ThinkVantage

Implementierungshandbuch für ThinkVantage Technologies

Inhalt:

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

ThinkVantage

Implementierungshandbuch für ThinkVantage Technologies

Erste Ausgabe (Oktober 2005)

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
ThinkVantage Technologies Deployment Guide,
Teilenummer 41R9863,
herausgegeben von International Business Machines Corporation, USA

Herausgegeben von:
SW TSC Germany
Kst. 2877
Oktober 2005

Inhaltsverzeichnis

Vorwort

Dieses Handbuch richtet sich an IT-Administratoren und andere Mitarbeiter, die für die Implementierung von Rescue and Recovery auf den Computern ihres Unternehmens verantwortlich sind. Durch Rescue and Recovery sollen Kosten reduziert werden, indem die Anzahl der Anrufe beim Help-Desk und die Vor-Ort-Besuche verringert und die Benutzerproduktivität gesteigert wird. Mit diesem wichtigen Tool können Benutzer und Administratoren Sicherungen wiederherstellen, auf Dateien zugreifen, Fehler bestimmen und Ethernet-Verbindungen herstellen, wenn das Microsoft® Windows-Betriebssystem nicht aufgerufen oder ordnungsgemäß ausgeführt werden kann. Außerdem ermöglicht es die Implementierung von kritischen Aktualisierungen auf beschädigten Systemen und auf Systemen außerhalb des Netzwerks sowie die automatische Ausführung von Programmkorrekturen auf Systemen bei einer Wiederherstellung. Dieses Handbuch enthält die erforderlichen Informationen für die Installation von Rescue and Recovery auf einem oder mehreren Computern, wenn Softwarelizenzen für die einzelnen Zielcomputer zur Verfügung stehen, sowie Informationen zu den vielen Möglichkeiten des Tools, das so angepasst werden kann, dass es IT- oder unternehmensinterne Richtlinien unterstützt. Informationen zum Verwenden der verschiedenen Komponenten des Arbeitsbereichs von Rescue and Recovery finden Sie im Onlinehilfesystem zu den Komponenten.

Rescue and Recovery bietet Hilfe zu Funktionen und Anwendungen. Informationen zum Verwenden der verschiedenen Komponenten des Arbeitsbereichs von Rescue and Recovery finden Sie im Onlinehilfesystem zu den Komponenten.

Dieses Implementierungshandbuch wurde in Zusammenarbeit mit IT-Spezialisten und unter Berücksichtigung der einzigartigen Herausforderungen der Arbeit dieser Spezialisten geschrieben. Bei Vorschlägen oder Bemerkungen Ihrerseits wenden Sie sich an Ihren autorisierten Lenovo Ansprechpartner. Diese Handbücher werden in regelmäßigen Abständen aktualisiert; auf der folgenden Website finden Sie ggf. eine aktuelle Version:

www.lenovo.com/ThinkVantage

Kapitel 1. Übersicht

Zielgruppe dieses Handbuchs sind Administratoren, IT-Sicherheits- und sonstige Mitarbeiter, die für die Implementierung und für den Einsatz von Sicherheitstechnologie in einem Unternehmen verantwortlich sind. ThinkVantage Rescue and Recovery besteht aus einer einzigartigen Kombination von ThinkVantage Technologies. Diese integrierte Anwendung bietet eine Suite leistungsfähiger Tools, die auch dann verwendet werden können, wenn das Microsoft Windows-Betriebssystem ausfällt.

In Unternehmen können diese Technologien IT-Spezialisten sowohl direkt als auch indirekt unterstützen. Alle ThinkVantage Technologies sind für IT-Spezialisten hilfreich, indem sie PCs bedienerfreundlicher und unabhängiger machen und leistungsfähige Tools bieten, die Implementierungen vereinfachen und erleichtern. ThinkVantage Technologies ermöglichen IT-Spezialisten, auf Dauer weniger Zeit für einzelne Computerprobleme zu verwenden und sich mehr auf ihre Kernaufgaben zu konzentrieren.

Hauptkomponenten

In diesem Handbuch werden folgende Hauptkomponenten beschrieben:

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

Jede dieser Komponenten wird im Folgenden näher beschrieben.

Rescue and Recovery

Rescue and Recovery besteht aus zwei Hauptkomponenten:

- Die Predesktop-Umgebung von Rescue and Recovery startet auch dann, wenn das Windows-Betriebssystem nicht gebootet werden kann.
- In der Windows-Umgebung von Rescue and Recovery können Sie das Betriebssystem und Dateien sichern und wiederherstellen.

Anmerkung: Einige Funktionen von Rescue and Recovery werden unter dem Windows-Betriebssystem ausgeführt. In einigen Fällen werden Systeminformationen, die von der Umgebung von Rescue and Recovery verwendet werden, erfasst, während Windows aktiv ist. Wenn das Windows-Betriebssystem nicht ordnungsgemäß funktioniert, wird die Ausführung der Umgebung von Rescue and Recovery allein dadurch nicht beeinträchtigt. Funktionen, die unter dem Windows-Betriebssystem ausgeführt werden, sind allerdings nicht konfigurierbar und werden daher in dem vorliegenden Implementierungshandbuch nicht behandelt.

Die Predesktop-Umgebung von Rescue and Recovery

Die Umgebung von Rescue and Recovery bietet einen Notfall-Arbeitsbereich für Endbenutzer, die Windows auf ihren Computern nicht starten können. Unter Windows PE (Preinstallation Environment) bietet diese Umgebung dasselbe Aussehen und dieselbe Funktionalität wie Windows und hilft Endbenutzern, Probleme zu lösen, ohne die Zeit von IT-Mitarbeitern in Anspruch nehmen zu müssen.

Die Umgebung von Rescue and Recovery weist vier Hauptkategorien von Funktionen auf:

- **Daten sichern und wiederherstellen**
  - **Übersicht zur Wiederherstellung:** Hier finden Benutzer Links zu Hilfethemen, in denen die verschiedenen Wiederherstellungsoptionen erläutert werden.
  - **Dateien sichern:** Bietet Benutzern die Möglichkeit, mit Windows-Anwendungen erstellte Dateien auf austauschbare Datenträger oder in ein Netzwerk zu kopieren und mit ihrer Arbeit fortzufahren, selbst wenn die Workstation inaktiviert ist.
  - **Über Sicherung wiederherstellen:** Bietet Benutzern die Möglichkeit, Dateien wiederherzustellen, die mit Hilfe von Rescue and Recovery gesichert wurden.
- **Konfigurieren**
  - **Übersicht zur Konfiguration:** Bietet Links zu Hilfethemen zur Konfiguration der Umgebung von Rescue and Recovery.
  - **Kennwort/Verschlüsselungstext zurücksetzen:** Ermöglicht einem Benutzer oder Administrator, ein Kennwort oder einen Verschlüsselungstext in der Umgebung von Rescue and Recovery zurückzusetzen.
  - **Zugriff auf das BIOS:** Zum Öffnen des BIOS-Konfigurationsprogramms.
- **Datenübertragung**
  - **Übersicht zur Datenübertragung:** Bietet Links zu verwandten Hilfethemen in der Umgebung von Rescue and Recovery.
  - **Browser öffnen:** Startet den Web-Browser ″Opera″. (Für den Zugriff auf das Internet oder auf ein Intranet ist eine Ethernet-Verbindung über ein Festnetz erforderlich.)
  - **Dateien herunterladen**
  - **Netzlaufwerk zuordnen:** Unterstützt Endbenutzer beim Zugriff auf Netzlaufwerke, um Software herunterzuladen oder Dateien zu übertragen.
- **Fehler beheben**
  - **Diagnose-Übersicht:** Bietet Links zu Hilfethemen, die die Funktionen der Diagnoseprogramme von Rescue and Recovery betreffen.
  - **Diagnose für Hardware durchführen:** Zum Öffnen der Anwendung ″PC Doctor″, die Hardwaretests ausführt und die Ergebnisse meldet.
  - **Diagnoseplatten erstellen**
  - **Bootvorgang von anderer Einheit aus**
  - **Systeminformationen:** Zum Anzeigen von Details zum Computer und zu den Hardwarekomponenten.
  - **Ereignisprotokoll:** Zum Anzeigen von Details zu den letzten Benutzeraktivitäten sowie einer Liste der Computerhardware als Hilfe bei der Fehlerbestimmung und -behebung. Mit der Protokollanzeigefunktion können Sie Protokolleinträge zu Benutzeraktivitäten und Ressourcen übersichtlich anzeigen.
  - **Gewährleistungsstatus**

Rescue and Recovery ist auf Lenovo und IBM PCs mit vorinstallierter Software verfügbar. Das Produkt kann auch in Form einer für den Download verfügbaren Datei käuflich erworben werden, so dass auch Organisationen mit Computern anderer Hersteller als Lenovo und IBM Rescue and Recovery verwenden können.

In Anhang B, „Einstellungen und Werte für die Datei TVT.TXT”, auf Seite 155 finden Sie Informationen zur Konfiguration der Umgebung von Rescue and Recovery für die Implementierung. Obwohl die Installation von Rescue and Recovery die Installation von Rapid Restore Ultra umfasst, werden diese beiden Programme in diesem Handbuch im Hinblick auf ihre Anpassung, Konfiguration und Implementierung als separate Komponenten behandelt.

Die Windows-Umgebung von Rescue and Recovery

Die Umgebung von Rapid Restore ermöglicht es Endbenutzern, verlorene Daten, Anwendungen und Betriebssysteme durch einfaches Klicken auf eine Schaltfläche wiederherzustellen. Dadurch können zeitaufwändige Anrufe beim Help-Desk vermieden werden, wodurch die Kosten für den Support gesenkt werden.

Sie können Sicherungen für alle Computer von Endbenutzern zeitlich planen und dadurch Risiken und Ausfallzeiten verringern. Rescue and Recovery bietet Ihren Kunden zusätzliche Unterstützung, indem automatische externe Sicherungen auf einem Server oder einer externen Speichereinheit vorkonfiguriert werden können.

Antidote Delivery Manager

Antidote Delivery Manager ist eine Infrastruktur zum Schutz vor Viren und Würmern, die in ThinkVantage Rescue and Recovery enthalten ist. Die zugehörigen Objekte sind leicht zu implementieren, effizient und ermöglichen einem Administrator, bei Meldung eines Fehlers innerhalb von Minuten eine Sperrung und Wiederherstellung einzuleiten. Das Programm kann von einem einzigen Administrator gestartet werden und funktioniert auch für Systeme, die nicht mit dem Netzwerk verbunden sind. Antidote Delivery Manager ersetzt vorhandene Antivirentools nicht, sondern ergänzt sie nur, so dass Sie weiterhin Tools zur Virensuche einsetzen und Patch-Code installieren müssen. Antidote Delivery Manager bietet die nötige Infrastruktur, um die Vernichtung von Daten zu stoppen und den erforderlichen Patch-Code auszuführen.

Sicherungen verschlüsseln

Sicherungen werden standardmäßig mit dem 256-Bit-AES-Schlüssel verschlüsselt. Wenn Sie Client Security Solution Version 6.0 installieren, können Sie die Verschlüsselung mit der GINA (Graphical Identification and Authentication) von Client Security Software durchführen.

Client Security Solution 6.0

Die Software Client Security Solution hat vor allem den Zweck, Benutzern dabei zu helfen, den PC als eine Ressource, vertrauliche Daten auf dem PC sowie die vom PC aufgebauten Netzverbindungen zu schützen. Bei Systemen mit den Markenzeichen IBM und Lenovo, die ein TCG-konformes (TCG - Trusted Computing Group) TPM (Trusted Platform Module) enthalten, verwendet die Software Client Security Solution (CSS) die Hardware als Sicherheitsbasis des Systems. Wenn das System keinen integrierten Sicherheitschip enthält, verwendet Client Security Solution Chiffrierschlüssel auf Softwarebasis als Sicherheitsbasis des Systems. Client Security Solution 6.0 weist folgende Funktionen auf:

- **Secure User Authentication**

  Benutzer benötigen einen hardwaregeschützten Client Security-Verschlüsselungstext, um auf die geschützten Funktionen von Client Security Solution zuzugreifen

- **Fingerprint User Authentication**

  Nutzt die integrierte und die über USB angeschlossene Fingerabdrucktechnologie zur Authentifizierung von Benutzern für kennwortgeschützte Anwendungen

- **Client Security Passphrase / Fingerprint Based Windows Logon**

  Benutzer müssen sich mit ihrem hardwaregeschützten Client Security-Verschlüsselungstext oder mit ihrem Fingerabdruck bei Windows anmelden

- **Protect Data**

  Verschlüsselung kritischer Dateien, indem sie an einer sicheren Stelle auf dem Festplattenlaufwerk gespeichert werden, an der eine gültige Benutzerauthentifizierung und ein ordnungsgemäß konfigurierter Sicherheitschip erforderlich ist
- **Manage Logon Passwords**

  Sichere Verwaltung und Speicherung von kritischen Anmeldedaten, wie Benutzer-IDs und Kennwörtern
- **End User Password/Passphrase Recovery**

  Benutzer können ein vergessenes Windows-Kennwort oder einen vergessenen Client Security-Verschlüsselungstext selbst wieder erhalten, indem sie bestimmte vorkonfigurierte Fragen beantworten
- **Audit Security Settings**

  Benutzer erhalten die Möglichkeit, eine ausführliche Liste der Sicherheitseinstellungen für die Workstation anzuzeigen und Änderungen vorzunehmen, um festgelegte Standards einzuhalten
- **Transfer Digital Certificates**

  Hardwareschutz für den privaten Schlüssel für Benutzer- und Maschinenzertifikate

Client Security-Verschlüsselungstext

Der Client Security-Verschlüsselungstext ist eine zusätzliche Form der Benutzerauthentifizierung, die erhöhte Sicherheit für Client Security Solution-Anwendungen bietet. Der Client Security-Verschlüsselungstext muss folgende Bedingungen erfüllen:

- Er muss aus mindestens acht Zeichen bestehen
- Er muss mindestens eine Ziffer enthalten
- Er muss sich von den letzten drei Verschlüsselungstexten unterscheiden
- Er darf höchstens zwei wiederholte Zeichen enthalten
- Er darf nicht mit einer Ziffer beginnen
- Er darf nicht mit einer Ziffer enden
- Er darf nicht die Benutzer-ID enthalten
- Er darf nicht geändert werden, wenn der aktuelle Verschlüsselungstext weniger als drei Tage alt ist
- Er darf nicht drei aufeinanderfolgende Zeichen enthalten, die auch in dem aktuellen Verschlüsselungstext enthalten sind, unabhängig von ihrer Position
- Er darf nicht mit dem Windows-Kennwort übereinstimmen.

Der Client Security-Verschlüsselungstext ist nicht für die gleiche Art von Angriffen anfällig wie das Windows-Kennwort. Bitte beachten Sie, dass ein Client Security-Verschlüsselungstext nur dem betreffenden Benutzer bekannt ist, und die einzige Möglichkeit, einen vergessenden Client Security-Verschlüsselungstext wieder zu erhalten, darin besteht, die Kennwortwiederherstellungsfunktion von Client Security zu verwenden. Wenn der Benutzer die Antworten auf die Wiederherstellungsfragen vergisst, gibt es keine Möglichkeit mehr, die durch den Client Security-Verschlüsselungstext geschützten Daten wiederherzustellen.

Client Security-Kennwortwiederherstellung

Diese optionale Einstellung ermöglicht registrierten Benutzern, ein vergessenes Windows-Kennwort oder einen vergessenen Client Security-Verschlüsselungstext durch das Beantworten dreier Fragen wieder zu erhalten. Wenn diese Funktion während der Registrierung eines Endbenutzers bei Client Security aktiviert ist, wird jeder Benutzer aufgefordert, drei Antworten auf zehn vorgegebene Fragen auszuwählen. Wenn der Benutzer sein Windows-Kennwort oder den Client Security-Verschlüsselungstext vergisst, kann er diese drei Fragen beantworten, um sein Kennwort oder den Verschlüsselungstext selbst zurückzusetzen.

Anmerkungen:

1. Bei Verwendung des Client Security-Verschlüsselungstextes ist dies die einzige Möglichkeit, einen vergessenen Verschlüsselungstext wiederherzustellen. Vergisst der Benutzer die Antwort auf die drei Fragen, muss er den Registrierungsassistenten erneut ausführen und verliert alle zuvor mit Client Security geschützten Daten.
2. Bei Verwendung von Client Security zum Schutz der Predesktop-Umgebung von Rescue and Recovery zeigt die Option zur Kennwortwiederherstellung den Client Security-Verschlüsselungstext und/oder das Windows-Kennwort des Benutzers an. Die Predesktop-Umgebung kann nämlich nicht automatisch eine Änderung des Windows-Kennworts durchführen. Dies trifft auch zu, wenn der Benutzer einer lokal zwischengespeicherten Domäne, die nicht an das Netzwerk angeschlossen ist, diese Funktion bei der Windows-Anmeldung ausführt.

ThinkVantage Fingerprint Software

Die biometrischen Fingerabdrucktechnologien von Lenovo sollen Kunden helfen, die Kosten für die Verwaltung von Kennwörtern zu senken, die Sicherheit ihrer Systeme zu erhöhen und gesetzliche Bestimmungen einzuhalten. Zusammen mit unseren Lesegeräten für Fingerabdrücke ermöglicht ThinkVantage Fingerprint Software die Authentifizierung per Fingerabdruck bei PCs und Netzwerken. Diese Lösung kann in Client Security Solution Version 6.0 integriert werden, um eine erweiterte Funktionalität zu bieten. Unter der folgenden Adresse können Sie diese Software herunterladen oder weitere Informationen zu Lenovo Fingerabdrucktechnologien finden:

www.thinkpad.com/fingerprint

Die ThinkVantage Fingerprint Software bietet folgende Funktionen:

- **Client-Software-Funktionen**
  - **Ersetzen des Microsoft Windows-Kennworts**

    Ersetzen des Windows-Kennworts durch Ihren Fingerabdruck für einen einfachen, schnellen und sicheren Systemzugriff.
  - **Ersetzen des BIOS-Kennworts (des Startkennworts) und des Kennworts für das Festplattenlaufwerk**

    Ersetzen Sie diese Kennwörter durch Ihren Fingerabdruck, um die Sicherheit und den Komfort bei der Anmeldung zu erhöhen.
  - **Zugriff auf Windows mit einer einzigen Überprüfung:**

    Ein Benutzer muss seinen Fingerabdruck nur ein einziges Mal überprüfen lassen, um Zugriff auf das BIOS UND auf Windows zu erhalten und dadurch Zeit zu sparen.

- **Integration in Client Security Solution** zur Verwendung mit dem CSS Password Manager und zur Nutzung des TPM. Nach einer Überprüfung des Fingerabdrucks können Benutzer auf Websites zugreifen und Anwendungen auswählen.

- **Administratorfunktionen**
  - **Umschalten zwischen verschiedenen Sicherheitsmodi:**

    Ein Administrator kann zwischen einem sicheren und einem komfortableren Modus hin- und herschalten, um die Zugriffsberechtigungen von Benutzern mit eingeschränkter Berechtigung zu ändern.
  - **Managementkonsole:**

    Unterstützt Administratoren durch die Möglichkeit der Anpassung der Fingerprint Software per Remotezugriff über eine scriptgesteuerte Befehlszeilenschnittstelle.
- **Sicherheitsfunktionen**
  - **Softwaresicherheit:**
    Zum Schutz von Benutzervorlagen durch eine starke Verschlüsselung, wenn sie in einem System gespeichert sind und wenn sie vom Lesegerät zur Software übertragen werden.
  - **Hardwaresicherheit:**
    Lesegeräte verfügen über einen Sicherheits-Koprozessor, in dem Fingerabdruckschablonen, BIOS-Kennwörter und Verschlüsselungsschlüssel gespeichert und geschützt sind.

Password Manager

Mit dem Password Manager von Client Security können Sie alle Ihre sensiblen und leicht zu vergessenden Anmeldeinformationen für Anwendungen und Websites, wie Benutzer-IDs, Kennwörter und andere persönliche Informationen, aufbewahren und verwalten. Im Password Manager von Client Security werden alle Informationen über den integrierten Sicherheitschip gespeichert, so dass Ihr Zugriff auf Anwendungen und Websites völlig sicher ist.

Das heißt, dass Sie sich nicht mehr eine Menge verschiedener Kennwörter merken müssen, für die unterschiedliche Regeln und Ablaufdaten gelten, sondern sich nur noch ein einziges Kennwort oder einen Verschlüsselungstext merken und Ihren Fingerabdruck abgeben müssen, oder es wird eine Kombination von Identifizierungselementen verwendet.

Der Password Manager von Client Security bietet die folgenden Funktionen:

- **Verschlüsselung aller gespeicherten Informationen durch den integrierten Sicherheitschip**

  Der Password Manager von Client Security verschlüsselt automatisch alle Daten über den integrierten Sicherheitschip. Dadurch wird sichergestellt, dass alle Ihre kritischen Kennwortinformationen durch die Verschlüsselungsschlüssel von Client Security Solution gesichert werden.
- **Schnelle Übertragung von Benutzer-IDs und Kennwörtern und einfache Verwendung einer benutzerfreundlichen Schnittstelle zum Eingeben und Übertragen**

  Mit der Schnittstelle zum Eingeben und Übertragen des Password Managers von Client Security können Sie Informationen direkt in die Anmeldeschnittstelle eines Browsers oder einer Anwendung eingeben. Dadurch werden Eingabefehler vermieden, und Sie können alle Ihre Informationen sicher über den integrierten Sicherheitschip speichern.

- **Autokey-Benutzer-IDs und -Kennwörter**

  Der Password Manager von Client Security automatisiert Ihren Anmeldeprozess, indem Ihre Anmeldeinformationen beim Zugriff auf eine Anwendung oder eine Website, deren Anmeldeinformationen im Password Manager von Client Security gespeichert sind, automatisch eingegeben werden.
- **Generierung von Kennwörtern per Zufallsgenerator**

  Mit dem Password Manager von Client Security können Sie für jede Anwendung oder Website Kennwörter per Zufallsgenerator generieren. Dadurch können Sie die Sicherheit Ihrer Daten erhöhen, da für jede Anwendung ein strengerer Kennwortschutz aktiviert ist. Per Zufallsgenerator festgelegte Kennwörter sind deutlich sicherer als benutzerdefinierte Kennwörter, da die meisten Benutzer erfahrungsgemäß leicht zu merkende persönliche Informationen, die oft relativ leicht zu erraten sind, als Kennwörter verwenden.
- **Bearbeitung von Einträgen über die Schnittstelle des Password Managers von Client Security**

  Mit dem Password Manager von Client Security können Sie alle Ihre Benutzerkontoeinträge und alle optionalen Kennwortfunktionen über eine einzige benutzerfreundliche Schnittstelle bearbeiten und konfigurieren. Die Verwaltung Ihrer Kennwörter und Ihrer persönlichen Informationen erfolgt dadurch schnell und einfach.
- **Über die Symbolleiste auf der Arbeitsoberfläche von Microsoft(R) Windows(R) oder über einen einfachen Tastaturkurzbefehl auf Ihre Anmeldedaten zugreifen**

  Das Password Manager-Symbol bietet Ihnen jedes Mal, wenn Sie eine neue Anwendung oder Website im Password Manager hinzufügen möchten, einen bequemen Zugriff auf Ihre Anmeldedaten. Jede Funktion des Password Managers von Client Security kann auch durch einen einfachen Tastaturkurzbefehl aufgerufen werden.
- **Anmeldeinformationen exportieren und importieren**

  Mit dem Password Manager von Client Security können Sie Ihre kritischen Anmeldeinformationen exportieren, um sie sicher von einem Computer zum anderen zu übertragen. Wenn Sie Ihre Anmeldeinformationen aus dem Password Manager von Client Security exportieren, wird eine kennwortgeschützte Exportdatei erstellt, die auf einem austauschbaren Datenträger gespeichert werden kann. Mit dieser Datei können Sie überall auf Ihre Benutzerinformationen und Kennwörter zugreifen oder Ihre Einträge auf einem anderen Computer mit Password Manager importieren.

  Anmerkung: Das Importieren funktioniert nur mit Client Security Solution Version 6.0. Von Client Security Software Version 5.4X oder älteren Versionen kann nicht in den Password Manager von Client Security Solution 6.0 importiert werden.

SafeGuard PrivateDisk

Schützen Sie Ihre Daten mit SafeGuard PrivateDisk. Fast alle Benutzer speichern vertrauliche Daten auf dem PC. SafeGuard PrivateDisk schützt vertrauliche Daten. Das Programm funktioniert wie ein ″elektronischer Tresor″ für vertrauliche und wertvolle Informationen auf Ihrem Computer sowie auf allen Plattenlaufwerken und mobilen Datenträgern. Unbefugte Personen können auf geschützte Informationen nicht zugreifen oder sie lesen.

Wie funktioniert SafeGuard PrivateDisk? SafeGuard PrivateDisk basiert auf dem Prinzip der virtuellen Platte.

- Eine virtuelle Platte kann auf jedem verfügbaren Laufwerk erstellt werden.
  - Mobile Speichermedien (wie Platten, USB-Sticks, CD-ROMs, DVDs oder Zip-Laufwerke)
  - Festplatten, Netzlaufwerke
- Der Treiber funktioniert wie ein Festplattenlaufwerk
  - Das Betriebssystem sendet Schreib- und Lesebefehle transparent an den Treiber.
  - Der Treiber verwaltet den verschlüsselten Speicher.
  - Alle Daten und Verzeichnisinformationen sind verschlüsselt.
- SafeGuard PrivateDisk arbeitet mit Client Security Solution und TPM zusammen, um mit PrivateDisk generierte digitale Zertifikate zu schützen.
- SafeGuard PrivateDisk verwendet einen symmetrischen Verschlüsselungsalgorithmus mit einem neuen, zufallsgenerierten AES-Schlüssel für jede virtuelle Platte
  - AES, 128 Bit, CBC-Modus
  - Neuer, zufallsgenerierter Schlüssel für jede virtuelle Platte
- Authentifizierung durch:
  - Kennwort
  - Privaten Schlüssel (Zertifikat X.509), optional Smartcard
  - Verwendung von automatisch generierten EFS-Zertifikaten möglich
- Kennwortschutz:
  - PKCS#5
  - Zeitverzögerung nach einer falschen Kennworteingabe
  - Kennworteingabedialog mit Abfangschutz

Security Advisor

Mit dem Tool ″Security Advisor″ können Sie eine Zusammenfassung der Sicherheitseinstellungen anzeigen, die zurzeit auf Ihrem Computer festgelegt sind. Sie können diese Einstellungen überprüfen, um Ihre aktuellen Sicherheitsstatus anzuzeigen oder um Ihre Systemsicherheit zu verbessern. Zu den angezeigten Sicherheitsthemen gehören Hardwarekennwörter, Windows-Benutzerkennwörter, die Windows-Kennwortrichtlinie, geschützter Bildschirmschoner und gemeinsamer Dateizugriff. Die angezeigten Standardwerte für die Kategorien können über die TVT.TXT-Datei auch geändert werden.

Assistent zur Übertragung von Zertifikaten

Der CSS-Assistent zur Übertragung von Zertifikaten leitet Sie durch den Prozess der Übertragung der Ihren Zertifikaten zugeordneten privaten Schlüssel vom softwarebasierten Microsoft Cryptographic Service Provider (CSP) zum hardwarebasierten Client Security Solution CSP. Nach dieser Übertragung sind Operationen, die die Zertifikate verwenden, sicherer, da die privaten Schlüssel durch den integrierten Sicherheitschip geschützt sind.

Funktion zum Zurücksetzen von Hardwarekennwörtern

Mit diesem Tool können Sie eine sichere Umgebung einrichten, die unabhängig von Windows ausgeführt wird und die Ihnen hilft, ein vergessenes Start- oder Festplattenkennwort zurückzusetzen. Ihre Identität wird überprüft, indem Sie eine Reihe von Fragen beantworten, die Sie vorher selbst festlegen. Diese sichere Umgebung sollte so früh wie möglich erstellt werden, bevor Sie ein Kennwort vergessen. Sie können ein vergessenes Kennwort erst zurücksetzen, wenn diese sichere Umgebung auf Ihrem Festplattenlaufwerk eingerichtet ist und Sie sich registriert haben. Dieses Tool steht nur auf ausgewählten ThinkCentre- und ThinkPad-Computern zur Verfügung.

Unterstützung für Systeme ohne TPM

Client Security Solution 6.0 unterstützt jetzt auch IBM und Lenovo Systeme, die über keinen kompatiblen integrierten Sicherheitschip verfügen. Dies ermöglicht eine Standardinstallation im gesamten Unternehmen, um eine homogene Sicherheitsumgebung zu schaffen. Die Systeme, die über die integrierte Sicherheitshardware verfügen, sind gegen Angriffe besser geschützt; auch die nur mit der Sicherheitssoftware ausgestatteten Systeme profitieren jedoch von einer höheren Sicherheit und einer besseren Funktionalität.

System Migration Assistant

Der System Migration Assistant (SMA) ist ein Software-Tool, mit dem Systemadministratoren die Arbeitsumgebung eines Benutzers von einem System zum anderen migrieren können. Zur Arbeitsumgebung eines Benutzers gehören die folgenden Elemente:

- Einstellungen des Betriebssystems, wie zum Beispiel Einstellungen der Arbeitsoberfläche und der Netzkonnektivität
- Dateien und Ordner
- Angepasste Anwendungseinstellungen, wie zum Beispiel Lesezeichen in einem Web-Browser oder Bearbeitungseinstellungen in Microsoft Word
- Benutzeraccounts

Systemadministratoren können mit dem SMA eine Standardarbeitsumgebung für ein Unternehmen einrichten oder den Computer eines einzelnen Benutzers aufrüsten. Einzelne Benutzer können mit dem SMA ihr System sichern oder Einstellungen und Dateien von einem Computer zum anderen migrieren, zum Beispiel von einem Desktop-Computer zu einem tragbaren Computer (Laptop).

Abweichungen bei OEM-Systemen

Client Security Solution 6.0 ist für OEM-Systeme zurzeit nicht verfügbar. Rescue and Recovery kann auf OEM-Systemen keine der CSS-Anwendungen nutzen.

Kapitel 2. Hinweise zur Installation

Bevor Sie ThinkVantage Rescue and Recovery installieren, sollten Sie die allgemeine Architektur dieser Anwendung kennen.

Rescue and Recovery

Rescue and Recovery verfügt über zwei Hauptschnittstellen. Die erste Schnittstelle wird in der Windows XP- oder Windows 2000-Umgebung ausgeführt. Die zweite Schnittstelle (die Predesktop-Umgebung von Rescue and Recovery) wird unabhängig von dem Betriebssystem Windows XP oder Windows 2000 in der Windows PE-Umgebung ausgeführt.

Anmerkungen:

1. Rescue and Recovery funktioniert nur dann mit der Nicht-BIOS-Version von Computrace, wenn Rescue and Recovery vor Computrace installiert wird. Siehe dazu Kapitel 8, „Bewährte Verfahren", auf Seite 127.
2. Wenn Sie versuchen, SMS auf einem System zu installieren, auf dem Rescue and Recovery installiert ist und die Windows PE-Umgebung bereits als virtuelle Partition installiert ist, schlägt die Installation von SMS fehl. Sowohl Windows PE als auch SMS verwenden das Verzeichnis C:\minint für ihr Dateisystem. Sie können beide gleichzeitig installieren, indem Sie Rescue and Recovery 2.0 als Partition vom Typ 12 installieren. Anweisungen zur Installation einer Partition vom Typ 12 finden Sie im Abschnitt „Rescue and Recovery auf einer Servicepartition vom Typ 12 installieren" auf Seite 142.
3. Die Installation von Microsoft Recovery Console auf einem System mit Rescue and Recovery birgt ein mögliches Sicherheitsrisiko. Microsoft Recovery Console sucht nach allen Ordnern mit dem Pfad C:*\system32\config\, und wenn das Programm diesen Pfad findet, nimmt es an, dass es sich hierbei um ein Betriebssystem handelt. Wenn die Einträge in der Registrierungsdatenbank, die ein Windows-Kennwort erforderlich machen, nicht vorhanden sind, erlaubt Microsoft Recovery Console einem Benutzer, das Betriebssystem auszuwählen und anschließend auf das gesamte Festplattenlaufwerk zuzugreifen, ohne ein Kennwort einzugeben.

Hinweise zur Installation über ältere Versionen

Rescue and Recovery Version 3.0 kann über Rescue and Recovery 2.0 installiert werden.

Nach der Installation von Rescue and Recovery 3.0 wird eine neue Sicherung empfohlen. Dies kann entweder mit Hilfe eines Scripts oder über die Benutzerschnittstelle erfolgen.

Um einen bereinigten Sicherungssatz zu erstellen, gehen Sie wie folgt vor:

1. Kopieren Sie ältere Sicherungen auf ein CD-/DVD-Laufwerk oder auf ein USB-Festplattenlaufwerk (falls gewünscht).
2. Löschen Sie aktuelle Sicherungen.
3. Führen Sie eine Basissicherung durch.

