID and the password for that user ID was changed on a different machine; the password that was last used when logged onto the system needing recovery will need to be known in order to decrypt System Base Key for recovery. For example, during deployment a Client Security Solution Administrator user ID and password will be configured, if the password for this user changes on a different machine, then the original password set during deployment will be the required authorization in order to recovery the system.

Motherboard Swap - Take Ownership

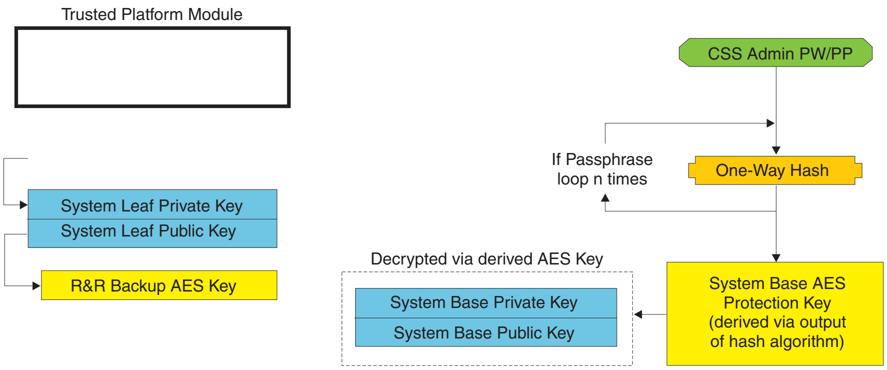


Figure 3.

Follow these steps to perform the system board swap:

1. Client Security Solution Administrator logs on to operating system
2. Logon-executed code (cssplanarswap.exe) recognizes the security chip is disabled and requires reboot to enable. (This step can be avoided by enabling the security chip through the BIOS.)
3. System is rebooted and security chip is enabled.
4. The Client Security Solution Administrator logs on; the new Take Ownership process is completed.
5. System Base Key is decrypted using System Base AES Protection Key that is derived by the Client Security Solution Administrator's authentication. System Base Key is imported to the new SRK and reestablishes the System Leaf Key and all credentials protected by it.
6. The system is now recovered.

Motherboard Swap - Enroll User

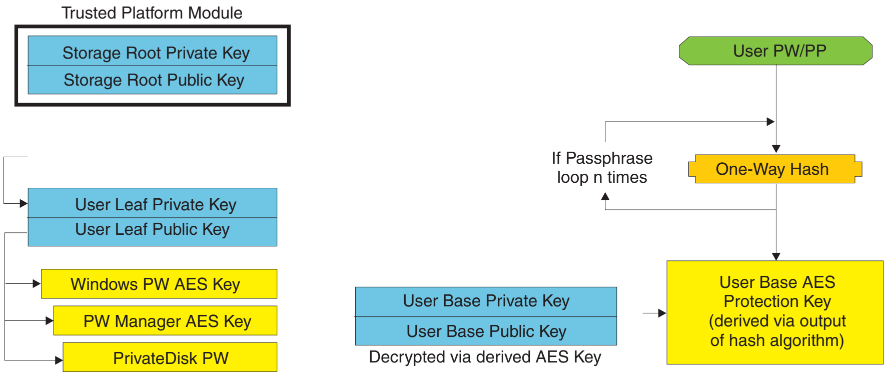


Figure 4.

As each user logs onto the system, the User Base Key is automatically decrypted through the User Base AES Protection Key derived from User authentication and imported to the new SRK created through the Client Security Solution Administrator.

XML Schema

The purpose of the xml scripting is to enable IT Administrators to create custom scripts that can be used to deploy Client Security Solution. All of the functions that are available in the Client Security Solution Setup Wizard is also available through scripting. The scripts can be protected by the xml_crypt_tool executable (with a password (AES encryption) or an obscurity). Once created, the virtual machine (vmserver.exe) accepts the scripts as input. The virtual machine calls the same functions as the Setup Wizard to configure the software.

Usage

All of the scripts consist of one tag to specify the xml encoding type, the xml schema, and at least one function to perform. The schema is used to validate the xml file and check to see that the required parameters are present. The use of schema is not currently enforced. Each function is enclosed in a function tag. Each function contains an order, this specifies in what order the command will be executed by the virtual machine (vmserver.exe). Each function has a version number as well; currently all of the functions are at version 1.0. For clarity, each of the example scripts below only contain one function. However, in practice a script would most likely contain multiple functions. The Client Security Solutions Setup Wizard can be used to create such a script. See “Client Security Wizard” on page 147 (refer to the setup wizard documentation for details).

Note: If the parameter <DOMAIN_NAME_PARAMETER> is left out in any of the functions that require a domain name, then the default computer name of the system will be used.

Examples

AUTO_ENROLL_ADMIN_FOR_RNR_ONLY

This command enables the system Administrator to generate the necessary security keys needed to encrypt backups with Rescue and Recovery. This command should only be executed once per system; it should not be executed for each user, only the Administrator.

Note: For Rescue and Recovery only installations, an Administrator must be assigned as the TPM owner if backups are going to be encrypted with the TPM. Use the following script file to automatically assign an Administrator user ID and password. This Windows User ID and password will be used for TPM recovery purposes. (All other CSS XML script functions are not applicable if only Rescue and Recovery is installed.)

- **USER_NAME_PARAMETER**

  The Windows user ID of the Administrator user.
- **DOMAIN_NAME_PARAMETER**

  The domain name for the Administrator user.
- **RNR_ONLY_PASSWORD**

  he Windows password for the Administrator user.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
        <FUNCTION>
         <ORDER>0001</ORDER
         <COMMAND>AUTO_ENROLL_ADMIN_FOR_RNR_ONLY</COMMAND>
         <VERSION>1.0</VERSION>
         <USER_NAME_PARAMETER>WinAdminName</USER_NAME_PARAMETER
```

```
          <DOMAIN_NAME_PARAMETER>MyCorp</DOMAIN_NAME_PARAMETER>
          <RNR_ONLY_PASSWORD>WinPassw0rd<RNR_ONLY_PASSWORD>
         </FUNCTION>
</CSSFile>
```

ENABLE_TPM_FUNCTION

This command enables the Trusted Platform Module and uses the argument SYSTEM_PAP. If the system already has a BIOS Administrator/Supervisor password set, then this argument must be provided. Otherwise, this command is optional.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>ENABLE_TPM_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
          <SYSTEM_PAP>PASSWORD</SYSTEM_PAP>
         </FUNCTION>
</CSSFile>
```

DISABLE_TPM_FUNCTION

This command uses the argument SYSTEM_PAP. If the system already has a BIOS Administrator/Supervisor password set, then this argument must be provided. Otherwise, this command is optional.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>DISABLE_TPM_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
          <SYSTEM_PAP>password</SYSTEM_PAP>
         </FUNCTION>
</CSSFile>
```

ENABLE_ENCRYPT_BACKUPS_FUNCTION

When you use Rescue and Recovery, this command enables protection of the backups with Client Security Solution.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>ENABLE_ENCRYPT_BACKUPS_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

DISABLE_ENCRYPT_BACKUPS_FUNCTION

When using Rescue and Recovery to protect the backups, this command disables protection of the backups with Client Security Solution.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>DISABLE_ENCRYPT_BACKUPS_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_PWMGR_FUNCTION

This command enables the password manager for all Client Security Solution users.

```
 <?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>ENABLE_PWMGR_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_CSS_GINA_FUNCTION

This command enables the Client Security Solution Logon.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>ENABLE_CSS_GINA_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_UPEK_GINA_FUNCTION

If the ThinkVantage Fingerprint Software is installed, this command enables the Logon.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>ENABLE_UPEK_GINA_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_UPEK_GINA_WITH_FUS_FUNCTION

If the ThinkVantage Fingerprint Software is installed, this command enables the Logon with Fast User Switching support.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>ENABLE_UPEK_GINA_WIH_FUS_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_NONE_GINA_FUNCTION

If either the ThinkVantage Fingerprint Software or Client Security Solution Logon is enabled, this command disables both the ThinkVantage Fingerprint Software and Client Security Solution Logons.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>ENABLE_CSS_NONE_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

SET_PP_FLAG_FUNCTION

This command writes a flag that Client Security Solution reads to determine whether to use the Client Security passphrase or a Windows password.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
        <FUNCTION>
         <ORDER>0001</ORDER
         <COMMAND>SET_PP_FLAG_FUNCTION</COMMAND>
        <PP_FLAG_SETTING_PARAMETER>USE_CSS_PP</PP_FLAG_SETTING_PARAMETER>
        <VERSION>1.0</VERSION>
        </FUNCTION>
</CSSFile>
```

ENABLE_PRIVATEDISK_PROTECTION_FUNCTION

This command enables SafeGuard PrivateDisk to be used on the system. Each user must still be specifically setup to use Safeguard PrivateDisk by the ENABLE_PD_USER_FUNCTION.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
        <FUNCTION>
         <ORDER>0001</ORDER
         <COMMAND>ENABLE_PRIVATEDISK_PROTECTION_FUNCTION</COMMAND>
         <VERSION>1.0</VERSION>
        </FUNCTION>
</CSSFile>
```

SET_ADMIN_USER_FUNCTION

This command writes a flag that Client Security Solution reads to determine who the Client Security Solution Administrator user is. The parameters are:

- **USER_NAME_PARAMETER**

  The user name of the Admin user.

- **DOMAIN_NAME_PARAMETER**

  The domain name of the Admin user.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
        <FUNCTION>
         <ORDER>0001</ORDER
         <COMMAND>SET_ADMIN_USER_FUNCTION</COMMAND>
         <USER_NAME_PARAMETER>sabedi</USER_NAME_PARAMETER>
         <DOMAIN_NAME_PARAMETER>IBM-2AA92582C79<DOMAIN_NAME_PARAMETER>
         <VERSION>1.0</VERSION>
         <SYSTEM_PAP>PASSWORD</SYSTEM_PAP>
        </FUNCTION>
</CSSFile>
```

ENABLE_PD_USER_FUNCTION

This command allows a particular user to use PrivateDisk. The parameters are:

- **USER_NAME_PARAMETER**

  The user name of the user to enable PrivateDisk.

- **DOMAIN_NAME_PARAMETER**

  The domain name of the user to enable PrivateDisk.

- **PD_VOLUME_SIZE_PARAMETER**

  The size of the PrivateDisk volume in megabytes.

- **PD_VOLUME_PATH_PARAMETER**

  The path of the PrivateDisk volume to be created.

- **PD_VOLUME_NAME_PARAMETER**

  The name of the PrivateDisk volume to be created. If the value PD_USE_DEFAULT_OPTION is specified, then a default value will automatically be used.

- **PD_VOLUME_DRIVE_LETTER_PARAMETER**

  The drive letter of the PrivateDisk volume to be created. If the value PD_USE_DEFAULT_OPTION is specified, then a default value will automatically be used.
- **PD_VOLUME_CERT_PARAMETER**

  If the value PD_USE_CSS_CERT is passed in, then PrivateDisk will either create a new certificate or use an existing certificate and have it protected with the Client Security Solution CSP. The mounting/unmounting of this volume will then be tied to the CSP instead of the css passphrase/windows password.. If the value PD_USE_DEFAULT_OPTION is specified, then no certificate is used and we default to the user's css passphrase/windows password.
- **PD_USER_PASSWORD**

  The password that Client Security Solution passes PrivateDisk to mount/create the PrivateDisk volume. If the value PD_RANDOM_VOLUME_PWD is specified, then Client Security Solution will generate a random volume password.
- **PD_VOLUME_USER_PASSWORD_PARAMETER**

  A user specific password to mount the PrivateDisk volume. This password is intended to be a backup to the PD_USER_PASSWORD password. If for any reason, Client Security Solution fails in the future, the value passed in for this argument will be independent of Client Security Solution. If the value PD_USE_DEFAULT_OPTION is specified, then no value will be used.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>ENABLE_PD_USER_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
          <USER_NAME_PARAMETER>sabedi</USER_NAME_PARAMETER>
          <DOMAIN_NAME_PARAMETER>IBM-2AA92582C79<DOMAIN_NAME_PARAMETER>
          <PD_VOLUME_SIZE_PARAMETER>500</PD_VOLUME_SIZE_PARAMETER>
          <PD_VOLUME_PATH_PARAMETER>C:\Documents and Settings\sabedi\My Documents\
             </PD_VOLUME_PATH_PARAMETER>
          <PD_VOLUME_NAME_PARAMETER>PD_USE_DEFAULT_OPTION</PD_VOLUME_NAME_PARAMETER>
          <PD_VOLUME_DRIVE_LETTER_PARAMETER>PD_USE_DEFAULT_OPTION</PD_VOLUME_DRIVE
             _LETTER_PARAMETER>
          <PD_VOLUME_CERT_PARAMETER>PD_USE_DEFAULT_OPTION</PD_VOLUME_CERT_PARAMETER>
          <PD_VOLUME_USER_PASSWORD_PARAMETER>PD_USE_DEFAULT_OPTION</PD_VOLUME_
             USER_PASSWORD_
             PARAMETER>
          <PD_USER_PASSWORD>PD_RANDOM_VOLUME_PWD</PD_USER_PASSWORD>
         </FUNCTION>
</CSSFile>
```

INITIALIZE_SYSTEM_FUNCTION

This command initializes the system to Client Security Solution to be used on the system. All of the system wide keys get generated through this function call. The parameters are:

- **NEW_OWNER_AUTH_DATA_PARAMETER**

  The owner password initializes the system. If the owner password is not set, the value passed in for this argument will become the new owner password. If an owner passphrase is already set and the administrator use the same password, then it can be passed in. In this case that the admin wants to use a new owner passphrase, then the desired password should be passed in this parameter.
- **CURRENT_OWNER_AUTH_DATA_PARAMETER**

The current owner password of the system. If the system already has a 5.4x owner password, then this parameter should pass in the 5.4x password. Otherwise, if a new owner password is desired, the current owner password should be passed in this parameter. If no password change is desired, then the value NO_CURRENT_OWNER_AUTH should be passed.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>INITIALIZE_SYSTEM_FUNCTION</COMMAND>
          <NEW_OWNER_AUTH_DATA_PARAMETER>pass1word</NEW_OWNER_AUTH_DATA_
              PARAMETER>
          <CURRENT_OWNER_AUTH_DATA_PARAMETER>No_CURRENT_OWNER_AUTH</CURRENT
              _OWNER_AUTH_DATA_PARAMETER>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

CHANGE_TPM_OWNER_AUTH_FUNCTION

This command changes the Client Security Solution administrator authorization and updates the system keys accordingly. All of the system wide keys get regenerated through this function call. The parameters are:

- NEW_OWNER_AUTH_DATA_PARAMETER

  The new owner password of the Trusted Platform Module.

- CURRENT_OWNER_AUTH_DATA_PARAMETER

  The current owner password of the Trusted Platform Module.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>CHANGE_TPM_OWNER_AUTH_FUNCTION</COMMAND>
          <NEW_OWNER_AUTH_DATA_PARAMETER>newPassWord</NEW_OWNER_AUTH_DATA_
              PARAMETER>
          <CURRENT_OWNER_AUTH_DATA_PARAMETER>oldPassWord</CURRENT_OWNER_AUTH
              _DATA_PARAMETER>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENROLL_USER_FUNCTION

This command enrolls a particular user to use Client Security Solution. This function creates all of the user specific security keys for a given user. The parameters are:

- **USER_NAME_PARAMETER**

  The user name of the user to enroll.

- **DOMAIN_NAME_PARAMETER**

  The domain name of the user to enroll.

- **USER_AUTH_DATA_PARAMETER**

  The Trusted Platform Module passphrase/windows password to create the user's security keys with.

- **WIN_PW_PARAMETER**

  The Windows password.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>ENROLL_USER_FUNCTION</COMMAND>
          <USER_NAME_PARAMETER>sabedi</USER_NAME_PARAMETER>
          <DOMAIN_NAME_PARAMETER>IBM-2AA92582C79<DOMAIN_NAME_PARAMETER>
          <USER_AUTH_DATA_PARAMETER>myCssUserPassPhrase</USER_AUTH_DATA_PARAMETER>

          <WIN_PW_PARAMETER>myWindowsPassword</WIN_PW_PARAMETER>
          <VERSION>1.0</VERSION>
          </FUNCTION>
</CSSFile>
```

USER_PW_RECOVERY_FUNCTION

this command sets up a particular Trusted Platform Module user's password recovery. The parameters are:

- **USER_NAME_PARAMETER**

  The user name of the user to enroll.
- **DOMAIN_NAME_PARAMETER**

  The domain name of the user to enroll.
- **USER_PW_REC_QUESTION_COUNT**

  The number of questions the user must answer.
- **USER_PW_REC_ANSWER_DATA_PARAMETER**

  The stored answer to a particular question. Note, the actual name of this parameter is concatenated with a number corresponding to which question it answers. Refer to the example for this command below.
- **USER_PW_REC_STORED_PASSWORD_PARAMETER**

  The stored password that is presented to the user once all of the questions are answered correctly.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>USER_PW_RECOVERY_FUNCTION</COMMAND>
          <USER_NAME_PARAMETER>sabedi</USER_NAME_PARAMETER>
          <DOMAIN_NAME_PARAMETER>IBM-2AA92582C79<DOMAIN_NAME_PARAMETER>
          <USER_PW_REC_ANSWER_DATA_PARAMETER>Test1</USER_PW_REC_ANSWER_DATA_PARA
              METER>
          <USER_PW_REC_ANSWER_DATA_PARAMETER>Test2</USER_PW_REC_ANSWER_DATA_PARA
              METER>
          <USER_PW_REC_ANSWER_DATA_PARAMETER>Test3</USER_PW_REC_ANSWER_DATA_PARA
              METER>
          <USER_PW_REC_QUESTION_COUNT>3</USER_PW_REC_QUESTION_COUNT>
          <USER_PW_REC_QUESTION_LIST>20000,20001,20002</USER_PW_REC_QUESTION_LIST>
         </USER_PW_REC_STORED_PASSWORD_PARAMETER>Pass1word</USER_PW_REC_STORED_PASS
              WORD_PARAMETER>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

SET_WIN_PE_LOGON_MODE_FUNCTION

This command writes a flag that the program reads to determine whether to require user authorization when entering the Windows PE environment. The parameter is:

- **WIN_PE_LOGON_MODE_AUTH_PARAMETER**

  The two valid choices are:
  - NO_AUTH_REQUIRED_FOR_WIN_PE_LOGON
  - AUTH_REQUIRED_FOR_WIN_PE_LOGON

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
```

```
          <ORDER>0001</ORDER
          <COMMAND>SET_WIN_PE_LOGON_MODE_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
          <WIN_PE_LOGON_MODE_AUTH_PARAMETER>AUTH_REQUIRED_FOR_WIN_PE_LOGON</WIN
             _PE_LOGON_MODE_AUTH_PARAMETER>
          <SYSTEM_PAP>PASSWORD</SYSTEM_PAP>
         </FUNCTION>
</CSSFile>
```

Chapter 5. System Migration Assistant customization

There are two customizable portions of System Migration Assistant:

- Editing or modifying a command file
- Migrating additional application settings

Creating a command file

During the capture phase, SMA 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 SMA in the default location, this file is located in the D:\%RR%\migration\bin directory.

Note: System Migration Assistant 5.0 uses XML technology to describe its command file commands.

Consider the following points concerning SMA 5.0 command files:

- The command file follows XML version 1.0 syntax. The command file 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 SMA. If SMA 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 might be flawed.

Command 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 10.