Das folgende Script kopiert Sicherungen auf ein USB-Festplattenlaufwerk, löscht die aktuellen Sicherungen, und führt anschließend eine Basissicherung durch.


```
@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

Bei der Implementierung von Client Security Solution 6.0 müssen Sie folgende Aspekte beachten.

Im Code von Client Security Solution sind die nötigen Treiber sowie die Softwareunterstützung enthalten, um die Sicherheitshardware (TPM) der Maschine zu aktivieren, auf der Client Security Solution 6.0 installiert werden soll. Die Aktivierung der Hardware erfordert mindestens einen Neustart, da der Chip vom BIOS gesteuert wird und eine erfolgreiche BIOS-Authentifizierung erforderlich ist, um die Prozedur zu beenden. Wenn ein BIOS-Administratorkennwort festgelegt ist, muss es folglich angegeben werden, um TPM zu aktivieren oder zu inaktivieren.

Bevor TPM irgendwelche Funktionen ausführen kann, muss das Eigentumsrecht ("Ownership") initialisiert werden. Jedes System erhält einen einzigen CSS-Administrator, der die CSS-Optionen verwaltet. Dieser Administrator muss über Windows-Administratorrechte verfügen. Der Administrator kann mit Hilfe von XML-Implementierungsscripts initialisiert werden.

Nachdem das Eigentumsrecht für das System konfiguriert ist, wird für jeden weiteren Windows-Benutzer, der sich am System anmeldet, automatisch der Konfigurationsassistent von Client Security aufgerufen, damit der Benutzer sich registrieren kann und die entsprechenden Sicherheitsschlüssel und Berechtigungsnachweise initialisiert werden.

Software-Emulation für TPM

Client Security Solution kann auf bestimmten Systemen ohne TPM ausgeführt werden. Die Funktionalität ist dabei genau dieselbe, außer dass anstelle von hardwaregeschützten Schlüsseln Schlüssel auf Softwarebasis verwendet werden. Die Software kann auch mit einem Schalter installiert werden, der es zwingt, immer Schlüssel auf Softwarebasis anstelle des TPM zu verwenden. Diese Einstellung muss bei der Installation vorgenommen werden. Sie kann nachträglich nur durch eine Deinstallation und erneute Installation der Software vorgenommen werden.

Die Syntax zum Erzwingen einer Software-Emulation von TPM lautet wie folgt:

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

Upgrade-Szenarios

Informationen zum Upgrade von älteren Versionen von Client Security Solution finden Sie im Abschnitt „Szenarios für installierte Software" auf Seite 113.

Kapitel 3. Rescue and Recovery anpassen

Dieses Kapitel enthält Informationen zum Anpassen von ThinkVantage Rescue and Recovery.

Einfache Implementierung mit einem Symbol für die Erstellung einer Basissicherung auf dem Desktop

Stellen Sie vor dem Starten dieser Prozedur sicher, dass sich Dateien mit der Erweiterung TVT, wie z. B. z062zaa1025us00.tvt, in demselben Verzeichnis wie die ausführbare Datei oder die MSI-Datei befinden. Andernfalls schlägt die Installation fehl. Wenn Ihre Datei setup_tvtrnr3_1027**c**.exe heißt, haben Sie das kombinierte Paket heruntergeladen. Diese Anweisungen gelten für die Dateien, die gesondert von der Downloadseite *Large Enterprise individual language files* heruntergeladen werden können.

Gehen Sie wie folgt vor, um eine einfache Implementierung auszuführen, bei der auf dem Desktop des Benutzers ein Sicherungssymbol erstellt wird:

1. Extrahieren Sie die Datei SETUP_TVTRNR*XXXX*.EXE (wobei *XXXX* für die Build-ID steht) in ein temporäres Verzeichnis:

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

2. Passen Sie die Datei TVT.TXT entsprechend an. Sie können z. B. eine wöchentliche Sicherung um 15.00 Uhr an jedem Dienstag planen. Fügen Sie die folgenden Einträge zum Abschnitt [Rescue and Recovery] der Datei TVT.TXT hinzu, um die Implementierung entsprechend anzupassen. (Zusätzliche Informationen zu den verschiedenen Einstellungen finden Sie in Anhang B, „Einstellungen und Werte für die Datei TVT.TXT", auf Seite 155.)

   ```
   ScheduleHour=15

   ScheduleMinute=00

   ScheduleDayOfTheWeek=2
   ```

3. Kopieren Sie die Datei Z062ZAA1025US00.TVT auch in das Verzeichnis C:\tvtrr. Die TVT-Datei muss sich im selben Ordner wie die MSI-Datei befinden.
4. Leiten Sie die MSI-Installation ohne Neustart bei Abschluss der Installation ein:

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

   Anmerkung: Der oben genannte Befehl wurde so geändert, dass er auf diese Seite passt. Geben Sie diesen Befehl als eine einzige Zeichenfolge in einer Zeile ein.
5. Passen Sie die Umgebung von Rescue and Recovery an. (Ausführliche Informationen hierzu finden Sie im Abschnitt „Predesktop Area" auf Seite 20.)
6. Löschen Sie die temporären Dateien im Verzeichnis C:\TVTRR. (Informationen hierzu finden Sie im Abschnitt „Windows-Umgebung" auf Seite 17.)
7. Schreiben Sie eine Befehlsdatei, die folgende Befehle enthält:

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

   Anmerkung: Der oben genannte Befehl wurde so geändert, dass er auf diese Seite passt. Geben Sie diesen Befehl als eine einzige Zeichenfolge in einer Zeile ein.

8. Erstellen Sie eine Verknüpfung mit der Bezeichnung ″Basissicherung erstellen″ auf dem Desktop für alle Benutzer (unter \All Users\Desktop). (Geben Sie dazu den Pfad im Feld **Geben Sie den Ort des Objekts ein:** an.)
9. Führen Sie auf dem System das Dienstprogramm ″Sysprep″ aus.
10. Erstellen Sie das Image für die Implementierung.

Nachdem der Clientbenutzer das Image erhalten und den Computer personalisiert hat, kann er auf das Symbol **Basissicherung erstellen** klicken, um Rescue and Recovery zu starten und die Basissicherung zu speichern.

Sysprep-Image in Basissicherung erfassen

Gehen Sie wie folgt vor, um ein Image des Dienstprogramms ″Sysprep″ in der Basissicherung zu erfassen:

1. Führen Sie eine administrative Installation aus:

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

2. Fügen Sie den folgenden Abschnitt am Ende der Datei TVT.TXT im Verzeichnis C:\TVTRR\Program Files\IBM ThinkVantage\Rescue and Recovery ein:

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

3. Installieren Sie Rescue and Recovery unter Verwendung von MSIEXE:
   a. Fügen Sie für alle MSIs den folgenden Code zum Generieren eines Installationsprotokolls hinzu:

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

   b. Installieren Sie die Installationsdateien unter Verwendung von MSIEXE, indem Sie folgenden Befehl eingeben:

```
: Perform the install of Rescue and Recovery

 msiexec /i "C:\TVTRR\Rescue and Recovery - Client
Security Solution.msi"
```

   c. Installieren Sie die Installationsdateien unter Verwendung von MSIEXE wie folgt unbeaufsichtigt:

      Geben Sie für den Neustart am Ende der Installation den folgenden Befehl ein:

```
: 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
```

      Geben Sie für den unterdrückten Neustart den folgenden Befehl ein:

```
: 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. Geben Sie die folgenden Befehle ein:

```
: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"
```

Wenn Sie ein Kennwort verwenden möchten, fügen Sie die Syntax `password=`*`Kennwort`* hinzu.

5. Führen Sie Ihre spezifische Sysprep-Implementierung durch, sobald die folgende oder eine ähnliche Nachricht angezeigt wird:

```
**********************************************************************
** Für Sysprep-Sicherung bereit.                                    **
** FÜHREN SIE SYSPREP JETZT AUS, UND FAHREN SIE DAS SYSTEM HERUNTER.**
**                                                                  **
** Beim nächsten Booten der Maschine wird die                       **
** Predesktop Area aufgerufen und eine Sicherung erstellt.          **
**********************************************************************
```

6. Fahren Sie das System herunter, und starten Sie es erneut, sobald Sysprep beendet ist.

   Anmerkung: Das Betriebssystem wird in der Predesktop Area von Rescue and Recovery gestartet. Sie sehen eine Statusleiste mit der Nachricht darüber, dass sich die Systemwiederherstellung in Verarbeitung befindet.
7. Nach der Beendigung erhalten Sie die Nachricht, dass die Sysprep-Sicherung abgeschlossen ist.
8. Schalten Sie das System mit dem Netzschalter aus.
9. Erfassen Sie das Image für die Implementierung.

System mit mehreren Partitionen erfassen und Dateien in einer Sysprep-Sicherung ausschließen

Gehen Sie wie folgt vor, um mehrere Partitionen in einer Sicherung mit dem Dienstprogramm ″Sysprep″ zu erfassen:

1. Führen Sie eine administrative Installation aus:

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

2. Fügen Sie den folgenden Abschnitt am Ende der Datei TVT.TXT im Verzeichnis C:\\″Program Files″\″IBM ThinkVantage\Rescue and Recovery″:\tvtrr\ ein:

```
[Backup0]
BackupVersion=2.0

[BackupDisk]
CustomPartitions=0
```

   Fügen Sie Folgendes in die Datei TVT.TXT ein, um eine Partition AUSZUSCHLIESSEN:

```
[BackupDisk]
CustomPartitions=1

[PartitionX].
IncludeInBackup=0
```

   Hierbei steht **X** für die Partitionsnummer.
3. Wenn Sie MPG- und JPG-Dateien von Sicherungen ausschließen möchten, fügen Sie diese wie im folgenden Beispiel zur Datei IBMFILTER.TXT hinzu:

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

4. Installieren Sie Rescue and Recovery unter Verwendung von MSIEXE:
   a. Fügen Sie für alle MSIs den folgenden Code zum Generieren eines Installationsprotokolls hinzu:

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

   b. Installieren Sie die Installationsdateien unter Verwendung von MSIEXE, indem Sie folgenden Befehl eingeben:

      ```
      : Perform the install of Rescue and Recovery

       msiexec /i "C:\TVTRR\Rescue and Recovery - Client Security Solution.msi"
      ```

   c. Installieren Sie die Installationsdateien unter Verwendung von MSIEXE wie folgt unbeaufsichtigt:

      Geben Sie für den Neustart am Ende der Installation den folgenden Befehl ein:

      ```
      : 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
      ```

      Geben Sie für den unterdrückten Neustart den folgenden Befehl ein:

      ```
      : 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"
      ```

5. Geben Sie die folgenden Befehle ein:

   ```
   :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"
   ```

   Wenn Sie ein Kennwort verwenden möchten, fügen Sie die Syntax password=*Kennwort* hinzu.

6. Führen Sie Ihre spezifische Sysprep-Implementierung durch, sobald die folgende oder eine ähnliche Nachricht angezeigt wird:

   ```
   ********************************************************************
   ** Für Sysprep-Sicherung bereit.                                  **
   ** FÜHREN SIE SYSPREP JETZT AUS, UND FAHREN SIE DAS SYSTEM HERUNTER.**
   **                                                                **
   ** Beim nächsten Booten der Maschine wird die                     **
   ** Predesktop Area aufgerufen und eine Sicherung erstellt.        **
   ********************************************************************
   ```

7. Fahren Sie das System herunter, und starten Sie es erneut, sobald Sysprep beendet ist.

   Anmerkung: Das Betriebssystem wird in der Predesktop Area von Rescue and Recovery gestartet. Sie sehen eine Statusleiste mit der Nachricht darüber, dass sich die Systemwiederherstellung in Verarbeitung befindet.

8. Nach der Beendigung erhalten Sie die Nachricht, dass die Sysprep-Sicherung abgeschlossen ist.

9. Schalten Sie das System mit dem Netzschalter aus.
10. Erfassen Sie das Image für die Implementierung.

Windows-Umgebung

Dateien in Sicherungen einschließen oder ausschließen

Rescue and Recovery verfügt über zahlreiche Möglichkeiten zum Ein- und Ausschließen von Daten bei Sicherungsvorgängen. Es können einzelne Dateien, Ordner und sogar ganze Partitionen ein- bzw. ausgeschlossen werden.

Die Funktionen zum Ein- und Ausschließen von Dateien werden über die im Folgenden angegebenen Dateien (nach Ausführungspriorität geordnet) gesteuert. Alle Dateien befinden sich im Verzeichnis C:\program files\ibm thinkvantage\rescue and recovery.
1. IBMFILTER.TXT
2. GUIEXCLD.TXT

Der Endbenutzer kann standardmäßig einzelne Dateien und Ordner auswählen, die für die Sicherung ausgeschlossen werden sollen. Diese Dateien und Ordner werden in der Datei GUIEXCLD.TXT angegeben.

Der Administrator kann bei Bedarf bestimmte Dateinamen und -typen in der Datei IBMFILTER.TXT angeben, wenn sichergestellt werden soll, dass die betreffenden Dateien bzw. Ordner auf jeden Fall gesichert werden. In dieser Datei angegebene Elemente werden unabhängig von den Angaben in der Datei GUIEXCLD.TXT bei jedem Sicherungsvorgang gesichert.

Administratoren können auch Dateien, Ordner oder Partitionen immer von Sicherungsvorgängen ausschließen.

Die folgenden Elemente sind immer von allen Sicherungen ausgeschlossen:
- PAGEFILE.SYS
- HIBERFILE.SYS
- C:\SYSTEM VOLUME INFORMATION

Bei einer Wiederherstellung werden die Dateien PAGEFILE.SYS und HIBERFILE-.SYS automatisch von Windows erneut generiert. Darüber hinaus werden nach einer Wiederherstellung über Sicherungsdateien von Windows automatisch auch die Daten für die Windows-Systemwiederherstellung mit einem neuen Wiederherstellungspunkt erneuert.

IBMFILTER.TXT

Das Dateiformat lautet wie folgt:
- Eine Einschluss-/Ausschlussregel steht in einer einzelnen Zeile.
- Wenn für eine Datei oder für einen Ordner mehrere Regeln enthalten sind, gilt die letzte Regel. Einträge, die in der Datei weiter unten stehen, haben Vorrang.
- Einträge müssen mit einem der folgenden Zeichen beginnen:
  - **;**

    für einen Kommentar
  - **I**

    zum Einschließen von Dateien oder Ordnern, die mit dem Eintrag übereinstimmen

– **X**

  zum Ausschließen von Dateien oder Ordnern, die mit dem Eintrag übereinstimmen

– **S**

  zum Einschließen von Einzelinstanzspeicher (Single Instance Storage) für eine Datei oder einen Ordner

– **i**

  für Dateien oder Ordner, die Sie zum Einschließen auswählen können

– **x**

  für Dateien oder Ordner, die Sie zum Ausschließen auswählen können

– **s**

  optional verwendet zum Angeben einer Datei oder eines Ordners als Einzelinstanzspeicher, die/der normalerweise eingeschlossen würde

```
  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
```

Andere Aspekte von Rescue and Recovery anpassen

Sie können zahlreiche Aspekte von Rescue and Recovery über die externe Datei TVT.TXT anpassen, die vor der Installation erstellt wird. Die Datei TVT.TXT befindet sich im Unterverzeichnis C:\Program Files\IBM ThinkVantage\.

Die Datei TVT.TXT entspricht dem Windows-Standarddateiformat für INI-Dateien. Die Daten sind deshalb in Abschnitten angeordnet, die durch eckige Klammern ([]) begrenzt werden, und jede Zeile dieser Datei enthält einen Eintrag in folgendem Format:

```
Einstellung=Wert
```

Wenn Sie beispielsweise nicht alle Sicherungsdaten verschlüsseln möchten, müssen Sie dazu folgende Zeilen in die Datei TVT.TXT aufnehmen:

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

Der Parameter `0` für die Einstellung ″EncryptBackupData″ weist Rescue and Recovery an, die Sicherung nicht zu verschlüsseln.

Eine vollständige Liste der Zeichenfolgen und Parameter für die verschiedenen Einstellungen sowie der Standardeinstellungen für den Abschnitt [Rescue and Recovery] in der Datei TVT.TXT finden Sie in Anhang B, „Einstellungen und Werte für die Datei TVT.TXT”, auf Seite 155.

Trouble-Ticket

Derzeit gibt es keine Möglichkeit, Daten aus der Umgebung von Rescue and Recovery automatisch über FTP oder E-Mail zu übertragen. Der Endbenutzer wird dazu aufgefordert, die im Browser integrierte E-Mail-Funktion und die Position der zu übertragenden Dateien zu verwenden. Die dynamische Datenübertragung wird nicht unterstützt; die Protokollierungsfunktion fasst jedoch die Protokollereignisse in einer Datei zusammen und teilt dem Benutzer die Position dieser Datei und deren Dateinamen mit, damit er diese mit einer E-Mail übertragen kann. Dadurch wird die XML-Datei *Req 115 Trouble Ticket* erstellt, in der alle Informationen zusammengefasst sind, die in den Systeminformationen (Current HW, eGatherer und PCDR-Diagnoseprotokolldaten) enthalten sind. Diese Informationen werden in einer Position gespeichert, die einfach zu finden ist und auf die sowohl von der Umgebung von Rescue and Recovery als auch vom Betriebssystem aus unter C:\IBMSHARE zugegriffen werden kann.

Diagnoseprogramm: Dies ist eine Basisanwendung, die in der Predesktop Area verfügbar ist und die Sie bei der Fehlerbestimmung unterstützt. Die Ausgabedaten der Tests werden so gespeichert, dass sie angezeigt und an den Help-Desk übermittelt werden können. Rescue and Recovery stellt Tools bereit, die den vorher gesicherten Stand der Windows-Umgebung des Benutzers wiederherstellen.

Rescue and Recovery umfasst Tools, mit denen Sie eine vollständige Wiederherstellung einer Benutzerpartition auf den vorherigen Stand ausführen können, sowie Tools, mit denen Sie einzelne Dateien wiederherstellen können. Die Tools stellen den Zugriff auf eine Sicherung der Daten des Benutzers bereit. Die Funktionalität zur Wiederherstellung aller Daten oder eines Teils der Daten wird von diesen Tools bereitgestellt.

OSFILTER.TXT

Diese Datei stellt das Betriebssystem und Anwendungen eines Benutzers wieder her, ohne einen Einfluss auf die Daten des Benutzers zu haben. Mit Rescue and Recovery können Sie bestimmte Dateien und Order (einschließlich der Unterordner) selektiv wiederherstellen. Dabei wird eine explizite Aufzählung und eine Filterung mit Platzhaltern verwendet, und es werden keine anderen Daten gelöscht. Eine externe Datei definiert mit Hilfe von Platzhalterzeichnen, welche Dateien, Ordner oder Dateitypen das Betriebssystem und die Anwendungen umfassen. Diese Datei kann der Administrator anpassen, und eine externe Standarddatei wird bereitgestellt. Wenn der Benutzer das Betriebssystem wiederherstellen möchte, wird ein Menü angezeigt, in dem er mit der folgenden Option von Windows nur die Wiederherstellung auswählt: Nur Dateien, die den in dieser externen Datei enthaltenen Regeln entsprechen, werden wiederhergestellt. Der Administrator kann den Inhalt dieser externen Datei anpassen.

Wenn Sie die Datei OSFILTER.txt anzeigen möchten, können Sie den folgenden Pfad verwenden: `cd %RR%`. Weitere Informationen zum Dateiformat finden Sie im Abschnitt „IBMFILTER.TXT" auf Seite 17.

Predesktop Area

Wenn Sie Teile der Predesktop Area von Rescue and Recovery anpassen möchten, die auch dann gestartet wird, wenn das Betriebssystem nicht gestartet werden kann, können Sie mit dem Dienstprogramm RRUTIL.EXE Dateien abrufen und speichern. Diese Dateien und die zugehörigen Anpassungsoptionen sind in der folgenden Tabelle aufgeführt:

Tabelle 1. RRUTIL.exe-Dateien und zugehörige Anpassungsoptionen

Datei / Verzeichnis	**Anpassungsoptionen**
\MININT\SYSTEM32 WINBOM.INI	Statische IP-Adresse hinzufügen, Grafikauflösung ändern
\MININT\INF \MININT\SYSTEM32\DRIVERS	Einheitentreiber hinzufügen
MAINBK.BMP	Hintergrund der Umgebung ändern
MINIMAL_TOOLBAR(1).INI	Adressleiste inaktivieren
NORM1.INI	Browser "Opera" konfigurieren, Adressleiste von Opera inaktivieren, Proxy-Einstellungen von Opera ändern, festgelegtes Downloadverzeichnis angeben, der Liste der für den Download verfügbaren Dateien bestimmte Dateierweiterungen hinzufügen, Verhalten von Dateien mit bestimmten Erweiterungen ändern
OPERA_010.CMD	Windows-Favoriten des Benutzers ausschließen
OPERA6.INI	Browser "Opera" konfigurieren, Adressleiste inaktivieren
PEACCESS*xx*.INI (wobei *xx* für den Sprachencode steht)	Preboot-Umgebung: wichtige GUI-Schriftarten, Hintergrund der Umgebung, Einträge und Funktionen des linken und des rechten Fensters, HTML-Hilfesystem
STANDARD_MENU.INI	Anzeige des Fensters zum Speichern von Dateien und Ordnern aktivieren

RRUTIL.EXE verwenden

Das Dienstprogramm RRUTIL.EXE und andere in diesem Handbuch erwähnte Dienstprogramme können Sie über die Website herunterladen, über die dieses Handbuch bereitgestellt wird.

Mit den folgenden Schritten können Sie Dateien aus der Umgebung von Rescue and Recovery abrufen oder in ihr speichern. Die angegebenen Schritte fallen bei allen Anpassungen von Dateien in der Umgebung von Rescue and Recovery an.

Gehen Sie wie folgt vor, um RRUTIL.EXE zu verwenden:

1. Kopieren Sie RRUTIL.EXE in das Stammverzeichnis von Laufwerk C.
2. Erstellen Sie die Datei GETLIST.TXT durch die Eingabe der folgenden Syntax:

   `\preboot\usrintfc\`*`Dateiname`*

   Speichern Sie die Datei unter C:\TEMP\GETLIST.TXT.
3. Geben Sie an einer Eingabeaufforderung den Befehl RRUTIL.EXE mit einem der in der folgenden Tabelle beschriebenen Schalter ein. Schließen Sie dann den Befehl mit den entsprechenden Parametern ab (siehe folgende Tabelle).

Tabelle 2. Befehls- und Schalteroptionen

Befehls- und Schalteroptionen	Ergebnis
`RRUTIL -l1`	Listet den Inhalt des Verzeichnisses ″preboot″ auf.
`RRUTIL -l2`	Listet den Inhalt des Verzeichnisses ″minint″ auf.
`RRUTIL -l4`	Listet den Inhalt des Stammverzeichnisses von Laufwerk C bzw. der Partition vom Typ 12 auf.
`RRUTIL -g C:\temp\getlist.txt C:\temp`	Ruft Dateien aus der Preboot-Partition ab.
`RRUTIL -d C:\temp\ dellist.txt`	Löscht Dateien aus der Preboot-Partition.
`RRUTIL -p C:\temp`	Fügt Dateien in der Preboot-Partition hinzu bzw. ersetzt Dateien in diesem Bereich.
`RRUTIL -r` *`Pfad \alter_Name.ext neuer_Name.ext`* `RRUTIL -r \temp\rr\test.txt test2.txt` (Die Datei befindet sich im Verzeichnis preboot\rr.)	Benennt eine Datei in der Predesktop Area um.
`RRUTIL -bp C:\temp`	Aktualisiert bzw. ersetzt Dateien in der virtuellen Partition RRUBACKUPS.
`RRUTIL -bl` *`Pfad`* RRUTIL -bl listet die Daten in `C:\rr-list.txt` auf `rrutil -bl c:\rrtemp`	Listet das Verzeichnis RRBACKUPS auf
`RRUTIL -br RRbackups\C\n` (wobei n für die Sicherungsnummer steht)	Löscht den Inhalt der Sicherung.
`RRUTIL -bg C:\temp\bgetlist.txt C:\temp`	Kopiert einzelne Dateien aus dem Verzeichnis \RRUBACKUPS.
`RRUTIL -s`	Zeigt den von RRUBACKUPS verwendeten Speicherplatz an.

4. Nach Ausführung der Abrufroutine (-g) können Sie die Datei mit einem Standardtexteditor bearbeiten.

Beispiel: PEACCESSIBMxx.INI

Dieses Beispiel bezieht sich auf die Datei PEACCESSIBM*xx*.INI, bei der es sich um eine Konfigurationsdatei handelt ist, in der Sie Elemente der Umgebung von Rescue and Recovery anpassen können (siehe „Preboot-Umgebung anpassen" auf Seite 23).

Anmerkung: Die Zeichen *xx* im Dateinamen stehen für die folgenden Sprachencodes aus zwei Buchstaben:

Tabelle 3. Sprachencodes

Sprachencode	Sprache
br	Brasilianisches Portugiesisch
dk	Dänisch
en	Englisch
fi	Finnisch
fr	Französisch
gr	Deutsch
it	Italienisch
jp	Japanisch
kr	Koreanisch
nl	Niederländisch
no	Norwegisch
po	Portugiesisch
sc	Vereinfachtes Chinesisch
sp	Spanisch
sv	Schwedisch
tc	Traditionelles Chinesisch

Gehen Sie wie folgt vor, um die Datei PEACCESSIBMEN.INI aus der Umgebung von Rescue and Recovery abzurufen:

1. Erstellen Sie die Datei GETLIST.TXT mit den folgenden Parametern:
   ```
   \preboot\reboot\usrintfc\PEAccessIBMen.ini
   ```
2. Speichern Sie die Datei unter C:\TEMP\GETLIST.TXT.
3. Geben Sie an einer Eingabeaufforderung den folgenden Befehl ein:
   ```
   C:\RRUTIL-g C:\temp\getlist.txt C:\temp
   ```

Gehen Sie wie folgt vor, um die Datei PEACCESSIBMEN.INI zurück in die Umgebung von Rescue and Recovery zu speichern. Geben Sie an einer Eingabeaufforderung den folgenden Befehl ein:

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

Anmerkung: Die Speicherungsroutine (**-p**) verwendet die Verzeichnisstruktur, die mit der Abrufroutine (**-g**) erstellt wurde. Damit die bearbeitete Datei korrekt gespeichert wird, müssen Sie sicherstellen, dass sich die bearbeitete Datei wie im nachfolgenden Beispiel angegeben in dem Verzeichnis befindet, das in der Datei GETLIST.TXT verwendet wird:

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

Beispiel: Einheitentreiber zur Predesktop Area hinzufügen

1. Rufen Sie die jeweiligen Einheitentreiber von der Website der Herstellerfirma oder über eine andere Quelle ab.
2. Erstellen Sie die folgenden Verzeichnisstrukturen:

   ```
   C:\TEMP\MININT\INF

   C:\TEMP\MININT\SYSTEM32\DRIVERS
   ```
3. Kopieren Sie alle INF-Dateien für Netztreiber in das Verzeichnis MININT\INF. (Die Datei E100B325.INF muss sich beispielsweise im Verzeichnis \MININT\INF befinden.)
4. Kopieren Sie alle SYS-Dateien in das Verzeichnis \MININT\SYSTEM32\DRIVERS. (Die Datei E100B325.SYS muss sich beispielsweise im Verzeichnis \MININT\SYSTEM32\DRIVERS befinden.)
5. Kopieren Sie alle zugehörigen Dateien mit der Erweiterung DLL und EXE oder sonstigen Dateien in das Verzeichnis \MININT\SYSTEM32\DRIVERS. (Die Dateien E100B325.DIN oder INTELNIC.DLL müssen sich beispielsweise im Verzeichnis MININT\SYSTEM32\DRIVERS befinden.)

   Anmerkungen:
   a. Katalogdateien sind nicht erforderlich, da sie in der Umgebung von Rescue and Recovery nicht verarbeitet werden. Die oben genannten Anweisungen gelten für alle Einheitentreiber, die für die Konfiguration des Computers erforderlich sein können.
   b. Aufgrund der Einschränkungen bei Windows Professional Edition müssen Sie möglicherweise einige Konfigurationsanwendungen bzw. -einstellungen manuell in Form von Aktualisierungen der Registrierungsdatenbank ausführen.
6. Geben Sie die folgende Befehlszeile ein, um die Einheitentreiber in die Umgebung von Rescue and Recovery zu stellen:

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

Preboot-Umgebung anpassen

Durch die Bearbeitung der Konfigurationsdatei PEAACCESSIBM*xx*.INI (wobei *xx* für den Sprachencode steht) können Sie die folgenden Elemente der Umgebung von Rescue and Recovery anpassen:

- Schriftarten der grafischen Hauptbenutzerschnittstelle (GUI)
- Hintergrund der Umgebung
- Einträge und Funktionen im linken Fenster der Benutzerschnittstelle
- HTML-Hilfesystem für die Umgebung von Rescue and Recovery

Anmerkung: Weitere Informationen zum Abrufen, Bearbeiten und Ersetzen der Datei PEACCESSIBMEN.INI finden Sie im Abschnitt „Beispiel: PEACCESSIBMxx.INI" auf Seite 22.

Schriftart der grafischen Hauptbenutzerschittstelle ändern

Sie können die Schriftart der grafischen Hauptbenutzerschnittstelle (GUI) ändern. Beachten Sie, dass bei Verwendung der Standardeinstellungen, je nach Sprache und Zeichen, möglicherweise nicht alle Zeichen korrekt angezeigt werden. Der Abschnitt [Fonts] in der Datei PEACCESSIBM*xx*.INI (wobei *xx* für den Sprachencode steht) enthält die Standardeinstellungen für die angezeigte Schriftart. Für die meisten Einzelbytezeichensätze gelten die folgenden Standardeinstellungen:

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

Je nach Zeichensatz und optischen Anforderungen können auch die nachfolgend angegebenen Schriftarten für die Umgebung von Rescue and Recovery verwendet werden. An dieser Stelle nicht genannte Schriftarten sind möglicherweise ebenfalls kompatibel, wurden jedoch nicht getestet:
- Courier
- Times New Roman
- Comic Sans MS

Hintergrund der Umgebung ändern

Beim Hintergrund im rechten Fenster handelt es sich um eine Bitmap-Datei (MAINBK.BMP). Diese Bitmap-Datei befindet sich im Verzeichnis \PREBOOT\USRINTFC. Wenn Sie eine eigene Bitmap-Datei für den Hintergrund im rechten Fenster erstellen möchten, müssen Sie folgende Abmessungen verwenden:
- Breite: 620 Pixel
- Höhe: 506 Pixel

Sie müssen die Datei in das Verzeichnis \PREBOOT\USRINTFC stellen, damit Rescue and Recovery den gewünschten Hintergrund darstellt.

Anmerkung: Weitere Informationen zum Abrufen, Bearbeiten und Ersetzen der Datei MAINBK.BMP finden Sie im Abschnitt „RRUTIL.EXE verwenden" auf Seite 21.

Einträge und Funktionen im linken Fenster ändern

Zum Ändern der Einträge im linken Fenster ist es erforderlich, die Datei PEACCESSIBM*xx*.INI zu bearbeiten (wobei *xx* für den Sprachencode steht). Weitere Informationen zum Abrufen der Datei PEACCESSIBM*xx*.INI aus der Umgebung von Rescue and Recovery und zum Ersetzen der Datei finden Sie im Abschnitt „RRUTIL.EXE verwenden" auf Seite 21.

Rescue and Recovery weist im linken Fenster 21 Einträge auf. Obwohl es sich um verschiedene Funktionen handelt, haben die einzelnen Einträge dieselben Grundelemente. Im Folgenden ein Beispiel eines Eintrags im linken Fenster:

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

Tabelle 4. Einträge im linken Fenster und Anpassungsoptionen

Eintrag	Anpassungsoptionen
00-01	Ist vollständig anpassbar.
02	Muss eine Schaltfläche vom Typ 1 bleiben (siehe Tabelle 5 auf Seite 25). Der Text kann geändert werden. Es kann eine Anwendung oder Hilfefunktion definiert werden. Ein Symbol kann nicht hinzugefügt werden.
03-06	Ist vollständig anpassbar.
07	Muss eine Schaltfläche vom Typ 1 bleiben. Der Text kann geändert werden. Es kann eine Anwendung oder Hilfefunktion definiert werden. Ein Symbol kann nicht hinzugefügt werden.
08-10	Ist vollständig anpassbar.
11	Muss eine Schaltfläche vom Typ 1 bleiben. Der Text kann geändert werden. Es kann eine Anwendung oder Hilfefunktion definiert werden. Ein Symbol kann nicht hinzugefügt werden.

Tabelle 4. Einträge im linken Fenster und Anpassungsoptionen (Forts.)

Eintrag	Anpassungsoptionen
16	Muss eine Schaltfläche vom Typ 1 bleiben. Der Text kann geändert werden. Es kann eine Anwendung oder Hilfefunktion definiert werden. Ein Symbol kann nicht hinzugefügt werden.
17–22	Ist vollständig anpassbar.

Eintragstypen definieren: **Button00** muss eine eindeutige Kennung darstellen. Die Zahl bestimmt die Reihenfolge, in der die Schaltflächen im linken Fenster angezeigt werden.

Button00=[0-8] Dieser Parameter bestimmt den Schaltflächentyp. Es kann eine ganze Zahl von 0 bis 8 angegeben werden. Typ und Verhalten der einzelnen Schaltflächen können Sie der folgenden Tabelle entnehmen:

Tabelle 5. Parameter des Eintragstyps

Parameter	Schaltflächentyp
0	Leeres Feld. Verwenden Sie diesen Wert, wenn eine Zeile nicht verwendet werden und leer bleiben soll.
1	Bereichsüberschrift. Verwenden Sie diese Einstellung, um eine Überschrift für eine größere Gruppe oder einen Bereich anzugeben.
2	Anwendungsaufruf. Definiert eine Anwendungs- bzw. Befehlsdatei, die gestartet werden soll, wenn der Benutzer auf die betreffende Schaltfläche bzw. den jeweiligen Text klickt.
3	Opera-Hilfe für die Umgebung von Rescue and Recovery. Definiert das Hilfethema, das mit dem Browser "Opera" aufgerufen werden soll.
4	Zeigt vor dem Start der Funktion ein Nachrichtenfenster an. Verwenden Sie diese Werte, um die GUI anzuweisen, dem Benutzer eine Nachricht darüber anzuzeigen, dass der Computer erneut gestartet werden muss, bevor die angegebene Funktion ausgeführt wird.
5	Reserviert für Lenovo Group Ltd
6	Reserviert für Lenovo Group Ltd
7	Start mit Rückkehrcode. Die nachfolgenden Felder bewirken, dass die Umgebung auf einen Rückkehrcode der gestarteten Anwendung wartet, bevor mit der Verarbeitung fortgefahren wird. Als Rückkehrcode wird ein Wert in der Umgebungsvariablen %errorlevel% erwartet.
8	Anwendung starten. Die GUI ruft vor dem Start der Anwendung den Landes- und Sprachencode ab. Diese Einstellung wird für Web-Links verwendet, denen CGI-Scripts zugeordnet sind, mit denen eine Webseite mit einem bestimmten Landes- bzw. Sprachencode aufgerufen wird.
9	Reserviert für Lenovo Group Ltd
10	Reserviert für Lenovo Group Ltd

Eintragsfelder definieren:

Button00=[0-10], "Titel"
Der auf den Parameter für den Schaltflächentyp folgende Text gibt den Text bzw. Titel der betreffenden Schaltfläche an. Zu lange Texte, die über den Rand des linken Fensters hinausreichen, werden abgeschnitten und durch Auslassungspunkte ergänzt, um anzuzeigen, dass weitere Zeichen folgen. Bei Verwendung der Kurzinfo wird der vollständige Titel angezeigt.

Button00=[0-10], "Titel", file.bmp
Nach dem Titeltext können Sie den Namen der Bitmap-Datei angeben, die als Symbol für die neue Schaltfläche verwendet werden soll. Die Bitmap-Datei wird nur korrekt platziert, wenn sie eine Größe von 15 x 15 Pixel nicht überschreitet.

Button00=[0-10], "Titel", file.bmp, [0 oder 1]
Diese Einstellung bewirkt, dass der Eintrag von der Umgebung angezeigt bzw. ausgeblendet wird. Bei einem Wert von `0` wird der Eintrag ausgeblendet. In diesem Fall wird mit dem Wert `0` eine Leerzeile angezeigt. Bei einem Wert von 1 wird der Eintrag angezeigt.

Button00=[0-10], "Titel", file.bmp, [0 oder 1], 1
Dies ist eine reservierte Funktion, die immer den Wert 1 aufweisen muss.

Button00=[0-10], "Titel", file.bmp, [0 oder 1], 1, [0 oder 1]
Geben Sie an dieser Stelle eine 1 an, wenn vor dem Start einer Anwendung ein Kennwort angefordert werden soll. Wenn Sie diesen Wert auf `0` setzen, wird vor dem Start der angegebenen Anwendung kein Kennwort angefordert.

Button00=[0-10], "Titel", file.bmp, [0 oder 1], 1, [0 oder 1], %sysdrive%[Pfad\ausführbare Datei]
Der Wert von `%sysdrive@` muss ein Laufwerkbuchstabe eines Bootlaufwerks sein. Auf den Laufwerkbuchstaben muss ein vollständig qualifizierter Pfad zu der jeweiligen Anwendung bzw. Befehlsdatei folgen.

Button00=[0-10], "Titel", file.bmp, [0 oder 1], 1, [0 oder 1],%sysdrive%[Pfad\ausführbare Datei], [Parameter]
Sie können eine beliebige Anzahl von Parametern angeben, die für die Zielanwendung erforderlich sind, die gestartet wird.

Wenn Sie für einige Felder keine Werte angeben möchten, müssen Sie die erforderlichen Kommazeichen eingeben, damit die Schaltflächendefinition nicht ungültig wird und ordnungsgemäß ausgeführt werden kann. Wenn Sie beispielsweise die Gruppenüberschrift ″Wiederherstellen″ erstellen möchten, müssen Sie für diesen Eintrag folgenden Code eingeben:

```
Button04=1, "Wiederherstellen",,,,,,
```

Die Einträge 02, 07, 11 und 16 müssen als Typ `0` (oder als Überschrift) definiert sein und werden immer korrekt in den Zahlen eingereiht. Die Verfügbarkeit der Einträge, die zu den Überschriften gehören, kann verringert werden, indem Sie die vollständig anpassbaren Einträge im linken Fenster mit dem Typ 0 (Leerzeilen) definieren. Die Gesamtzahl der Einträge darf jedoch nicht über 23 liegen.

In der folgenden Tabelle finden Sie eine Übersicht über die Funktionen und Dateien, die Sie über die Einträge im linken Fenster starten können:

Tabelle 6. Funktionen und ausführbare Dateien im linken Fenster

Funktion	Ausführbare Datei
Dateien wiederherstellen	WIZRR.EXE
Über Sicherung wiederherstellen	WIZRR.EXE
Migrationsdatei erstellen	WIZRR.EXE
Browser öffnen	OPERA.EXE
Netzlaufwerk zuordnen	MAPDRV.EXE
Diagnose für Hardware durchführen	RDIAGS.CMD; startet nur bei von IBM und Lenovo vorinstallierten Modellen die Anwendung "PC Director"
Diagnosedisketten erstellen	DDIAGS.CMD

Einträge und Funktionen im rechten Fenster ändern

Zum Ändern der Einträge im rechten Fenster ist es erforderlich, die Datei PEACCESSIBM*xx*.INI zu bearbeiten (wobei *xx* für den Sprachencode steht). Informationen zum Abrufen der Datei PEACCESSIBM*xx*.INI aus der Umgebung von Rescue and Recovery und zum Ersetzen der Datei finden Sie im Abschnitt „Beispiel: PEACCESSIBMxx.INI" auf Seite 22.

Sie können die Funktionsverknüpfungen und die Benutzernachrichten sowie den Fensterstatus des rechten Fensters anpassen.

Funktionsverknüpfungen im rechten Fenster anpassen: Die Funktionsverknüpfungen im oberen Bereich des rechten Fensters können Sie über den Abschnitt [TitleBar] der Datei PEACCESSIBM*xx*.INI ändern (wobei *xx* für den Sprachencode steht). Diese Verknüpfungen verhalten sich ähnlich wie die Einträge im linken Fenster. Es können Schaltflächenwerte von 00 bis 04 angegeben werden. Anwendungen, die im linken Fenster aufgerufen werden können, können auch über Einträge im Abschnitt [TitleBar] gestartet werden. Eine vollständige Liste der ausführbaren Dateien, die über die Titelleiste gestartet werden können, finden Sie im Abschnitt „RRUTIL.EXE verwenden" auf Seite 21.

Benutzernachrichten und Fensterstatus ändern: PEACCESSIBM*xx*.INI (wobei *xx* für den Sprachencode steht) enthält zwei Abschnitte mit Nachrichten für den Benutzer, die Sie ändern können:

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

Die Eingangsanzeige wird im Abschnitt [Welcome] der Datei PEACCESSIBM*xx*.INI definiert (wobei *xx* für den Sprachencode steht). Je nachdem, welche Änderungen im linken Fenster vorgenommen wurden, können Sie die Angaben in der Titelzeile und in den Zeilen 01 bis 12 ändern.

Sie können die Schriftart für Titel, Kopfzeile und Fettdruck im folgenden Abschnitt festlegen:

```
[Welcome]
Title = "Willkommen bei Rescue and Recovery"
Line01 = "Der Arbeitsbereich von Rescue and Recovery(TM) enthält Tools,
mit denen Sie Fehler beheben können, die den Zugriff auf die Windows(R)-Umgebung
verhindern."
Line02 = "Sie können Folgendes tun:"
Line03 = "* Ihre Dateien, Ordner oder Sicherungskopien mit Rescue and Recovery(TM)
sichern und wiederherstellen"
Line05 = "* Ihre Systemeinstellungen"
Line06 = "und Kennwörter konfigurieren"
Line07 = "* Über das Internet"
Line08 = "kommunizieren und eine Verbindung zur Lenovo Unterstützungssite aufbauen"
Line09 = "* Fehler"
Line10 = "mit dem Diagnoseprogramm erkennen und beheben"
Line11 = "Die Funktionen können je nach Installationsoptionen unterschiedlich
ausfallen. Weitere Informationen finden Sie, indem Sie auf 'Einführung' im
Menü von Rescue and Recovery klicken."
Line12 = "HINWEIS:"
Line13 = "Durch die Verwendung dieser Software sind Sie
an die Bedingungen der Lizenzvereinbarung gebunden. Klicken Sie
zum Anzeigen der Lizenz in der Symbolleiste von Rescue and Recovery
auf 'Hilfe' und dann auf 'Lizenzvereinbarung anzeigen'."
Continue = "Weiter"
NowShow = "Diese Informationen nicht mehr anzeigen"
NoShowCk =0
WelcomeTitle = "Arial Bold"
WelcomeText = "Arial"
WelcomeBold = "Arial Bold"
```

Die folgenden Einstellungen gelten für Hilfefunktionen zur Titelleiste in der Benutzerschnittstelle:

Command0
Zu startende HTML-Seite für die Basishilfetextseite

Command1
HTML-Seite für die Lenovo Lizenzvereinbarung

HELP Hilfe

LICENSE
Lizenz

CANCEL
Abbruch

Command0
%sysdrive%Preboot\Helps\en\f_welcom.htm

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

Wenn die Eingangsanzeige übersprungen werden soll, müssen Sie den Eintrag `NoShowCk=0` in `NoShowCk=1` ändern. Die Bildschirmschriftarten für Titel und Begrüßungstext können Sie ändern, indem Sie die letzten drei Zeilen des Abschnitts wie gewünscht anpassen.

Anmerkung: Die Zeilen 13 und 14 dürfen nicht geändert oder gelöscht werden.

Im Abschnitt [REBOOT] der Datei PEACCESSIBM*xx*.INI (wobei *xx* für den Sprachencode steht) können Sie die Werte der folgenden Zeilen ändern:

```
NoShowChk=
RebootText=
```

Für "NoShowChk" kann `0` oder `1` angegeben werden, so dass der Benutzer den Begrüßungstext bei Bedarf ausblenden kann. Wenn der Benutzer beim Anzeigen des Begrüßungstexts auf das entsprechende Markierungsfeld klickt, wird der Wert auf `0` gesetzt. Wenn die Nachricht angezeigt werden soll, ändern Sie den Wert in `1`. Bei Bedarf können Sie auch die für Nachrichten verwendete Schriftart im Abschnitt [REBOOT] ändern. Dieser Wert kann beispielsweise wie folgt angegeben werden:

```
RebootText = "Arial"
```

Anmerkung: Die Abschnitte [Messages], [EXITMSG] und [HelpDlg] der Datei PEACCESSIBM*xx*.INI (wobei *xx* für den Sprachencode steht) können nicht angepasst werden.

Den Browser "Opera" konfigurieren

Der Browser "Opera" verfügt über zwei Konfigurationsdateien. Eine davon enthält die Standardkonfiguration. Die andere Datei enthält die aktive Konfiguration. Ein Endbenutzer kann die aktive Konfiguration ändern. Diese Änderungen gehen jedoch beim erneuten Start von Rescue and Recovery verloren.

Wenn Sie die Browser-Einstellungen dauerhaft ändern möchten, müssen Sie die Kopien der Dateien OPERA6.INI und NORM1.INI auf dem Laufwerk %systemdrive% (C:) im Verzeichnis C:\PREBOOT\OPERA\PROFILE bearbeiten. Die temporäre, "aktive" Kopie der Datei OPERA6.INI befindet sich auf dem RAM-Laufwerk (Z:) im Verzeichnis Z:\PREBOOT\OPERA\PROFILE.

Anmerkungen:

1. Weitere Informationen zum Abrufen, Bearbeiten und Speichern der Dateien OPERA6.INI und NORM1.INI finden Sie im Abschnitt „RRUTIL.EXE verwenden" auf Seite 21.
2. Der Arbeitsbereich von Opera wurde geändert, um die Sicherheitsfunktionen zu verbessern. Einige Browser-Funktionen stehen deshalb nicht mehr zur Verfügung.

E-Mail

Rescue and Recovery stellt Unterstützung für webbasierte E-Mail über den Browser "Opera" bereit. Opera bietet zwar E-Mail über IMAP, das über umfangreiche unternehmensweite Konfigurationen aktiviert werden kann; dies wird jedoch nicht unterstützt. Weitere Informationen zum Aktivieren dieser Unterstützung finden Sie im Handbuch für Systemadministratoren im World Wide Web unter der Adresse:

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

Adressleiste inaktivieren

Gehen Sie wie folgt vor, um die Adressleiste von Opera zu inaktivieren:

1. Rufen Sie die Datei MINIMAL_TOOLBAR(1).INI im Verzeichnis C:\PREBOOT\OPERA\PROFILE\TOOLBAR unter Verwendung des Prozesses RRUTIL ab (siehe „RRUTIL.EXE verwenden" auf Seite 21).
2. Öffnen Sie die Datei zum Bearbeiten.
3. Suchen Sie den Abschnitt [Document Toolbar] in dieser Datei.
4. Suchen Sie den Eintrag "Address0".
5. Setzen Sie ein Semikolon (;) als Kommentarzeichen vor den Eintrag "Address0".

   Anmerkung: Wenn Sie nun mit Schritt 7 fortfahren, wird die Funktionsleiste von Opera inaktiviert, die Funktionsleistengrafik und die nicht mehr aktivierbare Schaltfläche "Go" werden jedoch weiterhin angezeigt. Zum Entfernen dieser Schaltfläche und der Funktionsleiste müssen Sie mit Schritt 6 fortfahren.
6. Setzen Sie jeweils ein Semikolon vor die folgenden Einträge:

   ```
   Button1, 21197=Go Zoom2
   ```
7. Speichern Sie die Datei.
8. Stellen Sie die Datei unter Verwendung des Prozesses RRUTIL in das entsprechende Verzeichnis (siehe „RRUTIL.EXE verwenden" auf Seite 21). Die Adressleiste ist während der Ausführung von Opera inaktiviert.

Lesezeichen anpassen

Opera wurde so vorkonfiguriert, dass Lesezeichen in der Datei Z:\OPERADEF6.ADR auf dem RAM-Laufwerk gelesen werden. Diese Datei wird beim Start von Rescue and Recovery über den Code in der Startroutine generiert. Die Startroutine importiert automatisch Windows Internet Explorer-Lesezeichen und fügt einige zusätzliche Lesezeichen hinzu. Die beim Start generierte Datei auf dem RAM-Laufwerk kann während des Systembetriebs geändert werden. Daher sollten Sie Lesezeichen im Internet Explorer hinzufügen. Diese werden beim Start der Umgebung von Rescue and Recovery automatisch importiert.

Sie können einige oder alle der im Internet Explorer definierten Favoriten ausschließen. Gehen Sie wie folgt vor, wenn Sie Favoriten von bestimmten Windows-Benutzern ausschließen möchten:

1. Rufen Sie die Datei C:\PREBOOT\STARTUP\OPERA_010.CMD unter Verwendung des Prozesses RRUTIL ab (siehe „RRUTIL.EXE verwenden" auf Seite 21).
2. Öffnen Sie die Datei zum Bearbeiten.
3. Suchen Sie in der CMD-Datei die folgende Zeile: PYTHON.EXE.FAVS.PYC Z:\OPERADEF6.ADR
4. Geben Sie am Ende dieser Codezeile die Namen der betreffenden Windows-Benutzer in Anführungszeichen an, deren Favoriten Sie ausschließen möchten. Wenn Sie beispielsweise die Favoriten von allen Benutzern und Administratoren ausschließen möchten, müssen Sie folgende Codezeile einfügen:

   ```
   python.exe favs.pyc z:\Operadef6.adr "All Users, Administrator"
   ```
5. Speichern Sie die Datei.
6. Stellen Sie die Datei unter Verwendung des Prozesses RRUTIL in das entsprechende Verzeichnis (siehe „RRUTIL.EXE verwenden" auf Seite 21).

Gehen Sie wie folgt vor, wenn kein Favorit aus dem Internet Explorer im Browser der Umgebung von Rescue and Recovery angezeigt werden soll:

1. Rufen Sie die Datei C:\PREBOOT\STARTUP\OPERA_010.CMD unter Verwendung des Prozesses RRUTIL zur Bearbeitung ab (siehe „RRUTIL.EXE verwenden" auf Seite 21).

2. Suchen Sie in der CMD-Datei die folgende Zeile: PYTHON.EXE.FAVS.PYC Z:\OPERADEF6.ADR
3. Führen Sie einen der folgenden Schritte aus:
   a. Geben Sie wie folgt am Anfang der Zeile REM ein:

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

   b. Löschen Sie diese Codezeile in der Datei.
4. Speichern Sie die Datei.
5. Stellen Sie die Datei unter Verwendung des Prozesses RRUTIL in das entsprechende Verzeichnis zurück (siehe „RRUTIL.EXE verwenden" auf Seite 21).

Proxy-Einstellungen ändern

Gehen Sie wie folgt vor, um die Proxy-Einstellungen von Opera zu ändern:

1. Rufen Sie die Datei C:\PREBOOT\OPERA\PROFILE\NORM1.INI unter Verwendung des Prozesses RRUTIL zur Bearbeitung ab (siehe „RRUTIL.EXE verwenden" auf Seite 21).
2. Fügen Sie folgenden Abschnitt am Ende der Datei NORM1.INI ein:

   Anmerkung: Die Variable [0 oder 1] gibt an, dass der betreffende Eintrag, dem ein Markierungsfeld zugeordnet ist, aktiviert (1) oder inaktiviert (0) ist.

   ```
   [Proxy]
   Use HTTPS=[0 oder 1]
   Use FTP=[0 oder 1]
   Use GOPHER=[0 oder 1]
   Use WAIS=[0 oder 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 oder 1]
   Use HTTP=[0 oder 1]
   Use Automatic Proxy Configuration= [0 oder 1]
   Automatic Proxy Configuration URL= [URL]
   No Proxy Servers Check= [0 oder 1]
   No Proxy Servers =<IP-Adressen>
   ```

3. Speichern Sie die Datei.
4. Stellen Sie die Datei unter Verwendung des Prozesses RRUTIL in das entsprechende Verzeichnis zurück (siehe „RRUTIL.EXE verwenden" auf Seite 21).

Geben Sie zum Hinzufügen eines HTTP-, HTTPS-, FTP-, Gopher- oder WAIS-Proxy nach der jeweiligen Zeile Folgendes ein: `=<Adresse des Proxy>`. Wenn die Adresse des Proxy-Servers z. B. "http://www.your company.com/proxy" lautet, muss die Zeile für den HTTP-Server wie folgt angegeben werden:

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

Wenn Sie eine Portangabe hinzufügen möchten, müssen Sie nach der Adresse ein Semikolon gefolgt von der Portnummer eingeben. Dasselbe gilt für die Felder "No Proxy Servers" und "Automatic Proxy Configuration URL".

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

Vollständigen Pfad zum Herunterladen aktivieren/angeben

Die Anzeige des Fensters zum Speichern von Dateien und Ordnern kann über verschiedene Einstellungen aktiviert werden. Im Folgenden wird die einfachste Variante beschrieben:

1. Rufen Sie die Datei C:\PREBOOT\OPERA\DEFAULTS\STANDARD_MENU.INI unter Verwendung des Prozesses RRUTIL ab (siehe „RRUTIL.EXE verwenden" auf Seite 21).
2. Suchen Sie im Abschnitt `[Link Popup Menu]` die folgende Zeichenfolge:

   ```
   ;;Item, 50761
   ```
3. Löschen Sie die zwei Semikolons, und speichern Sie die Datei. Beim nächsten Start von Rescue and Recovery kann der Endbenutzer die Option zum Speichern von Zieldateien und Zielordnern anzeigen, indem er mit der rechten Maustaste auf die entsprechende Verknüpfung klickt. Danach wird das Fenster zum Speichern von Dateien und Ordnern angezeigt.

   Anmerkung: Die oben angegebene Vorgehensweise gilt für direkte (d. h. nicht umgeleitete) Verknüpfungen. Wenn eine Verknüpfung z. B. auf ein Script mit der Erweiterung PHP verweist, speichert Opera nur das betreffende Script, jedoch nicht die Datei, auf die das Script verweist.
4. Stellen Sie die Datei unter Verwendung des Prozesses RRUTIL in die entsprechende Verzeichnisstruktur zurück (siehe „RRUTIL.EXE verwenden" auf Seite 21).

Gehen Sie wie folgt vor, um ein festes Verzeichnis für Downloads anzugeben:

1. Rufen Sie die Datei C:\PREBOOT\OPERA\NORM1.INI unter Verwendung des Prozesses RRUTIL ab (siehe „RRUTIL.EXE verwenden" auf Seite 21).
2. Suchen Sie in dieser Datei folgende Zeile:

   ```
   Download Directory=%OpShare%
   ```
3. Geben Sie für `%OpShare%` den vollständigen Pfad zu dem Verzeichnis an, in das die zu speichernden Dateien heruntergeladen werden sollen.
4. Speichern Sie die Datei NORM1.INI. Beim nächsten Start von Rescue and Recovery speichert Opera heruntergeladene Dateien im angegebenen Verzeichnis.
5. Stellen Sie die Datei unter Verwendung des Prozesses RRUTIL in das entsprechende Verzeichnis zurück (siehe „RRUTIL.EXE verwenden" auf Seite 21).

Anmerkungen:

1. Wenn Sie für den Pfad zum Herunterladen einen vollständigen Pfad angeben, stellen Sie dadurch nicht unbedingt sicher, dass Benutzer die Zieldatei speichern können, auch nicht, wenn es sich um eine umgeleitete Verknüpfung handelt.
2. Opera wurde so konfiguriert, dass nur die Dateitypen mit der Erweiterung ZIP, EXE und TXT heruntergeladen werden und dass sich nur das Verhalten von Opera für diese Dateitypen ändert. (Es gibt eine Vielzahl unterschiedlicher Erweiterungen mit drei Buchstaben. So wenig wie die Umgebung von Rescue and Recovery als Alternative für die Windows-Umgebung gedacht ist, so wenig soll der Browser "Opera" einen mit allen Diensten ausgestatteten Browser ersetzen. Der Internetzugriff soll es Benutzern ermöglichen, Dateien abzurufen und auszuführen. Die Anzahl der zulässigen Dateitypen ist naturgemäß begrenzt. Für Wiederherstellungszwecke sind die Dateitypen mit den Erweiterungen ZIP, EXE und TXT ausreichend. Wenn andere Dateitypen übertragen werden müssen, empfiehlt es sich allgemein, eine ZIP-Datei zu erstellen, die anschließend extrahiert werden kann.)

3. Die Dateitypen werden eher anhand des MIME-Typs als anhand der Dateierweiterung erkannt. Wird beispielsweise eine TXT-Datei in eine Datei mit der Erweiterung EUY umbenannt, wird diese Datei von Opera dennoch als Textdatei geöffnet.

Bestimmte Dateierweiterungen zur Liste der herunterladbaren Dateien hinzufügen

Sie können die Liste der Dateien, die vom Browser von Rescue and Recovery heruntergeladen werden können, bei Bedarf ergänzen. Gehen Sie wie folgt vor, um die Liste zu ergänzen:

1. Stellen Sie sicher, dass Opera und alle Opera-Fenster geschlossen sind, die Hilfedateien von Rescue and Recovery eingeschlossen.
2. Rufen Sie die Datei C:\PREBOOT\OPERA\NORM1.INI unter Verwendung des Prozesses RRUTIL ab (siehe „RRUTIL.EXE verwenden" auf Seite 21).
3. Suchen Sie den Abschnitt `[File Types]` in dieser Datei.
4. Überprüfen Sie mit der Suchfunktion, ob die gewünschte Dateierweiterung bereits in der Liste enthalten ist. Führen Sie anschließend einen der folgenden Schritte aus:
   - Gehen Sie wie folgt vor, wenn die gesuchte Erweiterung in der Liste enthalten ist, Dateien mit dieser Erweiterung jedoch nicht korrekt heruntergeladen werden:
     a. Ändern Sie den nach der Erweiterung angegebenen Wert von 8 in 1. (Der Wert 8 bewirkt, dass die betreffenden Dateien vom Browser ignoriert werden. Mit dem Wert 1 wird der Browser angewiesen, die Datei zu speichern.) Ändern Sie beispielsweise die Angabe

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

        in

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

     b. Suchen Sie in der Datei NORM1.TXT im Abschnitt [File Types Extension] den MIME-Typ der Datei. Suchen Sie beispielsweise nach der folgenden Angabe: VIDEO/MPEG=,8
     c. Ändern Sie den Wert ″,8″ wie folgt:

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

        Anmerkung: Ändern Sie den Wert nicht, wenn der gesetzte Wert bereits angegeben ist.
     d. Speichern Sie die Datei, und kopieren Sie sie in die Datei OPERA6.INI. Starten Sie Rescue and Recovery anschließend erneut, damit die Änderungen wirksam werden.
   - Gehen Sie wie folgt vor, wenn die gewünschte Erweiterung nicht in der Liste enthalten ist und Dateien des jeweiligen Typs nicht korrekt heruntergeladen werden:
     a. Suchen Sie in der Datei NORM1.INI im Abschnitt [File Types Extension] den temporären MIME-Eintrag, z. B. ″temporary=1,,,,lwp,prz,mwp,mas,smc,dgm,|″.
     b. Fügen Sie die gewünschte Dateierweiterung in der Liste hinzu. Verwenden Sie beispielsweise folgenden Eintrag, wenn Sie die Erweiterung CAB als zulässige Erweiterung angeben möchten:

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

Anmerkung: Komma und Verkettungszeichen müssen angegeben werden. Andernfalls wird diese Einstellung nicht korrekt umgesetzt. Wenn Komma oder Verkettungszeichen fehlen, werden möglicherweise alle Dateierweiterungen der Liste inaktiviert.

c. Speichern Sie die Datei im Verzeichnis C:\TEMP\.
d. Kopieren Sie die Datei nach OPERA6.INI.
e. Starten Sie den Arbeitsbereich von Rescue and Recovery erneut, damit die Änderungen wirksam werden.

Verhalten von Dateien mit bestimmten Erweiterungen ändern

Sie können das Verhalten von Dateien über die Werte in der Datei NORM1.INI steuern. Gehen Sie zum Ändern des Verhaltens von Dateien mit bestimmten Erweiterungen wie folgt vor:

1. Schließen Sie Opera und alle aktiven Opera-Fenster, einschließlich der Hilfedateien.
2. Öffnen Sie die Datei PREBOOT\OPERA\NORM1.INI unter Verwendung des Prozesses RRUTIL zur Bearbeitung (siehe „RRUTIL.EXE verwenden" auf Seite 21).
3. Suchen Sie im Abschnitt [File Types] der Datei die Erweiterung, mit der Sie arbeiten möchten. Gehen Sie beispielsweise wie folgt vor, wenn Sie alle TXT-Dateien im Ordner IBMSHARE speichern wollen.
4. Suchen Sie den folgenden Eintrag: TEXT/PLAIN=2,,,,TXT,|

   Anmerkung: Der Wert 2 bewirkt, dass der Text von Opera angezeigt wird. Mit dem Wert 1 wird der Browser angewiesen, die Zieldatei im Ordner IBMSHARE zu speichern.
5. Im vorliegenden Beispiel muss die Zeile für die Dateien mit der Erweiterung TXT anschließend wie folgt geändert werden:

   ```
   TEXT/PLAIN=1,,,,TXT,|
   ```
6. Speichern Sie die Datei, und stellen Sie sie unter Verwendung des Prozesses RRUTIL in das entsprechende Verzeichnis zurück (siehe „RRUTIL.EXE verwenden" auf Seite 21).
7. Starten Sie den Arbeitsbereich von Rescue and Recovery erneut, damit die Änderungen wirksam werden.

Statische IP-Adresse hinzufügen

Wenn Sie eine statische IP-Adresse hinzufügen möchten, müssen Sie die nachfolgend angegebenen Dateien ändern.

1. Rufen Sie die Datei \MININT\SYSTEM32 WINBOM.INI unter Verwendung des Prozesses RRUTIL ab (siehe „RRUTIL.EXE verwenden" auf Seite 21).
2. Fügen Sie in der Datei WINBOM.INI den Abschnitt [WinPE.Net] vor dem Abschnitt [PnPDriverUpdate] ein. Beachten Sie z. B. die folgende Datei: WINBOM.INI

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

```
[AppPreInstall]
```

Sie müssen im Abschnitt [WinPE.Net] die folgenden Zeilen hinzufügen.

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

Tabelle 7. Einträge der statischen IP-Adresse

Eintrag	Beschreibung
Gateway	Gibt die IP-Adresse eines IP-Routers an. Bei der Konfiguration eines Standard-Gateways wird eine Standardroute in der IP-Routetabelle erstellt. **Syntax:** Gateway = *xxx.xxx.xxx.xxx*
IPConfig	Gibt die IP-Adresse an, die von Windows PE verwendet wird, um eine Verbindung zum Netzwerk herzustellen. **Syntax:** IPConfig = *xxx.xxx.xxx.xxx*
StartNet	Gibt an, ob Netzservices gestartet werden sollen. **Syntax:** StartNet = *Yes* | *No*
SubnetMask	Gibt einen 32-Bit-Wert an, der es dem Empfänger des IP-Pakets ermöglicht, die Bestandteile Netz-ID und Host-ID in der IP-Adresse zu unterscheiden. **Syntax:** SubnetMask = *xxx.xxx.xxx.xxx*

3. Rufen Sie die Datei PREBOOT\IBMWORK NETSTART.TBI unter Verwendung des Prozesses RRUTIL ab (siehe „RRUTIL.EXE verwenden" auf Seite 21).
4. Ändern Sie

   ```
   factory -minint
   ```

   in

   ```
   factory -winpe
   ```
5. Setzen Sie die folgenden Zeilen auf Kommentar:

   ```
   regsvr32 /s netcfgx.dll
   netcfg -v -winpe
   net start dhcp
   net start nla
   ```
6. Stellen Sie die Dateien \IBMWORK NETSTART.TBI und \MININT\SYSTEM32 WINBOM.INI unter Verwendung des Prozesses RRUTIL zurück (siehe „RRUTIL.EXE verwenden" auf Seite 21).

Bildschirmauflösung ändern

Sie können die Bildschirmauflösung ändern, indem Sie die Standardauflösung des Predesktop (800 × 600 × 16 Bit) ändern. Gehen Sie wie folgt vor, um die Einstellungen zu ändern:

1. Rufen Sie die Datei MININT\SYSTEM32\WINBOM.INI unter Verwendung des Prozesses RRUTIL ab (siehe „RRUTIL.EXE verwenden" auf Seite 21).

2. Fügen Sie in der Datei WINBOM.INI die folgenden Einträge hinzu:

   ```
   [ComputerSettings]
   DisplayResolution=800x600x16 oder 1024x768x16
   Ändern Sie in der
   Datei "preboot\ibmwork\netstart.tbi" den Eintrag "factory-minint" in "factory-winpe".
   ```

   Beim Starten der Umgebung von Rescue and Recovery wird daraufhin ein zusätzliches Fenster mit den werkseitig vordefinierten Installationseinstellungen angezeigt. Die angezeigten Farben werden außerdem von Tausenden auf 256 reduziert.
3. Stellen Sie die Datei MININT\SYSTEM32\WINBOM.INI unter Verwendung des Prozesses RRUTIL in das entsprechende Verzeichnis zurück (siehe „RRUTIL.EXE verwenden" auf Seite 21).