Command	Parameters	Parameter Values and Examples

<Desktop>	• <accessability>
	• <active_desktop>
	• <colors>
	• <desktop_icons>
	• <display>
	• <icon_metrics>
	• <keyboard>
	• <mouse>
	• <pattern>
	• <screen_saver>
	• <sento_menu>
	• <shell>
	• <sound>
	• <start_menu>
	• <taskbar>
	• <wallpaper>
	• <window_metrics>
		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>`

<Applications>	<Application>
	See the *ThinkVantage System Migration Assistant User’s Guide* for a list of all the applications that are supported.
		For example:
		`<Applications>`
		`<Application>Lotus Notes</Application>`
		`<Application>Microsoft Office</Application>`
		`<//Applications>`
		or
		`<Applications>`
		`<Application>$(all)</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.

Table 10. (continued)

Command	Parameters	Parameter Values and Examples

<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\Jim</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)

<Printers>	<Printer>
	<PrinterName>
		This control statement is effective for both the source and the target compuer.
		To capture all printers, set the parameter to *&(all)*. Otherwise, specify each printer individually. to capture the default printer only , set the parameter to *&(DefaultPrinter)*.
		For example:
		`<Printers>`
		`  <Printer>&(all)</Printer>`
		`</Printers>`
		
		`<Printers>`
		`  <Printer>`
		`   <PrinterName>IBM 5589-L36</PrinterName>`
		`  </Printer>`
		`</Printers>`
		
		`<Printers>`
		`  <Printer>&(DefaultPrinter)</Printer>`
		`</Printers>`

Table 10. (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 “alse” or leave it unspecified.
	<log_file_location>	To specify the directory to which SMA writes log files, enter a fully qualified directory name. You can specify a shared directory on another system. If you do not set this parameter, SMA writes log files to d:/InstDir/, where d is the drive letter of the hard disk drive and /InstDir/ is the directory where the SMA installed.
	<temp_file_location>	To specify the directory to which SMA writes temporary files, enter a fully qualified directory name. You can specify a shared directory on another system. If you do not set this parameter, SMA writes temporary files to d:/InstDir/etc/data, where d is the drive letter of the hard disk drive and /InstDir/ is the directory where the SMA 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

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

SMA will select and deselect 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.

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 11.

Command	Parameter	What it does

<FilesAndFolders>	<run>	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>`

Table 11. (continued)

Command	Parameter	What it does

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

Table 11. (continued)

Command	Parameter	What it does

<Inclusions>	<IncDescriptions>
	<Description>
	<DateCompare>
	<Operand>
	<Date>
	<SizeCompare>
	<Operand>
	<Size>
	<Dest>
	<Operation> where
	• <Description> is the fully-qualified filename. You can use wildcard character for both filename and folder name.
	• <DateCompare> is an optional parameter, that specifies 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> 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.
		Searches for all matching files in the specified directories.
		For example:
		Example 1
		`<IncDescription>`
		`<Description>c:\MyWorkFolder\ls</Description>`
		`</IncDescription>`
		Note: To specify the folder name, add .\. at the end of the description
		Example 2
		`<IncDescription>`
		`<Descriptin>C:\MyWorkFolder\*.*</Decsription>`
		`<DateCompare>`
		`<Operand>NEWER</Operand>`
		`<Date>07/31/2005</Date>`
		`</DateCompare>`
		`</IncDescription>`
		Example 3
		`<IncDescription>`
		`<Description>C:\MyWorkFolder/*.*</Description>`
		`<SizeCompare>`
		`<Operand>SMALLER</Operand>`
		`<Size>200</Size>`
		`</SizeCompare>`
		`</IncDescription>`
		Example 4
		`<IncDescription>`
		`<Description>C:\MyWorkFolder\*.*</Description>`
		`<Dest>D:\MyNewWorkFolder</Dest>`
		`<Operation>`
		`<IncDescription>`

Table 11. (continued)

Command	Parameter	What it does

<Exclusions>	<ExDescriptions>
	<Description>
	<DateCompare>
	<Operand>
	<Date>
	<SizeCompare>
	<Operand>
	<Size> where
	• <Description> is a fully qualified file name or folder name. It can contain 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.
		Deselects all matching files in a specified directory
		For example:
		Example 1
		`<ExDescription>`
		`<Description>C:\YourWorkFolder</Description>`
		`</ExDescription>`
		Example 2
		`<ExDescription>`
		`<Description>C:\YourWorkFolder</Description>`
		`<DateCompare>`
		`<Operand>OLDER</Operand>`
		`<Date>07/31/2005</Date>`
		`</DateCompare>`
		`</ExDescription>`
		Example 3
		`<ExDescription>`
		`<Description>C:\YourWorkFolder</Description>`
		`<SizeCompare>`
		`<Operand>LARGER</Operand>`
		`<Size>200</Size></SizeCompare>`
		`</ExDescription>`

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

```
<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 under %windir% which specifies 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

Note: To create custom application files, you must have a thorough knowledge of the application, including the storage locations of customized settings. By default, SMA is preconfigured to migrate settings for several applications. For a list of applications supported by SMA, see the *System Migration Assistant User's Guide*. 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 d:\%RR%\Migration\bin\Apps, where *Apps* specifies the application and d is the drive letter of the hard disk drive. Priority is given to application.smaapp when both application.smaapp and application.xml custom applications files 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, when System Migration Assistant is installed, 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, SMA continues the operation and writes the errors to the log file

Table 12 shows information about application files:

Table 12.

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 SMA 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 SMA 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.			

Table 12. (continued)

Section	Command	Value	What it does
	<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. SMA 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>`
`<Regsitry>`
`<hive>HKLM</hive>`
`<keyname>Software\adobe\Acrobat Reader\5.0\InstallPath</keyname>`
`<value>(Default)</value>`
`</Registry>`
`</Install_Directory>`
`</Install_Directories>`			

	<OS>	A text string	OS specifies the operating system, and can be one of the following: • WinXP • Win2000 • WinNT • Win98
	<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.
<Files_From_Folders> Optional			

Table 12. (continued)

Section	Command	Value	What it does

	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>`
			SMA 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>`
			SMA 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>`
			SMA 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>`
			SMA 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", SMA 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.		

Table 12. (continued)

Section	Command	Value	What it does
<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: • 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>
<PreTargetBatchProcessing>			

Table 12. (continued)

Section	Command	Value	What it does

	`<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 an ASCII text editor to open an existing application.XML file. If you installed SMA in the default location, the application.XML files are located in the d:\d:\%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 → 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 d:\Program Files\ThinkVantage\SMA\Apps directory, where d 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">
<AppInfor>
        <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_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\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\Sof
tware\Adobe\Acrobat Reader\7.0"
          regfix "HKLM\Software\Adobe\Acrobat Reader\5.0\AdobeView
er" "HKLM\Software\Adobe\Acrobat Reader\7.0\AdobeViewer"
          goto Done
          :Update60
regfix "HKCU\Software\Adobe\Acrobat Reader\6.0" "HKCU\Softw
are\Adobe\Acrobat Reader\7.0"
          regfix "HKLM\Software\Adobe\Acrobat Reader\6.0\AdobeVi
ewer" "HKLM\Software\Adobe\Acrobat Reader\7.0\AdobeViewer"
          :Done
          ]]>
</TargetBatchProcessing>
</Application>

</Applications>
```

Chapter 6. Installation

The Rescue and Recovery/Client Security Solution Installation Package is developed with InstallShield 10.5 Premier as a Basic MSI project. InstallShield 10.5 Basic MSI Projects use the Windows Installer to install applications, which gives administrators many capabilities to customize installations such as setting property values from the command line. The sections following describe ways to use and execute the Rescue and Recovery 3.0 setup package. For a better understanding, read the entire chapter first before you begin to install the package.

Note: When installing this package, please refer to the Readme file that is posted on the Lenovo web page at:

www.Lenovo.com/ThinkVantage

The readme file contains up-to-the-minute information on such subjects as 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/Client Security Solution package. For best results, go to the following Web site to make sure that you have the latest version of the software:

www.Lenovo.com/ThinkVantage

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

Requirements for IBM- and Lenovo-branded computers

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

- Operating system: Microsoft Windows XP or Windows 2000
- Processor: As specified by Microsoft for Windows XP (Home or Professional) and Windows 2000
  - Service pack 1, at minimum
- Memory: 128 MB
  - In shared memory configurations, the BIOS setting for maximum shared memory must be set to no less than 4 MB and no greater than 8 MB.
  - In non-shared memory configurations, 120 MB of non-shared memory.

    Note: If a computer has less than 200 MB of non-shared memory, Rescue and Recovery will run. However, the user might be unable to start more than one application in the Rescue and Recovery environment.
- 1.5 GB of free hard disk space (the base installation requires 930 MB and does not include space required for Rescue and Recovery backups)
- VGA-compatible video that supports a resolution of 800 x 600 and 24-bit color
- Supported Ethernet card

Requirements for installing and use on non-IBM or non-Lenovo computers

Installation on non-IBM or non-Lenovo computers have the following requirements:

Installation requirements

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

Minimum system memory requirements

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

Hard disk drive configuration

The Rescue and Recovery program is not supported on the factory preloads for original equipment manufacturer (OEM) computers (non-IBM or non-Lenovo). For OEM computers, the hard disk drive must be configured according to recommendations in “Installing of Rescue and Recovery on non-IBM branded computers” on page 118.

Network adapters

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

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

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

Non-IBM/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 Bootability

Video requirements

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

Application compatibility

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

www.lenovo.com/ThinkVantage

Utilities

This guide refers to a number of utilities. These utilities can be found on this Web site:

www.Lenovo.com/ThinkVantage

Installation components for Rescue and Recovery

1. Main installation package (approximately 45 MB): This is the setup.exe built from the installation project source. The setup.exe file is renamed during the build process to a name representing the project ID, the media type, the build level, the country code (always US in this case), and the patch code – for example, Z096ZIS1001US00.exe. 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 files.
2. Predesktop US Base (approximately 135 MB): This is the password protected zip file that contains the entire predesktop US base. Its name is in the format Z062ZAA1001US00.TVT, where *AA* determines the compatibility of the predesktop and *001* is the level of the predesktop. This file is required to install the predesktop on all language systems. This file must be in the same directory as the main installation package (either setup.exe or Rescue and Recovery/Client Security Solution.msi if extracted or OEM install). The exceptions to this are if the predesktop 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 (any version) does not already exist. The setup.exe contains a file pdaversion.txt that contains the minimum version of the predesktop that can work with that version of Windows. The setup.exe installer will look for a predesktop file using the following logic:
   - **Old Predesktop (RNR 1.0 or 2.X) exists or no Predesktop 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 (RNR 3.0) Predesktop exists:**

     The installer will compare the current predesktop's compatibility code against the minimum version compatibility code and take the following actions based on the results:
     – **Current code > Minimum code:**

       The installer will present a message that the current environment is not compatible with this version of RNR.

     – **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 (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. If the current level is less than the minimum level, the installer will look for a .TVT file with a compatibility code (AA, 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 (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.

3. Predesktop language packs (approximately 5 – 30 MB each): There are 24 language packs for Windows PE that are supported in Rescue and Recovery 3.0. Each language pack is named in the format Z062ZAA1001CC00.TVT where the CC represents the language. One of these files is required if the predesktop 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 .TVT file. The language of the language pack must match the language of Windows, if Windows is non-English or a language not supported by the language packs. If the predesktop is being installed or updated and a language pack is required, the installation looks for a .TVT language pack where all fields in the file name match the US predesktop file name except the language code which must match the language of the system. The language packs are available in the following languages:
   - Arabic
   - Brazilian Portuguese
   - Portuguese
   - Czech
   - Danish
   - Finnish
   - French
   - Greek
   - German
   - Hebrew
   - Hong Kong
   - Chinese
   - Hungarian
   - Italian
   - Japanese
   - Korean
   - Dutch
   - Norwegian
   - Polish
   - Portuguese
   - Russian
   - Simplified Chinese
   - Spanish

- Swedish
- Traditional Chinese
- Turkish

Standard installation procedure and command-line parameters

Setup.exe can accept a set of command line parameters, which are described below. Command-line options that require a parameter must be specified with no space between the option and its parameter. For example, Setup.exe /s /v″/qn REBOOT=″R″″ is valid, while Setup.exe /s /v ″/qn REBOOT=″R″″ is not. Quotation marks around an option's parameter are required only if the parameter contains spaces.

Note: The default behavior of the installation when executed alone (just running setup.exe without any parameters), is to prompt the user to reboot at the end of the installation. A reboot is required for the program to function properly. The reboot can be delayed through a command line parameter for a silent install as documented above and in the example section.

The following parameters and descriptions were taken directly from the InstallShield Developer Help Documentation. Parameters that do not apply to Basic MSI projects were removed.

Table 13.

Parameter	Description
/a : Administrative installation	The /a switch causes Setup.exe to perform an administrative installation. An administrative installation copies (and uncompresses) your data files to a directory specified by the user, but does not create shortcuts, register COM servers, or create an uninstallation log.
/x : Uninstall mode	The /x switch causes Setup.exe to uninstall a previously installed product.
/s : Silent mode	The command Setup.exe /s suppresses the Setup.exe initialization window for a Basic MSI installation program, but does not read a response file. Basic MSI projects do not create or use a response file for silent installations. To run a Basic MSI product silently, run the command line Setup.exe /s /v/qn. (To specify the values of public properties for a silent Basic MSI installation, you can use a command such as Setup.exe /s /v″/qn INSTALLDIR=D:\Destination″.)
/v : pass arguments to Msiexec	The /v argument is used to pass command line switches and values of public properties through to Msiexec.exe.
/L : Setup language	Users can use the /L switch with the decimal language ID to specify the language used by a multi-language installation program. For example, the command to specify German is Setup.exe /L1031. Note: Not all of the languages referenced in Table 14 on page 78 are supported in the install.

Table 13. (continued)

Parameter	Description
/w : Wait	For a Basic MSI project, the /w argument forces Setup.exe to wait until the installation is complete before exiting. If you are using the /w option in a batch file, you may want to precede the entire Setup.exe command line argument with start /WAIT. A properly formatted example of this usage is as follows: `start /WAIT setup.exe /w`

Table 14.

Language	identifier
Arabic (Saudi Arabia)	1025
Basque	1069
Bulgarian	1026
Catalan	1027
Simplified Chinese	2052
Traditional Chinese	1028
Croatian	1050
Czech	1029
Danish	1030
Dutch (Standard)	1043
English	1033
Finnish	1035
French Canadian	3084
French	1036
German	1031
Greek	1032
Hebrew	1037
Hungarian	1038
Indonesian	1057
Italian	1040
Japanese	1041
Korean	1042
Norwegian (Bokmal)	1044
Polish	1045
Portuguese (Brazilian)	1046
Portuguese (Standard)	2070
Romanian	1048
Russian	1049
Slovak	1051
Slovene	1060

Table 14. (continued)

Language	identifier
Spanish	1034
Swedish	1053
Thai	1054
Turkish	1055

Administrative installation procedure and command-line parameters

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/Client Security Solution installation package, an administrative installation unpacks the installation source files to a specified location. To run an administrative installation, the setup package needs to be executed from the command line using the /a parameter:

```
Setup.exe /a
```

Launching an administrative installation presents a series of dialog screens prompting the administrative user to specify the location to unpack the setup files. The default extract location that is presented to the administrative user is C:\. A new location can be chosen which may include drives other than C: (such as other local drives and apped network drives). New directories can also be created during this step.

If an administrative installation is run silently, the public property TARGETDIR can be set on the command line to specify the extract location:

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

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

The following section describes the available command line parameters that can be used with msiexec as well as an example of how to use it. Public properties can also be set directly in the msiexec command line call.

MsiExec.exe command-line parameters

MsiExec.exe is the executable program of the Windows Installer used to interpret installation packages and install products on target systems:

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

Thefollowing table provides a detailed description of MsiExec.exe command line parameters. This table is taken directly from the Microsoft Platform SDK documentation on the Windows Installer.

Table 15.

Parameter	**Description**
/i *package* or *product code*	Use this format to install the product Othello: `msiexec /i "C:\WindowsFolder\Profiles\ UserName\Personal\MySetups\Othello\Trial Version\ Release\DiskImages\Disk1\Othello Beta.msi"` Product Code refers to the GUID that is automatically generated in the Product Code property of your product's project view.
/f [p|o|e|d|c|a|u|m|s|v] *package* or *product code*	Installing with the /f option will repair or reinstall missing or corrupted files. For example, to force a reinstall of all files, use the following syntax: `msiexec /fa "C:\WindowsFolder\Profiles\ UserName\Personal\MySetups\Othello\Trial Version\ Release\DiskImages\Disk1\Othello Beta.msi"` in conjunction with the following flags: • p reinstalls a file if it is missing • o reinstalls a file if it is missing or if an older version of the file is present on the user's system • e reinstalls a file if it is missing or if an equivalent or older version of the file is present on the user's system • c reinstalls a file if it is missing or if the stored checksum of the installed file does not match the new file's value • a forces a reinstall of all files • u or m rewrite all required user registry entries • s overwrites any existing shortcuts • v runs your application from the source and re-caches the local installation package
/a *package*	The /a option allows users with administrator privileges to install a product onto the network.
/x *package* or *product code*	The /x option uninstalls a product.
/L [i|w|e|a|r|u|c|m|p|v|+] *log file*	Building with the /L option specifies the path to the log file—these flags indicate which information to record in the log file: • i logs status messages • w logs non-fatal warning messages • e logs any error messages • a logs the commencement of action sequences • r logs action-specific records • u logs user requests • c logs initial user interface parameters • m logs out-of-memory messages • p logs terminal settings • v logs the verbose output setting • + appends to an existing file • * is a wildcard character that allows you to log all information (excluding the verbose output setting)

Table 15. (continued)

Parameter	Description
/q [n|b|r|f]	The /q option is used to set the user interface level in conjunction with the following flags: • q or qn creates no user interface • qb creates a basic user interface The user interface settings below display a modal dialog box at the end of installation: • qr displays a reduced user interface • qf displays a full user interface • qn+ displays no user interface • qb+ displays a basic user interface
/? or /h	Either command displays Windows Installer copyright information
TRANSFORMS	Use the TRANSFORMS command line parameter to specify any transforms that you would like applied to your base package. Your transform command line call might look something like this: msiexec /i "C:\WindowsFolder\Profiles\UserName\Personal\MySetups\Your Project Name\Trial Version\My Release-1\DiskImages\Disk1\ProductName.msi" TRANSFORMS="New Transform 1.mst" You can separate multiple transforms with a semicolon. Because of this, it is recommended that you do not use semicolons in the name of your transform, as the Windows Installer service will interpret those incorrectly.
Properties	All public properties can be set or modified from the command line. Public properties are distinguished from private properties by the fact that they are in all capital letters. For example, COMPANYNAME is a public property. To set a property from the command line, use the following syntax: PROPERTY=VALUE. If you wanted to change the value of COMPANYNAME, you would enter: msiexec /i "C:\WindowsFolder\Profiles\UserName\Personal\MySetups\Your *Project Name*\Trial Version\My Release-1\DiskImages\Disk1\ProductName.msi" COMPANYNAME="InstallShield"

Standard Windows Installer public properties

The Windows Installer has a set of standard built in public properties that can be set on the command line to specify certain behavior during the installation. The most common public properties used in the command line are described below. More documentation is available on the Microsoft website at: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/about_properties.asp

Table 16 shows the commonly used Windows Installer properties:

Table 16.

Property	**Description**
TARGETDIR	Specifies the root destination directory for the installation. During an administrative installation this property is the location to copy the installation package.
ARPAUTHORIZEDCDFPREFIX	URL of the update channel for the application.
ARPCOMMENTS	Provides Comments for the Add or Remove Programs on Control Panel.
ARPCONTACT	Provides Contact for the Add or Remove Programs on Control Panel.
ARPINSTALLLOCATION	Fully qualified path to the application's primary folder.
ARPNOMODIFY	Disables functionality that would modify the product.
ARPNOREMOVE	Disables functionality that would remove the product.
ARPNOREPAIR	Disables the Repair button in the Programs wizard.
ARPPRODUCTICON	Specifies the primary icon for the installation package.
ARPREADME	Provides a ReadMe for the Add or Remove Programs on Control Panel.
ARPSIZE	Estimated size of the application in kilobytes.
ARPSYSTEMCOMPONENT	Prevents display of application in the Add or Remove Programs list.
ARPURLINFOABOUT	URL for an application's home page.
ARPURLUPDATEINFO	URL for application-update information.
REBOOT	The REBOOT property suppresses certain prompts for a reboot of the system. An administrator typically uses this property with a series of installations to install several products at the same time with only one reboot at the end. Set REBOOT="R" to disable any reboots at the end of an install.
INSTALLDIR	This property contains the default destination folder for the files in your features and components.

Rescue and Recovery custom public properties

The install 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 17.

Property	Description
PDA	Specifies whether to install the predesktop, default value is 1. 1 = install predesktop, 0 = don't install predesktop. NOTE: This setting is not used if any version of the predesktop already exists.
CIMPROVIDER	Specifies whether to install the 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 TPM exists. Set EMULATIONMODE=1 on the command line to install in Emulation mode.
HALTIFCSS54X	If CSS 5.4X is installed and the installation is running in silent mode, the default is for the installation to proceed in emulation mode. Use the HALTIFCSS54X=1 property when running the installation in silent mode to halt the installation if CSS 5.4X is installed.
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 install from enabling the TPM
NOCSS	Set NOCSS=1 on the command line to prevent the Client Security Solution and its sub-features from being installed. This is meant to be used with a silent installation but can be used with a UI installation as well. In the UI installation, the CSS feature will not show up in the custom setup screen.
NOPRVDISK	Set NOPRVDISK=1 on the command line to prevent the SafeGuard PrivateDisk feature from being installed. This is meant to be used with a silent installation but can be used with a UI installation as well. In the UI installation, the SafeGuard PrivateDisk feature will not show up in the custom setup screen.
NOPWMANAGER	Set NOPWMANAGER=1 on the command line to prevent Password Manager feature from being installed. This is meant to be used with a silent installation but can be used with a UI installation as well. In the UI installation, the Password Manager feature will not show up in the custom setup screen.

Table 17. (continued)

Property	Description
NOCSSWIZARD	Set NOCSSWIZARD=1 on the command line to prevent the CSS Wizard from being displayed when an admin user logs on and has not been enrolled. This property is meant for someone who wants to install CSS, but use scripting later on to actually configure the system.
CSS_CONFIG_SCRIPT	Set CSS_CONFIG_SCRIPT="*filename*" or "*filename password*" to have a configuration file run after the user completes the install and reboots.
SUPERVISORPW	Set SUPERVISORPW="*password*" on the command line to supply the supervisor password to enable the chip in silent or non-silent install 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.

Installation log file

A log file rrinstall30.log is created in the %temp% directory if the setup is launched by setup.exe (either double clicking the main install exe, run the main exe without parameters, or extract msi and execute setup.exe). 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 examples using setup.exe:

Table 18.

Description	Example
Silent Install with no Reboot	`setup.exe /s /v"/qn REBOOT="R""`
Administrative Install	`setup.exe /a`
Silent Administrative Install specifying the extract location	`setup.exe /a /s /v"/qn TARGETDIR="F:\TVTRR""`
Silent Uninstall setup.exe /s /x /v/qn	`setup.exe /s /x /v/qn`
Install with no Reboot and create an installation log in temp directory	`setup.exe /v"REBOOT="R" /L*v %temp%\rrinstall30.log"`
Install without installing the predesktop setup.exe /vPDA=0	`setup.exe /vPDA=0`

The table below shows installation examples using Rescue and Recovery/Client Security Solution.msi:

Table 19.

Description	Example
Install	msiexec /i “C:\TVTRR\Rescue and Recovery/Client Security Solution.msi”
Silent Install with no Reboot	msiexec /i “C:\TVTRR\Rescue and Recovery/Client Security Solution.msi” /qn REBOOT=”R”
Silent Uninstall	msiexec /x “C:\TVTRR\Rescue and Recovery/Client Security Solution.msi” /qn
Install without installing the predesktop	msiexec /i “C:\TVTRR\Rescue and Recovery/Client Security Solution.msi” PDA=0

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. It is assumed that you have expertise in your image creation tool and that you will include other options that you require for your applications.

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

Using PowerQuest Drive Image based tools

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

Minimum script files

Table 20. X:\PQ\RRUSAVE.TXT

Script language	Result
`SELECT DRIVE 1`	Select first hard disk drive
`SELECT PARTITION ALL` (Needed if you have a type 12 partition or if you have multiple partitions in your image.)	Select all partitions
Store with compression high	Store the image

Table 21. X:\PQ\RRDEPLY.TXT

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

Image creation

Table 22. X:\PQ\PQIMGCTR / CMD=X:\PQ\RRUSAVE.TXT /MBI=1 / IMG=X:\IMAGE.PQI

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

Image deployment

Table 23. X:\PQ\PQIMGCTR / CMD=X:\PQ\RRDEPLY.TXT /MBI=1 / IMG=X:\IMAGE.PQI

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

Using Symantec Ghost-based tools

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

Installation components for Client Security Solution Version 6.0

The Client Security Solution 6.0 Installation Package is developed with InstallShield 10.5 Premier as a Basic MSI project. InstallShield 10.5 Basic MSI Projects use the Windows Installer to install applications, which gives administrators many capabilities to customize installations such as setting property values from the command line. The sections below describe ways to use and execute the CSS 6.0 setup package. For a better understanding, read all of the following instructions.

Installation components

The CSS 6.0 Installation consists of a single exe file (approximately 20 MB). This is the setup.exe built from the installation project source. The setup.exe file is renamed during the build process to a name representing the project ID, the media type, the build level, the country code (always US in this case), and the patch code – for example, 169ZIS1001US00.exe. 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.

Standard installation procedure and command-line parameters

Setup.exe can accept a set of command-line parameters, which are described following. Command line options that require a parameter must be specified with no space between the option and its parameter. For example,

```
Setup.exe /s /v"/qn REBOOT="R""
```

is valid, while

```
Setup.exe /s /v "/qn REBOOT="R""
```

is not. Quotation marks around an option's parameter are required only if the parameter contains spaces.

Note: The default behavior of the installation when executed alone (just running setup.exe without any parameters), is to prompt the user to reboot at the end of the installation. A reboot is required for the program to function properly. The reboot can be delayed through a command line parameter for a silent install as documented above and in the example section.

The parameters and descriptions below were taken directly from the InstallShield Developer Help Documentation. Parameters that do not apply to Basic MSI projects were removed.

Table 24.

Parameter	**Description**
/a : Administrative installation	The /a switch causes Setup.exe to perform an administrative installation. An administrative installation copies (and uncompresses) your data files to a directory specified by the user, but does not create shortcuts, register COM servers, or create an uninstallation log.
/x : Uninstall mode	The /x switch causes Setup.exe to uninstall a previously installed product.
/s : Silent mode	The command Setup.exe /s suppresses the Setup.exe initialization window for a Basic MSI installation program, but does not read a response file. Basic MSI projects do not create or use a response file for silent installations. To run a Basic MSI product silently, run the command line Setup.exe /s /v/qn. (To specify the values of public properties for a silent Basic MSI installation, you can use a command such as Setup.exe /s /v"/qn INSTALLDIR=D:\Destination".)
/v : pass arguments to Msiexec	The /v argument is used to pass command line switches and values of public properties through to Msiexec.exe.
/L : Setup language	Users can use the /L switch with the decimal language ID to specify the language used by a multi-language installation program. For example, the command to specify German is Setup.exe /L1031. Note: Not all of the languages referenced in Table 25 on page 88 are supported in the install.

Table 24. (continued)

Parameter	Description
/w : Wait	For a Basic MSI project, the /w argument forces Setup.exe to wait until the installation is complete before exiting. If you are using the /w option in a batch file, you may want to precede the entire Setup.exe command line argument with start /WAIT. A properly formatted example of this usage is as follows: `start /WAIT setup.exe /w`

Table 25.

Language	identifier
Arabic (Saudi Arabia)	1025
Basque	1069
Bulgarian	1026
Catalan	1027
Simplified Chinese	2052
Traditional Chinese	1028
Croatian	1050
Czech	1029
Danish	1030
Dutch (Standard)	1043
English	1033
Finnish	1035
French Canadian	3084
French	1036
German	1031
Greek	1032
Hebrew	1037
Hungarian	1038
Indonesian	1057
Italian	1040
Japanese	1041
Korean	1042
Norwegian (Bokmal)	1044
Polish	1045
Portuguese (Brazilian)	1046
Portuguese (Standard)	2070
Romanian	1048
Russian	1049
Slovak	1051
Slovene	1060

Table 25. (continued)

Language	identifier
Spanish	1034
Swedish	1053
Thai	1054
Turkish	1055

Administrative installation procedure and command-line parameters

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/Client Security Solution installation package, an administrative installation unpacks the installation source files to a specified location. To run an administrative installation the setup package needs to be executed from the command line using the /a parameter:

```
Setup.exe /a
```

Launching an administrative installation presents a series of dialog screens prompting the administrative user to specify the location to unpack the setup files. The default extract location that is presented to the administrative user is C:\. A new location can be chosen which may include drives other than C: (such as, other local drives and mapped network drives). New directories can also be created during this step.

If an administrative installation is run silently, the public property TARGETDIR can be set on the command line to specify the extract location:

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

Once an administrative installation has been completed, the administrative user can make customizations to the source files, such adding additional settings to tvt.txt. 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. The following section describes the available command line parameters that can be used with msiexec as well as an example of how to use it. Public properties can also be set directly in the msiexec command-line call.

MsiExec.exe command-line parameters

MsiExec.exe is the executable program of the Windows Installer used to interpret installation packages and install products on target systems:

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

The following table provides a detailed description of MsiExec.exe command line parameters. This table is taken directly from the Microsoft Platform SDK documentation on the Windows Installer.

Table 26.

Parameter	**Description**

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

f [p|o|e|d|c|a|u|m|s|v] *package* or *product code*	Installing with the /f option will repair or reinstall missing or corrupted files.
	For example, to force a reinstall of all files, use the following syntax:
	`msiexec /fa "C:\WindowsFolder\Profiles\UserName\`
	`Personal\MySetups\Othello\Trial Version\Release`
	`\DiskImages\Disk1\Othello Beta.msi"`
	in conjunction with the following flags:
	• p reinstalls a file if it is missing
	• o reinstalls a file if it is missing or if an older version of the file is present on the user's system
	• e reinstalls a file if it is missing or if an equivalent or older version of the file is present on the user's system
	• c reinstalls a file if it is missing or if the stored checksum of the installed file does not match the new file's value
	• a forces a reinstall of all files
	• u or m rewrite all required user registry entries
	• s overwrites any existing shortcuts
	• v runs your application from the source and re-caches the local installation package

/a *package*	The /a option allows users with administrator privileges to install a product onto the network.
/x *package* or *product code*	The /x option uninstalls a product.
/L [i|w|e|a|r|u|c|m|p|v|+] *log file*	Building with the /L option specifies the path to the log file—these flags indicate which information to record in the log file: • i logs status messages • w logs non-fatal warning messages • e logs any error messages • a logs the commencement of action sequences • r logs action-specific records • u logs user requests • c logs initial user interface parameters • m logs out-of-memory messages • p logs terminal settings • v logs the verbose output setting • + appends to an existing file • * is a wildcard character that allows you to log all information (excluding the verbose output setting)

Table 26. (continued)

Parameter	Description
/q [n|b|r|f]	The /q option is used to set the user interface level in conjunction with the following flags: • q or qn creates no user interface • qb creates a basic user interface The user interface settings below display a modal dialog box at the end of installation: • qr displays a reduced user interface • qf displays a full user interface • qn+ displays no user interface • qb+ displays a basic user interface
/? or /h	Either command displays Windows Installer copyright information
TRANSFORMS	Use the TRANSFORMS command-line parameter to specify any transforms that you would like applied to your base package. Your transform command-line call might look something like this: `msiexec /i "C:\WindowsFolder\Profiles\UserName\ Personal\MySetups\Your Project Name\Trial Version \My Release-1\DiskImages\Disk1\ProductName.msi" TRANSFORMS="New Transform 1.mst"` You can separate multiple transforms with a semicolon. Because of this, it is recommended that you do not use semicolons in the name of your transform, as the Windows Installer service will interpret those incorrectly.
Properties	All public properties can be set or modified from the command line. Public properties are distinguished from private properties by the fact that they are in all capital letters. For example, COMPANYNAME is a public property. To set a property from the command line, use the following syntax: PROPERTY=VALUE. If you wanted to change the value of COMPANYNAME, you would enter: `msiexec /i "C:\WindowsFolder\Profiles\UserName \Personal\MySetups\Your Project Name\Trial Version\My Release-1\DiskImages\Disk1\ProductName.msi" COMPANYNAME="InstallShield"`

Standard Windows Installer public properties

The Windows Installer has a set of standard built in public properties that can be set on the command line to specify certain behavior during the installation. The most common public properties used in the command line are described below. More documentation is available on Microsoft's website at: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/about_properties.asp

Table 27 shows the commonly used Windows Installer properties:

Table 27.

Property	Description
TARGETDIR	Specifies the root destination directory for the installation. During an administrative installation this property is the location to copy the installation package.
ARPAUTHORIZEDCDFPREFIX	URL of the update channel for the application.
ARPCOMMENTS	Provides Comments for the Add or Remove Programs on Control Panel.
ARPCONTACT	Provides Contact for the Add or Remove Programs on Control Panel.
ARPINSTALLLOCATION	Fully qualified path to the application's primary folder.
ARPNOMODIFY	Disables functionality that would modify the product.
ARPNOREMOVE	Disables functionality that would remove the product.
ARPNOREPAIR	Disables the Repair button in the Programs wizard.
ARPPRODUCTICON	Specifies the primary icon for the installation package.
ARPREADME	Provides a ReadMe for the Add or Remove Programs on Control Panel.
ARPSIZE	Estimated size of the application in kilobytes.
ARPSYSTEMCOMPONENT	Prevents display of application in the Add or Remove Programs list.
ARPURLINFOABOUT	URL for an application's home page.
ARPURLUPDATEINFO	URL for application-update information.
REBOOT	The REBOOT property suppresses certain prompts for a reboot of the system. An administrator typically uses this property with a series of installations to install several products at the same time with only one reboot at the end. Set REBOOT="R" to disable any reboots at the end of an install.
INSTALLDIR	This property contains the default destination folder for the files in your features and components.

Client Security Software custom public properties

The install package for the Client Security Software 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 28.

Property	Description
EMULATIONMODE	Specifies to force the installation in Emulation mode even if a 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 install from enabling the TPM
NOPRVDISK	Set NOPRVDISK=1 on the command line to prevent the SafeGuard PrivateDisk feature from being installed. This is meant to be used with a silent installation but can be used with a UI installation as well. In the UI installation, the SafeGuard PrivateDisk feature will not show up in the custom setup screen.
NOPWMANAGER	Set NOPWMANAGER=1 on the command line to prevent Password Manager feature from being installed. This is meant to be used with a silent installation but can be used with a UI installation as well. In the UI installation, the Password Manager feature will not show up in the custom setup screen.
NOCSSWIZARD	Set NOCSSWIZARD=1 on the command line to prevent the CSS Wizard from being displayed when an admin user logs on and has not been enrolled. This property is meant for someone who wants to install CSS, but use scripting later on to actually configure the system.
CSS_CONFIG_SCRIPT	Set CSS_CONFIG_SCRIPT=”*filename*” or “*filename password*” to have a configuration file run after the user completes the install and reboots.
SUPERVISORPW	Set SUPERVISORPW=”*password*” on the command line to supply the supervisor password to enable the chip in silent or non-silent install 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.

Installation log file

A log file cssinstall60.log is created in the %temp% directory if the setup is launched by setup.exe (either double clicking the main install exe, run the main exe without parameters, or extract msi and execute setup.exe). 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 examples using setup.exe:

Table 29.

Description	Example
Silent Install with no Reboot	`setup.exe /s /v"/qn REBOOT="R""`
Administrative Install	`setup.exe /a`
Silent Administrative Install specifying the extract location	`setup.exe /a /s /v"/qn TARGETDIR="F:\CSS60""`
Silent Uninstall setup.exe /s /x /v/qn	`setup.exe /s /x /v/qn`
Install with no Reboot and create an installation log in temp directory	`setup.exe /v"REBOOT="R" /L*v %temp%\cssinstall60.log"`
Install without installing the predesktop setup.exe /vPDA=0	`setup.exe /vPDA=0`

The table below shows installation examples using Client Security Solution.msi:

Table 30.

Description	Example
Install	`msiexec /i "C:\CSS60\Client Security Solution.msi"`
Silent Install with no Reboot	`msiexec /i "C:\CSS60\Client Security Solution.msi" /qn REBOOT="R"`
Silent Uninstall	`msiexec /x "C:\CSS60\Client Security Solution.msi" /qn`

System Migration Assistant installation

The System Migration Assistant installation procedure is documented in the *System Migration Assistant User's Guide*.

Fingerprint Software installation

The Fingerprint Software program setup.exe file can be started with the following parameters:

Silent install

Silent installation of the fingerprint software is also possible. Run Setup.exe in the Install directory on your CD-ROM drive.

Use the following syntax:

```
Setup.exe PROPERTY=VALUE /q /i
```

where *q* is for silent install and *i* is for install. For example:

```
Setup.exe INSTALLDIR="F:\Program Files\IBM fingerprint software" /q /i
```

To uninstall the software, use the /x parameter instead:

```
Setup.exe INSTALLDIR="F:\Program Files\IBM fingerprint software" /q /x
```

SMS install

SMS Installations are also supported. Open SMS Administrator Console, create a new package and set package properties in a standard way. Open the package and select New-Program in the Programs item. At the command line type:

```
Setup.exe /m yourmiffilename /q /i
```

You can use the same parameters as used for the silent install.

Setup normally reboots at the end of installation process. If you want to suppress all reboots during installation and reboot later (after installing more programs), add REBOOT=″ReallySuppress″ to the list of properties.

Options

The following options are supported by the Fingerprint Software:

Table 31.

Parameter	**Description**
CTRLONCE	Used to display the Control Center only once. The default is 0.
CTLCNTR	Used to run the Control Center on startup. the default is 1.
DEFFUS	• 0 = will not use Fast User Switching (FUS) settings • 1 = Will try to use FUS settings. The default is 0.
INSTALLDIR	The default fingerprint software installation directory
OEM	• 0 = install support for server passports/server authentication • 1 = Only standalone-computer mode with local passports
PASSPORT	Th default passport type set during installation. • 1 = Default - Local passport • 2 = Server passport The default is 1.

Table 31. (continued)

Parameter	Description
SECURITY	• 1 - = Install support for the secure mode • 0 = Do not install; only convenient mode exists
SHORTCUTFOLDER	Default name for shortcut folder in the Start menu
REBOOT	Can be used to suppress all reboots including prompts during installation by setting to ReallySuppress.

Installed Software scenarios

Table 32.