Systemstartanwendungen

Über die Windows PE-Umgebung von Rescue and Recovery können ein Systemstartscript, Systemstartprogramme und angepasste Systemstartprogramme unterstützt werden. Diese Scripts oder Programme werden verarbeitet, bevor die Windows PE-Umgebung von Rescue and Recovery die Hauptseite der PE-Schnittstelle aufruft.

Das Script oder die Programme müssen im Verzeichnis Preboot\Startup gespeichert werden. Scripts und Programme in diesem Verzeichnis werden alphanumerisch verarbeitet. So würde also das Script A.BAT vor dem Script 1.EXE verarbeitet werden.

Gehen Sie wie folgt vor, um ein Script oder ein Programm in diesem Verzeichnis zu speichern:

1. Fordern Sie RRUTIL auf der Lenovo Site für Verwaltungstools von Rescue and Recovery unter der folgenden Adresse an:

   www.lenovo.com/ThinkVantage
2. Erstellen Sie das Verzeichnis ″temp″.
3. Erstellen Sie im Verzeichnis ″\temp″ die Verzeichnisstruktur ″\preboot\startup″.
4. Speichern Sie das Script oder das Programm unter dem Pfad ″\temp\preboot\startup″.
5. Geben Sie in einer Befehlszeile Folgendes ein: RRUTIL –p \temp
6. Um zu überprüfen, ob das Script oder das Programm erfolgreich kopiert wurde, geben Sie in einer Befehlszeile Folgendes ein: RRUTIL –g. Dadurch wird eine Datei mit der Bezeichnung ″getlist.txt″ generiert.
7. Suchen Sie in der Datei ″getlist.txt″ das Verzeichnis ″\preboot\startup″. Das Script oder das Programm sollte unter dieser Struktur aufgelistet sein.

Kennwörter

In der Predesktop Area stehen vier Kennwortoptionen zur Verfügung:

- Predesktop- oder Hauptkennwort
- Benutzer-ID und Kennwort oder Verschlüsselungstext
- Sicherungskennwort
- Kein Kennwort

Predesktop- oder Hauptkennwort

Sie können ein unabhängiges Kennwort für die Predesktop Area festlegen. Dieses Kennwort wird über die Befehlszeilenschnittstelle festgelegt. Es handelt sich hierbei um die einzige verfügbare Kennwortoption, wenn Client Security Solution nicht installiert ist.

Sie können dieses Kennwort für die Predesktop Area mit Hilfe des folgenden Befehls erstellen: C:\Program Files\IBM ThinkVantage\Client Security Solution\pe_setupmasterpwde.exe.

Dieser Befehl hat die folgenden Parameter:

Tabelle 8.

Parameter	Beschreibung
create password	Über diesen Parameter wird das tatsächliche Kennwort erstellt.
verify password	Über diesen Parameter wird überprüft, ob das Kennwort gültig ist und verwendet werden kann.
change currentPassword *neuesKennwort*	Über diesen Parameter kann das aktuelle Kennwort geändert werden.
exists	Über diesen Parameter wird überprüft, ob das Kennwort vorhanden ist.
silent	Über diesen Parameter werden alle Nachrichten ausgeblendet.
setmode values	0 = Keine Authentifizierung erforderlich. 1 = Benutzerspezifische Authentifizierung erforderlich. 2 = Hauptkennwort erforderlich.

Anmerkung: Ein Benutzer mit eingeschränkter Berechtigung kann dieses Kennwort nicht ändern, während ein Benutzer mit Administratorberechtigung das Kennwort für einen Benutzer mit eingeschränkter Berechtigung zurücksetzen kann.

Benutzer-ID und Kennwort oder Verschlüsselungstext

Diese Option verwendet Client Security Solution-Code für die Verwaltung des Kennworts oder des Verschlüsselungstexts. Über die Client Security-Anmeldung wird der Benutzer beim Starten der Predesktop Area aufgefordert, dieses Kennwort oder diesen Verschlüsselungstext einzugeben. Dies bietet in einer Umgebung mit mehreren Benutzern höhere Sicherheit. Ein angemeldeter Benutzer hat nur Zugriff auf seine Dateien; auf die Dateien eines anderen Benutzers kann der Benutzer nicht zugreifen.

Diese Option kann über die CSS-GUI oder über XML-Scripts festgelegt werden.

Sicherungskennwort

Das Sicherungskennwort kann über die GUI zum Festlegen von Kennwörtern oder über die Befehlszeilenschnittstelle "rrcmd" mit der Angabe der Sicherung festgelegt werden. Beispiel:

```
rrcmd backup location=L name=Sicherung password=Kennwort
rrcmd basebackup location=L name=Basissicherung password=Kennwort
rrcmd sysprepbackup location=L name="Sysprep Backup" password=Kennwort
```

Kein Kennwort

Bei dieser Option wird keine Authentifizierung verwendet, der Benutzer kann ohne die Eingabe eines Kennworts auf die Predesktop Area zugreifen.

ID-Kennwortzugriff

Es gibt drei Optionen für den Kennwortzugriff:

- Hauptkennwort
- Benutzer-ID und Kennwort oder Verschlüsselungstext
- Kein Kennwort

Hauptkennwort

Das Hauptkennwort ist ein einzelnes Kennwort, mit dem Sie auf die Predesktop Area und auf Sicherungen zugreifen können. Es wird über die Befehlszeilenschnittstelle festgelegt. Es handelt sich hierbei um die einzige Kennwortoption, wenn Client Security Solution nicht installiert ist.

Benutzer-ID und Kennwort oder Verschlüsselungstext

Diese Option verwendet Client Security Solution-Code für die Verwaltung des Kennworts oder des Verschlüsselungstexts. Über die GINA von Client Security Solution wird der Benutzer beim Starten der Predesktop Area aufgefordert, dieses Kennwort oder diesen Verschlüsselungstext einzugeben. Dies bietet in einer Umgebung mit mehreren Benutzern höhere Sicherheit. Ein über die GINA angemeldeter Benutzer hat nur Zugriff auf seine Dateien; auf die Dateien eines anderen Benutzers kann der Benutzer nicht zugreifen.

Anmerkung: Dies gilt auch für die Daten in der verschlüsselten SecureDrive PrivateDisk-Datenträgerdatei des Benutzers.

Diese Option kann über die Befehlszeilenschnittstelle oder über die GUI festgelegt werden.

Kein Kennwort

Bei dieser Option wird keine Authentifizierung verwendet, der Benutzer kann ohne die Eingabe eines Kennworts auf die Predesktop Area zugreifen.

Typ wiederherstellen

Es gibt die folgenden Methoden zum Wiederherstellen von Dateien:

- Dateisicherung
- Wiederherstellung von einzelnen Dateien
- Betriebssystem und Anwendungen
- Erneuerung
- Vollständige Wiederherstellung
- Werkseitig installierter Festplatteninhalt/Image Ultra Builder

Anmerkung: Rescue and Recovery kann nach einer Wiederherstellung zwischengespeicherte Berechtigungsnachweise für einen Domänenbenutzer nicht in einer Datei speichern.

Dateisicherung (vor einer Wiederherstellung)

Über diese Funktion wird der Benutzer zur Eingabe der Speicherposition für die Sicherung aufgefordert, woraufhin der Benutzer eine Sicherung auswählt. Anschließend zeigt ThinkVantage Rescue and Recovery die Dateien an, auf die der angemeldete Benutzer Zugriff hat, und der Benutzer wählt die zu sichernden Dateien und/oder Ordner aus. Im Anschluss daran zeigt das System die verfügbaren Positionen an, an denen die Dateien gesichert werden können, wobei das lokale Festplattenlaufwerk ausgeschlossen ist. Der Benutzer wählt eine Zieladresse mit ausreichend Speicherkapazität für die Dateien aus, die daraufhin vom System gesichert werden.

Wiederherstellung von einzelnen Dateien

Über diese Funktion wird der Benutzer zur Eingabe der Speicherposition für die Sicherung aufgefordert, woraufhin der Benutzer eine Sicherung auswählt. Anschließend zeigt ThinkVantage Rescue and Recovery die Dateien an, auf die der angemeldete Benutzer Zugriff hat, und der Benutzer wählt die wiederherzustellenden Dateien und/oder Ordner aus, die daraufhin vom System an den zugehörigen ursprünglichen Positionen wiederhergestellt werden.

Betriebssystem und Anwendungen

Über diese Funktion kann der Benutzer eine Sicherung auswählen, woraufhin das System Dateien entsprechend den Regeln in der Datei "osfilter.txt" löscht. Im Anschluss daran werden diese von OSFILTER.TXT definierten Dateien von der ausgewählten Sicherung wiederhergestellt. Außerdem enthält die Datei "tvt.txt" Optionen, über die ein Programm vor oder nach einer Wiederherstellung ausgeführt werden kann. Informationen hierzu finden Sie bei den TVT-Einstellungen und -Werten in Anhang B, „Einstellungen und Werte für die Datei TVT.TXT", auf Seite 155.

Anmerkungen:

1. Betriebssystem und Anwendungen verwenden immer Kennwortpersistenz.
2. Die Wiederherstellung für Betriebssystem und Anwendungen ist nicht von einer CD/DVD-Sicherung aus möglich.

Sie können benutzerdefinierte Tasks zur Ausführung sowohl vor als auch nach Sicherungen und Wiederherstellungen hinzufügen. In Anhang B, „Einstellungen und Werte für die Datei TVT.TXT", auf Seite 155 finden Sie die Einstellungen für Sicherungen und Wiederherstellungen.

Erneuerung

Wenn Sie sich für die Erneuerung Ihres Systems entscheiden, optimiert Rescue and Recovery die Systemleistung über eine neue inkrementelle Sicherung und anschließende Defragmentierung Ihres Festplattenlaufwerks und Ihrer Sicherungen. Im Anschluss daran werden ausgewählte Einstellungen und Daten von einer Sicherung Ihrer Wahl wiederhergestellt. Die Operationen zur Erneuerung unterstützen die Beseitigung von Viren, Adware und Spyware, während gleichzeitig Ihre aktuellen Einstellungen und Daten erhalten bleiben. Die Ausführung dieser Operationen dauert möglicherweise etwas länger.

Gehen Sie wie folgt vor, um Ihr System zu erneuern:

1. Klicken Sie in der Schnittstelle von Rescue and Recovery auf das Symbol zum Wiederherstellen des Systems über eine Sicherung. Daraufhin wird das Fenster ″System wiederherstellen″ angezeigt.
2. Wählen Sie im Fenster ″System wiederherstellen″ die Option zum Erneuern des Systems aus.
3. Wählen Sie das Laufwerk und die Sicherung aus, die Sie für die Erneuerung Ihres Systems verwenden möchten. Gehen Sie dazu wie folgt vor:
   a. Wählen Sie das geeignete Laufwerk aus dem Dropdown-Menü der verfügbaren Laufwerke aus. Die Sicherungsdateien auf dem ausgewählten Laufwerk werden daraufhin in der Schnittstelle von Rescue and Recovery angezeigt.
   b. Wählen Sie die Sicherungsdatei aus, die Sie für die Erneuerung Ihres Systems verwenden möchten.
   c. Klicken Sie auf **Weiter**.
   d. Bestätigen Sie, dass es sich bei der ausgewählten Sicherung um die Sicherung handelt, die Sie für die Erneuerung Ihres Systems verwenden möchten. Klicken Sie anschließend auf **Weiter**, um mit dem Wiederherstellungsprozess zu beginnen. Es wird eine Nachricht angezeigt, dass Sie den Computer während dieser Operation nicht ausschalten dürfen.
   e. Klicken Sie auf **OK**, um fortzufahren. Ein Fortschrittsanzeiger wird angezeigt. Die Ausführung dieser Operation kann einige Zeit in Anspruch nehmen.

Sie können benutzerdefinierte Tasks zur Ausführung sowohl vor als auch nach einer Erneuerung hinzufügen. In Anhang B, „Einstellungen und Werte für die Datei TVT.TXT″, auf Seite 155 finden Sie die Einstellungen für Erneuerungen.

Anmerkung: Anwendungen, die nach der Erstellung der ausgewählten Sicherungen installiert oder deinstalliert wurden, müssen möglicherweise erneut installiert werden, um ordnungsgemäß zu funktionieren.
Achtung: Stellen Sie vor dem Einleiten einer Sicherung, einer Wiederherstellung, einer Erneuerung oder einer Archivierung sicher, dass das System an die Stromversorgung angeschlossen ist. Andernfalls können Daten verloren gehen, oder es kann ein nicht behebbarer Systemfehler auftreten.

Vollständige Wiederherstellung

Über diese Funktion werden alle Dateien auf dem lokalen Laufwerk gelöscht und anschließend über eine ausgewählte Sicherung wiederhergestellt. Wird Kennwortpersistenz ausgewählt, wird das letzte verfügbare Kennwort wiederhergestellt.

Werkseitig installierter Festplatteninhalt/Image Ultra Builder (IUB)

Über diese Funktion wird das Festplattenlaufwerk gelöscht und die gesamte werkseitig installierte Software erneut installiert.

Kennwortpersistenz

In der folgenden Tabelle finden Sie Hinweise, anhand derer Sie entscheiden können, ob Sie die Kennwortpersistenz verwenden möchten.

Tabelle 9. Hinweise zur Kennwortpersistenz

Aspekt	Auswirkung bei aktivierter Kennwortpersistenz
Wenn sich ein Benutzer mit dem aktuellen Benutzereintrag und dem aktuellen Kennwort an einer alten Sicherung anmeldet, kann er nicht mit Dateien und Ordnern des verschlüsselten Dateisystems arbeiten, da diese Dateien mit dem ursprünglichen Benutzereintrag und dem ursprünglichen Kennwort verschlüsselt wurden, und nicht mit dem persistenten Benutzereintrag und dem persistenten Kennwort.	• Der Benutzer verliert Daten des verschlüsselten Dateisystems. • Sie können das verschlüsselte Dateisystem nicht zusammen mit der Kennwortpersistenz verwenden.
Wenn Benutzer in einer bestimmten Sicherung nicht vorhanden waren, können diese nicht mit ihren Benutzerordnern oder -dateien arbeiten. Es sind keine Internet Explorer-Favoriten und keine Anwendungsdaten vorhanden.	• Die Dokumenteneinstellungen für die Benutzer-ID gehen verloren. • Datenverluste sind möglich.
Wenn ein Benutzer in den aktuellen Benutzereinträgen und Kennwörtern gelöscht wird, werden die zugehörigen Authentifizierungsinformationen aus allen Sicherungen entfernt.	• Der Benutzer hat keinen Zugriff auf Daten.
Wenn eine Führungskraft oder ein Netzadministrator den Zugriff für einige ehemalige Mitarbeiter löschen und das System über eine Basissicherung zurücksetzen und dabei alle Authentifizierungseinträge der Mitarbeiter entfernen möchte, können die Mitarbeiter bei aktivierter Kennwortpersistenz weiterhin auf Daten zugreifen.	• Dies widerspricht der Empfehlung von Microsoft für die Verwaltung von Benutzer-IDs.

Bei der Wiederherstellung über ein lokales Festplattenlaufwerk wird das aktuelle Kennwort verwendet, wenn Kennwortpersistenz ausgewählt ist. Bei der Wiederherstellung über USB oder über das Netzwerk wird das Kennwort der letzten Sicherung verwendet.

Funktion zum Zurücksetzen von Hardwarekennwörtern

Die Umgebung der Funktion zum Zurücksetzen von Hardwarekennwörtern wird unabhängig von Windows ausgeführt und ermöglicht die Wiederherstellung von vergessenen Startkennwörtern und Kennwörtern für Festplattenlaufwerke. Ihre Identität wird durch die Beantwortung einer Reihe von Fragen etabliert, die Sie während der Registrierung erstellen. Es ist empfehlenswert, diese sichere Umgebung so bald wie möglich zu erstellen, zu installieren und zu registrieren, bevor ein Kennwort vergessen wird. Sie können vergessene Hardwarekennwörter erst nach der Registrierung wiederherstellen. Dieser Wiederherstellungsdatenträger wird nur auf ausgewählten ThinkCentre- und ThinkPad-Computern unterstützt.

Die Erstellung dieser Umgebung unterstützt Sie nicht bei der Wiederherstellung von vergessenen Windows-Kennwörtern oder bei der Wiederherstellung des Kennworts für den Arbeitsbereich von Rescue and Recovery. Durch die Erstellung dieser Umgebung fügen Sie eine zusätzliche bootfähige Einheit zum Menü der Starteinheiten hinzu, von der aus Sie Ihre vergessenen Hardwarekennwörter wiederherstellen können. Sie können auf dieses Menü zugreifen, indem Sie die Taste F12 drücken, wenn Sie zur Eingabe des Startkennworts aufgefordert werden.

Es gibt drei Stadien bei der Einrichtung der Kennwortimplementierung:

1. Paketerstellung
2. Paketimplementierung
3. Registrierung

Legen Sie im BIOS ein Administratorkennwort fest, bevor Sie mit dieser Prozedur beginnen. Ohne ein festgelegtes BIOS-Administratorkennwort bietet die Umgebung nicht die Sicherheit, die mit einem solchen Kennwort möglich ist. Für alle Systeme, auf denen Sie das Paket zum Zurücksetzen von Kennwörtern implementieren möchten, muss ein Administratorkennwort festgelegt sein. Wenn Sie diese Prozedur abschließen, werden das Startkennwort und das Kennwort für das Festplattenlaufwerk dasselbe sein. Die nachfolgende Prozedur soll Sie beim Erstellen der sicheren Umgebung und beim Wiederherstellen von vergessenen Kennwörtern nach der Erstellung der sicheren Umgebung unterstützen.

Paketerstellung

Gehen Sie wie folgt vor, um eine sichere Umgebung zu erstellen:

1. Aktivieren Sie in der Installationsanwendung zum Zurücksetzen von Hardwarekennwörtern den Radioknopf zum Erstellen einer sicheren Umgebung zum Zurücksetzen von Hardwarekennwörtern.
2. Klicken Sie auf ″OK″. Das Fenster für das BIOS-Administratorkennwort wird geöffnet.
3. Geben Sie im entsprechenden Feld das Administratorkennwort ein. Hierbei handelt es sich um das Administratorkennwort, das Sie zuvor im BIOS zum Schutz Ihrer Hardwareeinstellungen festgelegt haben.
4. Klicken Sie auf ″OK″. Das Fenster zum Erstellen von Schlüsseln wird geöffnet.
5. Führen Sie im Bereich für die Schlüsselgenerierung einen der folgenden Schritte aus:

   Bei der ersten Erstellung dieser sicheren Umgebung müssen Sie einen neuen Schlüssel generieren. Ein Schlüssel ist eine Sicherheitseinrichtung, die zur Authentifizierung Ihrer Identität verwendet wird. Bei allen folgenden Erstellungen einer sicheren Umgebung haben Sie die Möglichkeit, denselben Schlüssel wie bei der ersten Erstellung zu nutzen, wenn Sie diesen Schlüssel exportieren. Sie können aber auch einen anderen Schlüssel generieren. Wenn Sie diese Umgebung nur für einen Computer erstellen, ist die Generierung eines neuen Schlüssels empfehlenswert. Sie können jedes Mal, wenn Sie eine neue sichere Umgebung erstellen, einen Schlüssel generieren. Diese Möglichkeit macht jedoch die Durchführung der Registrierung für jede Maschine erforderlich. Bei Verwendung desselben Schlüssels muss die Registrierung nicht mehrfach ausgeführt werden. Wenn Sie diese Umgebung für verschiedene Computer erstellen, möchten Sie möglicherweise denselben Schlüssel verwenden. Für diesen Fall wird jedoch empfohlen, dass Sie den Schlüssel an einem sicheren Ort aufbewahren.

Führen Sie im Bereich für die Schlüsselgenerierung einen der folgenden Schritte aus:

- Wenn Sie zum ersten Mal einen Schlüssel generieren und die sichere Umgebung nur auf diesem Computer erstellen möchten, aktivieren Sie den Radioknopf zum Generieren eines neuen Schlüssels.
- Wenn Sie zum ersten Mal einen Schlüssel generieren und eine sichere Umgebung erstellen möchten, die auch auf anderen Computern implementiert werden kann, aktivieren Sie den Radioknopf zum Generieren eines neuen Schlüssels. Aktivieren Sie anschließend das Markierungsfeld zum Exportieren des Schlüssels in eine Datei. Verwenden Sie die Schaltfläche zum Durchsuchen, um die Position anzugeben, an der der Schlüssel gespeichert werden soll.
- Wenn Sie bereits einen Schlüssel erstellt haben und diesen Schlüssel zum Erstellen einer sicheren Umgebung, die auch auf anderen Computern implementiert werden kann, verwenden möchten, aktivieren Sie den Radioknopf zum Importieren des Schlüssels aus einer Datei. Verwenden Sie die Schaltfläche zum Durchsuchen, um die Position des Schlüssels anzugeben, den Sie verwenden möchten. Sie benötigen den Schlüssel, der über die obige Option generiert wurde.

Richten Sie für jeden unterstützten Systemtyp beim Implementieren auf Thinkpad und Thinkcentre und für jede Sprache (z. B. Französisch, Deutsch, Japanisch) ein Donatorsystem ein. Dies dient der Sicherung des Betriebssystems, das auf der Partition von Rescue and Recovery basiert und für jedes System variiert.

6. Inaktivieren Sie im Installationsbereich das Markierungsfeld zum automatischen Installieren der Funktion zum Zurücksetzen von Hardwarekennwörtern nach deren Generierung.
7. Klicken Sie auf **OK**.
8. Klicken Sie auf **OK**, wenn ein Dialogfenster mit der Nachricht angezeigt wird, dass die Funktion für das Hardwarekennwort erst dann auf dem Computer aktiviert werden kann, wenn das Installationspaket ausgeführt wurde.

   Um den Pfad zu der ausführbaren Datei zu finden, geben Sie in einer Eingabeaufforderung Folgendes ein: cd %rr%\rrcd\passwordreset\pwdreset.exe

Paketimplementierung

Verwenden Sie das Verteilungsmedium Ihres Unternehmens für die Implementierung des erstellten Pakets.

Registrierung

Gehen Sie wie folgt vor, um die Funktion zum Zurücksetzen von Kennwörtern zu registrieren:

1. Führen Sie die Datei "pwdreset.exe" aus.
2. Klicken Sie auf "OK", um den Computer erneut zu starten. Der Computer wird erneut gestartet, und Sie werden zur Eingabe Ihrer BIOS-Kennwörter aufgefordert. Geben Sie Ihre BIOS-Kennwörter ein, und drücken Sie die **Eingabetaste**. Ihr Computer ruft die sichere Umgebung auf, in der das Eingangsfenster zur Funktion zum Zurücksetzen von Hardwarekennwörtern geöffnet wird.

3. Aktivieren Sie den Radioknopf zum Einrichten des Zurücksetzens von Hardware, wenn Sie zum ersten Mal die sichere Umgebung erstellen oder wenn Sie Ihren Computer und Ihre Festplattenlaufwerke erneut registrieren möchten.
4. Klicken Sie auf **Weiter**. Das Fenster zur Konfiguration der Festplattenlaufwerke wird geöffnet.
5. Aktivieren Sie im Bereich für die Seriennummer des Computers das Markierungsfeld neben dem Computer, den Sie einrichten möchten.
6. Klicken Sie auf **Weiter**. Das Fenster zum Eingeben des neuen Startkennworts wird geöffnet.
7. Geben Sie im entsprechenden Feld das neue Startkennwort ein, das Sie verwenden möchten. Wenn bereits ein Startkennwort festgelegt wurde, wird dieses durch das eingegebene Kennwort ersetzt. Außerdem wird dieses Kennwort für Ihr Kennwort für das Festplattenlaufwerk festgelegt.
8. Klicken Sie auf **Weiter**. Das Fenster zum Erstellen von Sicherheitsfragen und -antworten wird geöffnet.
9. Geben Sie in jedes der drei Fragefelder die Frage ein, die Sie verwenden möchten.
10. Geben Sie in jedes der drei Antwortfelder die Antwort zu der jeweiligen Frage ein. Wenn Sie Ihr Startkennwort vergessen, müssen Sie alle Antworten wissen, um das Kennwort wiederherstellen zu können.
11. Klicken Sie auf **Weiter** und anschließend auf **Fertig stellen**. Daraufhin wird Ihr Computer in der Windows-Umgebung erneut gestartet.

Im Folgenden sind die Fehlernachrichten des Installationsprogramms zur Funktion zum Zurücksetzen von Hardwarekennwörtern aufgeführt. Bei den beiden ersten Nachrichten handelt es sich um generische Titel, die in Verbindung mit den übrigen Nachrichten verwendet werden. In beiden Fällen wird empfohlen, das Produkt erneut zu installieren.

- **IDS_STRING_ERR** ″Error″ (Fehler)
- **IDS_STRING_ERR_INT** ″Internal Error″ (Interner Fehler)
- **IDS_STRING_ERR_CMDLINE** ″The command line option that you typed was not recognized.\n\nUsage: scinstall [/postenroll | /biosreset | /newplanar]″ (Die angegebene Befehlszeilenoption wurde nicht erkannt.\n\nSyntax: scinstall [/postenroll | /biosreset | /newplanar])
- **IDS_STRING_ERR_NOTSUPPORTED**

  Die Funktion zum Zurücksetzen von Hardwarekennwörtern wird auf diesem Computer nicht unterstützt.
- **IDS_STRING_ERR_MEM**

  Dieser Computer verfügt nicht über ausreichend Speicherkapazität, um die Funktion zum Zurücksetzen von Hardwarekennwörtern auszuführen.
- **IDS_STRING_ERR_ENVAR**

  Eine erforderliche Umgebungsvariable fehlt. Rescue and Recovery ab Version 3.0 muss installiert sein, damit die Funktion zum Zurücksetzen von Hardwarekennwörtern verwendet werden kann.
- **IDS_STRING_ERR_MISSINGDLL**

  Eine erforderliche DLL-Datei fehlt. Rescue and Recovery ab Version 3.0 muss installiert sein, damit die Funktion zum Zurücksetzen von Hardwarekennwörtern verwendet werden kann.

- **IDS_STRING_ERR_BIOSMAILBOX**

  BIOS-Aktualisierung zum Installieren der Funktion zum Zurücksetzen von Hardwarekennwörtern fehlgeschlagen. Schalten Sie den Computer aus. Starten Sie ihn anschließend erneut, und wiederholen Sie die Installation der Funktion zum Zurücksetzen von Hardwarekenn-
  wörtern.
- **IDS_STRING_ERR_INSTALLRETRY**

  Diese Operation wurde nicht erfolgreich beendet. Um es erneut zu versuchen, schalten Sie den Computer aus, führen Sie einen Neustart durch, und wiederholen Sie die Installation der Funktion zum Zurücksetzen von Hardwarekennwörtern.
- **IDS_STRING_ERR_INSTALLPUNT**

  Diese Operation wurde nicht erfolgreich beendet. Wenden Sie sich an Ihren Systemadministrator, um den Fehler zu beheben. Oder konsultieren Sie die Dokumentation zu Rescue and Recovery.

Kapitel 4. Client Security Solution anpassen

In diesem Kapitel werden Begriffe verwendet, die von der Trusted Computing Group (TCG) in Bezug auf das TPM (Trusted Platform Module) definiert wurden. Eine genauere Erklärung dieser Begriffe sowie Referenzen und Definitionen finden Sie auf der folgenden Site:

http://www.trustedcomputinggroup.org/

Vorteile des integrierten Sicherheitschips/TPM (Trusted Platform Module)

Bei einem TPM (Trusted Platform Module) handelt es sich um einen integrierten Sicherheitschip, der für Software sicherheitsrelevante Funktionen zur Verfügung stellt. Der integrierte Sicherheitschip ist in die Steuerplatine integriert und kommuniziert über einen Hardwarebus. Systeme mit einem TPM können Chiffrierschlüssel erstellen und verschlüsseln, so dass diese nur von demselben TPM wieder entschlüsselt werden können. Durch diesen Prozess, der oft auch als *Verpacken* eines Schlüssels umschrieben wird, wird der Schlüssel zusätzlich vor der Offenlegung geschützt. Auf einem System mit TPM wird der Master-Verpackungsschlüssel, der auch Speicher-Rootschlüssel (SRK, Storage Root Key) genannt wird, im TPM selbst gespeichert, so dass der private Bestandteil des Schlüssels nie ungeschützt ist. Im integrierten Sicherheitschip können auch andere Speicherschlüssel, Signierschlüssel, Kennwörter und andere kleine Dateneinheiten gespeichert werden. Jedoch ist die Speicherkapazität im TPM begrenzt, weshalb der SRK zum Verschlüsseln von anderen Schlüsseln für die Speicherung außerhalb des Chips verwendet wird. Da der SRK immer im integrierten Sicherheitschip verbleibt, bildet er die Basis für geschützten Speicher.

Wenn vom TPM geschützte Daten benötigt werden, werden die geschützten Daten in die gesicherte integrierte Hardwareumgebung zur Verarbeitung übergeben. Nach der erfolgreichen Authentifizierung und Entschlüsselung können die entschlüsselten Daten im System verwendet werden.

Systeme mit integriertem TPM sind gegenüber Attacken in dem Maße weniger anfällig, so wie es Hardware im Vergleich zu Software ist. Dies ist bei der Nutzung von Chiffrierschlüsseln von besonderer Bedeutung. Die privaten Bestandteile der asymmetrischen Schlüsselpaare werden vom Speicher getrennt gespeichert. Dieser Vorgang wird über das Betriebssystem gesteuert. Das TPM verwendet seine eigene interne Firmware und logischen Schaltkreise für die Verarbeitung von Anweisungen, ist unabhängig vom Betriebssystem und kann nicht über externe Software angegriffen werden.

Vollständige Sicherheit kann kein System gewährleisten, auch Systeme mit TPM-Technologie nicht. Der integrierte Sicherheitschip wurde so entwickelt, dass er das Vortäuschen einer anderen Identität erkennt oder elektrische Analysen verhindert. Um jedoch die durch ein TPM geschützten geheimen Daten zu entschlüsseln, ist physischer Zugriff auf die Maschine und zusätzliche Spezialhardware erforderlich, durch die geschützte Daten auf einer Plattform mit integriertem Sicherheitschip wesentlich sicherer sind als die Daten auf einem ausschließlichen Softwaresystem. Durch das Erschweren des Diebstahls von geheimen Daten von Systemen wird die allgemeine Sicherheit für den Einzelnen und das Unternehmen erhöht.

Bei der Verwendung eines integrierten Sicherheitschips handelt es sich um einen optionalen Vorgang, für den ein Client Security Solution-Administrator erforderlich ist. Sowohl für Einzelpersonen als auch für IT-Abteilungen eines Unternehmens muss das TPM initialisiert werden. Spätere Operationen, wie z. B. die Möglichkeit zur Wiederherstellung nach einem Festplattenausfall oder nach dem Austauschen der Systemplatine, müssen ebenfalls vom Client Security Solution-Administrator ausgeführt werden.

Wie Client Security Solution Chiffrierschlüssel verwaltet

Die internen Arbeitsabläufe von Client Security Solution werden von den beiden wichtigsten Implementierungsaktivitäten beschrieben: Eigentumsrecht übernehmen und Benutzer registrieren. Bei der ersten Ausführung des Konfigurationsassistenten von Client Security werden diese beiden Prozesse während der Initialisierung ausgeführt. Die Windows-Benutzer-ID, mit der der Konfigurationsassistent von Client Security ausgeführt wird, wird zum Client Security Solution-Administrator. Außerdem wird diese ID als ein aktiver Benutzer registriert. Jeder andere Benutzer, der sich am System anmeldet, wird automatisch aufgefordert, sich bei Client Security Solution zu registrieren.

- **Eigentumsrecht übernehmen - Client Security Solution-Administrator zuordnen**

  Eine einzige Windows-Benutzer-ID mit Administratorberechtigung wird als alleiniger Client Security Solution-Administrator für das System zugeordnet. Verwaltungsfunktionen von Client Security Solution müssen über diese Benutzer-ID ausgeführt werden. Bei der TPM-Autorisierung handelt es sich entweder um das Windows-Kennwort oder um den Client Security-Verschlüsselungstext von diesem Benutzer.

  Anmerkung: Es gibt nur zwei Möglichkeiten, um ein vergessenes Client Security Solution-Administratorkennwort oder einen vergessenen Verschlüsselungstext wiederherzustellen: die Deinstallation der Software mit gültigen Windows-Berechtigungen oder das Löschen des Sicherheitschips im BIOS. Bei beiden Möglichkeiten gehen die Daten, die über die dem TPM zugeordneten Schlüssel geschützt werden, verloren. Client Security Solution bietet außerdem einen optionalen Mechanismus, mit dessen Hilfe Sie ein vergessenes Kennwort oder einen vergessenen Verschlüsselungstext selbst wiederherstellen können. Dieser Mechanismus basiert auf Fragen und Antworten zur Identifizierung, die Bestandteil der Funktion "Benutzer registrieren" sind. Der Client Security Solution-Administrator entscheidet, ob diese Funktion verwendet wird.