Installed Software	Notes®
Client Security Software Version 5.4x	This is the only version of CSS supported for coexistence with Rescue and Recovery.
Rescue and Recovery Version 3.0 only	• Install via full product installation, with CSS deselected. • Some core Client Security Solution components are installed in the RnR-only install to support encryption of backups with the TPM, and for PDA Master Password configuration.
Client Security Solution Version 6.0 Standalone	• This is a separate installation package • You cannot install the full product and deselect Rescue and Recovery to get Client Security Solution only • CSS components (Private Disk and Password Manager) are optional.
Rescue and Recovery Version 3.0 and Client Security Solution Version 6.0	• Preload default - Install via normal product install • CSS components • Private Disk and Password Manager, are optional components

Software state modification

Table 33.

If installed software is....	And you wish to move to.....	Follow this process.....	Notes	Build
Client Security Software Version 5.4x	Client Security Software 5.4x and Rescue and Recovery Version 3.0	• Install product. • Only Rescue and Recovery component will be installed (no custom configuration screen displayed). • When prompted, indicate that you wish to keep Client Security Software installed.	• Client Security Software hooks for Rescue and Recovery are implemented using emulation mode • Only Master Password via Client Security Software is available in this mode	011
Client Security Software	Client Security Solution 6.0	• Uninstall Client Security Software 5.4x • Install Client Security Solution 6.0 Standalone	Attempting to install Client Security Solution Version 6.0 over Client Security Software Version 5.4x is not allowed. User is prompted to remove the old Client Security Software first	011
Client Security Software	Rescue and Recovery Version 3.0 and Client Security Solution Version 6.0	• Uninstall Client Security Software 5.4x • Install product.	Attempting to install the product over Client Security Software Version 5.4x will prompt about removing Client Security Software Version 5.4x first. If install proceeds without uninstall, only Rescue and Recovery will be installed.	011

Table 34.

If installed software is....	And you wish to move to.....	Follow this process.....	Notes	Build
Rescue and Recovery Version 3.0	Client Security Software 5.4x and Rescue and Recovery Version 3.0	• Uninstall Rescue and Recovery • Install Client Security Software Version 5.4x • Install the product as described above	• Client Security Software Version 5.4x cannot install over any product install. • Local backups are deleted during Rescue and Recovery Version 3.0 uninstall	011

Table 34. (continued)

If installed software is....	And you wish to move to.....	Follow this process.....	Notes	Build
Rescue and Recovery Version 3.0	Client Security Solution 6.0	• Uninstall Rescue and Recovery Version 3.0 • Install Client Security Solution Version 6.0 Standalone	• The uninstall of Rescue and Recovery Version 3.0 will delete user files and CSS registry settings. • Rescue and Recovery Version3.0 Backups protected with CSS will no longer be accessible. • Local backups are deleted during Rescue and Recovery Version 3.0 uninstall • Client Security Software Version 6.0 standalone install not permitted over any product install. • The 'Modify' option in Add/Remove Programs will only allow addition of Client Security Solution in this case. Rescue and Recovery cannot be removed via the 'Modify' option.	012
Rescue and Recovery Version 3.0	Rescue and Recovery Version 3.0 and Client Security Solution Version 6.0	• Select 'Modify' option from Add/Remove Programs. • Add CSS and any additional components.	• Local backups are deleted when CSS is added. • User will be warned when adding Client Security Solution that they should take new backups after adding Client Security Solution. • Client Security Solution settings and data files are deleted when Client Security Solution is added. • Client Security Solution Version 6.0 standalone install not permitted over any product install.	TBD

Table 35.

If installed software is....	And you wish to move to.....	Follow this process.....	Notes	Build
Client Security Solution Version 6.0 Standalone	Client Security Software 5.4x	• Uninstall Client Security Solution Version 6.0 • Install Client Security Software Version 5.4x	• Client Security Solution Version 5.4x cannot install over any product install. • The uninstall of Client Security Solution Version 6.0 will prompt for deletion of data files and settings. The option selected here does not impact Client Security Software Version 5.4x operation.	011
Client Security Solution Version 6.0 Standalone	Rescue and Recovery Version 3.0	• Uninstall Client Security Solution Version 6.0 • Install product and choose Rescue and Recovery only	• The uninstall of Client Security Solution Version 6.0 will prompt about deleting Client Security Solution Version user files and settings. • The install of Rescue and Recovery 3.0 will prompt the user to remove any existing Client Security Solution user files and settings. If the user does not choose to remove the files, the install will be cancelled.	012

Table 35. (continued)

If installed software is....	And you wish to move to.....	Follow this process.....	Notes	Build
Client Security Solution Version 6.0 Standalone	Rescue and Recovery Version 3.0 and Client Security Solution Version 6.0	• Run product install • Rescue and Recovery and Client Security Solution options cannot be deselected • Previously installed Client Security Solution components (Password Manager and Private Disk) selected by default, but can be deselected. Components not previously installed will be deselected by default, but can be selected.	• Client Security Solution Version 6.0 Standalone will be uninstalled behind the scenes. • Client Security Solution Version 6.0 data files and settings will be preserved. • Emulation/non-emulation state will be preserved. • After the product install is complete, Client Security Solution Wizard will not run because Client Security Solution was previously configured. • Option to protect Rescue and Recovery backups with Client Security Solution must be done via Rescue and Recovery GUI. There will be an option to run the Rescue and Recovery GUI after reboot on the last install screen • After install of the product, options in Add/Remove Programs include 'Remove', 'Repair' and 'Modify'. • The installed version of Client Security Solution Version 6.0 must be equal or less than the version of the product being installed, otherwise the user will get a message that the product cannot be installed.	012

Notes:

1. If the user installs Rescue and Recovery 3.0 silently, the Client Security Solution user files and settings are deleted automatically during the install.
2. In this scenario, the selection or de-selection of Password Manager and Private Disk during the product install (Rescue and Recovery 3.0 and Client Security Solution 6.0) determines the final state of the component after the product install. For exammple, if Password Manager was installed with Client Security Solution 6.0 and the user deselects it during the product install, it will no

longer be installed after the install completes. If running the product (Rescue and Recovery and Client Security Solution) install silently, both Password Manager and Private Disk are installed unless the respective properties NOPRVDISK=1 or NOPWMANAGER=1 are set in the install command.

Table 36.

If installed software is....	And you wish to move to.....	Follow this process.....	Notes	Build
Rescue and Recovery Version 3.0 and Client Security Solution Version 6.0	Client Security Software 5.4x	• Uninstall product • Install Client Security Solution Version 5.4x	• Client Security Software Version 5.4x cannot install over any product install. • The uninstall of the product will prompt for deletion of data files and settings. The option selected here does not impact Client Security Software Version 5.4x operation.	011
Rescue and Recovery Version 3.0 and Client Security Solution Version 6.0	Rescue and Recovery Version 3.0	• Select 'Modify' option from Add/Remove Programs. • Remove Client Security Solution.	• Local backups are deleted when Client Security Solution is removed. • Uninstall of Client Security Solution will warn about loss of PrivateDisk and Password Manager. • Rescue and Recovery Version 3.0 Backups protected with Client Security Solution will no longer be accessible. • Client Security Solution settings and data files will be deleted when Client Security Solution is removed from 'Modify'.	TBD Not in Build 12

Table 36. (continued)

If installed software is....	And you wish to move to.....	Follow this process.....	Notes	Build
Rescue and Recovery Version 3.0 and Client Security Solution Version 6.0	Client Security Solution Version 6.0	• Uninstall the product. • Uninstall will prompt for deletion of Client Security Solution files and settings. They may be kept if user wishes to maintain existing Client Security Solution configuration. • Install Client Security Solution Version 6.0 standalone	• Uninstall jthe product. • Uninstall will prompt for deletion of Client Security Solution files and settings. They may be kept if user wishes to maintain existing Client Security Solution configuration. • Install Client Security Solution Version 6.0 standalone	012

Notes:

1. During an uninstall of Client Security Solution 6.0 from either Add/Remove Programs or a user interface uninstall from the original source, the user is prompted to delete the CSS settings and data files. If the uninstall is run silently from the command line, the default is to delete the CSS settings and data files, however this action can be overridden by setting the property NOCSSCLEANUP=1 in the uninstall command.
2. During an uninstall of the product (Rescue and Recovery and Client Security Solution 6.0) from either Add/Remove Programs or a user interface uninstall from the original source, the user is prompted to delete the Client Security Solution settings and data files. If the uninstall is run silently from the command line, the default is to delete the Client Security Solution settings and data files, however this action can be overridden by setting the property NOCSSCLEANUP=1 in the uninstall command.

Chapter 7. Antidote Delivery Manager infrastructure

Antidote Delivery Manager works by delivering instructions from an administrator to each system and by supporting commands to combat a virus or a worm. The administrator prepares a script containing the actions desired on each system. The repository function delivers the script securely to the system within minutes and executes the commands. Commands include restricting network connections, displaying messages to the end users, restoring files from backups, downloading files, executing other system commands, and rebooting the machine either to the same operating system or to switch 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 end users if applied during normal working hours. In some circumstances, shifting to the Rescue and Recovery environment can be delayed or avoided by restricting the network capabilities. The next step is to get patches and cleanup code downloaded, 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 next 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.

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, check the signature if supplied and unpack all of the files into a local directory before executing GO.RRS.

The primary command script file (GO.RRS) follows the syntax of a Windows command file. It 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, system's might be grouped geographically be proximity to a file server. Or, systems could be grouped by function, such as engineering, sales, or support.

Antidote Delivery Manager commands and available Windows commands

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

Certain Microsoft commands are also available to Antidote Delivery Manager. The permitted commands include all commands built into command shell, 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.

Typical 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 end user. The easiest way to run this test and also test other scripts before deployment is to place the message in a repository that is a local directory on the administrator's personal computer. This 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

The example demonstrates one possible approach to combate 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**

   The first thing to accomplish is to inform the end user what is about to happen. If the attack is not extremely serious, the administrator can give the end user the option to defer the fix until later. In the most conservative case, this phase would be used to disable networking and provide a short window such as 15 minutes for the end user to save work in progress. RETRYONERROR is used to keep the script running and then the machine 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 end user can log in. Patches should be installed at this time. The machine can be rebooted for a final time if the newly installed patches require it. Now that all cleanup and patching has been completed, the network can be enabled and the end user 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 RETRYONERROR and tag files.

1. **Download Phase**

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

2. **Patch phase**

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

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 prior example does not work because networking is not available in Rescue and Recovery to download files and fixes.

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

Chapter 8. Best Practices

This chapter presents usages scenarios to illustrate the best practices of Rescue and Recovery, Client Security Solution, and ThinkVantage Fingerprint Software. This scenario starts with the configuration of the hard disk drive, continues through several updates, and follows the life cycle of a deployment. Installation on both IBM and non-IBM computers is described.

Deployment examples for installing Rescue and Recovery and Client Security Solution

Here are some examples of installing Rescue and Recovery and Client Security Solution on both a ThinkCentre machine and a ThinkPad.

ThinkCentre Deployment example

This is an example installation of an installation on a ThinkCentre using these hypothetical customer requirements:

- **Administration**
  - Create Sysprep Base Backup with Rescue and Recovery
  - Use local Administrator account for administration of the computer
- **Rescue and Recovery**
  - Use the Client Security passphrase to protect access to the Rescue and Recovery workspace
    - The user must login with their passphrase and will be able to open their SafeGuard PrivateDisk volume file to rescue files
- **Client Security Solution**
  - Install and run in Emulation Mode
    - Not all of the IBM systems have a Trusted Platform Module (security chip)
  - No Password Manager
    - The customer is using an enterprise Single-Sign On solution instead
  - Enable Client Security passphrase
    - Protect Client Security Solution applications via a passphrase
  - Enable Client Security Windows Logon
    - Login to Windows with Client Security passphrase
  - Create SafeGuard PrivateDisk for all users with a size of 500 MB
    - Each user needs 500 MB of space for storing data securely
  - Enable End-User Passphrase Recovery feature
    - Allow users to recover their passphrase by answering three user defined question and answers
  - Encrypt Client Security Solution XML Script with password = “XMLscriptPW”
    - Password protect the Client Security Solution configuration file

On the preparation machine:

1. Login with the Windows “local Administrator” account

2. Install the Rescue and Recovery and Client Security Solution program with the following options:

   ```
   setup_tvtrnr3_1027.exe /s /v"/qn "EMULATIONMODE=1" "NOPWMANAGER=1"
   "NOCSSWIZARD=1""
   ```

   Notes:

   a. Make sure the tvt file or files, such as z062zaa1025us00.tvt are located in the same directory as the executable file or install will fail.
   b. If your file is named setup_tvtrnr3_1027c.exe then you downloaded the combined package. These instructions are for the files that can be downloaded separately from the Large Enterprise individual language files download page.
   c. If you are performing an Administrator install, see "Installing Rescue and Recovery in a new rollout on Lenovo and IBM-branded computers" on page 112.
3. After reboot, login with the Windows local Administrator account and prepare the XML script for deployment. From the command line run this command

   ```
   "C:\Program Files\IBM ThinkVantage\Client Security Solution\css_wizarde.exe"
   /name:C:\ThinkCentre
   ```

   Select the following options in the Wizard:
   - Select **Advanced -> Next**
   - Select **Client Security passphrase -> Next**
   - Select **Log on with the Client Security Login Screen -> Next**
   - Type the Windows password for the Administrator account **-> Next**

     (WPW4Admin for example)
   - Type the Client Security passphrase for the Administrator account, check the **Use the Client Security passphrase to protect access to the Rescue and Recovery workspace** box **-> Next**

     (CSPP4Admin for example)
   - Check the **Enable Password Recovery** box and select three questions and answers for the Administrator account **-> Next**
     a. What was the name of your first pet?

        (Fluffy for example)
     b. What is your favorite movie?

        (Gone With The Wind for example)
     c. What is your favorite athletic team?

        (Washington Redskins for example)
   - Do not check **Create a PrivateDisk volume for each user, with the size selected below**. **-> Next**
   - Review Summary and select **Apply** to write the xml file to the following location C:\ThinkCentre.xml **-> Apply**
   - Select **Finish** to close the wizard.
4. Open the following file in a text editor (XML script editors or Microsoft Word 2003 have built-in XML format capabilities) and modify the following settings:
   - Remove all references to the Domain setting. This will inform the script to use the local machine name on each system instead. Save the file.
5. Use the tool found in C:\Program Files\IBM ThinkVantage\Client Security Solution\xml_crypt_tool.exe to encrypt the XML script with a password. Run the file from a command prompt, use the following syntax:

a. xml_crypt_tool.exe C:\ThinkCentre.xml /encrypt XMLScriptPW
b. The file will now be called C:\ThinkCentre.xml.enc and be protected by the password = XMLScriptPW

The file C:\ThinkCentre.xml.enc is now ready to be added to the deployment machine.

On the deployment machine:

1. Login with the Windows local Administrator account
2. Install the Rescue and Recovery and Client Security Solution programs with the following options:

   ```
   setup_tvtrnr3_1027.exe /s /v"/qn "EMULATIONMODE=1" "NOPWMANAGER=1"
   "NOCSSWIZARD=1""
   ```

   Notes:

   a. Make sure the tvt file or files, such as z062zaa1025us00.tvt are located in the same directory as the executable file or install will fail.
   b. If your file is named setup_tvtrnr3_1027c.exe then you downloaded the combined package. These instructions are for the files that can be downloaded separately from the Large Enterprise individual language files download page.
   c. If you are performing an Administrator install, see “Installing Rescue and Recovery in a new rollout on Lenovo and IBM-branded computers” on page 112.
3. After reboot, login with the Windows Local Administrator account
4. Add the ThinkCentre.xml.enc file prepared earlier to the C:\ root directory
5. Modify the Registry to set the default SafeGuard PrivateDisk Volume Size = 500 MB for all users. This is easily accomplished via importing a *reg* file
   a. Go to: HKEY_LOCAL_MACHINE\SOFTWARE\IBM ThinkVantage\Client Security Software
   b. Create a new String Value with the Value name: = PrivateDiskSize and a Value data: = 500
   c. Create a DWORD Value with the Value name: = UsingPrivateDisk and a Value data: = 1
6. Prepare the RunOnceEx command with the following parameters.
   - Add a new key to RunonceEx key called “0001”. It should be: HKEY_LOCAL_MACHINE \Software\Microsoft\Windows\Current Version\RunOnceEx\0001
   - In that key add a string value name “CSSEnroll” with the value: ″c:\program files\IBM ThinkVantage\Client Security Solution\vmservere.exe” C:\ThinkCenter.xml.enc XMLscriptPW
7. Run “%rr%\rrcmd.exe sysprepbackup location=L name=”Sysprep Backup”. After it has prepared the system you will see this output:

   ```
   **********************************************************
   ** 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.            **
   **********************************************************
   ```
8. Run your Sysprep implementation now.
9. Shutdown and reboot your machine. It will start the backup process in Windows PE.

Note: NOTE: It will say restore in progress but a backup is occurring. After the backup, TURN THE POWER™ OFF, do not restart.

Sysprep Base Backup is now complete

Thinkpad Deployment Example

This is an example installation of an installation on a ThinkPad using these hypothetical customer requirements:

- **Administration**
  - Install on systems already imaged and deployed
  - Use the domain Administrator account for administration of the computer
  - All computers have a BIOS supervisor password, BIOSpw
- **Client Security Solution**
  - Leverage the Trusted Platform Module
    - All machines have the security chip
  - Enable Password Manager
  - Disable SafeGuard PrivateDisk
    - Leveraging Utimaco SafeGuard Easy full hard drive encryption instead
  - Leverage User's Windows Password as authentication to Client Security Solution
    - Allows for single Windows password for authentication to Utimaco SafeGuard Easy, Client Security Solution and Windows Domain
  - Encrypt the Client Security Solution XML Script with password = "XMLscriptPW"
    - The password protects the Client Security Solution configuration file
- **ThinkVantage Fingerprint Software**
  - Do not want to leverage BIOS and Hard Drive passwords
  - Logon with Fingerprint
    - After an initial period for self-user enrollment, the user will switch to Secure Mode logon requiring a Fingerprint for non-Administrator users, thus effectively enforcing a dual factor authentication methodology
  - Include the Fingerprint Tutorial
    - The end-users can learn how to properly swipe their finger and get visual feedback on what they may be doing wrong

On the preparation machine:

1. From the off state, start the computer and press **F1** to go into BIOS and navigate to the security menu and clear the Security Chip. Save and exit the BIOS
2. Login with the Windows Domain Administrator account
3. Install the ThinkVantage Fingerprint Software Running the f001zpz2001us00.exe to extract the setup.exe file from the web package. This will automatically extract the setup.exe to the following location: C:\IBMTOOLS\APPS\TFS4.6-Build1153\Application\0409\setup.exe.
4. Install ThinkVantage Fingerprint Tutorial by running the f001zpz7001us00.exe to extract the tutess.exe file from the web package. This will automatically extract the setup.exe to the following location: C:\IBMTOOLS\APPS\tutorial\TFS4.6-Build1153\Tutorial\0409\tutess.exe.

5. Install ThinkVantage Fingerprint Console by running the f001zpz5001us00.exe to extract the fprconsole.exe file from the web package. Running f001zpz5001us00.exe will automatically extract the setup.exe to the following location: C:\IBMTOOLS\APPS\fpr_con\APPS\UPEK\FPR Console\TFS4.6-Build1153\Fprconsole\fprconsole.exe.
6. Install the Client Security Solution program with the following options:

   ```
   setup_tvtcss6_1027.exe /s /v"/qn NOPRVDISK=1 NOCSSWIZARD=1 SUPERVISORPW=
   "BIOSpw""
   ```
7. After rebooting, login with the Windows Domain Administrator account and prepare the XML script for deployment. From the command line run:

   ```
   "C:\Program Files\IBM ThinkVantage\Client Security Solution\css_wizard.exe"
   /name:C:\ThinkPad
   ```

   Select the following options in the Wizard to match the example script:
   - Select Advanced **-> Next**
   - Select Windows password **-> Next**
   - Select Log on with the fingerprint sensor **-> Next**
   - Type the Windows password for the Domain Administrator account **-> Next** (WPW4Admin for example)
   - • Uncheck Enable Password Recovery **-> Next**
   - • Review the Summary and select Apply to write the xml file to the following location C:\ThinkPad.xml
   - • Select **Finish** to close the wizard
8. Use the tool found at C:\Program Files\IBM ThinkVantage\Client Security Solution\xml_crypt_tool.exe to encrypt the XML script with a password. From a command Prompt, use the following syntax:
   a. xml_crypt_tool.exe C:\ThinkPad.xml /encrypt XMLScriptPW
   b. The file will now be called C:\ThinkPad.xml.enc and be protected by the password = XMLScriptPW

On the deployment machine:

1. Using your company's software distribution tools, deploy the ThinkVantage Fingerprint Software executable setup.exe that was extracted from the preparation machine to each deployment machine. When the setup.exe is pushed to the machine, install using the following command:

   ```
   setup.exe CTLCNTR=0 /q /i
   ```
2. Using your company's software distribution tools, deploy the ThinkVantage Fingerprint Tutorial executable tutess.exe that was extracted from the preparation machine to each deployment machine. When the tutess.exe is pushed to the machine, install using the following command:

   ```
   tutess.exe /q /i
   ```
3. Using your company's software distribution tools, deploy the ThinkVantage Fingerprint Console executable fprconsole.exe that was extracted from the preparation machine to each deployment machine.
   - Place the fprconsole.exe file in the "C:\Program Files\ThinkVantage Fingerprint Software\" directory
   - Turn off BIOS Power-on security support by running the following command: fprconsole.exe settings TBX 0
4. Using your company's software distribution tools, deploy the ThinkVantage Client Solution executable "setup_tvtcss6_1027.exe"

- When the setup_tvtcss6_1027.exe is pushed to the machine, install via the following command: setup_tvtcss6_1027.exe /s /v"/qn NOPRVDISK=1 NOCSSWIZARD=1 SUPERVISORPW="BIOSpw""
- The installation of the software will automatically enable the Trusted Platform Module hardware.

5. After rebooting the system, configure the system via the XML script file via the following procedure:
   - Copy the ThinkPad.xml.enc file prepared early to the C:\ directory.
   - Run C:\Program Files\IBM ThinkVantage\Client Security Solution\vmserver.exe C:\ThinkPad.xml.enc XMLScriptPW
6. After a Reboot, the system is now ready for Client Security Solution user enrollment. Each user can log into the system with their User ID and Windows password. Every user that logs into the system will automatically be prompted to enroll into Client Security Solution and then be able to enroll into the fingerprint reader.
7. After all users for the system have been enrolled in the ThinkVantage Fingerprint Software, the Secure Mode setting can be enabled to force all Windows Non-Administrator users to logon with their fingerprint.
   - Run the following command: C:\Program Files\ThinkVantage Fingerprint Software\fprconsole.exe settings securemode 1
   - To remove the message Press CTRL+ALT+DEL to logon using a password. From the logon screen, run the following command:

     ```
     C:\Program Files\ThinkVantage Fingerprint Software\fprconsole.exe settings
     CAD 0
     ```

Deployment of Client Security Solution 6.0 and ThinkVantage Fingerprint Software is now complete.

Installing Rescue and Recovery in a new rollout on Lenovo and IBM-branded computers

This section describes installing Rescue and Recovery in a new rollout.

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, you must clean out the Master Boot Record on the primary hard disk.

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

   Attention: Running this command will erase the entire contents of the target hard disk drive. After running, you will be unable to recover any data from the target hard disk drive.
2. Create a DOS boot diskette and place the 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.

Installation

This first step in the install process is 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 install time on each machine by roughly one-half.

1. Assuming that the install file is located in the root of the C drive, create a file EXE_EXTRACT.CMD, which will extract the file C:\SETUP_TVTRNR3_*XXXX*.EXE (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 install.
   @ECHO OFF
   :: This is the name of the EXE (Without the .EXE)
   set BUILDID=setup_tvtrnr3_1027.exe
   :: This is the drive letter for the Setu_tvtrnr3_1027.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
   :: Note: The TVT.TXT file must be copied into the same directory as the
   :: MSI.EXE file.
   start /WAIT %SOURCEDRIVE%\%BUILDID%.exe /a /s /v"/qn TARGETDIR=c:\RRTemp"
   Copy Z062ZAA1025US00.TVT C:\rrtemp\
   ```

2. You can make many customizations prior to the installation of Rescue and Recovery. Some examples in this scenario are:
   - Change maximum number of incremental backups to 4.
   - Set Rescue and Recovery to perform an incremental backup every day at 1:59 p.m. to the local hard disk and call it Scheduled.
   - Hide the Rescue and Recovery user interface to all users not in the local Administrators Group.
3. Create a custom TVT.TXT file. Some parameters can be modified. See Appendix B, "TVT.TXT settings and values," on page 131 for more information.

   ```
   [Scheduler]
   Task1=RescueRecovery
   Task2=egatherer
   Task3=logmon

   [egatherer]
   ScheduleMode=0x04
   Task=%TVT%\Rescue and Recovery\launcheg.exe
   ScheduleHour=0
   ScheduleMinute=0
   ScheduleDayOfTheWeek=0
   ScheduleWakeForBackup=0


   [RescueRecovery]
   LastBackupLocation=1
   CustomPartitions=0
   Exclude=0
   Include=0
   MaxNumberOfIncrementalBackups=5
   EncryptUsingCSS=0
   HideCSSEncrypt=0
   UUIDMatchRequired=0
   PasswordRequired=0
   DisableSchedule=0
   ```

```
DisableRestore=0
DisableSFR=0
DisableViewBackups=0
DisableArchive=0
DisableExclude=0
DisableSingleStorage=0
DisableMigrate=0
DisableDelete=0
DisableAnalyze=0
DisableSysprep=1
CPUPriority=3
Yield=0
Ver=4.1
DisableBackupLocation=0
DeletedBackupLocation=0
HideLocationNotFoundMsg=0
HideMissedBackupMessage=0
HideNoBatteryMessage=0
SkipLockedFiles=0
DisableBootDisc=0
DisableVerifyDisc=0
HideAdminBackups=0
HideBaseFromDelete=0
HidePasswordProtect=0
HideSuspendCheck=1
HideBootUSBDialog=0
HideBootSecondDialog=1
HideNumBackupsDialog=1
HidePasswordPersistence=0
HideDiffFilesystems=0
PwPersistence=0
ParseEnvironmentVariables=1
MinAnalyzeFileSize=20
HideLockHardDisk=1
LockHardDisk=0
ResumePowerLossBackup=1
MinPercentFreeSpace=0
MaxBackupSizeEnforced=0
PreRejuvenate=
PreRejuvenateParameters=
PreRejuvenateShow=
PostRejuvenate=
PostRejuvenateParameters=
PostRejuvenateShow=
RunSMA=1
SPBackupLocation=0
ScheduleMode=4
ScheduleFrequency=2
ScheduleHour=12
ScheduleMinute=0
ScheduleDayOfTheMonth=0
ScheduleDayOfTheWeek=3
ScheduleWakeForBackup=0
Task=%TVT%\Rescue and Recovery\rrcmd.exe
TaskParameters=BACKUP location=L name="Scheduled" scheduled
SetPPArchiveBeforeBackup=1

[RestoreFilesFolders]
WinHiddenFolders=%RRBACKUPS%,%MININT%,%PREBOOT%,%HIBERFIL%,%PAGEFILE%,
%SYSVOLINFO%,%RECYCLER%
PEHiddenFolders=%RRBACKUPS%,%MININT%,%PREBOOT%,%HIBERFIL%,%PAGEFILE%,
%SYSVOLINFO%,%RECYCLER%,Z:\
AllowDeleteC=FALSE

[logmon]
ScheduleMode=0x010
Task=%TVT%\Common\Logger\logmon.exe
```

4. In the same directory as the custom TVT.TXT file, create a INSTALL.CMD file, which will perform several actions:
   - Copy the custom TVT.TXT file into the install package created in the C:\RRTemp directory:
   - Perform a silent install 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 TVT.txt here
copy tvt.txt "c:\RRTemp\Program Files\IBM ThinkVantage\Rescue and Recovery"
:: Install using the MSI with no reboot (Remove "REBOOT="R"" to force a reboot)
start /WAIT msiexec /i "c:\TVTRR\Rescue and Recovery - client security
 solution.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\IBM
ThinkVantage\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=%PATH%;%SystemDrive%\Program Files\IBM ThinkVantage\Common\Python24
set PATHEXT=%PATHEXT%;.PYW;.PYO;.PYC;.PY
set TCL_LIBRARY=%SystemDrive%\Program Files\IBM ThinkVantage\Common\Python24
\tcl\tcl8.4
set TK_LIBRARY=%SystemDrive%\Program Files\IBM ThinkVantage\Common\Python24
\tcl\tk8.4
set PYTHONCASEOK=1
set RR=C:\Program Files\IBM ThinkVantage\Rescue and Recovery\
set PYTHONPATH=C:\Program Files\IBM ThinkVantage\Common\logger
:: The next line will create the ISO silently and not burn it
C:\Program Files\IBM ThinkVantage\Common\Python24\python C:\Program Files\IBM
ThinkVantage\Common\spi\mkspiim.pyc /scripted
:: Take the base backup... service must be started
c:
cd "C:\Program Files\IBM ThinkVantage\Rescue and Recovery"
RRcmd.exe backup location=L name=Base level=0
:: Reboot the system
C:\Program Files\IBM ThinkVantage\Common\BMGR\bmgr32.exe /R
```

Customization

You have deployed Rescue and Recovery in your environment and you want like to change the following items with Rescue and Recovery :

- You want more than 4 incremental backups and would like to change it to 10.
- The backup time of 1:59 p.m. interferes in some way with your environment. You would like to change the time to 10:24 a.m.
- You want to allow all users on your systems to access the Rescue and Recovery 3.0 user interface.

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

To make these changes on multiple machines:

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

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

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

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

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 system.

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 18 for more information.

To modify the Pre Desktop 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 Pre Desktop 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 PEACCESSIBMEN.INI file:

1. Change the line:

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

   TO

   ```
   button13 = 8, "Open browser", Internet.bmp, 1, 1, 0,
   %sysdrive%\Preboot\Opera\Opera.EXE,
    http://www.ibm.com/thinkvantage
   ```
2. Put the new version into the directory structure for placing files into the Rescue and Recovery environment. For details, refer to "Using RRUTIL.EXE" on page 18.
3. Reboot the system into the Rescue and Recovery environment.
4. You have done some analysis and determined that there are files that you must back up and there are other files that do not need to be backed up because they reside on the server and can be obtained after a system restore. To do this, you create a custom IBMFILTER.TXT file. This file is placed in a directory with the NSF.CMD file, which copies it into the proper location as shown in the following example:

   NSF.CMD:

   ```
   copy ibmfilter.txt "%RR%"
   ```

   IBMFILTER.TXT:

   ```
   x=*.nsf
   ```

Table 37. UPDATE_RR.CMD script

```
@ECHO OFF
::Obtain the PEAccessIBMen.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\PEAccessIBMen.ini
```

File will open automatically

```
pause
:: Make a copy of original file
copy
c:\RRDeployGuide\GuideExample\RROriginal\preboot\usrintfc\PEAccessIBMen.ini
c:\RRDeployGuide\GuideExample\RROriginal\preboot\usrintfc\
PEAccessIBMen.original.ini
notepad
c:\RRDeployGuide\GuideExample\RROriginal\preboot\usrintfc\PEAccessIBMen.ini
pause
copy c:\RRDeployGuide\GuideExample\RROriginal\preboot\usrintfc\
PEAccessIBMen.ini c:\RRDeployGuide\GuideExample\put\preboot\usrintfc
:: Place the updated version of the PEAccessIBMen 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\IBM ThinkVantage\Common\BMGR\bmgr32.exe /bw /r
```

Create GETLIST.TXT:

```
\preboot\usrintfc\PEAccessIBMen.ini
```

Installing of Rescue and Recovery on non-IBM branded computers

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

Some 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 hel[ensure Rescue and Recovery provides the desired functions and features:

Best practices for hard drive setup: Scenario 1

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

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

   ```
   Error 1722. There is a problem with this Windows
   Installer package. A program run as part of the
   setup did not finish as expected. Contact your
   personnel or package vendor.
   ```

If you are using an OEM image for the base 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 file available from the administrative tools section at:

   `http://www.lenovo.com/ThinkVantage`

   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: Scenario 2

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

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

Creating a bootable Rescue and Recovery CD

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

Because of the resources involved, only one instance of the CD burning application may be running at any given time. If it is running, attempting to start a second instance will produce an error message and the second instance will abort. In addition, due to the nature of accessing protected areas of the hard drive, only administrators can create the ISO; however, a limited end user can burn the ISO to a CD. These files and directories will be included on the recovery CD:

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

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

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

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

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

```
:: Set up the environment
set PATH=%PATH%;%SystemDrive%\Program Files\IBM ThinkVantage\Common\Python24
set PATHEXT=%PATHEXT%;.PYW;.PYO;.PYC;.PY
set TCL_LIBRARY=%SystemDrive%\Program Files\IBM ThinkVantage\Common\Python24
\tcl\tcl8.4
set TK_LIBRARY=%SystemDrive%\Program Files\IBM ThinkVantage\Common\Python24
\tcl\tk8.4
set PYTHONCASEOK=1
set RR=c:\Program Files\IBM ThinkVantage\Rescue and Recovery\
set PYTHONPATH=C:\Program files\IBM ThinkVantage\Common\logger
:: The next line will create the ISO silently and not burn it
c:\Program Files\IBM ThinkVantage\Common\Python24\python c:\Program Files\
IBM ThinkVantage\Common\spi\mkspiim.pyc /scripted
:: The next line will create the ISO with user interaction and not burn it
:: c:\Program Files\IBM ThinkVantage\Common\Python24\python c:\Program Files\
IBM ThinkVantage\Common\spi\mkspiim.pyc /scripted
/noburn
```

Installing Rescue and Recovery into 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 on the C:\ drive. You can use bmgr32 /info to determine where the type 12 partition resides on the HDD. For more information, see "Rescue and Recovery Boot Manager control (BMGR32)" on page 150.

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, restore the SP™.PQI file to the unallocated free-space.
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.

Switching Client Security Solution modes

If you switch the Client Security Solution mode from convenient to secure or vice-versa, and you are using Rescue and Recovery to backup your system, you should take a new base backup.

Sysprep Backup/Restore

Note that Password Persistence will not work with Sysprep Backup/Restore.

You should power off and reboot the system after completing a Sysprep Backup.

Computrace and Rescue and Recovery

On non-BIOS systems, Rescue and Recovery cannot be uninstalled once Computrace is installed.

Chapter 9. Fingerprint Software

The fingerprint console must be run from the Fingerprint Software installation folder. The basic syntax is FPRCONSOLE [USER | SETTINGS]. The USER or SETTINGS command specifies what set of operation will be used. The full command is then e.g. “fprconsole user add TestUser /FORCED”. When the command is not known or not all parameters are specified short command list is shown together with the parameters.

To download the Fingerprint Software and Management Console please use the following link

http://www.lenovo.com/think/support/site.wss/document.do?sitestyle=lenovo &indocid=TVAN-EAPFPR

User-specific commands

To enroll or edit users the USER section is used. When the current user does not have administrator’s rights the console behavior depends on the security mode of the FS. Convenient mode: ADD, EDIT and DELETE commands are possible for standard user. However the user can modify only his own passport (enrolled with his username). Secure mode: no commands are allowed. Syntax:

```
FPRCONSOLE USER command
```

where *command* is one of the following commands: ADD, EDIT, DELETE, LIST, IMPORT, EXPORT.

Table 38.

Command	Syntax	Description	Example

Enroll new user	`ADD [`*username* `[|` *domain*`\`*username*`]] [/FORCED]`	The /FORCED flag will disable the cancel button of the wizard so the enrollment must be then successfully finished. If the user name is not specified then the current user name is used.	`fprconsole add domain0\testuser`
			`fprconsole add testuser`
			`fprconsole add testuser /FORCED`

Edit enrolled user	`EDIT [`*username* `[|` *domain*`\`*username*`]]`	If the user name is not specified then the current user name is used.
		Note: The edited user must verify his fingerprint first .
			`fprconsole edit domain0\testuser`
			`fprconsole edit testuser`

Delete a user	`DELETE [`*username* `[|` *domain*`\`*username* `| /ALL]]`	The /ALL flag will delete all users enrolled on this computer. If the user name is not specified then the current user name is used	`fprconsole delete domain0\testuser`
			`fprconsole delete testuser`
			`fprconsole delete /ALL`

Enumerate enrolled users	`List`		

Table 38. (continued)

Command	Syntax	Description	Example
Export enrolled user to a file	`Syntax: EXPORT username [| domain\username] file`	This command will export an enrolled user to a file on the HDD. The user then can be imported using the IMPORT command on other computer or on the same computer if the user is deleted.	
Import enrolled user	`Syntax: IMPORT` *`file`*	The import will import the user from the specified file. **Note:** If the user in the file is already enrolled on the same computer using the same fingerprints then it is not guaranteed which user will have a precedence in the identification operation.	

Global settings commands

The global settings of the Fingerprint Software can be changed by the SETTINGS section. All the commands in this section need administrator's rights. The syntax is:

```
FPRCONSOLE SETTINGS command
```

where *command* is one of the following commands: SECUREMODE, LOGON, CAD, TBX, SSO.

Table 39.

Command	Description	Syntax	Example
Security mode	This setting switches between Convenient and Secure mode of the Fingerprint Software.	`SECUREMODE 0|1`	To set to convenient mode: `fprconsole settings securemode 0`
Logon type	This setting enables (1) or disables (0) the logon application. If the /FUS parameter is used the logon is enabled in Fast User Switching mode if the computer configuration allows this.	`LOGON 0|1 [/FUS]`	
CTRL+ALT+DEL message	This setting enables(1) or disables(0) the "Press CTRL+ALT+DEL" text in logon.	`CAD 0|1`	

Table 39. (continued)

Command	Description	Syntax	Example
Power-on security	This setting globally turns off (0) power-on security support in the fingerprint software. When the power-on security support is turned off no power-on security wizards or pages are shown and it does not matter what are the BIOS settings.	`TBX 0|1`	
Power-on security single sign-on	This setting enables(1) or disables(0) the usage of fingerprint used in BIOS in logon to automatically logon user when the user was verified in BIOS.	`SSO 0|1`	

Secure vs. Convenient mode

ThinkVantage Fingerprint Software can be run in two security modes, a convenient mode, and a secure mode.

The convenient mode is intended for home computers where a high security level is not so important. All the users can perform all operations, including editing passports of other users and possibility to log on to the system using password (without fingerprint authentication).

The secure mode is intended for situations when you want to achieve higher security. Special functions are reserved for administrators only. Only administrators can log on using password, without additional authentication.

An *Administrator* is any member of local Administrators group. After you set the secure mode, only administrator can toggle it back to the simple mode.

Secure Mode – Administrator

At Logon the Secure Mode displays the following message if the wrong user name or password is typed: ″Only administrators can log on this computer with user name and password.″ This is done to enhance security and avoid giving hackers information about why they are unable to logon.