- **Benutzer registrieren**

  Nachdem der Prozess "Eigentumsrecht übernehmen" abgeschlossen ist und ein Client Security Solution-Administrator erstellt wurde, kann ein Benutzerbasisschlüssel erstellt werden, um die Berechtigungsnachweise für den gerade angemeldeten Windows-Benutzer sicher zu speichern. Dadurch können sich mehrere Benutzer bei Client Security Solution registrieren und das einzelne TPM nutzen. Benutzerschlüssel werden über den Sicherheitschip gesichert, aber tatsächlich außerhalb des Chips auf der Festplatte gespeichert. Im Unterschied zu anderen Sicherheitstechnologien erstellt diese Technologie Festplattenspeicherplatz als den einschränkenden Speicherfaktor anstelle des tatsächlichen in den Sicherheitschip integrierten Speichers. Durch diese Herangehensweise wird die Anzahl der Benutzer, die dieselbe sichere Hardware nutzen können, in hohem Maße gesteigert.

Eigentumsrecht übernehmen

Die Sicherheitsbasis für Client Security Solution ist der System-Rootschlüssel (SRK, System Root Key). Dieser nicht migrierbare asymmetrische Schlüssel wird in der sicheren Umgebung des TPM (Trusted Platform Module) generiert und gegenüber dem System nie offengelegt. Die Autorisierung zur Nutzung des Schlüssels wird über das Windows-Administratorkonto im Laufe des Befehls "TPM_TakeOwnership" (TPM_Eigentumsrecht_übernehmen) abgeleitet. Wenn das System einen Client Security-Verschlüsselungstext verwendet, wird der Client Security-Verschlüsselungstext des Client Security Solution-Administrators zur Autorisierung für das TPM, andernfalls dient dazu das Windows-Kennwort des Client Security Solution-Administrators.

Schlüsselstruktur auf Systemebene - Eigentumsrecht übernehmen

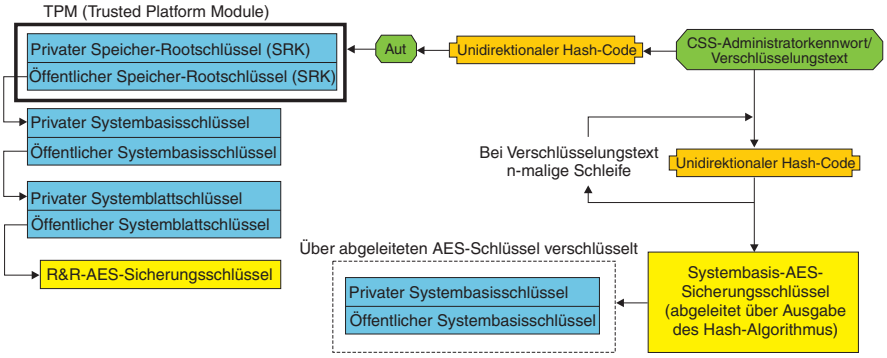

Abbildung 1.

Mit Hilfe des für das System erstellten SRK können andere Schlüsselpaare erstellt und verpackt oder geschützt durch die auf Hardware basierenden Schlüssel außerhalb des TPM gespeichert werden. Da es sich beim TPM, das den SRK enthält, um Hardware handelt und Hardware beschädigt werden kann, ist ein Wiederherstellungsmechanismus erforderlich, damit eine Beschädigung des Systems nicht die Datenwiederherstellung verhindert.

Um ein System wiederherzustellen, wird ein Systembasisschlüssel erstellt. Mit diesem migrierbaren asymmetrischen Speicherschlüssel kann der Client Security Solution-Administrator das System nach dem Austauschen der Systemplatine oder der geplanten Migration auf ein anderes System wiederherstellen.

Damit der Systembasisschlüssel geschützt ist und gleichzeitig bei normalem Betrieb oder bei einer Wiederherstellung auf ihn zugegriffen werden kann, werden zwei Instanzen des Schlüssels erstellt und auf zwei verschiedene Arten geschützt. Zum einen wird der Systembasisschlüssel mit einem symmetrischen AES-Schlüssel verschlüsselt, der vom Kennwort des Client Security Solution-Administrators oder vom Client Security-Verschlüsselungstext abgeleitet wird. Diese Kopie des Client Security Solution-Wiederherstellungsschlüssels dient ausschließlich zur Wiederherstellung von einem gelöschten TPM oder einer ausgetauschten Systemplatine aufgrund eines Hardwareausfalls.

Die zweite Instanz des Client Security Solution-Wiederherstellungsschlüssels wird durch den SRK für den Import in die Schlüsselhierarchie verpackt. Durch diese doppelte Instanz des Systembasisschlüssels kann das TPM mit ihm verbundene geheime Daten bei normalem Betrieb schützen. Außerdem ist eine Wiederherstellung einer fehlerhaften Systemplatine durch den Systembasisschlüssel möglich, der

mit einem AES-Schlüssel verschlüsselt ist, der über das Client Security Solution-Administratorkennwort oder den Client Security-Verschlüsselungstext entschlüsselt wird.

Anschließend wird ein Systemblattschlüssel erstellt. Dieser traditionelle Schlüssel wird zum Schutz von geheimen Daten auf Systemebene, wie z. B. dem AES-Schlüssel, den Rescue and Recovery zum Schützen von Sicherungen verwendet, erstellt.

Benutzer registrieren

Damit die Daten von allen Benutzern durch dasselbe TPM (Trusted Platform Module) geschützt werden können, muss jeder Benutzer seinen eigenen Benutzerbasisschlüssel erstellen. Dieser migrierbare asymmetrische Speicherschlüssel wird ebenfalls zweimal erstellt und durch einen symmetrischen AES-Schlüssel geschützt, der über das jeweilige Windows-Benutzerkennwort oder den Client Security-Verschlüsselungstext generiert wird. Die zweite Instanz des Benutzerbasisschlüssels wird dann in das TPM importiert und durch den System-SRK geschützt. Siehe Abb. 2.

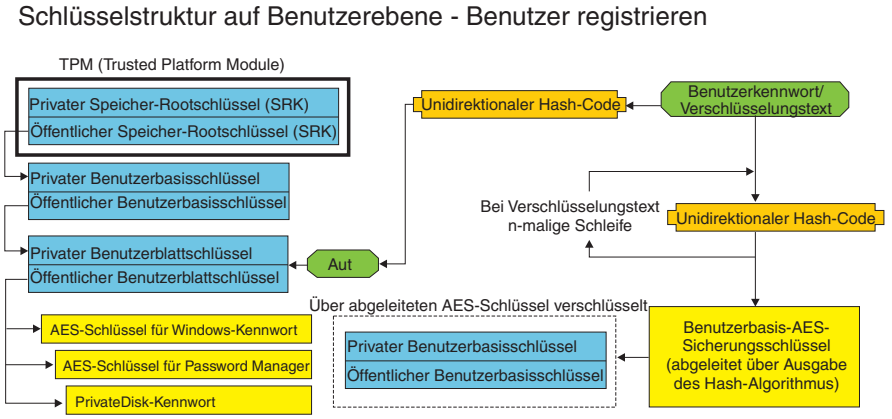

Abbildung 2.

Mit dem erstellten Benutzerbasisschlüssel wird ein zweiter asymmetrischer Schlüssel, der Benutzerblattschlüssel, erstellt, um die geheimen Daten der einzelnen Benutzer zu schützen. Hierzu zählen der AES-Schlüssel für Password Manager, der zum Schutz von Internetanmeldedaten dient, das PrivateDisk-Kennwort, mit dem Daten geschützt werden, und der AES-Schlüssel für das Windows-Kennwort, der den Zugriff auf das Betriebssystem schützt. Der Zugriff auf den Benutzerblattschlüssel wird über das Windows-Benutzerkennwort oder den Client Security Solution-Verschlüsselungstext gesteuert. Der Benutzerblattschlüssel wird bei der Anmeldung automatisch entsperrt.

Softwareemulation

Wenn ein System nicht über ein TPM (Trusted Platform Module) verfügt, wird eine auf Software basierende Sicherheitsbasis verwendet. Bei dieser Lösung steht dem Benutzer dieselbe Funktionalität zur Verfügung, mit der Ausnahme, dass keine so hohe Sicherheit gewährleistet werden kann, da die Sicherheitsbasis auf softwarebasierten Schlüsseln beruht. Der TPM-SRK wird durch einen softwarebasierten RSA-Schlüssel und einen AES-Schlüssel ersetzt, um den Schutz, den das TPM gewährt hat, zu bieten. Der AES-Schlüssel wird mit dem RSA-Schlüssel verpackt, und der AES-Schlüssel wird zum Verschlüsseln des nächsten RSA-Schlüssels in der Hierarchie verwendet.

Austausch der Systemplatine

Ein Austausch der Systemplatine bedeutet, dass der alte SRK, an den die Schlüssel gebunden waren, nicht mehr gilt, und dass ein anderer SRK erforderlich ist. Dieser Fall kann auch eintreten, wenn das TPM (Trusted Platform Module) über das BIOS gelöscht wird.

Der Client Security Solution-Administrator muss die Berechtigungsnachweise des Systems an einen neuen SRK binden. Es ist erforderlich, dass der Systembasisschlüssel über den Systembasis-AES-Sicherungsschlüssel entschlüsselt wird, der von den Berechtigungsnachweisen zur Autorisierung des Client Security Solution-Administrators abgeleitet wird. Siehe Abb. 3.

Anmerkung: Wenn es sich beim Client Security Solution-Administrator um eine Domänenbenutzer-ID handelt und das Kennwort für diese Benutzer-ID auf einer anderen Maschine geändert wurde, muss das Kennwort bekannt sein, dass bei der letzten Anmeldung auf dem System, das wiederhergestellt werden soll, verwendet wurde, um den Systembasisschlüssel für die Wiederherstellung zu entschlüsseln. Ein Bespiel: Bei der Implementierung wird eine Benutzer-ID und ein Kennwort des Client Security Solution-Administrators konfiguriert. Ändert sich das Kennwort von diesem Benutzer auf einer anderen Maschine, ist das ursprüngliche, bei der Implementierung festgelegte Kennwort für die Autorisierung erforderlich, um das System wiederherzustellen.

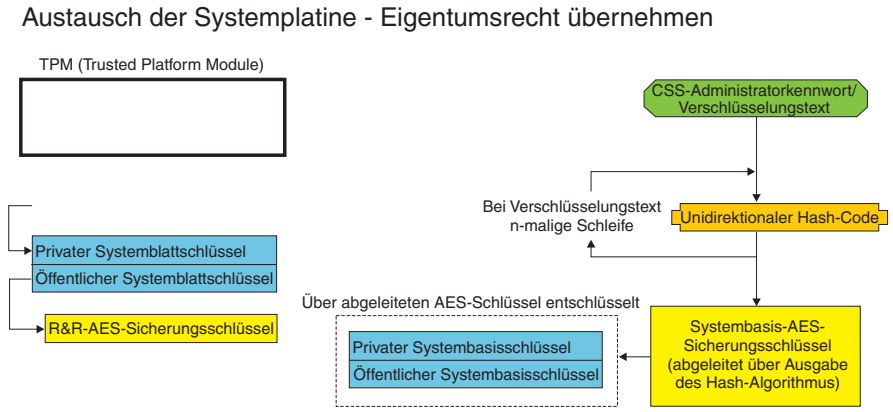

Abbildung 3.

Gehen Sie wie folgt vor, um die Systemplatine auszutauschen:

1. Melden Sie sich als Client Security Solution-Administrator am Betriebssystem an.
2. Der bei der Anmeldung ausgeführte Code (cssplanarswap.exe) erkennt, dass der Sicherheitschip nicht aktiviert ist und erfordert einen Neustart für die Aktivierung. (Dieser Schritt kann durch die Aktivierung des Sicherheitschips im BIOS umgangen werden.)
3. Das System wird erneut gestartet und der Sicherheitschip aktiviert.
4. Melden Sie sich als Client Security Solution-Administrator an. Der neue Prozess "Eigentumsrecht übernehmen" ist abgeschlossen.
5. Der Systembasisschlüssel wird über den Systembasis-AES-Sicherungsschlüssel entschlüsselt, der von der Authentifizierung des Client Security Solution-Administrators abgeleitet wird. Der Systembasisschlüssel wird in den neuen SRK importiert und erstellt den Systemblattschlüssel und alle durch ihn geschützten Berechtigungsnachweise erneut.

6. Das System ist nun wiederhergestellt.

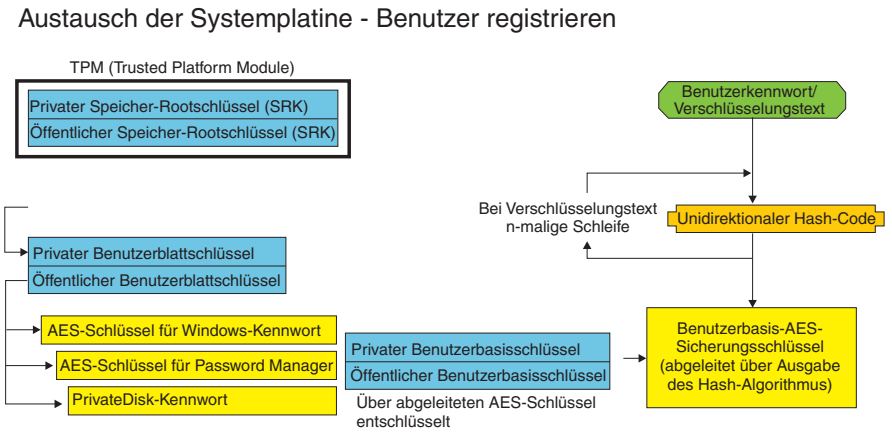

Abbildung 4.

Bei der Anmeldung der einzelnen Benutzer am System wird der jeweilige Benutzerbasisschlüssel automatisch über den Benutzerbasis-AES-Sicherungsschlüssel entschlüsselt, der von der Benutzerauthentifizierung abgeleitet wird, und in den neuen vom Client Security Solution-Administrator erstellten SRK importiert.

XML-Schema

Über die XML-Scripterstellung können IT-Administratoren angepasste Scripts zur Implementierung von Client Security Solution erstellen. Alle über den Konfigurationsassistenten von Client Security Solution verfügbaren Funktionen stehen auch über die Scripterstellung zur Verfügung. Die Scripts können über die ausführbare Funktion ″xml_crypt_tool″ (mit einem Kennwort (AES-Verschlüsselung) oder mit Verbergen) geschützt werden. Nach der Erstellung akzeptiert die virtuelle Maschine (vmserver.exe) die Scripts als Eingabe. Die virtuelle Maschine ruft dieselben Funktionen wie der Konfigurationsassistent zum Konfigurieren der Software auf.

Syntax

Alle Scripts bestehen aus einem Tag, das den XML-Codierungstyp, das XML-Schema und mindestens eine auszuführende Funktion angibt. Das Schema dient der Validierung der XML-Datei und überprüft, ob die erforderlichen Parameter vorhanden sind. Die Verwendung des Schemas wird derzeit nicht erzwungen. Jede Funktion wird in einem Funktionstag eingeschlossen und enthält die Reihenfolge, in der der Befehl von der virtuellen Maschine (vmserver.exe) ausgeführt wird. Außerdem verfügt jede Funktion über eine Versionsnummer; derzeit haben alle Funktionen Version 1.0. Zur besseren Veranschaulichung enthalten die folgenden Beispielscripts jeweils nur eine Funktion. In der Praxis ist es jedoch wahrscheinlicher, dass ein Script mehrere Funktionen enthält. Ein solches Script kann mit dem Konfigurationsassistenten von Client Security Solution erstellt werden. Siehe „Client Security-Assistent” auf Seite 174. (Ausführliche Informationen finden Sie in der Dokumentation zum Konfigurationsassistenten.)

Anmerkung: Wird in einer Funktion, die einen Domänennamen erfordert, der Parameter <DOMAIN_NAME_PARAMETER> nicht angegeben, wird der Standardcomputername des Systems verwendet.

Beispiele

AUTO_ENROLL_ADMIN_FOR_RNR_ONLY

Mit diesem Befehl kann der Systemadministrator die erforderlichen Sicherheitsschlüssel für die Verschlüsselung von Sicherungen mit Rescue and Recovery generieren. Dieser Befehl sollte pro System nur einmal und nur vom Administrator (nicht von jedem Benutzer) ausgeführt werden.

Anmerkung: Bei Installationen, die nur Rescue and Recovery umfassen, muss ein Administrator als TPM-Eigner zugeordnet sein, wenn Sicherungen mit dem TPM (Trusted Platform Module) verschlüsselt werden sollen. Verwenden Sie die folgende Scriptdatei, um automatisch eine Administrator-ID und ein Kennwort zuzuordnen. Diese Windows-Benutzer-ID und das zugehörige Kennwort werden zu TPM-Wiederherstellungszwecken verwendet. (Alle anderen CSS-XML-Scriptfunktionen sind nicht verfügbar, wenn ausschließlich Rescue and Recovery installiert ist.)

- **USER_NAME_PARAMETER**

  Die Windows-Benutzer-ID des Administrators.

- **DOMAIN_NAME_PARAMETER**

  Der Domänenname des Administrators.

- **RNR_ONLY_PASSWORD**

  Das Windows-Kennwort des Administrators.

```
<?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

Dieser Befehl aktiviert das TPM und verwendet das Argument SYSTEM_PAP. Wenn für das System bereits ein BIOS-Administratorkennwort festgelegt wurde, muss dieses Argument angegeben werden. Andernfalls ist dieses Argument 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

Dieser Befehl verwendet das Argument SYSTEM_PAP. Wenn für das System bereits ein BIOS-Administratorkennwort festgelegt wurde, muss dieses Argument angegeben werden. Andernfalls ist dieses Argument 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

Wenn Sie Rescue and Recovery verwenden, können Sie mit diesem Befehl den Schutz der Sicherungen mit Client Security Solution aktivieren.

```
<?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

Wenn Sie Rescue and Recovery zum Schutz der Sicherungen verwenden, können Sie mit diesem Befehl den Schutz der Sicherungen mit Client Security Solution inaktivieren.

```
<?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

Mit diesem Befehl können Sie den Password Manager für alle Client Security Solution-Benutzer aktivieren.

```
 <?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

Mit diesem Befehl können Sie die Client Security Solution-Anmeldung aktivieren.

```
<?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

Wenn die ThinkVantage Fingerprint Software installiert ist, können Sie mit diesem Befehl die Anmeldung aktivieren.

```
<?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

Wenn die ThinkVantage Fingerprint Software installiert ist, können Sie mit diesem Befehl die Anmeldung mit Unterstützung für schnelles Wechseln zwischen Benutzern aktivieren.

```
<?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

Wenn die Anmeldung über die ThinkVantage Fingerprint Software oder über Client Security Solution aktiviert ist, können Sie mit diesem Befehl sowohl die Anmeldung über die ThinkVantage Fingerprint Software als auch die Anmeldung über Client Security Solution inaktivieren.

```
<?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

Über diesen Befehl wird ein Flag geschrieben, das von Client Security Solution gelesen wird, um festzustellen, ob der Client Security-Verschlüsselungstext oder ein Windows-Kennwort verwendet wird.

```
<?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

Mit diesem Befehl können Sie SafeGuard PrivateDisk zur Verwendung auf dem System aktivieren. Dabei muss jeder Benutzer gesondert durch ENABLE_PD_USER_FUNCTION für die Verwendung von Safeguard PrivateDisk konfiguriert werden.

```
<?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

Über diesen Befehl wird ein Flag geschrieben, das von Client Security Solution gelesen wird, um festzustellen, wer der Client Security Solution-Administrator ist. Es gibt die folgenden Parameter:

- **USER_NAME_PARAMETER**

  Der Benutzername des Administrators.

- **DOMAIN_NAME_PARAMETER**

  Der Domänenname des Administrators.

```
<?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

Mit diesem Befehl kann ein bestimmter Benutzer PrivateDisk verwenden. Es gibt die folgenden Parameter:

- **USER_NAME_PARAMETER**

  Der Name des Benutzers, der PrivateDisk aktivieren kann.

- **DOMAIN_NAME_PARAMETER**

  Der Domänenname des Benutzers, der PrivateDisk aktivieren kann.

- **PD_VOLUME_SIZE_PARAMETER**

  Die Größe des PrivateDisk-Datenträgers in Megabyte.

- **PD_VOLUME_PATH_PARAMETER**

  Der Pfad zum zu erstellenden PrivateDisk-Datenträger.

- **PD_VOLUME_NAME_PARAMETER**

  Der Name des zu erstellenden PrivateDisk-Datenträgers. Wird der Wert PD_USE_DEFAULT_OPTION angegeben, wird automatisch ein Standardwert verwendet.

- **PD_VOLUME_DRIVE_LETTER_PARAMETER**

  Der Laufwerkbuchstabe des zu erstellenden PrivateDisk-Datenträgers. Wird der Wert PD_USE_DEFAULT_OPTION angegeben, wird automatisch ein Standardwert verwendet.

- **PD_VOLUME_CERT_PARAMETER**

  Wird der Wert PD_USE_CSS_CERT geladen, erstellt PrivateDisk entweder ein neues Zertifikat oder verwendet ein vorhandenes Zertifikat und schützt es mit dem Client Security Solution-CSP. Das Anhängen/Abhängen dieses Datenträgers ist dann an den CSP gebunden und nicht an CSS-Verschlüsselungstext/Windows-Kennwort. Wird der Wert PD_USE_DEFAULT_OPTION angegeben, wird kein Zertifikat, sondern standardmäßig der CSS-Verschlüsselungstext bzw. das Windows-Kennwort des Benutzers verwendet.

- **PD_USER_PASSWORD**

  Das Kennwort, das Client Security Solution PrivateDisk zum Anhängen/Erstellen des PrivateDisk-Datenträgers übergibt. Wird der Wert PD_RANDOM_VOLUME_PWD angegeben, generiert Client Security Solution ein zufälliges Kennwort für den Datenträger.

- **PD_VOLUME_USER_PASSWORD_PARAMETER**

  Ein benutzerspezifisches Kennwort zum Anhängen des PrivateDisk-Datenträgers. Dieses Kennwort soll als Sicherung für das PD_USER_PASSWORD-Kennwort dienen. Wenn Client Security Solution künftig aus einem beliebigen Grund fehlschlägt, ist der für dieses Argument angegebene Wert von Client Security Solution unabhängig. Wird der Wert PD_USE_DEFAULT_OPTION angegeben, wird kein Wert verwendet.

```
<?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

Dieser Befehl initialisiert das System so, dass Client Security Solution auf dem System verwendet wird. Alle systemweiten Schlüssel werden über diesen Funktionsaufruf generiert. Es gibt die folgenden Parameter:

- **NEW_OWNER_AUTH_DATA_PARAMETER**

  Das System wird über das Eignerkennwort initialisiert. Ist kein Eignerkennwort festgelegt, wird der für dieses Argument angegebene Wert das neue Eignerkennwort. Wenn bereits ein Eignerverschlüsselungstext festgelegt ist und der Administrator dasselbe Kennwort verwendet, kann dieses geladen werden. Für den Fall, dass der Administrator einen neuen Eignerverschlüsselungstext verwenden möchte, muss das gewünschte Kennwort in diesen Parameter geladen werden.

- **CURRENT_OWNER_AUTH_DATA_PARAMETER**

  Das aktuelle Eignerkennwort des Systems. Wenn das System bereits über ein 5.4x-Eignerkennwort verfügt, sollte dieser Parameter in das 5.4x-Kennwort geladen werden. Wenn ein neues Eignerkennwort gewünscht wird, sollte das aktuelle Eignerkennwort in diesen Parameter geladen werden. Wenn das Kennwort nicht geändert werden soll, sollte der Wert NO_CURRENT_OWNER_AUTH übergeben werden.

```
<?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

Dieser Befehl ändert die Client Security Solution-Administratorautorisierung und aktualisiert die Systemschlüssel entsprechend. Alle systemweiten Schlüssel werden über diesen Funktionsaufruf erneut generiert. Es gibt die folgenden Parameter:

- NEW_OWNER_AUTH_DATA_PARAMETER

  Das neue Eignerkennwort des TPM (Trusted Platform Module).
- CURRENT_OWNER_AUTH_DATA_PARAMETER

  Das aktuelle Eignerkennwort des TPM (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

Dieser Befehl registriert einen bestimmten Benutzer für die Verwendung von Client Security Solution. Diese Funktion erstellt alle benutzerspezifischen Sicherheitsschlüssel für einen angegebenen Benutzer. Es gibt die folgenden Parameter:

- **USER_NAME_PARAMETER**

  Der Name des Benutzers, der registriert werden soll.
- **DOMAIN_NAME_PARAMETER**

  Der Domänenname des Benutzers, der registriert werden soll.
- **USER_AUTH_DATA_PARAMETER**

  Der TPM-Verschlüsselungstext/das TPM-Windows-Kennwort zum Erstellen der Sicherheitsschlüssel für den Benutzer.
- **WIN_PW_PARAMETER**

  Das Windows-Kennwort.

```
<?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

Dieser Befehl konfiguriert die Kennwortwiederherstellung für einen bestimmten TPM-Benutzer. Es gibt die folgenden Parameter:

- **USER_NAME_PARAMETER**

  Der Name des Benutzers, der registriert werden soll.
- **DOMAIN_NAME_PARAMETER**

  Der Domänenname des Benutzers, der registriert werden soll.

- **USER_PW_REC_QUESTION_COUNT**

  Die Anzahl der Fragen, die der Benutzer beantworten muss.
- **USER_PW_REC_ANSWER_DATA_PARAMETER**

  Die gespeicherte Antwort auf eine bestimmte Frage. Beachten Sie, dass der tatsächliche Name dieses Parameters mit einer Nummer entsprechend der zu beantwortenden Frage verknüpft ist. Beachten Sie das unten angegebene Beispiel für diesen Befehl.
- **USER_PW_REC_STORED_PASSWORD_PARAMETER**

  Das gespeicherte Kennwort, dass angezeigt wird, wenn der Benutzer alle Fragen richtig beantwortet hat.

```
<?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

Über diesen Befehl wird ein Flag geschrieben, das vom Programm gelesen wird, um festzustellen, ob beim Zugriff auf die Windows PE-Umgebung eine Benutzerautorisierung erforderlich ist. Es gibt die folgenden Parameter:

- **WIN_PE_LOGON_MODE_AUTH_PARAMETER**

  Es gibt die zwei folgenden gültigen Auswahlmöglichkeiten:
  - 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>
```

Kapitel 5. System Migration Assistant anpassen

Der System Migration Assistant verfügt über zwei Bereiche, die angepasst werden können:

- Befehlsdatei bearbeiten oder ändern
- Zusätzliche Anwendungseinstellungen migrieren

Befehlsdatei erstellen

Während der Erfassungsphase liest der SMA den Inhalt der Befehlsdatei und archiviert Einstellungen. Dieser Abschnitt enthält Informationen zu Befehlsdateien und zu Anweisungen, die sie enthalten können.

Der System Migration Assistant stellt eine Standardbefehlsdatei (command.xml) zur Verfügung, die Sie als Schablone für die Erstellung einer angepassten Befehlsdatei verwenden können. Wenn Sie den SMA in der Standardposition installiert haben, befindet sich diese Datei im Verzeichnis D:\%RR%\migration\bin.

Anmerkung: Der System Migration Assistant 5.0 verwendet XML-Technologie für die Beschreibung seiner Befehle in der Befehlsdatei.

Beachten Sie die folgenden Punkte bezüglich der Befehlsdateien des SMA 5.0:

- Die Befehlsdatei verwendet die Syntax von XML Version 1.0. Außerdem muss die Groß-/Kleinschreibung beachtet werden.
- Jeder Befehls- und Parameterabschnitt muss mit <TagName> beginnen und mit </TagName> enden. Die zu den Abschnitten gehörenden Werte müssen zwischen diesen Tags stehen.
- Syntaxfehler können bei der Ausführung des SMA Fehler verursachen. Wenn der SMA einen Fehler feststellt, wird dieser in der Protokolldatei aufgezeichnet und der Betrieb fortgesetzt. Je nach Schweregrad des Fehlers können die Ergebnisse fehlerhaft sein.

Befehle der Befehlsdatei

Die folgende Tabelle enthält Informationen zu den Befehlen, die in einer Befehlsdatei verwendet werden können (mit Ausnahme der Befehle zur Dateimigration und zur Registrierungsdatenbank):

Tabelle 10.

Befehl	Parameter	Parameterwerte und Beispiele

<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>
		Um eine Desktopeinstellung auszuwählen, definieren Sie für den Parameter “true”. Andernfalls definieren Sie für den Parameter “false”, oder lassen Sie ihn unbestimmt.
		
		Zum Beispiel:
		`<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>
		Um eine Desktopeinstellung auszuwählen, definieren Sie für den Parameter “true”. Andernfalls definieren Sie für den Parameter “false”, oder lassen Sie ihn unbestimmt.
		
		Zum Beispiel:
		`<Network>`
		`<computer_name>true<computer_name>`
		`<mapped_drives>false</mapped_drives>`
		`</Network>`

<Applications>	<Application>
	
	Eine Liste mit allen unterstützten Anwendungen finden Sie im Benutzerhandbuch zum ThinkVantage System Migration Assistant.
		Zum Beispiel:
		`<Applications>`
		`<Application>Lotus Notes</Application>`
		`<Application>Microsoft Office</Application>`
		`<//Applications>`
		
		oder
		`<Applications>`
		`<Application>$(all)</Applications>`

<Registries>	• <Registry> • <hive> • <keyname> • <value>	Um die Registrierungseinstellungen zu erfassen und anzuwenden, geben Sie hive (logische Untereinheit), keyname (Schlüsselname) und value (Wert) als Parameter in der Befehlsdatei an.

Tabelle 10. (Forts.)

Befehl	Parameter	Parameterwerte und Beispiele

<IncUsers>	<UserName>	Um alle Benutzerprofile zu erfassen, definieren Sie $(all), oder verwenden Sie * als Platzhalterzeichen für alle Benutzer. Geben Sie andernfalls Benutzer einzeln an.
		
		Die folgenden Platzhalterzeichen stehen zur Verfügung:
		• * für eine variable Zeichenanzahl
		• % für eine festgelegte Zeichenanzahl (1 Zeichen)
		
		Zum Beispiel:
		`<IncUsers>`
		`<UserName>administrator</UserName>`
		`<UserName>domain\Jim</UserName>`
		`</IncUsers>`

<ExcUsers>	<UserName>	Um Benutzer vom Migrationsprozess auszuschließen, geben Sie die Domäne und den Benutzernamen des jeweiligen Benutzers an. Die folgenden Platzhalterzeichen stehen zur Verfügung: • * für eine variable Zeichenanzahl • % für eine festgelegte Zeichenanzahl (1 Zeichen)

<Printers>	<Printer>
	
	<PrinterName>
		Diese Steueranweisung gilt für den Ausgangs- und den Zielcomputer.
		
		Um alle Drucker zu erfassen, definieren Sie für den Parameter *&(all)*. Geben Sie andernfalls jeden Drucker einzeln an. Um nur den Standarddrucker zu erfassen, definieren Sie für den Parameter *&(DefaultPrinter)*.
		
		Zum Beispiel:
		`<Printers>`
		`  <Printer>&(all)</Printer>`
		`</Printers>`
		
		`<Printers>`
		`  <Printer>`
		`  <PrinterName>IBM 5589-L36</PrinterName>`
		`  </Printer>`
		`</Printers>`
		
		`<Printers>`
		`  <Printer>&(DefaultPrinter)</Printer>`
		`</Printers>`

Tabelle 10. (Forts.)

Befehl	Parameter	Parameterwerte und Beispiele
<MISC>	<bypass_registry>	Um die Auswahl von allen Registrierungseinstellungen zurückzunehmen, definieren Sie für den Parameter “true”. Andernfalls definieren Sie für den Parameter “false”, oder lassen Sie ihn unbestimmt.
	<overwrite existing files>	Um vorhandene Dateien zu überschreiben, definieren Sie für den Parameter “true”. Andernfalls definieren Sie für den Parameter “false”, oder lassen Sie ihn unbestimmt.
	<log_file_location>	Um das Verzeichnis, in das der SMA Protokolldateien schreibt, zu bestimmen, geben Sie einen vollständig qualifizierten Verzeichnisnamen an. Sie können ein gemeinsam genutztes Verzeichnis auf einem anderen System angeben. Wenn Sie diesen Parameter nicht definieren, schreibt der SMA Protokolldateien in das Verzeichnis ″d:/InstDir/″, wobei ″d″ für den Laufwerkbuchstaben des Festplattenlaufwerks und ″/InstDir/″ für das Verzeichnis, in dem der SMA installiert ist, steht.
	<temp_file_location>	Um das Verzeichnis, in das der SMA temporäre Dateien schreibt, zu bestimmen, geben Sie einen vollständig qualifizierten Verzeichnisnamen an. Sie können ein gemeinsam genutztes Verzeichnis auf einem anderen System angeben. Wenn Sie diesen Parameter nicht definieren, schreibt der SMA temporäre Dateien in das Verzeichnis ″d:/InstDir/etc/data″, wobei ″d″ für den Laufwerkbuchstaben des Festplattenlaufwerks und ″/InstDir/″ für das Verzeichnis, in dem der SMA installiert ist, steht.
	<resolve_icon_links>	Um nur Symbole mit aktiven Verknüpfungen zu kopieren, definieren Sie für diesen Parameter “true”. Andernfalls definieren Sie für den Parameter “false”, oder lassen Sie ihn unbestimmt.