Table 40.

Fingerprints	Description
Create a new passport	Administrators can create their own passport and they can also create the passport of a limited user.
Edit Passports	Administrators can edit *only* their own passport

Table 40. (continued)

Fingerprints	**Description**
Delete Passport	Administrators can delete all limited user and other administrator passports. If other users are using power-on security, the administrator will have the option to remove user templates from power-on security at this time.
Power-on Security	Administrators can delete Limited user and Administrator fingerprints used in power-on. **Note:** There must at least be one fingerprint present when power-on mode is enabled.
Settings	
Logon settings	Administrators can make changes to all logon settings
Protected screen saver	Administrators can access
Passport type	Administrators can access - Only relevant with server.
Security mode	Administrators can toggle between Secure and Convenient modes
Pro Servers	Administrators can access - Only relevant with server.

Secure Mode - Limited user

During a Windows logon, a Limited user must use a fingerprint to logon. If their fingerprint reader is not working, an administrator will need to change the fingerprint software setting to convenient mode to enable user name and password access.

Table 41.

Fingerprints	
Create a new passport	Limited user cannot access
Edit Passports	Limited user can edit only their own passport
Delete Passport	Limited user can delete only their own passport
Power-on Security	Limited user cannot access
Settings	
Logon settings	Limited user cannot modify Logon settings
Protected screen saver	Limited user can access
Passport type	Limited user cannot access
Security mode	Limited user cannot modify security modes
Pro Servers	Limited user can access - Only relevant with server.

Convenient Mode - Administrator

During a Windows logon, administrators can logon using either their user name and password or their fingerprint. .

Table 42.

Fingerprints	
Create a new passport	Administrators can create *only* their own passport
Edit Passports	Administrators can edit *only* their own passport
Delete Passport	Administrators can delete *only* their own passport
Power-on Security	Administrators can delete Limited user and Administrator fingerprints used in power-on. **Note:** There must be at least one fingerprint present when power-on mode is enabled.
Settings	
Logon settings	Administrators can make changes to all logon settings
Protected screen saver	Administrators can access
Passport type	Administrators can access - Only relevant with server
Security mode	Administrators can toggle between Secure and Convenient modes
Pro Servers	Administrators can access - Only relevant with server.

Convenient Mode - Limited User

During a Windows logon, Limited users can logon using either their user name and password or their fingerprint.

Table 43.

Fingerprints	
Create a new passport	Limited users can create only their own password.
Edit Passports	Limited users can edit only their own passport
Delete Passport	Limited users can delete only their own passport
Power-on Security	Limited users can delete only their own fingerprints.
Settings	
Logon settings	Limited users cannot modify Logon settings
Protected screen saver	Limited users can access
Passport type	Limited users cannot access - Only relevant with server
Security mode	Limited users cannot modify security modes

Table 43. (continued)

Fingerprints	
Pro Servers	Limited usesr can access - Only relevant with server.

ThinkVantage Fingerprint Software and Novell Netware Client

ThinkVantage Fingerprint Software and Novell user names and passwords must match.

If you have ThinkVantage Fingerprint Software installed on your computer and then install the Novell Netware Client, some items in the registry might be overwritten. If you encounter problems with ThinkVantage Fingerprint Software logon, go to the Logon settings screen and re-enable the Logon Protector.

If you have the Novell Netware Client installed on your computer but have not logged on to the client prior to installing the ThinkVantage Fingerprint Software, the Novell Logon screen will display. Provide the information requested by the screen.

To change Logon Protector Settings:

- Start the Control Center.
- Click **Settings**
- Click **Logon settings**
- Enable or disable Logon Protector.

  If you want to use fingerprint logon, check the Replace Windows logon with fingerprint-protected logon check box. Note that Enabling and disabling Logon Protector requires a reboot.
- Enable or disable fast user switching, when supported by your system.
- (Optional feature) Enable or disable automatic logon for a user authenticated by power-on boot security.
- Set Novell logon settings. The following settings are available when logging on to a Novell network:
  - **Activated**

    ThinkVantage Fingerprint Software automatically provides known credentials. If the Novell logon fails, the Novell Client logon screen is displayed along with a prompt to enter the correct data.
  - **Ask during logon**

    ThinkVantage Fingerprint Software displays the Novell Client logon screen and a prompt to enter the logon data.
  - **Disabled**

    ThinkVantage Fingerprint Software does not attempt a Novell logon.

Appendix A. Installation command-line parameters

The Microsoft Windows Installer provides several administrator functions through command-line parameters.

Administrative installation procedure and command-line parameters

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.

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

  ```
  Setup.exe /a
  ```

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

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

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

  Or

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

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

Using MSIEXEC.EXE

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

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

Note: Enter the above command as a single line with no spaces following the slashes.
Table 44 on page 128 describes the available command line parameters that can be used with MSIEXEC.EXE and examples of how to use it.

Table 44. Command line parameters

Parameter	Description

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

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

Table 44. Command line parameters (continued)

Parameter	Description

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

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

Appendix B. TVT.TXT settings and values

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

Table 45. TVT.TXT settings and values

Setting	Values
AccessFile (see GUIGroup)	*filename*, where *filename* is the fully qualified path to a file that contains the names of Windows local groups (not domain groups) that are permitted to perform Rescue and Recovery operations. If blank or missing, all users who can log onto the computer can launch the GUI and perform command line operations. By default the file is blank.
BackupPartition	1 = First partition on a specified drive 2 = Second partition on a specified drive 3 = Third partition on a specified drive 4 = Fourth partition on a specified drive Drives are specified in the following sections: [BackupDisk] = local hard disk drive [SecondDisk] = second local hard disk drive [USBDisk] = USB hard disk drive **Note:** Partitions must already exist. If not set, the user will be prompted to establish the partition (if there is more than one partition on the destination drive when the destination drive is selected in the user interface).
BatteryPercentRequired	Range is from 0 to 100. The default is 100.
CPUPriority	*n* where *n* = 1 to 5; 1 is the lowest priority and 5 is highest priority. The default is 3.
CustomPartitions -	0 = Back up every partition 1 = Look at IncludeInBackup in each partition
DisableAnalyze	0 = Enable analyze 1 = Disable analyze The default is 0.
DisableArchive	0 = Enable archive 1 = Disable archive The default is 0.

Table 45. TVT.TXT settings and values (continued)

Setting	Values
DisableBackupLocation	0 = Enable all destination 0x01 = Disable Local destination 0x02 = Disable Cd/DVD drive 0x08 = Disable USB/ HDD 0x10 = Disable Network 0x20 = Disable second HDD These can be combined to grey out multiple locations. For example, a value of 0x0A would disable CD/DVD and USB HDD, value of 0x38 would disable USB HDD, Network, and the second HDD. To only enable backup to local hard drive, you can use 0x3A (or even 0xFE))
DisableBootDisc	0 = Create bootable CD when creating CD/DVD backups 1 = Do not create bootable CD The Disable Boot Disc function is only for Backups not for Archive
DisableDelete	0 = Show delete backups option 1 = Hide this option The default is 0.
DisableExclude	0 = Show exclude file/folders option 1 = Hide exclude file/folders option The default is 0.
DisableLiveUpdate	0 = Show LiveUpdate option 1 = Hide this option The default is 0.
DisableMigrate	0 = Show create migration file from backup 1 = Hide this option The default is 0.
DisableRestore	0 = Enable restore 1 = Hide restore The default is 0.
DisableSchedule	0 = Show backup schedule option 1 = Hide backup schedule option The default is 0.
DisableSFR	0 = Enable single file restore 1 = Hide single file restore The default is 0.

Table 45. TVT.TXT settings and values (continued)

Setting	Values
DisableSingleStorage	0 = Show single storage option 1 = Hide this option The default is 0.
DisableViewBackups	0 = Show view backups option 1 = Hide this option The default is 0.
DisableVerifyDisc	0 = Verify optical write operations 1 = Don't verify optical write operations The default is 0.
Exclude (see Include)	0 = Do not apply GUIEXCLD.TXT 1 = Apply GUIEXCLD.TXT.txt **Notes:** 1. Exclude and select files can be defined prior to installation and be applied during the installation process. 2. Exclude and Include cannot both be 1.
GUIGroup (see AccessFile)	*group*, where *group* is a Windows local group (not a domain group) that is permitted to perform Rescue and Recovery operations. The list of privileged groups is stored in a file that is defined by the AccessFile entry.
HideAdminBackups	0 = Show administrator backups in list. 1 = Hide administrator backups. The default is 0.
HideBaseFromDelete	0 = Show base backup on Delete Backups dialog. 1 = Hide base backup on Delete Backups dialog. The default is 0.
HideBootUSBDialog	0 = Show prompt if backing up to a USB HDD and it's not bootable 1 = Hide prompt The default is 0.
HideDiffFileSystems	0 = Show FAT/FAT32 partitions when restoring/saving files 1 = Hide FAT/FAT32 partitions when restoring/saving files The default is 0.
HideCSSEncrypt	0 = Don't hide Encrypt backups using Client Security Solution 1 = Hide Encrypt backups using Client Security Solution The default is 0.
HideGUI	0 = Show the GUI to authorized users 1 = Hide the GUI from all users

Table 45. TVT.TXT settings and values (continued)

Setting	Values
HideLocationNotFoundMessage	0 = Show dialog message 1 = Hide dialog message The default is 0.
HideLockHardDisk	0 = Show protect hard disk from MBR corruption option 1 = Hide this option The default is 1.
HideMissedBackupMessages	0 = Show dialog box 1 = Hide dialog box The default is 0.
HideNoBatteryMessage	0 = Display message 1 = Hide message The default is 1
HideNumBackupsDialog	0 = Don't hide the dialog showing the user when they've reached the maximum number of backups 1 = Hide the dialog showing the user when they've reached the maximum number of backups The default is 1
HidePowerLossBackupMessage	0 = Show power loss with backup message 1 = Hide message The default is 0.
HidePasswordPersistence	0 = Hide GUI 1 = Sow GUI The default is 0.
HidePasswordProtect	0 = Show password protect checkbox. 1 = Hide password protect check box. The default is 0.
HideSuspendCheck	0 = Don't hide wake computer from suspend/hibernation check box 1 = Hide check box The default is 1.
Include (see Exclude)	0 = Do not apply GUIINCLD.TXT 1 = Apply GUIINCLD.TXT and display the option to set include files and folders **Notes:** 1. Exclude and select files can be defined prior to installation and be applied during the installation process. 2. Exclude and Include cannot both be 1.

Table 45. TVT.TXT settings and values (continued)

Setting	**Values**
LocalBackup2Location	*x*\foldername where *x* = the drive letter and *foldername* is any fully qualified folder name.) The default is this: `*1st partition letter on the second drive*:\IBMBackupData` **Notes:** 1. Because the drive letter can change over time, Rescue and Recovery will associate the drive letter to a partition at the time of install, and then use the partition information rather than the drive letter. 2. This is the location field of the `TaskParameters` entry.
LockHardDisk	0 = Don't lock the hard disk to protect the MBR, 1 = Lock the hard disk The default is 0.
MaxBackupSizeEnforced	*x*, where *x* is the size in GB. This value will not prevent a backup from exceeding this threshold. If the threshold is exceeded, however, the user will be warned about the file size the next time an "On Demand" backup is taken. The default is 0.
MaxNumberOf IncrementalBackups	default = 5, min = 2, max = 32
MinAnalyzeFileSize *n*	Where *n* is the minimum file size in MB to display a file to the user on the "Optimize backup storage space" screen. The default is 20
NetworkUNCPath	Network share using the format: `\\*computername*\*sharefolder*` There is no default. **Note:** This location will not be protected by the File Filter Driver.
NetworkUNCPath	*server share name*, for example, \\MYSERVER\SHARE\FOLDER
NumMinutes	*x*, where the task runs after *x* minutes have passed.
PasswordRequired	0 = No password required to open the Rescue and Recovery environment. 1 = Password required to open the Rescue and Recovery environment.
PDAPreRestore	*cmd*, where *cmd* is a fully qualified path to the program to run in the Rescue and Recovery environment prior to a restore operation.
PDAPreRestore *n*	*cmd*, where *cmd* is a fully qualified path to the program to run in the Rescue and Recovery environment prior to a restore operation.
PDAPreRestoreParameters	Parameters to be used in the PDARestore program.
PDAPreRestoreParameters *n*	Parameters to be used in the PDARestore program.
PDAPreRestoreShow	0 = Hide task 1 = Show task

Table 45. TVT.TXT settings and values (continued)

Setting	Values
PDAPreRestoreShow *n*	0 = Hide task 1 = Show task
PDAPostRestore	*cmd*, where *cmd* is a fully qualified path to the program to run in the Rescue and Recovery environment prior to a restore operation.
PDAPostRestore *n*	*cmd*, where *cmd* is a fully qualified path to the program to run in the Rescue and Recovery environment prior to a restore operation.
PDAPostRestoreParameters	Parameters to be used in the PDARestore program.
PDAPostRestoreParameters *n*	Parameters to be used in the PDARestore program.
PDAPostRestoreShow	0 = Hide task 1 = Show task
PDAPostRestoreShow *n*	0 = Hide task 1 = Show task
Post (see PostParameters)	*cmd*, where *cmd* is a fully qualified path to an executable file to run after to the primary task.
Post (see PostParameters) *n*	Where *n* is the backup number 0, 1, 2, 3...32 *cmd*, where *cmd* is a fully qualified path to an executable file to run after to the primary task. For example: • Post0=command.bat *path* This runs after base backup • Post1=command.bat *path* This runs after incremental backup **Note:** This is for Backup only
PostParameters (see Post)	*cmd*, where *cmd* is a fully qualified path to an executable file to run after to the primary task. This is for Backup only.
PostParameters *n* (see Post)	`parms`, where *parms* are parameters to be used in the post-task
	parms, where *parms* are parameters to be used in the post-task. **Note:** This is for Backup only
PostRestore	*cmd*, where *cmd* is a fully qualified path to the program to run in Windows after a restore operation has been completed
PostRestore *n*	*cmd*, where *cmd* is a fully qualified path to the program to run in Windows after a restore operation has been completed
PostRestoreParameters	Parameters to be used in the PostRestore program
PostRestoreParameters *n*	Parameters to be used in the PostRestore program
PostRestoreShow	0 = Hide restore-task 1 = Show restore-task
PostRestoreShow *n*	0 = Hide restore-task 1 = Show restore-task

Table 45. TVT.TXT settings and values (continued)

Setting	Values
PostShow	0 = Hide post-task 1 = Show post-task The default is 0.
PostShow *n*	0 = Hide post-task 1 = Show post-task The default is 0. Where *n* is the backup number 0, 1, 2, 3....32 **Note:** This is for Backup only
Pre (see PreParameters)	*cmd*, where *cmd* is a fully qualified path to an executable file to run prior to the primary task.
Pre (see PreParameters) *n*	Where *n* is the backup number 0, 1, 2, 3....32 *cmd*, where *cmd* is a fully qualified path to an executable file to run before to the primary task. For example: • Pre0=command.bat *path* This runs before base backup • Pre1=command.bat *path* This runs before incremental backup **Note:** This is for Backup only.
PreParameters (see Pre)	Where *parms* are the parameters to be used in the pre-task
PreRejuvenate *cmd*	Where *cmd* is the fully qualified path to the program to run in Windows prior to a rejuvenate operation
PreRejuvenateParameters *parms*	Where *parms* are the parameters to be used in the PreRejuvenate program.
PreRejuvenateShow	0 = Hide task 1 = Show task
PostRejuvenate *cmd*	*cmd*, where *cmd* is the fully qualified path to the program to run in Windows after a rejuvenate operation
PostRejuvenateParameters *parms*	Where *parms* are the parameters to be used in the PostRejuvenate program.
PostRejuvenateShow	0 = Hide task 1 = Show task
PreShow	0 = Hide pre-task 1 = Show pre-task The default is 1.
PreShow *n*	Where *n* is the backup number 0, 1, 2, 3....32 *cmd*, where *cmd* is a fully qualified path to an executable file to run before to the primary task. **Note:** This is for Backup only

Table 45. TVT.TXT settings and values (continued)

Setting	**Values**
PreWinRestore	*cmd*, where *cmd* is a fully qualified path to the program to run in Windows prior to a restore operation.
PreWinRestore *n*	*cmd*, where *cmd* is a fully qualified path to the program to run in Windows prior to a restore operation.
PreWinRestoreParameters	Parameters to be used in the PreWinRestore program
PreWinRestoreParameters *n*	Parameters to be used in the PreWinRestore program
PreWinRestoreShow	0 = Hide post-task 1 = Show post-task
PreWinRestoreShow *n*	0 = Hide post-task 1 = Show post-task
ResumePowerLossBackup	0 = Don't resume the backup process if power was lost in the middle of the last backup 1 = Resume the backup The default is 1.

RunBaseBackup	0 = Do not perform the base backup
	1 = Perform base backup
	The default is 0.
	`runbasebackuplocation=(`*`Location`*`)`
	The values are:
	L = Local
	U = USB
	N = Network
	S = Second HDD
	C = CD

ScheduleDayOfTheMonth	*x*, where *x* is equal to 1 to 28 or 35 for monthly backups only. 35 = the last day of the month
ScheduleDayOfTheWeek	For weekly backups only 0 = Sunday 1 = Monday 2 = Tuesday 3 = Wednesday 4 = Thursday 5 = Friday 6 = Saturday The default is 0 (Sunday).

Table 45. TVT.TXT settings and values (continued)

Setting	**Values**
ScheduleFrequency	0 = Not scheduled 1 = Daily 2 = Weekly 3 = Monthly The default is 2 (weekly).
ScheduleHour	*x*, where *x* is equal to 0 to 23 and 0 is 12:00 AM, 12 is noon, and 23 is 11:00 PM. The default is 0.
ScheduleMinute	*x*, where *x* is equal to 0 to 59 (which increments) represent the minute within the hour to start the incremental backup. The default is 0.
ScheduleWakeForBackup	0 = Do not wake the computer for scheduled backups 1 = Wake the computer, if it is a desktop for scheduled backups, but do not wake notebook computers 2 = Wake the computer regardless of whether it is a desktop or notebook The default is 2. **Note:** If a notebook wakes for a backup, but ac power is not detected, it will return to suspend/hibernate before a backup operation starts.
ScheduleMode	*x*, where *x* is a bit mask with a value of: • 0 = No schedule • 0x01 = Every minute • 0x02 = Every day • 0x04 = Every week • 0x08 = Every month • 0x10 = Every time the service starts (normally every machine boot) • 0x20 = The machine wakes from suspend/hibernate • 0x40 = USB HDD becomes attached • 0x80 = Network becomes attached • 0x100 = Network becomes detached • 0x200 = BIOS Password Reset • 0x400 = Motherboard replacement This parameter is automatically updated when the user changes values in the GUI. If the ScheduleFrequency value is changed by either manual changes to the TVT.TXT file or scripting, reloadsched will update this parameter. **Note:** The `USB HDD becomes attached` or `network becomes attached` bits do not need to be set for automatic synchronization of backups from local hard drive to USB HDD or network.)

Table 45. TVT.TXT settings and values (continued)

Setting	Values
SkipLockedFiles	0 = Display dialog box when a locked and corrupt file is encountered 1 = Always skip locked and corrupt files
SPBackupLocation=2	Used to set the backup of Service Partition. If this setting is not used, the default 500MB Service Partition will be restored when booting CD, restoring CD and other data on the Service Partition is removed.
Task	*cmd*, where *cmd* is a fully qualified path to the program to run as the primary task. **Note:** The number of tasks can be no more than 50.
TaskParameter	*parms* are parameters to be used in the task.
TaskShow	0 = Hide task 1 = Show task The default is 0.
UUIDMatchRequired	0 = Computer UUID match is not required. 1 = Computer UUID match is required. **Note:** Backups that have been captured when the UUIDMatchRequired was set to 1 will continue to require a UUID match, even if this setting is changed later.
Yield	*n* where *n* equals 0 to 8; 0 means that Rescue and Recovery does not yield and 8 means that Rescue and Recovery produces the maximum yield value. **Note:** A higher yield will incrementally slow down backup performance and provide better interactive performance. The default is 0.

After Rescue and Recovery is installed, the following configurations can be altered in the TVT.TXT file that is located in the installed directory. They will be initialized with the values assigned during installation.

TVT.txt backup and restore

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

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

Scheduling backups and associated tasks

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

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

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

```
[SCHEDULER]

Task1=rescuerecovery

[rescuerecovery]

Task="c:\program
files\ibm\Rescue and Recovery\

rrcmd.exebackup.bat"

TaskParameters=BACKUP
location=L name="Scheduled"

ScheduleFrequency=2

ScheduleDayOfTheMonth=31

ScheduleDayOfTheWeek=2

ScheduleHour=20

ScheduleMinute=0

ScheduleWakeForBackup=0

Pre="c:\program files\antivirus\scan.exe"

Post="c:\program files\logger\log.bat"
```

Managing different TVT.txt files

Since hard disk drives can have multiple partitions, the backup and restore program needs to know which partition will store the backup data. If a particular destination has multiple partitions and backup operations will be scripted, the following setting needs to be configured prior to the backup operation. If the backup operation can be initiated by the user, you can ignore this section.

For backups to the local hard drive, the configuration setting is found in the TVT.TXT file in the BackupDisk section. Backups to the second local hard drive use the SecondDisk section, and backups to the USB HDD would use the USBDisk section as shown:

```
BackupPartition=x
```

where *x* is a range of 0 - 3, where 0 represents the first partition on the appropriate drive).

Note: partitions must already exist. If not set, the user will be prompted, if there's more than one partition, when the appropriate destination is selected in the GUI For example: if it was desired to backup to the second partition on the USB HDD, then the TVT.TXT file entry would look like this:

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

Mapping a network drive for backups

The map network drive function relies on the MAPDRV.INI file which is located in the C:\Program Files\IBM ThinkVantage\Common\MND directory. All information is stored in the DriveInfo section.

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:

```
[DriveInfo]

UNC=\\server\share

NetPath=\\9.88.77.66\share

User=11622606415119207723014918505422010521006401209203708202015...

Pwd=11622606415100000000014918505422010521006401209203708202015...
```

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

Setting up user accounts for network backups

When the 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.

Appendix C. Command-line tools

ThinkVantage Technologies features can also be invoked locally or remotely by corporate IT administrators through the command-line interface. Configuration settings can be maintained through remote text file settings.

Antidote Delivery Manager

Mailman

This uses the command C:\program files|IBM ThinkVantage\Rescue and Recovery\ADM\mailman.exe. This program will check the Antidote Repository for tasks to be run. There are no command-line arguments.

Antidote wizard

This command, AWizard.exe is located wherever the administrator installs it. There are no command-line arguments.

Set Passwords

For a discussion about passwords, see "Passwords" on page 31.

CFGMOD

CFGMOD provides a method of updating the TVT.TXT file via a script. The CFGMOD command can be found in the C:\Program Files\IBM ThinkVantage\Rescue and Recovery\ directory. If you modify the backup schedule this command must be followed by RELOADSCHED. This utility must be run with administrator privileges.

Syntax:

```
cfgmod TVT.TXT mod file
```

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

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

Client Security Solution

The Client Security Solution has the following command-line tools:

SafeGuard PrivateDisk

The command-line interface is located in the C:\Program Files\IBM ThinkVantage\SafeGuard PrivateDisk\ folder. The syntax is:

```
PDCMD
 [ADDCERT volumename /pw adminpassword /sn certSN [/acc access]]  |
 [LIST]  |
 [MOUNT volumename [/pw userpassword [/pt authmode]] [/ro]]  |
 [NEW volumename [/sz size] [/dl driveletter] [/fs filesystem]
   [/pw adminpassword] [/pwu userpassword]]  |
 [UNMOUNT volumename /f]  |
 [UNMOUNTALL [/f]]  |
 [SETPASSWORD volumename /pw adminpassword /pwu userpassword [/ro]]
```

The parameters are shown in Table 46:

Table 46.

Parameter	Result
ADDCDERT	Adds certificate to PrivateDisk volume
LIST	Lists PrivateDisk volumes for this user
MOUNT	Mounts a specific PrivateDisk volume
NEW	Creates a new PrivateDisk volume
UNMOUNT	Unmounts a particular PrivateDisk volume
UNMOUNTALL	Unmounts all PrivateDisk volumes
SETPASSWORD	Sets user password on a PrivateDisk volume
volumename	The name of the file that contains the PrivateDisk files
pw	The password
sn	The serial number of the certificate.
acc	The access type of the certificate to be added. Valid values are: • **adm** administrator access • **uro** user read-only access • **usr** user write access (default)
pt	Method of authentication. Valid values are: • **0** Administrator access (default) • **1** User password • **2** PIN for a certificate-based login
ro	Read only
sz	Size (in Kbyes
dl	Drive letter for the PrivateDisk volume (default=next available drive letter)
fs	The File System. Default values are: • FAT (default) • NTFS
pwu	User password
f	Force operation

Security Advisor

To run this from the GUI, click **Start->Programs->ThinkVantage->Client Security Solution**. Click **Advanced**, and choose **Audit Security Settings**. It runs C:\Program Files\IBM ThinkVantage\Common\WST\wst.exe for a default installation.

The parameters are:

Table 47.

Parameters	Description
HardwarePasswords	1 will show this section, 0 will hide. The default is 1.
PowerOnPassword	Sets value that a PowerOn password should be enabled, or setting will be flagged.
HardDrivePassword	Sets value that a Hard Drive password should be enabled, or setting will be flagged.
AdministratorPassword	Sets value that a Administrator password should be enabled, or setting will be flagged.
WindowsUsersPasswords	Can be 1 or 0, 1 will show this section, 0 will hide. If not present then it is shown by default.
Password	Sets value that the users password should be enabled, or setting will be flagged.
PasswordAge	Sets value of what Windows password age should be on this machine, or setting will be flagged.
PasswordNeverExpires	Sets value that windows password can never expire, or setting will be flagged.
WindowsPasswordPolicy	Can be 1 or 0, 1 will show this section, 0 will hide. If not present then it is shown by default.
MinimumPasswordLength	Sets value of what password length should be on this machine, or setting will be flagged.
MaximumPasswordAge	Sets value of what password age should be on this machine, or setting will be flagged
ScreenSaver	Can be 1 or 0, 1 will show this section, 0 will hide. If not present then it is shown by default.
ScreenSaverPasswordSet	Sets value that screen saver should have password, or setting will be flagged.
ScreenSaverTimeout	Sets value of what screensaver timeout should be on this machine, or setting will be flagged.
FileSharing	Can be 1 or 0, 1 will show this section, 0 will hide. If not present then it is shown by default.
AuthorizedAccessOnly	Sets value that authorized access should be set for filesharing, or setting will be flagged.

Table 47. (continued)

Parameters	Description
ClientSecurity	Can be 1 or 0, 1 will show this section, 0 will hide. If not present then it is shown by default.
EmbeddedSecurityChip	Sets value that security chip should be enabled, or setting will be flagged.
ClientSecuritySolution	Sets value of what version CSS should be on this machine, or setting will be flagged.

Another option for all of the values is ignore, which means show the value, but do not include this value in the comparison. While the Security Advisor is running, there is an HTML file written to c:\ibmshare\wst.html and a raw data XML file written to c:\ibmshare\wst.xml

Example

Here is a [WST] Section that shows all of the sections and has all of the settings set to their default value:

```
[wst]
HardwarePasswords=1
PowerOnPassword=enabled
HardDrivePassword=enabled
AdministratorPassword=enabled

WindowsUsersPasswords=1
Password=enabled
PasswordAge=180
PasswordNeverExpires=false

WindowsPasswordPolicy=1
MinimumPasswordLength=6
MaximumPasswordAge=180

ScreenSaver=1
ScreenSaverPasswordSet=true
ScreenSaverTimeout=15

FileSharing=1
AuthorizedAccessOnly=true

ClientSecurity=1
EmbeddedSecurityChip=Enabled
ClientSecuritySolution=6.0.0.0
```

In order to hide or customize the Security Advisor, add a section in the TVT.txt file name WST. There are several values that can either be hidden or customized, but must be added into the TVT.txt file.

If you don’t want to use the Security Advisor and don’t want it to show up enabled in the GUI, remove the following executable:

```
C:\Program Files\IBM ThinkVantage\Common\WST\wst.exe
```

Certificate Transfer Wizard

If you don’t want to use the Certificate Transfer Wizard and don’t want it to show up enabled in the GUI, remove the following executable:

```
C:\Program Files\IBM ThinkVantage\Client Security Solution
\certificatetransferwizard.exe
```

Client Security Wizard

This Wizard is used to Take Ownership of the hardware, configure the software, and enroll users. It is also used to generate deployment scripts via XML files. The following command can be run to understand the functions of the wizard:

```
C:\Program Files\IBM ThinkVantage\Client Security Solution\css_wizard.exe /?
```

Table 48.

Parameter	Result
/h or /?	Displays the help message box
/name:*FILENAME*	Precedes the fully qualified path and filename for the generated deployment file. The file will have an .xml extension.
/encrypt	Encrypts the script file using AES encryption. The filename will be appended with .enc if it is encrypted. If the /pass command is not used, a static passphrase is used to obscure the file.
/pass:	Precedes the passphrase for protection of the encrypted deployment file.
/novalidate	Disables the Password and Passphrase checking capabilities of the wizard so a script file can be created on a already configured machine. For example, the Administrator password on the current machine might not be the Administrator password desired across the enterprise. Use the /novalidate command to allow you to type a different Administrator password it into the css_wizard GUI during xml file creation.

Here is an example of this command:

```
css_wizard.exe /encrypt /pass:my secret /name:C:\DeployScript /novalidate
```

Note: If the system is running in emulation mode, then the executable name is css_wizarde.exe

Deployment File Encrypt/Decrypt tool

This tool is used to encrypt/decrypt Client Security XML deployment files. The following command can be run to understand the functions of the tool:

```
C:\Program Files\IBM ThinkVantage\Client Security Solution\xml_crypt_tool.exe. /?
```

The parameters are shown in Table 49:

Table 49.

Parameters	Results
/h or /?	Displays the help message
FILENAME	The fully qualified path name and filename with either .xml or .enc extension
encrypt or decrypt	Select /encrypt for .xml files and /decrypt for .enc files

Table 49. (continued)

Parameters	Results
PASSPHRASE	An optional parameter that is required if a passphrase is used to protect the file.

Examples:

```
xml_crypt_tool.exe "C:\DeployScript.xml" /encrypt "my secret"
```

and

```
xml_crypt_tool.exe "C:\DeployScript.xml.enc" /decrypt "my secret"
```

Deployment File processing tool

The tool vmserver.exe processes the Client Security XML deployment scripts. The following command can be run to understand the functions of the wizard:

```
C:\Program Files\IBM ThinkVantage\Client Security Solution\vmserver.exe /?
```

Table 50.

Parameter	Result
FILENAME	The FILENAME parameter must have either an xml or enc file extension
PASSPHRASE	The PASSPHRASE parameter is used to decrypt a file with the enc extension

Here is an example of this command:

```
Vmservere.exe  C:\DeployScript.xml.enc "my secret"
```

Note: If the system is running in emulation mode, then the executable name is vmserver.exe

TPMENABLE.EXE

The TPMENABLE.EXE file is used to turn the security chip on or off.

Table 51.

Parameter	Description
/enable or /disable (Turn on or off the security chip)	Turns the security chip on or off.
/quiet	Hides prompts for BIOS Password or errors
sp:*password*	BIOS Administrator/Supervisor password, don't use quotes around the password

Sample Command:

```
tpmenable.exe /enable /quiet /sp:My BiosPW
```

eGatherer

The eGatherer command can be found in C:\Program Files\IBM ThinkVantage\common\egatherer\egather2.exe.

The egathere2.exe creates an EG2 output with the collected information. It can also create a local XML output file that it stores in the home folder. Note that the EG2 file is an internal format.

Two XML files will be created, one for the system information and one for the demographic information. The name of the XML file is created by combining manufacturer, model-type and serial number.For example: IBM-2373Q1U-99MA4L7.XML, IBM-2373Q1U-99MA4L7.DEMOGRAPHICS.XML .

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

egather2.exe [-help] [-batch] [-silent] [-nolimit] [-local] [-listprobes] [-probe probename *probename*]

- **-help**
  Show a short help message.
- **-batch**
  Do not show the disclaimer.
- **-silent**
  Do no show anything during operation
- **-nolimit**
  Collect entire event log. The default is the last 500 entries.
- **-local**
  Create a local XML file.
- **-listprobes**
  List the probes available.
- **-probe**
  Run the specified probes.

MAPDRV

The MAPDRV command will invoke the user interface to map a network drive. The MAPDRV.EXE command can be found in the C:\Program Files\IBM ThinkVantage\Common\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

Table 52. MAPDRV parameters

Parameter	Result
`/nodrive`	Make network connection without assigning drive letter to the connection
`/pwd`	The password for this user on this share.
`/set`	Sets the share, user and password used by Backup and Restore. The return codes are:

Table 52. MAPDRV parameters (continued)

Parameter	Result
/s	Silent. Do not prompt the user regardless of whether connection is made.
/timeout	Sets the timeout value.
/unc	The sharename of the form \\server\share
/user	The username for this share.

When the /SET command is used the following section will be added to the TVT.TXT file. This is shown in the following example where the /UNC/USER and PWD parameters are used:

```
mapdrv /set /unc sharename /user username /pwd password
[mapdrv]
UNC=\\test\test
User=1EE22597AE4D
PWD=04E22197B34D95943ED5A169A0407C5C
```

Rescue and Recovery Boot Manager control (BMGR32)

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

Table 53. BMGR32 parameters

bmgr32	Result
/B0	Boot to partition 0 (based on the order in the partition table)
/B1	Boot to partition 1
/B2	Boot to partition 2
/B3	Boot to partition 3
/BS	Boot to the Service Partition
/BW	Boot to the Rescue and Recovery protected partition
/BWIN	Reset request to boot to WINPE. This must be called prior to booting.
/CFG*file*	Apply the configuration file parameters. See “RRCMD command-line interface” on page 153 for details regarding the configuration file.
/DS	Return the 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 HDD information (checks for 8 free sectors)
/INFOP	Display HDD information (checks for 16 free sectors)

Table 53. BMGR32 parameters (continued)

bmgr32	Result
`/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- or IBM-brandedPreload Only)
`/OEM`	Computer is not an IBM 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 an MBR patch program can access.
`Patchfile`*filename*	Used for installation program only to install an MBR patch
`/PRTC`	Used for installation program only, to retrieve patch return code
`/IBM`	System is an IBM or Lenovo-branded computer
`/Q`	silent
`/V`	verbose
`/R`	Reboot computer
`/REFRESH`	Reset partition table entries in data sector
`/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
`/F`*mbr*	Load the RRE master boot record program.
`/U`	Unload RRE master boot record program.
`/UF`	Force install or uninstall of MBR program
`/?`	List command-line options.

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

- **Additional MBR**

  Sector numbers containing the MBR, other than the first sector.
- **Data**

  Sector number of the data sector used by the MBR.
- **Patch indices**

  Sector numbers of any patches applied using the MBR.
- **Checksum return**

  This should be 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 MBR is stored.
- **IBM Flag**

  Value from the data sector (1 if IBM or Lenovo-branded system, 0 if not)
- **Boot Config**

  Describes 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**

  This is the number of ¼ seconds to wait if the F11 Message is displayed to the screen.
- **Scan Code**

  Which key is used when booting to the Service Area. 85 is for the F11 key.
- **RR**

  Not used by BMGR, this is set by Rescue and Recovery.
- **Prev Active Part**

  While booted to the Service Area, this value contains the partition table index of the previously active partition.
- **Boot State**

  Used by MBR to determine the current state of the Machine. 0 – Boot normal to OS, 1 – Boot to Service OS, 2 – Boot back to normal OS from Service OS.
- **Alt Boot Flag**

  Boot to alternate OS, DOS for example
- **Previous Partition type**

  When booted to the Service Area, this value contains the partition type that the Service Partition was set to prior to booting to it.
- **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

RELOADSCHED

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

Sample Command:

```
C:\Program Files\IBM ThinkVantage\Rescue and Recovery\reloadsched
```

RRCMD command-line interface

The primary Rescue and Recovery command-line interface is RRCMD. The command is located in the C:\Program Files\IBM ThinkVantage\Rescue and Recovery\reloadsched.exe subdirectory. Refer to the following information to use the command-line interface for Rescue and Recovery.

Syntax:

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

Table 54. 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 will 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 sysprepbackup to the network then the password file will not be written to the backup location until an incremental backup is taken. Here are two workarounds: 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.
`Copy`	Copy backups from one location to another. This is also known as archive, and must include the location.
`Rejuvenate`	Rejuvenate operating system to the specified backup
`Delete`	Delete backups. This must include the location
`Changebase`	Change files in all backups based on file.txt contents. Options in file.txt are: **A** Add **D** Delete **RS** Replace
`migrate`	Create migration file from a backup

Table 54. RRcmd parameters (continued)

Command	Result
`filter=`*`filterfile`*	Identifies what files and folders will be restored and does not alter other files. This 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 HDD **S** For second local hard drive **N** For network **C** For CD/DVD Restore
`name=`*`abc`*	Where *abc* is the name of the backup
`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>`

System Migration Assistant

The module is command-line program compatible with old SMA4.2 SMABAT.EXE. Command parameters and control card (Commands.TXT) to the module should be compatible with SMA 4.2.

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 available update 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\TVT\ActiveUpdate
```

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

To disable Active Update Launcher menu item from help menu for all TVTs:

1. Go to the HKLM\Software\ThinkVantage\ActiveUpdate registry key
2. Rename or delete the ActiveUpdate key

To disable Active Update Launcher menu item from help menu for individual TVT:

1. Go to the registry key:
   - For Rescue and Recovery - HKLM\Software\IBM Thinkvantage\Rescue and Recovery
   - For Client Security - HKLM\Software\IBM Thinkvantage\Client Security Software
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\IBM Thinkvantage\Rescue and Recovery
   - For Client Security - HKLM\Software\IBM Thinkvantage\Client Security Software
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. Currently, only TargetApp (the TVT name) is passed as shown in this example:

```
<root>
      <TargetApp>ACCESSIBM</TargetApp>
</root>
```

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

Appendix D. Administrator tools

ThinkVantage technologies offers tools that can be invoked by corporate IT administrators.

Antidote wizard

For information on the Antidote wizard, see Appendix F, “Antidote Delivery Manager command reference and examples,” on page 163.

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. Example, SafeGuard Easy, SafeBoot, and MBR version of Computrace etc.
2. Tool should be run before installing Rescue and Recovery.
3. Use the cleanmbr.exe for DOS and the CleanMBR32.exe can be used in Windows.
4. After running DOS CleanMBR, run FDISK /MBR; it will put on the MBR.

The parameters for CleanMBR32.exe are:

Table 55.

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

CLEANDRV.EXE

Cleans the drive of all files. There will be no operating system after running this command. See “Installing Rescue and Recovery into a type 12 service partition” on page 120 for more information.

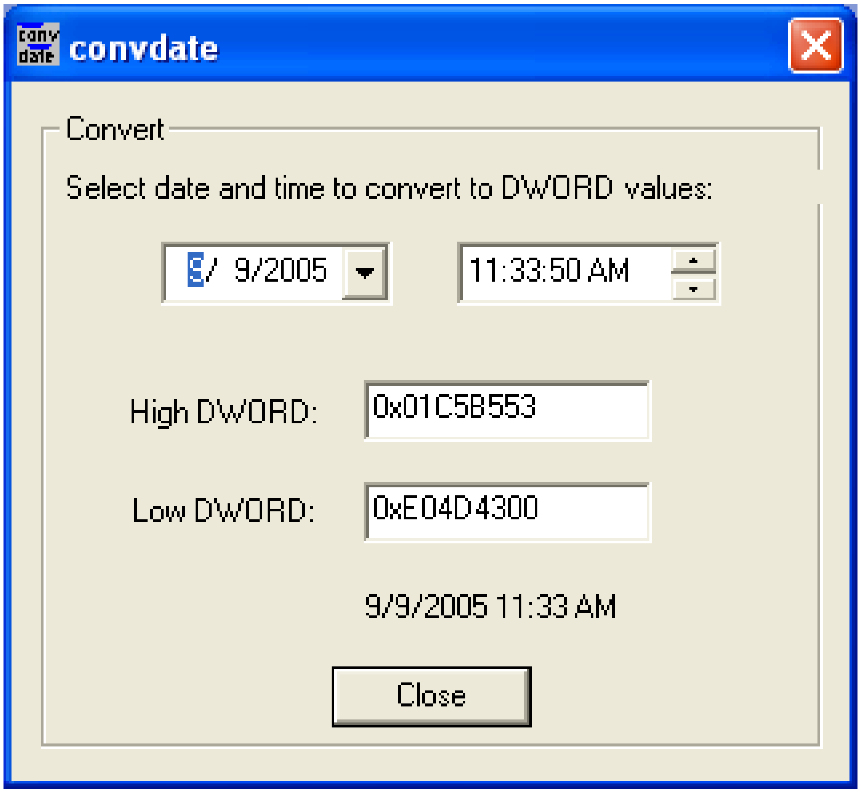
CONVDATE

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 TVT.TXT

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

To run the utility, do the following:

1. Extract the Rescue and Recovery Administration tools from http://www.lenovo.com/thinkvantage
2. Open a CMD windows
3. Type in Convdate



Select date and time to convert to DWORD values:

9/ 9/2005 11:33:50 AM

High DWORD: 0x01C5B553

Low DWORD: 0xE04D4300

9/9/2005 11:33 AM

Figure 5. Convdate window

4. Type in the Date and Time in the fields under Select date and time to convert DWORD Values.
5. The corresponding TVT..TXT file values are:
   - High DWORD=StartTimeHigh
   - Low Dword=StartTimeLow

CREAT SP

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 CREAT SP are:

Table 56.

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

RRUTIL.EXE

For information on the RRUTIL.EXE, see “Predesktop area” on page 17.

SP.PQI

This file can be used to create a Type 12 service partition. See “Installing Rescue and Recovery into a type 12 service partition” on page 120 for more information.

Appendix E. User Tasks

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

Windows XP

The following table presents the tasks that Limited, Power, and Administrative users can perform in Rescue and Recovery in a Windows XP environment.

Table 57. 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 HDD bootable media	No	No	Yes
Initiate backup	Yes	Yes	Yes
Initialize restore in Rescue and Recovery Environment (RRE)	Yes	Yes	Yes
Perform single-file restore in RRE	No (Windows) Yes (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

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 58. 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 HDD bootable media	No	No	Yes
Initiate backup	Yes	Yes	Yes
Initialize restore in Rescue and Recovery Environment (RRE)	Yes	Yes	Yes

Table 58. Windows 2000 user tasks (continued)

Windows 2000 users can perform the following:	**Limited User**	**Power User**	**Administrator**
Perform single-file restore in 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 will enable you to make the required ISO file and it will be automatically be placed in the C:\Program Files\IBM ThinkVantage\Rescue and Recovery\rrcd\ directory:

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

```
C:\Program Files\IBM ThinkVantage\Common\Python24\python" "C:\Program Files\IBM
  ThinkVantage\Common\spi\mkspiim.pyc /scripted


 /scripted
```

```
:: This line will create the ISO with user interaction and not burn it
```

```
C:\Program Files\IBM ThinkVantage\Common\Python24\python C:\Program Files\IBM
  ThinkVantage\Common\spi\mkspiim.pyc /noburn
 /noburn
```

Appendix F. Antidote Delivery Manager command reference and examples

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

Antidote Delivery Manager command guide

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

Table 59. Antidote Delivery Manager commands

Commands	Description
`APKGMES [/KEY keyfile|/NEWKEY keyfile|/NOSIG] message_directory message_name`	For APKGMES /KEY a message file will be created from the contents of *TVT.TXTmessage_directory*. The directory must contain a file named GO.RRS. If the /KEY parameter is used, a signing key will be retrieved from keyfile.prv and the key in keyfile.pub must have been distributed to all clients that will process the message. By default, the key file “KEYFILE.PRV” will be used. The /NEWKEY parameter can be used to create a key. If signing is not desired, specifying /NOSIG will prevent signing. A date stamp will be appended to the end of the message name, 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 execute this script a finite number of times as specified by the retries parameter. If no number is specified, the default value is 3. A global default value can be set in the TVT.TXT file in the rescue section `retries = retries`. Retries can also be set to FOREVER which could cause an infinite loop to occur.

Table 59. Antidote Delivery Manager commands (continued)

Commands	**Description**
`MSGBOX /msg` *message text* `[/head` *header_text*`] [/OK] [/CANCEL]| [/TIMER` *timeout*`] /B3`	The MSGBOX command will display a message to the end user, if logged on. The message will remain displayed and the script will block until time out occurs, the cancel button is pressed or the **OK** button is pushed (if /OK is specified). A cancel button will not be on the panel if /CANCEL is not specified, and it will not be easy to get rid of the display. The command will return: • 0 = OK was pressed • 1 = CANCEL • 2 = Timer expired The text in the message can be formatted using \n and \t to represent newline and tab respectively.
`NETWK [/D|/E|/A [/IP` *ip_address* `| /DN` *domain_name*`] [/NM` *netmask*`]`	NETWK /D (disable) will stop all network traffic by disabling all network adapters. Networking will be disabled until a NETWK /E (enable) command is run. NETWK /A restricts networking to the IP address specified by either the /IP switch (dotted decimal) or /DN (DNS name). The /NM switch provides the network mask. If /NM is not provided, then only the single machine specified by /IP or /DN will be accessible. The state of this command persists over reboots, so networking must be explicitly enabled.
`APUBKEY [/ADD|/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. Be aware that if there are any keys specified in the TVT.TXT, unsigned messages (those built with /NOSIG) can no longer be used.
`AUNCPW [/ADD|/CHANGE|/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 59. Antidote Delivery Manager commands (continued)

Commands	Description
`xmltool.exe` *`filename xpath function comparator value`*	XML tool for conditionals such as eGatherer and current hardware information Where: • **filename** The path and filename to the XML file • **xpath** The fully qualified xpath to the value • **Usage:** xmltool.exe *filename xpath function comparator value* where: – **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 • **Example:** `xmltool.exe %SWSHARE%\\egath.xml //system_summary/bios_version /C GEQ 1UET36WW`

Table 59. Antidote Delivery Manager commands (continued)

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

Supported Microsoft Commands

Table 60. Supported Microsoft commands

Commands	Description
`ATTRIB.EXE`	Displays or changes file attributes
`CACLS.EXE`	Displays or modifies access control liss (ACLs) of files
`CHKDSK.EXE`	Checks a disk and displays a status report
`COMP.EXE`	Compares the contents of two files or sets of files
`COMPACT.EXE`	Displays or alters the compression of files on NTFS partitions
`CONVERT.EXE`	Converts FAT volumes to NTFS. You cannot convert the current drive
`DISKPART.EXE`	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

Table 60. Supported Microsoft commands (continued)

Commands	Description
`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 RR Sorts input
`SORT.EXE`	Sorts input
`SUBST.EXE`	Associates a path with a drive letter
`XCOPY.EXE`	Copies files and directory trees

Preparation and installation

Preparation

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

Configuration

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

Repository

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

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

Schedule Information

The Schedule Mode is the frequency of checks.

Table 61. 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

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

[rescue]
ScheduleFrequency=0
ScheduleMode=0x02
TaskShow=1
Task=c:\Program Files\IBM ThinkVantage\Rescue and Recovery\adm\mailman.exe
ScheduleHour=11
ScheduleMinute=28
ScheduleDayOfTheWeek=3
ScheduleWakeForBackup=0
```

Signing Key

If signing keys will be used, they must be distributed to the client. The file keyfile.pub created by they APKGMES command contains the key. Each authorized public signing key appears in the TVT.TXT file as: `pubkeyX = ...` where *X* is replaced by an integer, and up to 9 public keys can be stored. Use APUBKEY function to set this value `nosig =` If it is set to 1, it will allow unsigned packages (packages built with the /NOSIG parameter) to be run.

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

Network Drives

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

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

Installation on Clients

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

Server Infrastructure

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

Simple System Test – Display Notification

Script Preparation and Packaging

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

Deployment

Before deploying the Antidote Delivery Manager you should perform these steps:

1. Determine locations for the mailboxes:
   - *Mailboxes* are defined as directories on network shares, a local system on HDD or removable media, or on an 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 mailboxes in the TXT.TXT file:
   - On a donor system with Rescue and Recovery installed, edit the TVT.TXT file located in the *C:\Program Files\IBM\ ThinkVantage* directory.
   - Create a new `rescue` section in the TVT.TXT file.
   - Add the following entry in the rescue section:

     ```
     mailbox=
     ```

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

     ```
     [rescue]
     mailbox=C:\ADM\Mailbox,
      \\Network\Share
     ```

     Mailboxes on an FTP site would look like this:

     ```
     ftp://ftp.yourmailbox.com
     ```

     Mailboxes on a shared network drive would look like this:

     ```
     \\Network\Share
     ```

     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://ftp.yourmailbox.com, \\Network\Share
     ```

     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 username and password are required for an FTP or HTTP connection, use this format:

   ```
   ftp//username:password@ftp.yourmailbox.com
   ```
4. For username and password network shares mailboxes:

   Username and password entries are stored encrypted in the TVT.TXT file. To add an entry on the donor system:

a. Open a DOS window

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

c. Run this command:

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

This command creates the following entry in the TVT.TXT file:

```
[RscDrv0]
UNC=\\Network\Share
 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 10 network shares can be used by Antidote Delivery Manager.

c. In addition to the 10 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 59 on page 163.

5. Create the Antidote Delivery Manager Public/Private key pair. We recommend that you 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\IBM ThinkVantage\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\IBM ThinkVantage\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 TVT.TXT in the [rescue] section: `pubkey0=906253....`

- Up to 10 public keys can be stored in the TVT.TXT.
- The APUBKEY.EXE file has other functions which can be used for Public key management. At the command line, enter `APUBKEY /?` or see Table 59 on page 163.

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 20 minutes, the following should be added to the TVT.TXT file on the donor system:

   ```
   [Scheduler]
   Task1=rescuerecovery
   Task2=egatherer
   Task3=rescue

   [rescue]
   ScheduleFrequency=0
   ScheduleMode=0x01
   NumMinutes=20
   TaskShow=1
   Task=C:\Program Files\IBM ThinkVantage\Rescue and Recovery\ADM\antidote
   \mailman.exe
   ```

   where *ScheduleMode* is the event that will trigger the delivery of the Antidote Delivery Manager package. The parameters are:

Table 62. Antidote Delivery Manager parameters

Parameter	Value
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

   Notes:

   a. The scheduler does not run in the Pre_Desktop Area.
   b. For more information, see “Scheduling backups and associated tasks” on page 141.

7. Create an Antidote Delivery Manager package.

   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\IBM ThinkVantage\Rescue and Recovery\ADM
   e. Run this command:

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

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

8. Copy the HELLOPKGYY*MMDDHHMM*.ZAP to a mailbox location specified in step 2.
9. Invoke 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\IBM ThinkVantage\Rescue and Recovery\ADM\mailman.exe

Examples

Following are some examples of ways you can use Antidote Delivery Manager:

Example 1

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

1. Assume the reason the client computer is displaying a blue screen is because of a virus that is executed through the Run Key in the registry. To fix this, a file called go.rrs needs to be created that runs *reg*. See "Supported Microsoft Commands" on page 166 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 IBM button/F11 or the Enter key to enter the Pre_Desktop 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, such as *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.

   ```
   set custos
   if errorlevel 1 set custos=%systemDrive%
   %custos%\Program Files\IBM ThinkVantage\Rescue and Recovery\ADM\retryonerror
   /on 10
   %custos%\Program Files\IBM ThinkVantage\Rescue and Recovery\ADM\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.

Ways to check if a package is completed or not

- **Fail log**

  This file is typically stored in the *c:\ibmtools\utils\rescue\* 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:\ibmshare* 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:\ibmtools\utils\rescue\* 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 Pre_Desktop Area:

1. Define an external Web site for packages:

   ```
   ftp.yourmailbox.com
   ```

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

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

4. When the user presses Access IBM/F11 or the Enter key, to enter the PreDesktopArea, the Antidote Delivery Manager package executes at boot time in the Pre_Desktop 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 execute patch or whatever action
   ```

Major Worm Attack

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

Go.RRS

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

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

inRR.exe
if errorlevel 2 goto ERROR
if errorlevel 1 goto InOS
if errorlevel 0 goto inRR

:InOS
cd
if exist %tagfile% goto DONE

msgbox /msg "Antidote has detected a new message \n  \n ..... \n  \n Don't worry; be Happy!
Antidote will fix your system for you" /ok /timer 30
call nettest.cmd %pingtarg%
set el=%errorlevel%
if %el% == 0 msgbox /msg "Network is working" /timer 5 /head "Correct"
if not %el% == 0 msgbox /msg "Network is disabled" /timer 5 /head Failure
NetWk.exe /d
msgbox.exe /msg "Antidote Recovery Process is running. \n  \n Networking has been disabled." /head
"Networking" /timer 15
call nettest.cmd %pingtarg%
set el=%errorlevel%
if %el% == 0 msgbox /msg "Network is working" /timer 5 /head "Failure"
if not %el% == 0 msgbox /msg "Network is disabled" /timer 5 /head "Correct"
msgbox.exe /msg "System will reboot in 20 seconds \n  \n Press OK to reboot now, or Cancel to
reboot later."
/head "Select Repair Urgency" /timer 20 /ok /cancel
if errorlevel 2 goto PENOW
if errorlevel 1 goto PELATER
if errorlevel 0 goto PENOW

:PENOW
reboot /rr
goto NOT_DONE


:PELATER
%custos%\ibmtools\utils\bmgr32.exe /bw
msgbox.exe /msg "System will apply fix next time you reboot" /head "Reboot" /ok
goto NOT_DONE

:inRR
REM DISABLE NETWORKING
msgbox.exe /msg "Networking will be disabled in 5 seconds. \n  \n  Network disable pending"
/head "Network shutdown" /timer 5
NetWk.exe /d

REM USE EGATHERER VALUES FOR CONDITIONAL BRANCH

msgbox /msg "Checking Registry" /timer 5
```

```
xmltool %ibmshare%\ibmegath.xml //EG_GATHERED_DATA/EG_INSTALLED_MICROSOFT_SOFTWARE/
EG_SOFTWARE_PACKAGE[@ID='DirectX']/EG_VERSION GEQ \"4.09.00.0901\"
if errorlevel 1 goto FILECOPY

msgbox.exe /msg "Applying Registry fix. \n  \n Press OK to continue..." /head "Registry Fixeroo" /ok
reg.exe load HKLM\tempSW %custos%\windows\system32\config\SOFTWARE
reg.exe add "HKLM\tempSW\IBM\eGatherer\Local Viewer\scans\banka" /v benke /d binki /f
reg.exe add "HKLM\tempSW\IBM\eGatherer\Local Viewer\scans\banka" /v bonko /d bunku /f
reg.exe delete "HKLM\tempSW\IBM\eGatherer\Local Viewer\scans\banka" /v bonko /f
reg.exe unload HKLM\tempSW

:FILECOPY
msgbox /msg "Registry Now OK \n  \n Applying Fix" /timer 5
copy payload.txt %custos%\

REM RE-ENABLE NETWORK
msgbox.exe /msg "Networking will be enabled in 5 seconds. \n  \n Network enable pending" /head
"Network shutup" /timer 5
NetWk.exe /e

REM TAG IT
echo 1 > %tagfile%

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

:ERROR
:NOT_DONE
exit 1

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

NETTEST.CMD

```
PING –n 1 %1 > nul 2>&
```

PAYLOAD.TXT

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

Appendix G. 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
500 Park Offices Drive, Hwy 54
Research Triangle Park, NC 27709
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
ThinkPad
ThinkCentre
ThinkVantage
Rapid Restore

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®, and Lotus Notes

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

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

Glossary

Administrator (ThinkCentre)/Supervisor (ThinkPad) BIOS Password. The Administrator or Supervisor password is used to control the ability to change BIOS settings. This includes the capability to enable/disable the embedded security chip and to clear the Storage Root Key stored within the Trusted Platform Module.

Advanced Encryption Standard (AES). *Advanced Encryption Standard* is a *symmetric key* encryption technique. The U.S.government adopted the algorithm as its encryption technique in October 2000, replacing the DES encryption it used. AES offers higher security against brute-force attack than the 56-bit DES keys, and AES can use 128, 192 and 256-bit keys, if necessary.

Cryptography systems. Cryptography systems can be broadly classified into symmetric-key encryption that use a single key that both encrypts and decrypts the data, and Public-key encryption that use two keys, a public key known to everyone and a private key that only the owner of the key pair has access to.

Embedded Security Chip. The embedded security chip is another name for a Trusted Platform Module.

Public-key/Asymmetric-key encryption. Public-key algorithms typically use a pair of two related keys — one key is private and must be kept secret, while the other is made public and can be widely distributed; it should not be possible to deduce one key of a pair given the other. The terminology of ″public-key cryptography″ derives from the idea of making part of the key public information. The term asymmetric-key cryptography is also used because not all parties hold the same information. In a sense, one key ″locks″ a lock (encrypts); but a different key is required to unlock it (decrypt).

Storage Root Key (SRK). The storage root key (SRK) is a 2,048-bit (or larger) public key pair. It is initially empty and is created when the TPM owner is assigned. This key pair never leaves the embedded security chip. It is used to encrypt (wrap) private keys for storage outside the Trusted Platform Module and to decrypt them when they are loaded back into the Trusted Platform Module. The SRK can be cleared by anyone that has access to the BIOS.

Symmetric-key encryption. Symmetric key encryption ciphers use the same key for encryption and decryption of data. Symmetric key ciphers are simpler and faster, but their main drawback is that the two parties must somehow exchange the key in a secure way. Public-key encryption avoids this problem because the public key can be distributed in a non-secure way, and the private key is never transmitted. Advanced Encryption Standard is an example of a symmetric-key.

Trusted Platform Module (TPM). Trusted Platform Modules are special-purpose integrated circuits built into systems to enable strong user authentication and machine verification. The main purpose of the TPM is to prevent inappropriate access to confidential and sensitive information. The TPM is a hardware based root of trust that can be leveraged to provide a variety of cryptographic services on a system. Another name for TPM is the embedded security chip.

ThinkVantage™

Printed in USA