Befehle zur Dateimigration

Der SMA verarbeitet Befehle zur Dateimigration in der folgenden Reihenfolge: Befehle zum Einschließen von Dateien werden zuerst ausgeführt; anschließend werden die Befehle zum Ausschließen von Dateien von den Einschlussdateien aus ausgeführt.

Der SMA wählt die Dateien auf der Grundlage der ursprünglichen Position der Dateien und Ordner auf dem Ausgangscomputer aus. Das Aufheben der Auswahl erfolgt auf gleiche Weise. Anweisungen zur Dateiumleitung werden im Profil gespeichert und während der Anwendungsphase interpretiert.

Bei der Verarbeitung von Datei- und Verzeichnisnamen muss die Groß-/Kleineibung nicht beachtet werden.

Die folgende Tabelle enthält Informationen zu den Befehlen zur Dateimigration. Alle Befehle zur Dateimigration sind optional.

Tabelle 11.

Befehl	Parameter	Beschreibung

<FilesAndFolders>	<run>	Um eine Dateimigration zu erfassen oder auszuführen, definieren Sie für den Parameter “true”. Andernfalls definieren Sie für den Parameter “false”, oder lassen Sie ihn unbestimmt.
		
		Zum Beispiel:
		`<FilesAndFolders>`
		`<run>true</run>`
		`</FilesAndFolders>`

<Exclude_drives>	<Drive>	Geben Sie den Laufwerkbuchstaben an, um das entsprechende Laufwerk von der Überprüfung auszuschließen.
		
		Zum Beispiel:
		`<ExcludeDrives>`
		`<Drive>D</Drive>`
		`<Drive>E</Drive>`
		`</ExcludeDrive>`

Tabelle 11. (Forts.)

Befehl	Parameter	Beschreibung

<Inclusions>	<IncDescriptions>
	<Description>
	<DateCompare>
	<Operand>
	<Date>
	<SizeCompare>
	<Operand>
	<Size>
	<Dest>
	<Operation> wobei
	• <Description> für den vollständig qualifizierten Dateinamen steht. Sie können sowohl für den Dateinamen als auch für den Ordnernamen Platzhalterzeichen verwenden.
	• <DateCompare> für einen optionalen Parameter steht, der Dateien basierend auf dem Datum ihrer Erstellung spezifiziert.
	– <Operand> entweder NEWER oder OLDER ist.
	– <Date> für ein Ausgangsdatum mit dem Format MM/TT/JJJJ steht.
	• <SizeCompare> für den optionalen Parameter zum Auswählen von Dateien basierend auf ihrer Größe steht.
	– <Operand> entweder LARGER oder SMALLER ist.
	– <Size> für die Dateigröße in MB steht.
	• <Dest> für einen optionalen Parameter steht, der den Namen des Zielordners auf dem Zielsystem angibt, in den die Dateien geschrieben werden.
	• <Operation> für einen optionalen Parameter steht, der die Handhabung des Dateipfads angibt. Geben Sie eine der folgenden Optionen an:
	– P - erhält den Pfad der Datei und erstellt die Datei auf dem Zielsystem erneut, wobei die durch den Parameter <Dest> angegebene Position den Anfangspunkt bildet.
	– R - entfernt den Pfad der Datei und verschiebt die Datei direkt an die durch den Parameter <Dest> angegebene Position.
		Sucht nach allen passenden Dateien in den angegebenen Verzeichnissen.
		
		Zum Beispiel:
		
		Beispiel 1
		`<IncDescription>`
		`<Description>c:\MyWorkFolder\ls</Description>`
		`</IncDescription>`
		
		Anmerkung: Um den Ordnernamen anzugeben, fügen Sie am Ende der Beschreibung .\. hinzu.
		
		Beispiel 2
		`<IncDescription>`
		`<Description>C:\MyWorkFolder\*.*</Decsription>`
		`<DateCompare>`
		`<Operand>NEWER</Operand>`
		`<Date>07/31/2005</Date>`
		`</DateCompare>`
		`</IncDescription>`
		
		Beispiel 3
		`<IncDescription>`
		`<Description>C:\MyWorkFolder/*.*</Description>`
		`<SizeCompare>`
		`<Operand>SMALLER</Operand>`
		`<Size>200</Size>`
		`</SizeCompare>`
		`</IncDescription>`
		
		Beispiel 4
		`<IncDescription>`
		`<Description>C:\MyWorkFolder\*.*</Description>`
		`<Dest>D:\MyNewWorkFolder</Dest>`
		`<Operation>`
		`<IncDescription>`

Tabelle 11. (Forts.)

Befehl	Parameter	Beschreibung

<Exclusions>	<ExDescriptions>
	<Description>
	<DateCompare>
	<Operand>
	<Date>
	<SizeCompare>
	<Operand>
	<Size> wobei
	• <Description> für einen vollständig qualifizierten Dateinamen oder Ordnernamen steht. Sowohl Dateiname als auch Ordnername können Platzhalterzeichen enthalten.
	• <DateCompare> für einen optionalen Befehl steht, mit dem Sie Dateien basierend auf dem Datum ihrer Erstellung auswählen können.
	– <Operand> entweder NEWER oder OLDER ist.
	– <Date> für ein Ausgangsdatum mit dem Format MM/TT/JJJJ steht.
	• <SizeCompare> für den optionalen Parameter zum Auswählen von Dateien basierend auf ihrer Größe steht.
	– <Operand> entweder LARGER oder SMALLER ist.
	– <Size> für die Dateigröße in MB steht.
		Nimmt die Auswahl von allen passenden Dateien in einem angegebenen Verzeichnis zurück.
		Zum Beispiel:
		Beispiel 1
		`<ExDescription>`
		`<Description>C:\YourWorkFolder</Description>`
		`</ExDescription>`
		Beispiel 2
		`<ExDescription>`
		`<Description>C:\YourWorkFolder</Description>`
		`<DateCompare>`
		`<Operand>OLDER</Operand>`
		`<Date>07/31/2005</Date>`
		`</DateCompare>`
		`</ExDescription>`
		Beispiel 3
		`<ExDescription>`
		`<Description>C:\YourWorkFolder</Description>`
		`<SizeCompare>`
		`<Operand>LARGER</Operand>`
		`<Size>200</Size></SizeCompare>`
		`</ExDescription>`

Beispiele für Befehle zur Dateimigration

Dieser Abschnitt enthält Beispiele für Befehle zur Dateimigration. Diese Beispiele veranschaulichen die Vorgehensweise beim Kombinieren von Befehlen zum Einschließen und zum Ausschließen von Dateien, um die Dateiauswahl zu optimieren. Im Folgenden werden nur die Dateiverwaltungsabschnitte in der Befehlsdatei dargestellt.

Dateien während der Erfassungsphase auswählen

Dieser Abschnitt enthält Codebeispiele für die Auswahl von Dateien während der Erfassungsphase.

Beispiel 1

Das folgende Codebeispiel wählt alle Dateien mit der Erweiterung DOC (Microsoft Word-Dokumente) aus und verschiebt sie in das Verzeichnis "d:\My Documents". Anschließend werden alle Dateien im Verzeichnis d:\No_Longer_Used ausgeschlossen.

```
<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>
```

Beispiel 2

Das folgende Codebeispiel wählt den Inhalt des Laufwerks aus, wobei alle Dateien im Stammverzeichnis von Laufwerk d: und alle Dateien mit der Erweiterung TMP ausgeschlossen sind.

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

Beispiel 3

Das folgende Codebeispiel wählt den gesamten Inhalt von Laufwerk c: aus, wobei alle Dateien unter %windir% (dem angegebenen Windows-Verzeichnis) ausgeschlossen sind.

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

Beispiel 4

Das folgende Codebeispiel wählt den gesamten Inhalt des Ordners %USERPROFILE% aus, wobei alle Dateien mit der Dateierweiterung DAT und alle Dateien im Unterordner “Local Settings” ausgeschlossen sind. (%USERPROFILE% steht für den Pfad zum Benutzerprofil des aktuell angemeldeten Benutzers.)

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

Zusätzliche Anwendungseinstellungen migrieren

Anmerkung: Um angepasste Anwendungsdateien zu erstellen, müssen Sie die Anwendung, einschließlich der Speicherpositionen der angepassten Einstellungen, sehr gut kennen. Standardmäßig ist der SMA für die Migration der Einstellungen für verschiedene Anwendungen vorkonfiguriert. Eine Liste der vom SMA unterstützten Anwendungen finden Sie im Benutzerhandbuch zum System Migration Assistant. Es ist möglich, eine angepasste Anwendungsdatei auch für die Migration der Einstellungen für zusätzliche Anwendungen zu erstellen.

Diese Datei muss den Namen ″application.xml″ oder ″application.smaapp″ erhalten und sich im Verzeichnis ″d:\%RR%\Migration\bin\Apps″ befinden, wobei *Apps* für die Anwendung und d: für den Laufwerkbuchstaben des Festplattenlaufwerks steht. Wenn für eine Anwendung beide angepasste Anwendungsdateien (also sowohl application.smaapp als auch application.xml) vorhanden sind, erhält die Datei ″application.smaapp″ höhere Priorität.

Um eine neue Anwendung zu unterstützen, können Sie eine vorhandene Anwendungsdatei kopieren und die notwendigen Änderungen vornehmen. Bei Microsoft_Access.xml handelt es sich z. B. um eine vorhandene Anwendungsdatei.

Beachten Sie die folgenden Punkte in Bezug auf Anwendungsdateien:

- *application*.xml
  - Wenn der System Migration Assistant installiert ist, ist standardmäßig nur application.xml vorhanden.
  - Ein in <!-″ und ″->″ eingeschlossener <Tag> wird als Kommentar behandelt. Zum Beispiel:

    ```
    <!--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-->
    ```

  - Jeder Befehl muss in einem separatem Abschnitt beschrieben werden.
  - Jeder Abschnitt beginnt mit einem in Tags eingeschlossenen Befehl, wie z. B. <AppInfo> oder <Install_Directories>. Sie können ein oder mehrere Felder in einem Abschnitt eingeben; dabei muss jedes Feld in einer separaten Zeile stehen.
  - Wenn die Anwendungsdatei Syntaxfehler enthält, fährt der SMA mit der Ausführung der Operation fort und schreibt die Fehler in die Protokolldatei.

In Tabelle 12 finden Sie Informationen zu Anwendungsdateien:

Tabelle 12.

Abschn.	Befehl	Wert	Beschreibung
<Applications>			
	<Family>	Eine Textzeichenfolge. Führende Leerzeichen werden ignoriert. Schließen Sie die Textzeichenfolge nicht in Anführungszeichen ein.	Gibt den nichtversionsspezifischen Namen der Anwendung an. Wenn Sie den SMA im Batchmodus ausführen, verwenden Sie diese Zeichenfolge im Anwendungsabschnitt ″Applications″ der Befehlsdatei. Zum Beispiel: `<Family>adobe Acrobat Reader</Family>`
	<SMA_Version>	Ein numerischer Wert.	Gibt die Versionsnummer des SMA an. Zum Beispiel: `<SMA_Version>SMA 5.0</SMA_Version`
	<App>	*ShortName* Dabei steht ShortName für einen versionsspezifischen Kurznamen für eine Anwendung.	Gibt einen versionsspezifischen Kurznamen für eine oder mehrere Anwendungen an. Zum Beispiel: `<APP>Acrobat_Reader_50</APP>`
<Application ShortName=*ShortName*> Dabei steht *ShortName* für den Kurznamen für eine Anwendung, die im Anwendungsabschnitt “Applications” angegeben ist.			
	<Name>	Eine Textzeichenfolge.	Gibt den Namen der Anwendung an.
	<Version>	Ein numerischer Wert.	Gibt die Version der Anwendung an.

	<Detects>
	<Detect>
		Root, PathAndKey	Gibt einen Registrierungsschlüssel an. Der SMA ermittelt durch die Suche nach dem angegebenen Registrierungsschlüssel eine Anwendung.
			Zum Beispiel:
			`<Detects>`
			`<Detect>`
			`<hive>HKLM</hive>`
			`<keyname>Software\Adobe\Acrobat Reader\5.0\</keyname>`
			`</Detect>`
			`</Detects>`

Tabelle 12. (Forts.)

Abschn.	Befehl	Wert	Beschreibung

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

	<OS>	Eine Textzeichenfolge.	OS gibt das Betriebssystem an, bei dem es sich um eines der folgenden handeln kann: • WinXP • Win2000 • WinNT • Win98
	<Registry>	*hive* ist entweder HKLM oder HKCU. Bei *keyname* handelt es sich um den Schlüsselnamen. *value* ist ein optionaler Befehl, der den migrierten Registrierungswert angibt.	Gibt das Installationsverzeichnis an, wie es in der Registrierungsdatenbank angezeigt wird.
<Files_From_Folders> Optional			

Tabelle 12. (Forts.)

Abschn.	Befehl	Wert	Beschreibung

	SMAVariable\Location[|File][/s]
	
	wobei
	• SMAvariable für eine der folgenden Variablen, die die Position der Anpassungsdateien angeben, steht:
	– %Windows Directory% (Position der Betriebssystemdateien)
	– %Install Directory% (Position der Anwendung entsprechend der Definition im Abschnitt "Install_Directories")
	– %Appdata Directory% (das Anwendungsdatenverzeichnis, bei dem es sich um ein Unterverzeichnis des Benutzerprofilverzeichnisses handelt)
	– %LocalAppdata Directory% (das Anwendungsdatenverzeichnis im Ordner "Local Settings", bei dem es sich um ein Unterverzeichnis des Benutzerprofilverzeichnisses handelt)
	– %Cookies Directory% (das Cookies-Verzeichnis, bei dem es sich um ein Unterverzeichnis des Benutzerprofilverzeichnisses handelt)
	– %Favorites Directory% (das Favoritenverzeichnis, bei dem es sich um ein Unterverzeichnis des Benutzerprofilverzeichnisses handelt)
	– %%Personal Directory% (das persönliches Verzeichnis, bei dem es sich um ein Unterverzeichnis (My Documents) des Benutzerprofilverzeichnisses handelt - Diese Umgebungsvariable kann unter Windows NT4 nicht verwendet werden.)
			Gibt die Anpassungsdateien an, die Sie migrieren möchten.
			
			Zum Beispiel:
			`<Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi</Files_And_Folders>`
			
			Der SMA erfasst die Dateien im Ordner %AppData Directory%\Adobe\Acrobat\Whapi. Die Dateien in den Unterverzeichnissen sind nicht mit eingeschlossen.
			`<Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi\ /s</Files_From_Folder>`
			
			Der SMA erfasst die Dateien im Ordner %AppData Directory%\Adobe\Acrobat\Whapi. Die Dateien in den Unterverzeichnissen sind mit eingeschlossen.
			`<Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi\*.*</Files_From_Folder>`
			
			Der SMA erfasst die Dateien im Ordner %AppData Directory%\Adobe\Acrobat\Whapi. Die Dateien in den Unterverzeichnissen sind nicht mit eingeschlossen.
			`<Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi\*.* /s</Files_From_Folder>`
			
			Der SMA erfasst die Dateien im Ordner %AppData Directory%\Adobe\Acrobat\Whapi. Die Dateien in den Unterverzeichnissen sind mit eingeschlossen.
			`<Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi</Files_From_Folder>`
			
			Wenn hinter "Whapi" nicht "\" verwendet wird, behandelt der SMA "Whapi" nicht als Ordner, sondern als Datei.

Tabelle 12. (Forts.)

Abschn.	Befehl	Wert	Beschreibung
	• *Location* eine vollständig qualifizierte Datei oder ein Verzeichnis angibt. Sie können im Dateinamen, aber nicht im Pfad Platzhalterzeichen verwenden. Wenn Sie ein Verzeichnis angeben, werden alle Dateien kopiert. • *[File]* ein optionaler Parameter ist, der nur verwendet werden kann, wenn über den Parameter "Location" ein Verzeichnis angegeben wird. "File" steht dabei für die zu kopierende Datei. Sie können im Dateinamen, aber nicht im Pfad Platzhalterzeichen verwenden. • *[\s]* ein optionaler Parameter ist. Wenn Sie [/s] verwenden, werden alle Dateien in den Unterverzeichnissen kopiert. • Benutzer des SMA5.0 Windows-Umgebungsvariablen verwenden können. Die Umgebungsvariable des Benutzers, der den SMA gestartet hat, wird als der Wert einer Windows-Umgebungsvariable verwendet.		
<Registries> Optional			

	hive ist entweder HKLM oder HKCU.
	
	Bei *keyname* handelt es sich um den Schlüsselnamen. "value" ist ein optionaler Befehl, der den migrierten Registrierungswert angibt.
			Gibt die Registrierungseinträge an, die Sie migrieren möchten.
			
			Zum Beispiel:
			`<Registries>`
			`<Registry>`
			`<hive>HKCU</hive>`
			`<keyname>Software\Adobe\Acrobat</keyname>`
			`<value></value>`
			`</Registry>`
			`</Registries>`

<Registry_Excludes> Optional			

	hive ist entweder HKLM oder HKCU.
	
	Bei *keyname* handelt es sich um den Schlüsselnamen. "value" ist ein optionaler Befehl, der den migrierten Registrierungswert angibt.
			Gibt die Registrierungsschlüssel und -werte an, die Sie von den ausgewählten Registrierungseinträgen ausschließen möchten.
			
			Zum Beispiel:
			`<Registry_Excludes>`
			`<Registry>`
			`<hive>HKCU</hive>`
			`<keyname>Software\Adobe\Acrobat Reader\5.0\AdobeViewer</keyname>`
			`<value>xRes</value>`
			`</Registry>`
			`</Registry_Excludes>`

Tabelle 12. (Forts.)

Abschn.	Befehl	Wert	Beschreibung
<Files_Through_Registry>			

	<OS>
	
	Gibt das Betriebssystem an, bei dem es sich um eines der folgenden handeln kann:
	• WinXP
	• Win2000
	• WinNT
	• Win98
	
	<Registry> gibt den Registrierungseintrag an und hat das Format "hive,keyname,value", wobei:
	• hive entweder HKLM oder HKCU ist.
	• keyname der Schlüsselname ist.
	• value ein optionaler Befehl ist, der den migrierten Registrierungswert angibt. Bei "File" handelt es sich um den Dateinamen. Sie können Platzhalterzeichen verwenden.
	
	Bei "File" handelt es sich um den Dateinamen. Sie können Platzhalterzeichen verwenden.
			Gibt die zu migrierenden Anpassungsdateien an.
			
			Zum Beispiel:
			`<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>			

	`<PreTargetBatchProcessing>`
	`<!CDAT[batch commands]]`
	`<PreTargetBatchProcessing>`
			<PreTargetBatchProcessing> veranlasst die Batch-Verarbeitung vor der <Registries>-Verarbeitung durch Ausführung.
			
			Zum Beispiel:
			`<PreTargetBatchProcessing>`
			`<!CDATA[copy /y c:\temp\*.* c:\migration`
			`del c:\migration\*.mp3`
			`</PreTargetBatchProcessing>`

<TargetBatchProcessing>			

	`<TargetBatchProcessing>`
	`<!CDAT[batch commands]]`
	`<TargetBatchProcessing>`
			<TargetBatchProcessing> veranlasst die Batch-Verarbeitung nach der <Registries>-Verarbeitung durch Ausführung.
			
			Zum Beispiel:
			`<TargetBatchProcessing>`
			`<!CDATA[copy /y c:\temp\*.* c:\migration`
			`del c:\migration\*.mp3`
			`<TargetBatchProcessing>`

Anwendungsdatei erstellen

Um festzustellen, welche Anwendungseinstellungen für angepasste Anwendungsdateien migriert werden müssen, müssen Sie die Anwendungen gründlich testen.

Gehen Sie wie folgt vor, um eine Anwendungsdatei zu erstellen:

1. Öffnen Sie eine vorhandene application.XML-Datei in einem ASCII-Texteditor. Wenn der SMA in der Standardposition installiert wurde, befinden sich die application.XML-Dateien im Verzeichnis "d:\%RR%\Migration\bin\Apps", wobei d: für den Laufwerkbuchstaben des Festplattenlaufwerks steht.
2. Ändern Sie diese application.XML-Datei für die Anwendung und für die Anwendungseinstellungen, die Sie migrieren möchten.
3. Ändern Sie die Informationen im Abschnitt <Applications>.
4. Ändern Sie die Befehle <Name> und <Version> im Abschnitt <Application Shortname=*Shortname*>.
5. Bestimmen Sie die Registrierungsschlüssel, die migriert werden müssen:
   a. Klicken Sie auf **Start → Ausführen**. Das Fenster "Ausführen" wird geöffnet. Geben Sie im Feld **Öffnen:** regedit ein, und klicken Sie auf **OK**. Das Fenster "Registrierungs-Editor" wird geöffnet.
   b. Erweitern Sie im linken Fenster den Knoten **HKEY_LOCAL_MACHINE**.
   c. Erweitern Sie den Knoten **Software**.
   d. Erweitern Sie den herstellerspezifischen Knoten, wie z. B. **Adobe**.
   e. Navigieren Sie weiter, bis Sie den Registrierungsschlüssel für die Anwendung gefunden haben. Bei diesem Beispiel lautet der Registrierungsschlüssel SOFTWARE\Adobe\Acrobat Reader\6.0.
   f. Definieren Sie den Wert für das Feld "Detect". Zum Beispiel:

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

6. Ändern Sie die Befehle "Name" und "Version" im Abschnitt "Install_Directories".
7. Bestimmen Sie den Pfad zu den Installationsverzeichnissen für die Anwendung.
   a. Navigieren Sie im Fenster "Registrierungs-Editor" zum Knoten HKLM\SOFTWARE\Adobe\Acrobat Reader\6.0\InstallPath.
   b. Fügen Sie den geeigneten Befehl zum Abschnitt "Install_Directories" in der Anwendungsdatei hinzu. Zum Beispiel:

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

Anmerkung: Wenn Sie im Verzeichnis ″HKLM\Software\Microsoft\Windows\CurrentVersion\AppPaths″ kein anwendungsspezifisches Verzeichnis finden, müssen Sie ein Verzeichnis bestimmen, das den Installationspfad an einer anderen Stellen in der HKLM\Software-Baumstruktur enthält. Verwenden Sie anschließend diesen Schlüssel im Abschnitt <Install_Directories>.

8. Geben Sie im Abschnitt <Files_From Folders> die Anpassungsdateien an, die Sie migrieren möchten.
   a. Da viele Anwendungen standardmäßig Dateien im Unterverzeichnis ″Documents and settings″ (Dokumente und Einstellungen) speichern, überprüfen Sie das Verzeichnis ″Application data″ (Anwendungsdaten) auf Verzeichnisse hin, die zu dieser Anwendung gehören. Gibt es ein solches, können Sie mit dem folgenden Befehl das Verzeichnis und die Dateien migrieren:

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

      wobei Location\ für eine vollständig qualifizierte Datei oder ein Verzeichnis steht, und [File] ein optionaler Parameter ist, der nur verwendet werden kann, wenn über Location\ ein Verzeichnis angegeben wird. Bei dem Beispiel mit Adobe Reader befinden sich die Anpassungsdateien im Verzeichnis ″Preferences″.
   b. Überprüfen Sie alle zugehörigen Verzeichnisse auf persönliche Einstellungen hin, die dort gespeichert sein könnten.
   c. Überprüfen Sie das Verzeichnis ″Local Settings″ (Lokale Einstellungen).
9. Bestimmen Sie Registrierungseinträge, die Sie migrieren möchten. Sie finden sie unter HKCU (HKEY_CURRENT_USER). Fügen Sie im Abschnitt <Registries> in der Anwendungsdatei die geeigneten Befehle hinzu.
10. Speichern Sie die application.XML-Datei im Verzeichnis ″d:\Program Files\ThinkVantage\SMA\Apps″, wobei d: für den Laufwerkbuchstaben des Festplattenlaufwerks steht.
11. Testen Sie die neue Anwendungsdatei.

Beispiel einer application.XML-Datei für Adobe Reader

Dieser Abschnitt enthält eine Anwendungsdatei für 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 Reader 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>
```

Systemaktualisierung

Active Update

Um festzustellen, ob das Programm "Active Update Launcher" installiert ist, überprüfen Sie, ob es den folgenden Registrierungsschlüssel gibt:

```
HKLM\Software\TVT\ActiveUpdate
```

Um festzustellen, ob das Programm "Active Update Launcher" für Active Update konfiguriert ist, überprüft das TVT innerhalb des eigenen Registrierungsschlüssels den Wert des Attributs "EnableActiveUpdate". Ist EnableActiveUpdate=1, fügt das TVT den Menüeintrag von Active Update unter dem Hilfemenü hinzu.

Um Active Update aufzurufen, startet das aufrufende TVT das Programm "Active Update Launcher" und übergibt eine Parameterdatei.

Gehen Sie wie folgt vor, um Active Update aufzurufen:

1. Öffnen Sie den Registrierungsschlüssel von Active Update Launcher:
   ```
   HKLM\software\TVT\ActiveUpdate
   ```
2. Rufen Sie den Wert des Attributs "Path" ab.
3. Rufen Sie den Wert des Attributs "Program" ab.

Kapitel 6. Installation

Das Installationspaket für Rescue and Recovery/Client Security Solution wurde mit InstallShield 10.5 Premier als Basic MSI-Projekt entwickelt. InstallShield 10.5 Basic MSI-Projekte verwenden das Windows-Installationsprogramm zum Installieren von Anwendungen, mit denen Administratoren zahlreiche Möglichkeiten zum Anpassen von Installationen haben. Sie können zum Beispiel Werte für Merkmale über eine Befehlszeile festlegen. In den folgenden Abschnitten wird beschrieben, wie das Installationspaket für Rescue and Recovery 3.0 verwendet und ausgeführt wird. Lesen Sie zum besseren Verständnis zunächst das ganze Kapitel, bevor Sie mit der Installation des Pakets beginnen.

Anmerkung: Lesen Sie für die Installation dieses Pakets die Readme-Datei auf der Lenovo Webseite unter folgender Adresse:

www.Lenovo.com/ThinkVantage

Die Readme-Datei enthält Echtzeitdaten zu Themen wie Softwareversionen, unterstützten Systemen und Systemvoraussetzungen sowie weitere Hinweise, die für Sie beim Installationsprozess hilfreich sind.

Installationsvoraussetzungen

Dieser Abschnitt enthält die Systemvoraussetzungen zum Installieren des Pakets für Rescue and Recovery/Client Security Solution. Rufen Sie die folgende Website auf, um zu prüfen, ob Sie über die aktuellste Softwareversion verfügen:

www.Lenovo.com/ThinkVantage

Einige herkömmliche IBM Computer unterstützen Rescue and Recovery, sofern sie die angegebenen Systemvoraussetzungen erfüllen. Informationen dazu, welche IBM Computer Rescue and Recovery unterstützen, finden Sie im Internet auf der Downloadseite.

Voraussetzungen für IBM und Lenovo Computer

IBM und Lenovo Computer müssen mindestens die folgenden Voraussetzungen erfüllen, damit Rescue and Recovery verwendet werden kann:

- Betriebssystem: Microsoft Windows XP oder Windows 2000
- Prozessor: Wie unter Microsoft for Windows XP (Home oder Professional) und Windows 2000 angegeben
  - mindestens Service-Pack 1
- Speicher: 128 MB
  - Bei Konfigurationen mit gemeinsam genutztem Speicher muss die BIOS-Einstellung für den maximal gemeinsam genutzten Speicher mindestens 4 MB und höchstens 8 MB betragen.
  - Bei Konfigurationen mit nicht gemeinsam genutztem Speicher beträgt diese Einstellung 120 MB an nicht gemeinsam genutztem Speicher.

    Anmerkung: Wenn der Computer über eine Kapazität von weniger als 200 MB nicht gemeinsam genutzten Speichers verfügt, kann Rescue and Recovery ausgeführt werden. Allerdings kann ein Benutzer möglicherweise nur eine Anwendung in der Umgebung von Rescue and Recovery aufrufen.

- 1,5 GB freier Festplattenspeicherplatz (für die Basisinstallation sind 930 MB erforderlich, hierbei ist jedoch noch nicht der erforderliche Speicherplatz für Rescue and Recovery-Sicherungen inbegriffen)
- VGA-kompatibler Bildschirm, der eine Auflösung von 800 x 600 und 24-Bit-Farbmodus unterstützt
- Unterstützte Ethernet-Karte

Voraussetzungen für die Installation und Verwendung von Computern anderer Hersteller

Für die Installation auf Computern anderer Hersteller gelten die folgenden Voraussetzungen:

Installationsvoraussetzungen

1,5 GB freier Festplattenspeicherplatz. Die Basisinstallation belegt 930 MB.

Mindestvoraussetzungen für Systemspeicher

Computer anderer Hersteller müssen über 128 MB Systemarbeitsspeicher für die Installation von Rescue and Recovery verfügen.

Konfiguration des Festplattenlaufwerks

Das Programm ″Rescue and Recovery″ wird nicht auf werkseitigen Vorinstallationen für OEM-Computer (Original Equipment Manufacturer) anderer Hersteller unterstützt. Für OEM-Computer muss das Festplattenlaufwerk entsprechend den Empfehlungen im Abschnitt „Rescue and Recovery auf Computern anderer Hersteller installieren” auf Seite 140 konfiguriert werden.

Netzwerkadapter

Die Umgebung von Rescue and Recovery unterstützt nur verdrahtete, PCI-basierte Ethernet-Netzwerkadapter. Die Netzeinheitentreiber in der Umgebung von Rescue and Recovery entsprechen den vorinstallierten Treibern des Betriebssystems Microsoft Windows XP Professional. Die Treiber sind vom Windows-Betriebssystem unabhängig. Für unterstützte Lenovo und IBM Computer sind die erforderlichen Treiber in der Software ″Rescue and Recovery″ enthalten.

Wenn eine OEM-Netzeinheit auf Ihrem Computer nicht unterstützt wird, lesen Sie in der Dokumentation zu dieser Einheit die Abschnitte, die Anweisungen zum Hinzufügen von Unterstützung für systemspezifische Netztreiber enthalten. Fordern Sie diese Treiber vom Hersteller (OEM) an.

Unterstützung für das Booten von externen Datenträgern (CD/DVD und USB)

Computer und Einheiten anderer Hersteller (USB-Festplattenlaufwerke, CD-R/RW, DVD-R/RW/RAM oder DVD+R/RW) müssen mindestens eine der folgenden Spezifikationen vollständig unterstützen:

- ATAPI-BIOS-Spezifikation für austauschbare Datenträger
- Erweiterte BIOS-Plattenlaufwerkservices - 2
- Compaq Phoenix Intel BIOS-Bootspezifikation
- El Torito-Spezifikation für bootfähiges CD-ROM-Format
- Übersicht zur USB-Massenspeicherklassenspezifikation (Alle Einheiten müssen die Befehlsblockspezifikation in Abschnitt 2.0, Unterklassencode, in der Übersicht zur USB-Massenspeicherklassenspezifikation (″USB Mass Storage Class Specification Overview″) einhalten.)
- USB-Massenspeicherspezifikation für Bootfähigkeit

Videovoraussetzungen

- **Videokompatibilität:** VGA-kompatibler Bildschirm, der eine Auflösung von 800 x 600 und 24-Bit-Farbmodus unterstützt
- **Bildspeicher:**
  - Bei nicht gemeinsam genutzten Bildspeichersystemen: mindestens 4 MB Video-RAM
  - Bei gemeinsam genutzten Bildspeichersystemen: mindestens 4 MB und höchstens 8 MB können als Bildspeicher zugeordnet werden.

Anwendungskompatibilität

Einige Anwendungen mit komplexen Filtertreiberumgebungen (wie z. B. Antivirensoftware) sind möglicherweise nicht mit der Software "Rescue and Recovery" kompatibel. Informationen zur Kompatibilität finden Sie im World Wide Web in der README-Datei zur Software "Rescue and Recovery" unter folgender Adresse:

www.lenovo.com/ThinkVantage

Dienstprogramme

In diesem Handbuch wird auf einige Dienstprogramme verwiesen. Diese Dienstprogramme finden Sie auf der Website unter der folgenden Adresse:

www.Lenovo.com/ThinkVantage

Installationskomponenten für Rescue and Recovery

1. Hauptinstallationspaket (ca. 45 MB): Hierbei handelt es sich um die Datei "setup.exe" aus der Quelle der Installationsprojekte. Die Datei "setup.exe" erhält während des Erstellungsprozesses einen Namen, der die Projekt-ID, den Datenträgertyp, die Erstellungsstufe, den Landescode (in diesem Fall immer US, deutsch: GR) und den Patch-Code angibt. Beispiel: Z096ZIS1001US00.exe (deutsch: Z096ZIS1001GR00.exe). Hierbei handelt es sich um ein selbst-extrahierendes Installationspaket, das die Quellendateien für die Installation extrahiert und den Installationsprozess mit Hilfe des Windows-Installationsprogramms startet. Das Paket enthält die Installationslogik und die Windows-Anwendungsdateien. Es enthält jedoch keine Predesktopdateien.
2. Predesktop US Base (ca. 135 MB, deutsch: GR): Dies ist die kennwortgeschützte, komprimierte Datei, die das gesamte Predesktop US-Basispaket enthält. Der Name hat das Format Z062ZAA1001US00.TVT (deutsch: Z062ZAA1001GR00.TVT), wobei *AA* die Kompatibilität des Predesktops und *001* die Predesktop-Stufe angibt. Diese Datei ist für die Predesktop-Installation auf allen Sprachsystemen erforderlich. Die Datei muss sich in demselben Verzeichnis befinden wie das Hauptinstallationspaket (entweder "setup.exe" oder "Rescue and Recovery/Client Security Solution.msi" wenn die Datei extrahiert ist oder bei einer OEM-Installation). Ausnahmen hierbei sind Fälle, in denen der Predesktop bereits installiert ist und nicht aufgerüstet werden muss oder wenn das Merkmal PDA=0 bei der Ausführung der Installation über eine Befehlszeile festgelegt wird und der Predesktop (beliebige Version) noch nicht vorhanden ist. Die Datei "setup.exe" enthält eine Datei "pdaversion.txt" mit der Nummer der Mindestversion des Predesktops, die unter dieser Version von Windows funktioniert. Dieses setup.exe-Installationsprogramm sucht unter Verwendung der folgenden Logik nach einer Predesktop-Datei:
   - **Veralteter Predesktop (RNR 1.0 oder 2.X) oder kein Predesktop vorhanden:**

     Das Installationsprogramm sucht nach einer Datei mit der Erweiterung .TVT und einem Kompatibilitätscode (z. B. AA, AB), der gleich dem Kompatibilitätscode der Mindestversion ist und die gleiche oder eine höhere Stufe als

die Mindestversion aufweist (alle anderen Versionsfelder im Namen der .TVT-Datei müssen genau mit der Mindestversion übereinstimmen). Wenn keine Datei gefunden wird, die diesen Kriterien entspricht, läuft die Installation in einer Endlosschleife.

- **Neue Version des Predesktops (RNR 3.0) vorhanden:**

  Das Installationsprogramm vergleicht den Kompatibilitätscode des aktuellen Predesktops mit dem Kompatibilitätscode der Mindestversion und ergreift anhand des Ergebnisses eine der folgenden Maßnahmen:

  – **Aktueller Code > Code der Mindestversion:**

    Das Installationsprogramm zeigt eine Nachricht an, dass die aktuelle Umgebung nicht mit dieser RNR-Version kompatibel ist.

  – **Aktueller Code = Code der Mindestversion:**

    Das Installationsprogramm vergleicht die Stufe der aktuellen Version mit der Stufe der Mindestversion. Wenn die aktuelle Stufe größer oder gleich der Stufe der Mindestversion ist, sucht das Installationsprogramm nach einer Datei mit der Erweiterung .TVT und einem Kompatibilitätscode (AA, AB...) der gleich dem Kompatibilitätscode der Mindestversion ist und eine höhere Stufe aufweist als die aktuelle Version (alle anderen Versionsfelder im Namen der .TVT-Datei müssen genau mit der Mindestversion übereinstimmen.) Wenn keine solche Datei gefunden wird, wird der Installationsprozess ohne Aktualisierung des Predesktops fortgesetzt. Wenn die aktuelle Stufe kleiner als die Stufe der Mindestversion ist, sucht das Installationsprogramm nach einer Datei mit der Erweiterung .TVT und einem Kompatibilitätscode (AA, AB...) der gleich dem Kompatibilitätscode der Mindestversion ist und die gleiche oder eine höhere Stufe aufweist als die Mindestversion (alle anderen Versionsfelder im Namen der .TVT-Datei müssen genau mit der Mindestversion übereinstimmen.) Wenn keine Datei gefunden wird, die diesen Kriterien entspricht, läuft die Installation in einer Endlosschleife.

  – **Aktueller Code < Code der Mindestversion:**

    Das Installationsprogramm sucht nach einer Datei mit der Erweiterung .TVT und einem Kompatibilitätscode (AA, AB...), der gleich dem Kompatibilitätscode der Mindestversion ist und die gleiche oder eine höhere Stufe als die Mindestversion aufweist (alle anderen Versionsfelder im Namen der .TVT-Datei müssen genau mit der Mindestversion übereinstimmen). Wenn keine Datei gefunden wird, die diesen Kriterien entspricht, läuft die Installation in einer Endlosschleife.

3. Predesktop-Sprachenpakete (jeweils ca. 5 bis 30 MB): Es gibt 24 Sprachenpakete für Windows PE, die von Rescue and Recovery 3.0 unterstützt werden. Jedes Sprachenpaket ist im Format Z062ZAA1001CC00.TVT benannt, wobei CC die jeweilige Sprache angibt. Eine dieser Dateien ist erforderlich, wenn der Predesktop auf einem System mit einer anderen Sprache als Englisch oder auf einem System mit einer nicht unterstützten Sprache installiert wird. Die Datei muss sich in demselben Verzeichnis befinden wie die Hauptinstallation und die englische (US) Predesktop-Datei mit der Erweiterung .TVT. Die Sprache des Sprachenpakets muss mit der Sprache von Windows übereinstimmen, wenn Windows in einer anderen Sprache als Englisch oder in einer Sprache vorliegt, die nicht von den Sprachenpaketen unterstützt wird. Wenn der Predesktop gerade installiert oder aktualisiert wird und ein Sprachenpaket erforderlich ist, sucht das Installationsprogramm nach einem Sprachenpaket mit der Erweiterung .TVT, in dem alle Felder im Dateinamen mit dem Namen der Predesktop-Datei der US-amerikanischen Version übereinstimmen und nur der Sprachencode mit der Sprache des Systems übereinstimmt.

Die Sprachenpakete sind in den folgenden Sprachen verfügbar:

- Arabisch
- Brasilianisches Portugiesisch
- Chinesisch
- Chinesisch (Hongkong)
- Dänisch
- Deutsch
- Finnisch
- Französisch
- Griechisch
- Hebräisch
- Italienisch
- Japanisch
- Koreanisch
- Niederländisch
- Norwegisch
- Polnisch
- Portugiesisch
- Russisch
- Schwedisch
- Spanisch
- Traditionelles Chinesisch
- Tschechisch
- Türkisch
- Ungarisch
- Vereinfachtes Chinesisch

Standardinstallationsverfahren und Befehlszeilenparameter

Setup.exe kann eine Reihe von Befehlszeilenparametern akzeptieren, die nachfolgend beschrieben sind. Befehlszeilenoptionen, für die ein Parameter erforderlich ist, müssen ohne Leerzeichen zwischen der Option und dem zugehörigen Parameter angegeben werden. Beispiel: Setup.exe /s /v″/qn REBOOT=″R″″ ist gültig, hingegen ist Setup.exe /s /v ″/qn REBOOT=″R″″ ungültig. Anführungszeichen vor und nach einem Parameter sind nur dann erforderlich, wenn der Parameter Leerzeichen enthält.

Anmerkung: Das Standardverhalten bei einer allein ausgeführten Installation (Ausführung der Datei ″setup.exe″ ohne Parameter) besteht darin, dass der Benutzer nach Abschluss der Installation dazu aufgefordert wird, den Computer erneut zu starten. Ein Neustart ist für das ordnungsgemäße Funktionieren des Programms erforderlich. Der Neustart kann durch einen Befehlszeilenparameter für eine unbeaufsichtigte Installation verzögert werden (eine Beschreibung dazu finden Sie oben im Abschnitt mit den Beispielen).

Die folgenden Parameter und Beschreibungen wurden direkt aus der Dokumentation zur Hilfe für InstallShield Developer entnommen. Parameter, die nicht für Basic MSI-Projekte gelten, wurden entfernt.

Tabelle 13.

Parameter	Beschreibung
/a : Administrative Installation	Durch den Schalter /a führt Setup.exe eine administrative Installation aus. Bei einer administrativen Installation werden Ihre Datendateien in ein durch den Benutzer angegebenes Verzeichnis kopiert (und entpackt), aber es werden keine Verknüpfungen erstellt, keine COM-Server registriert und kein Protokoll zur Deinstallation erstellt.
/x : Uninstall mode	Durch den Schalter /x deinstalliert Setup.exe ein zuvor installiertes Produkt.
/s : Silent mode	Durch den Befehl Setup.exe /s wird das Initialisierungsfenster von Setup.exe für ein Basic MSI-Installationsprogramm unterdrückt, aber es wird keine Antwortdatei gelesen. Bei Basic MSI-Projekten werden keine Antwortdateien für unbeaufsichtigte Installationen erstellt oder verwendet. Um ein Basic MSI-Produkt unbeaufsichtigt auszuführen, führen Sie die Befehlszeile Setup.exe /s /v/qn aus. (Zur Angabe der Werte von öffentlichen Merkmalen für eine unbeaufsichtigte Basic MSI-Installation können Sie einen Befehl wie z. B. Setup.exe /s /v"/qn INSTALLDIR=D:\Destination" verwenden.)
/v : pass arguments to Msiexec	Das Argument /v wird verwendet, um Befehlszeilenschalter und Werte von öffentlichen Merkmalen an Msiexec.exe zu übergeben.
/L : Setup language	Benutzer können den Schalter /L mit der dezimalen Sprachen-ID verwenden, um die Sprache anzugeben, die in einem mehrsprachigen Installationsprogramm verwendet werden soll. Der Befehl, um Deutsch als Sprache anzugeben, lautet beispielsweise Setup.exe /L1031. Anmerkung: Es werden nicht alle in Tabelle 14 auf Seite 91 angegebenen Sprachen bei der Installation unterstützt.
/w : Wait	Bei einem Basic MSI-Projekt wird Setup.exe durch das Argument /w gezwungen, mit dem Beenden bis zum Abschluss der Installation zu warten. Wenn Sie die Option /w in einer Batchdatei verwenden, möchten Sie dem Befehlszeilenparameter von Setup.exe möglicherweise start /WAIT voranstellen. Ein Beispiel im richtigen Format hierzu sieht wie folgt aus: `start /WAIT setup.exe /w`

Tabelle 14.

Sprache	**Kennung**
Arabisch (Saudi-Arabien)	1025
Baskisch	1069
Brasilianisches Portugiesisch	1046
Bulgarisch	1026
Dänisch	1030
Niederländisch (Standard)	1043
Englisch	1033
Finnisch	1035
Französisch (Kanada)	3084
Französisch	1036
Deutsch	1031
Griechisch	1032
Hebräisch	1037
Indonesisch	1057
Italienisch	1040
Japanisch	1041
Katalanisch	1027
Koreanisch	1042
Kroatisch	1050
Norwegisch (Bokmal)	1044
Polnisch	1045
Portugiesisch (Standard)	2070
Rumänisch	1048
Russisch	1049
Schwedisch	1053
Slowakisch	1051
Slowenisch	1060
Spanisch	1034
Tschechisch	1029
Thailändisch	1054
Traditionelles Chinesisch	1028
Türkisch	1055
Ungarisch	1038
Vereinfachtes Chinesisch	2052

Verfahren und Befehlszeilenparameter für die administrative Installation

Das Windows-Installationsprogramm kann eine administrative Installation einer Anwendung oder eines Produkts in einem Netzwerk zur Verwendung durch Arbeitsgruppen oder zur kundenspezifischen Anpassung durchführen. Für das Installationspaket für Rescue and Recovery/Client Security Solution werden bei der administrativen Installation die Quellendateien für die Installation an eine angegebene Position entpackt. Um eine administrative Installation auszuführen, muss das Installationspaket über die Befehlszeile mit Hilfe des Parameters /a ausgeführt werden:

```
Setup.exe /a
```

Beim Starten einer administrativen Installation wird eine Reihe von Dialogfenstern angezeigt, in denen der Administrator dazu aufgefordert wird, die Position anzugeben, an der die Konfigurationsdateien entpackt werden sollen. Die Standardposition zum Entpacken, die dem Administrator angezeigt wird, ist C:\. Es kann eine neue Position ausgewählt werden, zu der auch andere Laufwerke als C: gehören können (z. B. andere lokale Laufwerke oder zugeordnete Netzlaufwerke). Bei diesem Schritt können auch neue Verzeichnisse erstellt werden.

Wenn eine administrative Installation unbeaufsichtigt ausgeführt wird, kann das öffentliche Merkmal TARGETDIR in der Befehlszeile festgelegt werden, um die Position zum Entpacken anzugeben:

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

Wenn eine administrative Installation abgeschlossen ist, kann der Administrator die Quellendateien anpassen, indem er beispielsweise weitere Einstellungen zu tvt.txt hinzufügt. Zum Starten der Installation aus den extrahierten Quellendateien muss der Benutzer nach Abschluss der Anpassungen die Datei msiexec.exe über eine Befehlszeile öffnen und dabei den Namen der extrahierten msi-Datei angeben.

Der folgende Abschnitt enthält eine Beschreibung der verfügbaren Befehlszeilenparameter, die in Verbindung mit msiexec verwendet werden können, sowie ein Anwendungsbeispiel. Öffentliche Merkmale können auch direkt in der Befehlszeilenaufforderung von msiexec festgelegt werden.

Befehlszeilenparameter von MsiExec.exe

Bei MsiExec.exe handelt es sich um ein ausführbares Programm des Windows-Installationsprogramms, das zur Interpretation von Installationspaketen und zur Installation von Produkten auf den Zielsystemen verwendet wird:

```
msiexec. /i "C:Windows-Ordner/Profiles\Benutzername\Persona\MySetups\Projektname
  \Produktkonfiguration\Name_des_Releases\DiskImages\Disk1\Produktname.msi
```

Die folgende Tabelle enthält eine genaue Beschreibung der Befehlszeilenparameter von MsiExec.exe. Diese Tabelle wurde der Dokumentation zu Microsoft Platform SDK im Windows-Installationsprogramm direkt entnommen.

Tabelle 15.

Parameter	Beschreibung
/i *Paket* oder *Produktcode*	Verwenden Sie das folgende Format, um das Produkt "Othello" zu installieren: `msiexec /i "C:\Windows-Ordner\Profiles\ Benutzername\Personal\MySetups\Othello\Trial Version\ Release\DiskImages\Disk1\Othello Beta.msi"` Der Produktcode bezieht sich auf die GUID, die automatisch in den Merkmalen des Produktcodes in der Ansicht Ihres Produkts generiert wird.
/f [p|o|e|d|c|a|u|m|s|v] *Paket* oder *Produktcode*	Durch die Installation mit dem Parameter /f werden fehlende oder beschädigte Dateien repariert oder erneut installiert. Verwenden Sie beispielsweise die folgende Syntax, um zu erzwingen, dass alle Dateien erneut installiert werden: `msiexec /fa "C:\Windows-Ordner\Profiles\ Benutzername\Personal\MySetups\Othello\Trial Version\ Release\DiskImages\Disk1\Othello Beta.msi"` zusammen mit folgenden Flags: • p installiert eine Datei erneut, wenn diese fehlt • o installiert eine Datei erneut, wenn diese fehlt oder in einer älteren Version auf dem System des Benutzers vorhanden ist • e installiert eine Datei erneut, wenn diese fehlt oder eine entsprechende oder eine ältere Version dieser Datei auf dem System des Benutzers vorhanden ist • c installiert eine Datei erneut, wenn diese fehlt oder wenn die gespeicherte Kontrollsumme der installierten Datei nicht mit dem Wert der neuen Datei übereinstimmt. • a erzwingt das erneute Installieren aller Dateien • u oder m schreiben alle erforderlichen Einträge in der Benutzer-Registrierungsdatenbank erneut • s überschreibt alle vorhandenen Verknüpfungen • v führt die Anwendung von der Quelle aus und stellt die lokale Installation erneut in den Zwischenspeicher
/a *Paket*	Mit Hilfe des Parameters /a können Administratoren ein Produkt im Netzwerk installieren.
/x *Paket* oder *Produktcode*	Durch den Parameter /x wird ein Produkt deinstalliert.

Tabelle 15. (Forts.)

Parameter	Beschreibung
/L [i|w|e|a|r|u|c|m|p|v|+] *Protokolldatei*	Mit dem Parameter /L wird der Pfad für die Protokolldatei angegeben. Die Flags geben an, welche Informationen in der Protokolldatei aufgezeichnet werden sollen: • i protokolliert Statusnachrichten • w protokolliert nicht schwerwiegende Warnungen • e protokolliert alle Fehlernachrichten • a protokolliert die Fortführung von Aktionsfolgen • r protokolliert aktionsspezifische Datensätze • u protokolliert Benutzeranfragen • c protokolliert Schnittstellenparameter von Erstbenutzern • m protokolliert Nachrichten zu fehlender Speicherkapazität • p protokolliert Terminaleinstellungen • v protokolliert die Einstellung für ausführliche Ausgabe • + hängt die Informationen an eine vorhandene Datei an • * dient als Platzhalterzeichen, mit dem Sie alle Informationen protokollieren können (außer der Einstellung für ausführliche Ausgabe)
/q [n|b|r|f]	Der Parameter /q wird verwendet, um die Ebene der Benutzerschnittstelle zusammen mit den folgenden Flags festzulegen: • q oder qn erstellt keine Benutzerschnittstelle • qb erstellt eine Basisbenutzerschnittstelle Die folgenden Einstellungen für die Benutzerschnittstelle bewirken die Anzeige eines Modaldialogfensters am Ende der Installation: • qr zeigt eine verkleinerte Benutzerschnittstelle an • qf zeigt eine vollständige Benutzerschnittstelle an • qn+ zeigt keine Benutzerschnittstelle an • qb+ zeigt eine Basisbenutzerschnittstelle an
/? oder /h	Mit beiden Befehlen wird der Copyrightvermerk des Windows-Installationsprogramms angezeigt.
TRANSFORMS	Mit dem Befehlszeilenparameter TRANSFORMS können Sie alle Umsetzungen angeben, die für das Basispaket ausgeführt werden sollen. Dabei kann der TRANSFORMS-Aufruf über die Befehlszeile z. B. wie folgt verwendet werden: `msiexec /i "C:\`*`Windows-Ordner`*`\Profiles\` *`Benutzername`*`\Personal\MySetups\`*`Projektname`*`\Trial Version\My Release-1\DiskImages\Disk1\ProduktName.msi" TRANSFORMS="New Transform 1.mst"` Mehrere Umsetzungen können durch Semikolons voneinander getrennt werden. Aus diesem Grund sollten Sie keine Semikolons in den Namen der Umsetzungen verwenden, da das Windows-Installationsprogramm diese Zeichen nicht korrekt interpretieren kann.

Tabelle 15. (Forts.)

Parameter	Beschreibung
Merkmale	Alle öffentlichen Merkmale können über die Befehlszeile festgelegt oder geändert werden. Die öffentlichen Merkmale unterscheiden sich von den privaten Merkmalen durch die ausschließliche Verwendung von Großbuchstaben. Beispiel: FIRMENNAME ist ein öffentliches Merkmal. Um ein Merkmal über die Befehlszeile festzulegen, verwenden Sie die folgende Syntax: MERKMAL=WERT. Angenommen, Sie möchten den Wert für FIRMENNAME ändern, würden Sie Folgendes eingeben: `msiexec /i "C:\Windows-Ordner\Profiles\Benutzername \Personal\MySetups\Projektname\Trial Version\My Release-1\DiskImages\Disk1\ProduktName.msi" FIRMENNAME="InstallShield"`

Öffentliche Standardmerkmale des Windows-Installationsprogramms

Das Windows-Installationsprogramm verfügt über eine Reihe von standardmäßig integrierten Merkmalen, die über die Befehlszeile festgelegt werden können, um ein bestimmtes Verhalten bei der Installation anzugeben. Die üblichsten öffentlichen Merkmale, die in der Befehlszeile verwendet werden, sind nachfolgend beschrieben. Weitere Dokumentation ist auf der Microsoft-Website unter der Adresse http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/about_properties.asp verfügbar.

Tabelle 16 zeigt die im Allgemeinen verwendeten Merkmale des Windows-Installationsprogramms:

Tabelle 16.

Merkmal	Beschreibung
TARGETDIR	Gibt das Stammzielverzeichnis für die Installation an. Bei einer administrativen Installation gibt dieses Merkmal die Position an, an die das Installationspaket kopiert wird.
ARPAUTHORIZEDCDFPREFIX	Der URL des Aktualisierungskanals der Anwendung.
ARPCOMMENTS	Stellt Kommentare zum Hinzufügen oder Entfernen von Programmen in der Systemsteuerung bereit.
ARPCONTACT	Stellt den Kontakt zum Hinzufügen oder Entfernen von Programmen in der Systemsteuerung her.
ARPINSTALLLOCATION	Der vollständig qualifizierte Pfad zum Primärordner der Anwendung.
ARPNOMODIFY	Inaktiviert die Funktionalität, durch die das Produkt geändert werden könnte.
ARPNOREMOVE	Inaktiviert die Funktionalität, durch die das Produkt entfernt werden könnte.
ARPNOREPAIR	Inaktiviert die Schaltfläche zum Reparieren im Programmassistenten.

Tabelle 16. (Forts.)

Merkmal	Beschreibung
ARPPRODUCTICON	Gibt das primäre Symbol für das Installationspaket an.
ARPREADME	Stellt eine Readme-Datei zum Hinzufügen oder Entfernen von Programmen in der Systemsteuerung bereit.
ARPSIZE	Die geschätzte Größe der Anwendung in Kilobytes.
ARPSYSTEMCOMPONENT	Verhindert das Anzeigen von Anwendungen in der Liste zum Hinzufügen und Entfernen von Programmen.
ARPURLINFOABOUT	URL der Homepage einer Anwendung.
ARPURLUPDATEINFO	URL für Informationen zur Anwendungsaktualisierung.
REBOOT	Das Merkmal REBOOT unterdrückt bestimmte Aufforderungen für einen Neustart des Systems. Ein Administrator verwendet dieses Merkmal normalerweise bei einer Reihe von gleichzeitigen Installationen verschiedener Produkte, bei denen am Ende nur ein Neustart durchgeführt wird. Legen Sie REBOOT="R" fest, um alle Neustarts am Ende der einzelnen Installationen zu inaktivieren.
INSTALLDIR	Dieses Merkmal enthält den Standardzielordner für die Dateien zu Ihren Produktmerkmalen und Komponenten.

Angepasste öffentliche Merkmale von Rescue and Recovery

Das Installationspaket für das Programm "Rescue and Recovery" verfügt über eine Reihe von angepassten öffentlichen Merkmalen, die bei der Ausführung der Installation über die Befehlszeile festgelegt werden können. Die folgenden angepassten öffentlichen Merkmale sind verfügbar:

Tabelle 17.

Merkmal	Beschreibung
PDA	Gibt an, ob der Predesktop installiert werden soll. Der Standardwert ist 1. 1 = Predesktop installieren, 0 = Predesktop nicht installieren. ANMERKUNG: Diese Einstellung wird nicht verwendet, wenn bereits eine Version des Predesktops vorhanden ist.
CIMPROVIDER	Gibt an, ob die Komponente "CIM Provider" installiert werden soll. In der Standardeinstellung wird die Komponente nicht installiert. Geben Sie in der Befehlszeile CIMPROIVIDER=1 ein, um die Komponente zu installieren.

Tabelle 17. (Forts.)

Merkmal	Beschreibung
EMULATIONMODE	Gibt an, dass die Installation im Emulationsmodus erzwungen wird, auch wenn bereits ein TPM vorhanden ist. Geben Sie in der Befehlszeile EMULATIONMODE=1 ein, um die Installation im Emulationsmodus vorzunehmen.
HALTIFCSS54X	Wenn CSS 5.4X installiert ist und die Installation im Befehlszeilenmodus ausgeführt wird, lautet die Standardeinstellung für die Installation, dass sie im Emulationsmodus fortgesetzt wird. Verwenden Sie das Merkmal HALTIFCSS54X=1, wenn die Installation im Befehlszeilenmodus ausgeführt wird, um die Installation anzuhalten, wenn CSS 5.4X installiert ist.
HALTIFTPMDISABLED	Wenn sich das TPM im inaktivierten Status befindet und die Installation im Befehlszeilenmodus ausgeführt wird, lautet die Standardeinstellung für die Installation, dass sie im Emulationsmodus fortgesetzt wird. Verwenden Sie das Merkmal HALTIFTPMDISABLED=1, wenn die Installation im Befehlszeilenmodus ausgeführt wird, um die Installation anzuhalten, wenn das TPM inaktiviert ist.
ENABLETPM	Legen Sie ENABLETPM=0 in der Befehlszeile fest, um zu verhindern, dass das TPM durch die Installation aktiviert wird.
NOCSS	Legen Sie in der Befehlszeile NOCSS=1 fest, um zu verhindern, dass Client Security Solution und zugehörige Unterfunktionen installiert werden. Diese Einstellung soll insbesondere bei unbeaufsichtigten Installationen verwendet werden, kann aber auch bei Installationen über die Benutzerschnittstelle verwendet werden. Bei der Installation über die Benutzerschnittstelle wird die CSS-Funktion nicht im Fenster für die angepasste Installation angezeigt.
NOPRVDISK	Legen Sie in der Befehlszeile NOPRVDISK=1 fest, um zu verhindern, dass die Funktion ″SafeGuard PrivateDisk″ installiert wird. Diese Einstellung soll insbesondere bei unbeaufsichtigten Installationen verwendet werden, kann aber auch bei Installationen über die Benutzerschnittstelle verwendet werden. Bei der Installation über die Benutzerschnittstelle wird die Funktion ″SafeGuard PrivateDisk″ nicht im Fenster für die angepasste Installation angezeigt.

Tabelle 17. (Forts.)

Merkmal	Beschreibung
NOPWMANAGER	Legen Sie in der Befehlszeile NOPWMANAGER=1 fest, um zu verhindern, dass die Funktion "Password Manager" installiert wird. Diese Einstellung soll insbesondere bei unbeaufsichtigten Installationen verwendet werden, kann aber auch bei Installationen über die Benutzerschnittstelle verwendet werden. Bei der Installation über die Benutzerschnittstelle wird die Funktion "Password Manager" nicht im Fenster für die angepasste Installation angezeigt.
NOCSSWIZARD	Legen Sie in der Befehlszeile NOCSSWIZARD=1 fest, um zu verhindern, dass der CSS-Assistent angezeigt wird, wenn sich ein Administrator anmeldet, der nicht registriert ist. Dieses Merkmal ist dafür gedacht, wenn CSS installiert werden soll, das System jedoch erst später mit Hilfe von Scripts konfiguriert werden soll.
CSS_CONFIG_SCRIPT	Legen Sie CSS_CONFIG_SCRIPT="*Dateiname*" oder "*Dateiname_Kennwort*" fest, um eine Konfigurationsdatei zu erhalten, die ausgeführt wird, nachdem ein Benutzer die Installation abgeschlossen und einen Neustart durchgeführt hat.
SUPERVISORPW	Legen Sie in der Befehlszeile SUPERVISORPW="*Kennwort*" fest, um ein Administratorkennwort bereitzustellen, um den Chip für die Installation im Befehlszeilenmodus oder in einem anderen Modus zu aktivieren. Wenn der Chip inaktiviert ist und die Installation im Befehlszeilenmodus ausgeführt wird, muss das richtige Administratorkennwort eingegeben werden, um den Chip zu aktivieren. Andernfalls wird der Chip nicht aktiviert.

Installationsprotokolldatei

Im Verzeichnis %temp% wird eine Protokolldatei mit dem Namen rrinstall30.log erstellt, wenn die Installation über die Datei "setup.exe" gestartet wird (durch Doppelklicken auf die Datei für die Hauptinstallation (mit der Erweiterung .exe), durch Ausführen der ausführbaren Datei für die Hauptinstallation ohne Parameter oder durch Extrahieren von msi und Ausführen der Datei "setup.exe"). Diese Datei enthält Protokollnachrichten, die zum Beheben von Installationsfehlern verwendet werden können. Diese Protokolldatei wird nicht erstellt, wenn die Installation direkt über das msi-Paket ausgeführt wird. Dazu gehören auch die Aktionen, die über die die Option zum Hinzufügen und Entfernen von Programmen ("Software") ausgeführt werden. Um eine Protokolldatei für alle MSI-Aktionen zu erstellen, können Sie die Richtlinie für die Protokollierung in der Registrierungsdatenbank aktivieren. Erstellen Sie hierfür den folgenden Wert:

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

Installationsbeispiele

In der folgenden Tabelle sind Beispiele für die Verwendung der Datei ″setup.exe″ dargestellt:

Tabelle 18.

Beschreibung	Beispiel
Unbeaufsichtigte Installation ohne Neustart	`setup.exe /s /v"/qn REBOOT="R""`
Administrative Installation	`setup.exe /a`
Unbeaufsichtigte administrative Installation, bei der die Position zum Entpacken angegeben wird	`setup.exe /a /s /v"/qn TARGETDIR="F:\TVTRR""`
Unbeaufsichtigte Deinstallation setup.exe /s /x /v/qn	`setup.exe /s /x /v/qn`
Installation ohne Neustart mit Erstellung eines Installationsprotokolls im temporären Verzeichnis	`setup.exe /v"REBOOT="R" /L*v %temp%\rrinstall30.log"`
Installation ohne Predesktop-setup.exe /vPDA=0	`setup.exe /vPDA=0`

In der folgenden Tabelle sind Beispiele für die Installation mit Hilfe von Rescue and Recovery/Client Security Solution.msi dargestellt:

Tabelle 19.

Beschreibung	Beispiel
Installation	msiexec /i “C:\TVTRR\Rescue and Recovery/Client Security Solution.msi”
Unbeaufsichtigte Installation ohne Neustart	msiexec /i “C:\TVTRR\Rescue and Recovery/Client Security Solution.msi” /qn REBOOT=”R”
Unbeaufsichtigte Deinstallation	msiexec /x “C:\TVTRR\Rescue and Recovery/Client Security Solution.msi” /qn
Installation ohne Installation des Predesktops	msiexec /i “C:\TVTRR\Rescue and Recovery/Client Security Solution.msi” PDA=0

Rescue and Recovery in ein Plattenimage einschließen

Sie können mit einem Tool Ihrer Wahl ein Plattenimage mit Rescue and Recovery erstellen. Dieses Implementierungshandbuch bietet grundlegende Informationen zu PowerQuest und Ghost in Bezug auf diese Anwendung und diese Installation. Sie sollten über Erfahrung mit den Funktionen Ihres Tools zum Erstellen von Images verfügen. Wahrscheinlich möchten Sie noch andere Optionen hinzufügen, die für Ihre Anwendungen erforderlich sind.

Anmerkung: Wenn Sie ein Image erstellen möchten, müssen Sie den Master-Bootsatz erfassen. Der Master-Bootsatz ist unbedingt erforderlich, damit die Umgebung von Rescue and Recovery ordnungsgemäß funktioniert.

Auf PowerQuest Drive Image basierende Tools verwenden

Wenn das Tool ″PowerQuest DeployCenter″ (PQIMGCTR) an der Position (X:\PQ) installiert ist, können Sie mit den nachfolgenden Scripts ein Image mit Rescue and Recovery erstellen und implementieren:

Mindestvoraussetzung an Scriptdateien

Tabelle 20. X:\PQ\RRUSAVE.TXT

Scriptsprache	Ergebnis
SELECT DRIVE 1	Wählt das erste Festplattenlaufwerk aus.
SELECT PARTITION ALL (Erforderlich, wenn das Image eine Partition vom Typ 12 oder mehrere Partitionen enthalten soll).	Wählt alle Partitionen aus
Store with compression high	Speichert das Image.

Tabelle 21. X:\PQ\RRDEPLY.TXT

Scriptsprache	Ergebnis
SELECT DRIVE 1	Wählt das erste Festplattenlaufwerk aus.
DELETE ALL	Löscht alle Partitionen.
SELECT FREESPACE FIRST	Wählt den ersten freien Speicherbereich aus.
SELECT IMAGE ALL	Wählt alle Partitionen im Image aus.
RESTORE	Stellt das Image wieder her.

Image erstellen

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

Scriptsprache	Ergebnis
SELECT DRIVE 1	Wählt das erste Festplattenlaufwerk aus.
X:\PQ\PQIMGCTR	Imageprogramm
/CMD=X:\PQ\RRUSAVE.TXT	PowerQuest-Scriptdatei
/MBI=1	Erfasst den Boot-Manager von Rescue and Recovery.
/IMG=X:\IMAGE.PQI	Imagedatei

Image implementieren

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

Scriptsprache	Ergebnis
SELECT DRIVE 1	Wählt das erste Festplattenlaufwerk aus.
X:\PQ\PQIMGCTR	Imageprogramm
/CMD=X:\PQ\RRDEPLY.TXT	PowerQuest-Scriptdatei
/MBR=1	Stellt den Boot-Manager von Rescue and Recovery wieder her.
/IMG=X:\IMAGE.PQI	Imagedatei

Auf Symantec Ghost basierende Tools verwenden

Beim Erstellen des Ghost-Images müssen Sie den Befehlszeilenschalter `-ib` (der möglicherweise in die Datei GHOST.INI integriert wird) verwenden, um den Boot-Manager von Rescue and Recovery zu erfassen. Außerdem muss das Image die gesamte Festplatte und alle Partitionen erfassen. Genauere Informationen zu Ghost finden Sie in der Dokumentation von Symantec.

Installationskomponenten für Client Security Solution Version 6.0

Das Installationspaket für Client Security Solution 6.0 wurde mit InstallShield 10.5 Premier als Basic MSI-Projekt entwickelt. InstallShield 10.5 Basic MSI-Projekte verwenden das Windows-Installationsprogramm zum Installieren von Anwendungen, mit denen Administratoren zahlreiche Möglichkeiten zum Anpassen von Installationen haben, wie zum Beispiel Merkmale über eine Befehlszeile festzulegen. In den folgenden Abschnitten wird beschrieben, wie das Installationspaket für CSS 6.0 verwendet und ausgeführt wird. Lesen Sie alle folgenden Anweisungen, um den Prozess besser nachvollziehen zu können.

Installationskomponenten

Die Installation von CSS 6.0 besteht aus einer einzelnen exe-Datei (ca. 20 MB). Hierbei handelt es sich um die Datei ″setup.exe″ aus dem Ausgangsordner des Installationsprojekts. Die Datei ″setup.exe″ erhält während des Erstellungsprozesses einen Namen, der die Projekt-ID, den Datenträgertyp, die Erstellungsstufe, den Landescode (in diesem Fall immer US, deutsch: GR) und den Patch-Code angibt. Beispiel: 169ZIS1001US00.exe (deutsch: 169ZIS1001GR00.exe). Hierbei handelt es sich um ein selbst-extrahierendes Installationspaket, das die Quellendateien für die Installation extrahiert und den Installationsprozess mit Hilfe des Windows-Installationsprogramms startet. Das Paket enthält die Installationslogik und die Windows-Anwendungsdateien.

Standardinstallationsverfahren und Befehlszeilenparameter

Setup.exe kann eine Reihe von Befehlszeilenparametern akzeptieren, die nachfolgend beschrieben sind. Befehlszeilenparameter, für die ein Parameter erforderlich ist, müssen ohne Leerzeichen zwischen der Option und dem zugehörigen Parameter angegeben werden. Z. B. ist

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

gültig. Dagegen ist

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

ungültig. Anführungszeichen vor und nach einem Parameter sind nur dann erforderlich, wenn der Parameter Leerzeichen enthält.

Anmerkung: Das Standardverhalten bei einer allein ausgeführten Installation (Ausführung der Datei ″setup.exe″ ohne Parameter) besteht darin, dass der Benutzer nach Abschluss der Installation dazu aufgefordert wird, den Computer erneut zu starten. Ein Neustart ist für das ordnungsgemäße Funktionieren des Programms erforderlich. Der Neustart kann durch einen Befehlszeilenparameter für eine unbeaufsichtigte Installation verzögert werden (eine Beschreibung dazu finden Sie oben im Abschnitt mit den Beispielen).

Die folgenden Parameter und Beschreibungen wurden direkt aus der Dokumentation zur Hilfe für InstallShield Developer entnommen. Parameter, die nicht für Basic MSI-Projekte gelten, wurden entfernt.

Tabelle 24.

Parameter	Beschreibung
/a : Administrative Installation	Durch den Schalter /a führt Setup.exe eine administrative Installation aus. Bei einer administrativen Installation werden Ihre Datendateien in ein durch den Benutzer angegebenes Verzeichnis kopiert (und entpackt), aber es werden keine Verknüpfungen erstellt, keine COM-Server registriert und kein Protokoll zur Deinstallation erstellt.
/x : Uninstall mode	Durch den Schalter /x deinstalliert Setup.exe ein zuvor installiertes Produkt.
/s : Silent mode	Durch den Befehl Setup.exe /s wird das Initialisierungsfenster von Setup.exe für ein Basic MSI-Installationsprogramm unterdrückt, aber es wird keine Antwortdatei gelesen. Bei Basic MSI-Projekten werden keine Antwortdateien für unbeaufsichtigte Installationen erstellt oder verwendet. Um ein Basic MSI-Produkt unbeaufsichtigt auszuführen, führen Sie die Befehlszeile Setup.exe /s /v/qn aus. (Zur Angabe der Werte von öffentlichen Merkmalen für eine unbeaufsichtigte Basic MSI-Installation können Sie einen Befehl wie z. B. Setup.exe /s /v"/qn INSTALLDIR=D:\Destination" verwenden.)
/v : pass arguments to Msiexec	Das Argument /v wird verwendet, um Befehlszeilenschalter und Werte von öffentlichen Merkmalen an Msiexec.exe zu übergeben.
/L : Setup language	Benutzer können den Schalter /L mit der dezimalen Sprachen-ID verwenden, um die Sprache anzugeben, die in einem mehrsprachigen Installationsprogramm verwendet werden soll. Der Befehl, um Deutsch als Sprache anzugeben, lautet beispielsweise Setup.exe /L1031. Anmerkung: Es werden nicht alle in Tabelle 25 auf Seite 103 angegebenen Sprachen bei der Installation unterstützt.
/w : Wait	Bei einem Basic MSI-Projekt wird Setup.exe durch das Argument /w gezwungen, mit dem Beenden bis zum Abschluss der Installation zu warten. Wenn Sie die Option /w in einer Batchdatei verwenden, möchten Sie dem Befehlszeilenparameter von Setup.exe möglicherweise start /WAIT voranstellen. Ein Beispiel im richtigen Format hierzu sieht wie folgt aus: `start /WAIT setup.exe /w`

Tabelle 25.

Sprache	**Kennung**
Arabisch (Saudi-Arabien)	1025
Baskisch	1069
Bulgarisch	1026
Katalanisch	1027
Vereinfachtes Chinesisch	2052
Traditionelles Chinesisch	1028
Kroatisch	1050
Tschechisch	1029
Dänisch	1030
Niederländisch (Standard)	1043
Englisch	1033
Finnisch	1035
Französisch (Kanada)	3084
Französisch	1036
Deutsch	1031
Griechisch	1032
Hebräisch	1037
Ungarisch	1038
Indonesisch	1057
Italienisch	1040
Japanisch	1041
Koreanisch	1042
Norwegisch (Bokmal)	1044
Polnisch	1045
Brasilianisches Portugiesisch	1046
Portugiesisch (Standard)	2070
Rumänisch	1048
Russisch	1049
Slowakisch	1051
Slowenisch	1060
Spanisch	1034
Schwedisch	1053
Thailändisch	1054
Türkisch	1055

Verfahren und Befehlszeilenparameter für die administrative Installation

Das Windows-Installationsprogramm kann eine administrative Installation einer Anwendung oder eines Produkts in einem Netzwerk zur Verwendung durch Arbeitsgruppen oder zur kundenspezifischen Anpassung durchführen. Für das Installationspaket für Rescue and Recovery/Client Security Solution werden bei der administrativen Installation die Quellendateien für die Installation an eine angegebene Position entpackt. Um eine administrative Installation auszuführen, muss das Installationspaket über die Befehlszeile mit Hilfe des Parameters /a ausgeführt werden:

```
Setup.exe /a
```

Beim Starten einer administrativen Installation wird eine Reihe von Dialogfenstern angezeigt, in denen der Administrator dazu aufgefordert wird, die Position anzugeben, an der die Konfigurationsdateien entpackt werden sollen. Die Standardposition zum Entpacken, die dem Administrator angezeigt wird, ist C:\. Es kann eine neue Position ausgewählt werden, zu der auch andere Laufwerke als C: gehören können (z. B. andere lokale Laufwerke oder zugeordnete Netzlaufwerke). Bei diesem Schritt können auch neue Verzeichnisse erstellt werden.

Wenn eine administrative Installation unbeaufsichtigt ausgeführt wird, kann das öffentliche Merkmal TARGETDIR in der Befehlszeile festgelegt werden, um die Position zum Entpacken anzugeben:

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

Wenn eine administrative Installation abgeschlossen ist, kann der Administrator die Quellendateien anpassen, indem er beispielsweise weitere Einstellungen zu tvt.txt hinzufügt. Zum Starten der Installation aus den extrahierten Quellendateien muss der Benutzer nach Abschluss der Anpassungen die Datei msiexec.exe über eine Befehlszeile öffnen und dabei den Namen der extrahierten msi-Datei angeben. Der folgende Abschnitt enthält eine Beschreibung der verfügbaren Befehlszeilenparameter, die in Verbindung mit msiexec verwendet werden können, sowie ein Anwendungsbeispiel. Öffentliche Merkmale können auch direkt in der Befehlszeilenaufforderung von msiexec festgelegt werden.

Befehlszeilenparameter von MsiExec.exe

Bei MsiExec.exe handelt es sich um ein ausführbares Programm des Windows-Installationsprogramms, das zur Interpretation von Installationspaketen und zur Installation von Produkten auf den Zielsystemen verwendet wird:

```
msiexec. /i "C:Windows-Ordner/Profiles\Benutzername\Persona\MySetups\Projektname
  \Produktkonfiguration\Name_des_Releases\DiskImages\Disk1\Produktname.msi
```

Die folgende Tabelle enthält eine genaue Beschreibung der Befehlszeilenparameter von MsiExec.exe. Diese Tabelle wurde der Dokumentation zu Microsoft Platform SDK im Windows-Installationsprogramm direkt entnommen.

Tabelle 26.

Parameter	Beschreibung
/i *Paket* oder *Produktcode*	Verwenden Sie das folgende Format, um das Produkt "Othello" zu installieren: `msiexec /i "C:\Windows-Ordner\Profiles\Benutzername\ Personal\MySetups\Othello\Trial Version\Release \DiskImages\Disk1\Othello Beta.msi"` Der Produktcode bezieht sich auf die GUID, die automatisch in den Merkmalen des Produktcodes in der Ansicht Ihres Produkts generiert wird.
f [p|o|e|d|c|a|u|m|s|v] *Paket* oder *Produktcode*	Durch die Installation mit dem Parameter /f werden fehlende oder beschädigte Dateien repariert oder erneut installiert. Verwenden Sie beispielsweise die folgende Syntax, um zu erzwingen, dass alle Dateien erneut installiert werden: `msiexec /fa "C:\Windows-Ordner\Profiles\Benutzername\ Personal\MySetups\Othello\Trial Version\Release \DiskImages\Disk1\Othello Beta.msi"` zusammen mit folgenden Flags: • p installiert eine Datei erneut, wenn diese fehlt • o installiert eine Datei erneut, wenn diese fehlt oder in einer älteren Version auf dem System des Benutzers vorhanden ist • e installiert eine Datei erneut, wenn diese fehlt oder eine entsprechende oder eine ältere Version dieser Datei auf dem System des Benutzers vorhanden ist • c installiert eine Datei erneut, wenn diese fehlt oder wenn die gespeicherte Kontrollsumme der installierten Datei nicht mit dem Wert der neuen Datei übereinstimmt. • a erzwingt das erneute Installieren aller Dateien • u oder m schreiben alle erforderlichen Einträge in der Benutzer-Registrierungsdatenbank erneut • s überschreibt alle vorhandenen Verknüpfungen • v führt die Anwendung von der Quelle aus und stellt die lokale Installation erneut in den Zwischenspeicher
/a *Paket*	Mit Hilfe des Parameters /a können Administratoren ein Produkt im Netzwerk installieren.
/x *Paket* oder *Produktcode*	Durch den Parameter /x wird ein Produkt deinstalliert.

Tabelle 26. (Forts.)

Parameter	Beschreibung
/L [i|w|e|a|r|u|c|m|p|v|+] *Protokolldatei*	Mit dem Parameter /L wird der Pfad für die Protokolldatei angegeben. Die Flags geben an, welche Informationen in der Protokolldatei aufgezeichnet werden sollen: • i protokolliert Statusnachrichten • w protokolliert nicht schwerwiegende Warnungen • e protokolliert alle Fehlernachrichten • a protokolliert die Fortführung von Aktionsfolgen • r protokolliert aktionsspezifische Datensätze • u protokolliert Benutzeranfragen • c protokolliert Schnittstellenparameter von Erstbenutzern • m protokolliert Nachrichten zu fehlender Speicherkapazität • p protokolliert Terminaleinstellungen • v protokolliert die Einstellung für ausführliche Ausgabe • + hängt die Informationen an eine vorhandene Datei an • * dient als Platzhalterzeichen, mit dem Sie alle Informationen protokollieren können (außer der Einstellung für ausführliche Ausgabe)
/q [n|b|r|f]	Der Parameter /q wird verwendet, um die Ebene der Benutzerschnittstelle zusammen mit den folgenden Flags festzulegen: • q oder qn erstellt keine Benutzerschnittstelle • qb erstellt eine Basisbenutzerschnittstelle Die folgenden Einstellungen für die Benutzerschnittstelle bewirken die Anzeige eines Modaldialogfensters am Ende der Installation: • qr zeigt eine verkleinerte Benutzerschnittstelle an • qf zeigt eine vollständige Benutzerschnittstelle an • qn+ zeigt keine Benutzerschnittstelle an • qb+ zeigt eine Basisbenutzerschnittstelle an
/? oder /h	Mit beiden Befehlen wird der Copyrightvermerk des Windows-Installationsprogramms angezeigt.
TRANSFORMS	Mit dem Befehlszeilenparameter TRANSFORMS können Sie alle Umsetzungen angeben, die für das Basispaket ausgeführt werden sollen. Dabei kann der TRANSFORMS-Aufruf über die Befehlszeile z. B. wie folgt verwendet werden: `msiexec /i "C:\`*`Windows-Ordner`*`\Profiles\`*`Benutzername`*`\ Personal\MySetups\`*`Projektname`*`\Trial Version \My Release-1\DiskImages\Disk1\ProduktName.msi" TRANSFORMS="New Transform 1.mst"` Mehrere Umsetzungen können durch Semikolons voneinander getrennt werden. Aus diesem Grund sollten Sie keine Semikolons in den Namen der Umsetzungen verwenden, da das Windows-Installationsprogramm diese Zeichen nicht korrekt interpretieren kann.

Tabelle 26. (Forts.)

Parameter	Beschreibung
Merkmale	Alle öffentlichen Merkmale können über die Befehlszeile festgelegt oder geändert werden. Die öffentlichen Merkmale unterscheiden sich von den privaten Merkmalen durch die ausschließliche Verwendung von Großbuchstaben. Beispiel: FIRMENNAME ist ein öffentliches Merkmal. Um ein Merkmal über die Befehlszeile festzulegen, verwenden Sie die folgende Syntax: MERKMAL=WERT. Angenommen, Sie möchten den Wert für FIRMENNAME ändern, würden Sie Folgendes eingeben: `msiexec /i "C:\Windows-Ordner\Profiles\Benutzername \Personal\MySetups\Projektname\Trial Version\My Release-1\DiskImages\Disk1\ProduktName.msi" FIRMENNAME="InstallShield"`

Öffentliche Standardmerkmale des Windows-Installationsprogramms

Das Windows-Installationsprogramm verfügt über eine Reihe von standardmäßig integrierten Merkmalen, die über die Befehlszeile festgelegt werden können, um ein bestimmtes Verhalten bei der Installation anzugeben. Die üblichsten öffentlichen Merkmale, die in der Befehlszeile verwendet werden, sind nachfolgend beschrieben. Weitere Dokumentation ist auf der Microsoft'-Website unter der Adresse http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/about_properties.asp verfügbar.

Tabelle 27 zeigt die im Allgemeinen verwendeten Merkmale des Windows-Installationsprogramms:

Tabelle 27.

Merkmal	Beschreibung
TARGETDIR	Gibt das Stammzielverzeichnis für die Installation an. Bei einer administrativen Installation gibt dieses Merkmal die Position an, an die das Installationspaket kopiert wird.
ARPAUTHORIZEDCDFPREFIX	Der URL des Aktualisierungskanals der Anwendung.
ARPCOMMENTS	Stellt Kommentare zum Hinzufügen oder Entfernen von Programmen in der Systemsteuerung bereit.
ARPCONTACT	Stellt den Kontakt zum Hinzufügen oder Entfernen von Programmen in der Systemsteuerung her.
ARPINSTALLLOCATION	Der vollständig qualifizierte Pfad zum Primärordner der Anwendung.
ARPNOMODIFY	Inaktiviert die Funktionalität, durch die das Produkt geändert werden könnte.
ARPNOREMOVE	Inaktiviert die Funktionalität, durch die das Produkt entfernt werden könnte.
ARPNOREPAIR	Inaktiviert die Schaltfläche zum Reparieren im Programmassistenten.

Tabelle 27. (Forts.)

Merkmal	Beschreibung
ARPPRODUCTICON	Gibt das primäre Symbol für das Installationspaket an.
ARPREADME	Stellt eine Readme-Datei zum Hinzufügen oder Entfernen von Programmen in der Systemsteuerung bereit.
ARPSIZE	Die geschätzte Größe der Anwendung in Kilobytes.
ARPSYSTEMCOMPONENT	Verhindert das Anzeigen von Anwendungen in der Liste zum Hinzufügen und Entfernen von Programmen.
ARPURLINFOABOUT	URL der Homepage einer Anwendung.
ARPURLUPDATEINFO	URL für Informationen zur Anwendungsaktualisierung.
REBOOT	Das Merkmal REBOOT unterdrückt bestimmte Aufforderungen für einen Neustart des Systems. Ein Administrator verwendet dieses Merkmal normalerweise bei einer Reihe von gleichzeitigen Installationen verschiedener Produkte, bei denen am Ende nur ein Neustart durchgeführt wird. Legen Sie REBOOT="R" fest, um alle Neustarts am Ende der einzelnen Installationen zu inaktivieren.
INSTALLDIR	Dieses Merkmal enthält den Standardzielordner für die Dateien zu Ihren Produktmerkmalen und Komponenten.

Angepasste öffentliche Merkmale von Client Security Software

Das Installationspaket für das Programm "Client Security Software" verfügt über eine Reihe von angepassten öffentlichen Merkmalen, die bei der Ausführung der Installation über die Befehlszeile festgelegt werden können. Die folgenden angepassten öffentlichen Merkmale sind verfügbar:

Tabelle 28.

Merkmal	Beschreibung
EMULATIONMODE	Gibt an, dass die Installation im Emulationsmodus erzwungen wird, auch wenn bereits ein TPM vorhanden ist. Geben Sie in der Befehlszeile EMULATIONMODE=1 ein, um die Installation im Emulationsmodus vorzunehmen.
HALTIFTPMDISABLED	Wenn sich das TPM im inaktivierten Status befindet und die Installation im Befehlszeilenmodus ausgeführt wird, lautet die Standardeinstellung für die Installation, dass sie im Emulationsmodus fortgesetzt wird. Verwenden Sie das Merkmal HALTIFTPMDISABLED=1, wenn die Installation im Befehlszeilenmodus ausgeführt wird, um die Installation anzuhalten, wenn das TPM inaktiviert ist.

Tabelle 28. (Forts.)

Merkmal	Beschreibung
ENABLETPM	Legen Sie ENABLETPM=0 in der Befehlszeile fest, um zu verhindern, dass das TPM durch die Installation aktiviert wird.
NOPRVDISK	Legen Sie in der Befehlszeile NOPRVDISK=1 fest, um zu verhindern, dass die Funktion ″SafeGuard PrivateDisk″ installiert wird. Diese Einstellung soll insbesondere bei unbeaufsichtigten Installationen verwendet werden, kann aber auch bei Installationen über die Benutzerschnittstelle verwendet werden. Bei der Installation über die Benutzerschnittstelle wird die Funktion ″SafeGuard PrivateDisk″ nicht im Fenster für die angepasste Installation angezeigt.
NOPWMANAGER	Legen Sie in der Befehlszeile NOPWMANAGER=1 fest, um zu verhindern, dass die Funktion ″Password Manager″ installiert wird. Diese Einstellung soll insbesondere bei unbeaufsichtigten Installationen verwendet werden, kann aber auch bei Installationen über die Benutzerschnittstelle verwendet werden. Bei der Installation über die Benutzerschnittstelle wird die Funktion ″Password Manager″ nicht im Fenster für die angepasste Installation angezeigt.
NOCSSWIZARD	Legen Sie in der Befehlszeile NOCSSWIZARD=1 fest, um zu verhindern, dass der CSS-Assistent angezeigt wird, wenn sich ein Administrator anmeldet, der nicht registriert ist. Dieses Merkmal ist dafür gedacht, wenn CSS installiert werden soll, das System jedoch erst später mit Hilfe von Scripts konfiguriert werden soll.
CSS_CONFIG_SCRIPT	Legen Sie CSS_CONFIG_SCRIPT=″*Dateiname*″ oder ″*Dateiname_Kennwort*″ fest, um eine Konfigurationsdatei zu erhalten, die ausgeführt wird, nachdem ein Benutzer die Installation abgeschlossen und einen Neustart durchgeführt hat.
SUPERVISORPW	Legen Sie in der Befehlszeile SUPERVISORPW=″*Kennwort*″ fest, um ein Administratorkennwort bereitzustellen, um den Chip für die Installation im Befehlszeilenmodus oder in einem anderen Modus zu aktivieren. Wenn der Chip inaktiviert ist und die Installation im Befehlszeilenmodus ausgeführt wird, muss das richtige Administratorkennwort eingegeben werden, um den Chip zu aktivieren. Andernfalls wird der Chip nicht aktiviert.

Installationsprotokolldatei

Im Verzeichnis %temp% wird eine Protokolldatei mit dem Namen cssinstall60.log erstellt, wenn die Installation über die Datei ″setup.exe″ gestartet wird (durch Doppelklicken auf die Datei für die Hauptinstallation (mit der Erweiterung .exe), durch Ausführen der ausführbaren Datei für die Hauptinstallation ohne Parameter oder durch Extrahieren von msi und Ausführen der Datei ″setup.exe″). Diese Datei enthält Protokollnachrichten, die zum Beheben von Installationsfehlern verwendet werden können. Diese Protokolldatei wird nicht erstellt, wenn die Installation direkt über das msi-Paket ausgeführt wird. Dazu gehören auch die Aktionen, die über die die Option zum Hinzufügen und Entfernen von Programmen (″Software″) ausgeführt werden. Um eine Protokolldatei für alle MSI-Aktionen zu erstellen, können Sie die Richtlinie für die Protokollierung in der Registrierungsdatenbank aktivieren. Erstellen Sie hierfür den folgenden Wert:

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

Installationsbeispiele

In der folgenden Tabelle sind Beispiele für die Verwendung der Datei ″setup.exe″ dargestellt:

Tabelle 29.

Beschreibung	Beispiel
Unbeaufsichtigte Installation ohne Neustart	`setup.exe /s /v"/qn REBOOT="R""`
Administrative Installation	`setup.exe /a`
Unbeaufsichtigte administrative Installation, bei der die Position zum Entpacken angegeben wird	`setup.exe /a /s /v"/qn TARGETDIR="F:\CSS60""`
Unbeaufsichtigte Deinstallation setup.exe /s /x /v/qn	`setup.exe /s /x /v/qn`
Installation ohne Neustart mit Erstellung eines Installationsprotokolls im temporären Verzeichnis	`setup.exe /v"REBOOT="R" /L*v %temp%\cssinstall60.log"`
Installation ohne Predesktop-setup.exe /vPDA=0	`setup.exe /vPDA=0`

In der folgenden Tabelle sind Beispiele für die Installation mit Hilfe von Client Security Solution.msi dargestellt:

Tabelle 30.

Beschreibung	Beispiel
Installation	`msiexec /i "C:\CSS60\Client Security Solution.msi"`
Unbeaufsichtigte Installation ohne Neustart	`msiexec /i "C:\CSS60\Client Security Solution.msi" /qn REBOOT="R"`
Unbeaufsichtigte Deinstallation	`msiexec /x "C:\CSS60\Client Security Solution.msi" /qn`

Installation über System Migration Assistant

Das Installationsverfahren über den System Migration Assistant ist im *System Migration Assistant User's Guide* beschrieben.

Fingerprint Software installieren

Die Datei "setup.exe" für das Programm mit der Fingerprint Software kann mit Hilfe der folgenden Parameter gestartet werden:

Unbeaufsichtigte Installation

Eine unbeaufsichtigte Installation der Fingerprint Software ist ebenfalls möglich. Führen Sie die Setup.exe im Installationsverzeichnis über das CD-ROM-Laufwerk aus.

Verwenden Sie die folgende Syntax:

```
Setup.exe MERKMAL=WERT /q /i
```

wobei *q* für die unbeaufsichtigte Installation und *i* für die Installation steht. Beispiel:

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

Verwenden Sie zum Deinstallieren der Software den Parameter /x:

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

SMS-Installation

SMS-Installationen werden ebenfalls unterstützt. Rufen Sie die SMS-Administratorkonsole auf, erstellen Sie ein neues Paket, und legen Sie die Merkmale des Pakets in der herkömmlichen Weise fest. Öffnen Sie das Paket, und wählen Sie im Programm die Option für neue Programme aus. Geben Sie in einer Befehlszeile Folgendes ein:

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

Sie können dieselben Parameter wie bei der unbeaufsichtigten Installation verwenden.

Bei der Konfiguration wird in der Regel am Ende des Installationsprozesses ein Neustart durchgeführt. Wenn Sie alle Neustarts während der Installation unterdrücken möchten und den Neustart später durchführen möchten (nach der Installation weiterer Programme), fügen Sie REBOOT="ReallySuppress" zur Liste mit den Merkmalen hinzu.

Parameter

Die folgenden Parameter werden von der Fingerprint Software unterstützt:

Tabelle 31.

Parameter	Beschreibung
CTRLONCE	Wird dazu verwendet, um das Control Center (Steuerzentrale) nur ein Mal anzuzeigen. Der Standardwert ist 0.
CTLCNTR	Wird dazu verwendet, dass das Control Center (Steuerzentrale) beim Systemstart ausgeführt wird. Der Standardwert ist 1.
DEFFUS	• 0 = Einstellungen für schnelles Wechseln zwischen Benutzern (FUS, Fast User Switching) werden nicht verwendet • 1 = Einstellungen für FUS werden verwendet Der Standardwert ist 0.
INSTALLDIR	Das Standardinstallationsverzeichnis der Fingerprint Software.
OEM	• 0 = Unterstützung für Serverberechtigungsnachweise /Serverauthentifizierung • 1 = Nur Modus für Standalone-Computer mit lokalen Berechtigungsnachweisen
PASSPORT	Der bei der Installation festgelegte Standardtyp für Berechtigungsnachweise. • 1 = Standardeinstellung - Lokaler Berechtigungsnachweis • 2 = Serverberechtigungsnachweis Der Standardwert ist 1.
SECURITY	• 1 - = Unterstützung bei der Installation für den sicheren Modus • 0 = Nicht installieren; nur komfortabler Modus vorhanden
SHORTCUTFOLDER	Standardname für den verknüpften Ordner im Startmenü
REBOOT	Kann zum Unterdrücken aller Neustarts einschließlich der Aufforderungen während der Installation verwendet werden, indem ReallySuppress festgelegt wird.

Szenarios für installierte Software

Tabelle 32.

Installierte Software	Bemerkungen
Client Security Software Version 5.4x	Dies ist die einzige Version von CSS, die zusammen mit Rescue and Recovery verwendet werden kann.
Nur Rescue and Recovery Version 3.0	• Installation über die vollständige Produktinstallation mit abgewähltem CSS. • Einige Kernkomponenten von Client Security Solution werden nur bei der RnR--Installation installiert, um die Verschlüsselung von Sicherungen mit dem TPM und die Konfiguration des PDA-Hauptkennworts zu unterstützen.
Client Security Solution Version 6.0 Standalone	• Hierbei handelt es sich um ein separates Installationspaket. • Sie können nicht das vollständige Produkt installieren und Rescue and Recovery abwählen, um nur Client Security Solution zu installieren • Die CSS-Komponenten (Private Disk und Password Manager) sind optional.
Rescue and Recovery Version 3.0 und Client Security Solution Version 6.0	• Vorinstallation Standard - Installation über normale Produktinstallation • CSS-Komponenten • Private Disk und Password Manager sind optionale Komponenten

Änderung des Softwarestatus

Tabelle 33.

Ist die installierte Software ...	Und Sie möchten wechseln zu ...	Gehen Sie wie folgt vor ...	Bemerkungen	Build
Client Security Software Version 5.4x	Client Security Software 5.4x und Rescue and Recovery Version 3.0	• Installieren Sie das Produkt. • Es wird nur die Rescue and Recovery-Komponente installiert (es wird keine benutzerdefinierte Konfiguration angezeigt). • Geben Sie bei entsprechender Aufforderung an, dass die Client Security Software installiert bleiben soll.	• Client Security Software-Anbindungspunkte für Rescue and Recovery werden mit Hilfe des Emulationsmodus implementiert • In diesem Modus ist nur das Hauptkennwort über Client Security Software verfügbar	011
Client Security Software	Client Security Solution 6.0	• Deinstallieren Sie Client Security Software 5.4x • Installieren Sie Client Security Solution 6.0 Standalone	Es ist nicht zulässig, Client Security Solution Version 6.0 über Client Security Software Version 5.4x zu installieren. Der Benutzer wird dazu aufgefordert, zunächst die alte Version von Client Security Software zu entfernen.	011
Client Security Software	Rescue and Recovery Version 3.0 und Client Security Solution Version 6.0	• Deinstallieren Sie Client Security Software 5.4x • Installieren Sie das Produkt.	Bei dem Versuch, das Produkt über Client Security Software Version 5.4x zu installieren, wird eine Aufforderung angezeigt, dass zunächst die Client Security Software Version 5.4x entfernt werden muss. Wenn die Installation ohne die Deinstallation fortgesetzt wird, wird nur Rescue and Recovery installiert.	011

Tabelle 34.

Ist die installierte Software ...	Und Sie möchten wechseln zu ...	Gehen Sie wie folgt vor ...	Bemerkungen	Build
Rescue and Recovery Version 3.0	Client Security Software 5.4x und Rescue and Recovery Version 3.0	• Deinstallieren Sie Rescue and Recovery • Installieren Sie Client Security Software Version 5.4x • Installieren Sie das Produkt wie oben beschrieben.	• Client Security Software Version 5.4x kann nicht über eine andere Produktinstallation installiert werden. • Bei der Deinstallation von Rescue and Recovery Version 3.0 werden lokale Sicherungen gelöscht.	011

Tabelle 34. (Forts.)

Ist die installierte Software ...	Und Sie möchten wechseln zu ...	Gehen Sie wie folgt vor ...	Bemerkungen	Build
Rescue and Recovery Version 3.0	Client Security Solution 6.0	• Deinstallieren Sie Rescue and Recovery Version 3.0 • Installieren Sie Client Security Solution Version 6.0 Standalone	• Bei der Deinstallation von Rescue and Recovery Version 3.0 werden Benutzerdateien und Einstellungen der CSS-Registrierungsdatenbank gelöscht. • Sicherungen von Rescue and Recovery Version 3.0, die mit CSS geschützt sind, sind nicht länger zugänglich. • Bei der Deinstallation von Rescue and Recovery Version 3.0 werden lokale Sicherungen gelöscht. • Die Installation von Client Security Software Version 6.0 Standalone kann nicht über andere Produktinstallationen durchgeführt werden. • In diesem Fall kann Client Security Solution über die Option 'Ändern' unter "Software" nur hinzugefügt werden. Rescue and Recovery kann über die Option 'Ändern' nicht entfernt werden.	012
Rescue and Recovery Version 3.0	Rescue and Recovery Version 3.0 und Client Security Solution Version 6.0	• Wählen Sie unter "Software" die Option 'Ändern' aus. • Fügen Sie CSS und alle weiteren Komponenten hinzu.	• Lokale Sicherungen werden gelöscht, wenn CSS hinzugefügt wird. • Die Benutzer erhalten während des Hinzufügens von Client Security Solution eine Warnmeldung, dass nach diesem Vorgang neue Sicherungen vorgenommen werden müssen. • Client Security Solution-Einstellungen und Datendateien werden beim Hinzufügen von Client Security Solution gelöscht. • Die Installation von Client Security Solution Version 6.0 Standalone kann nicht über andere Produktinstallationen durchgeführt werden.	TBD

Tabelle 35.

Ist die installierte Software ...	**Und Sie möchten wechseln zu ...**	**Gehen Sie wie folgt vor ...**	**Bemerkungen**	**Build**
Client Security Solution Version 6.0 Standalone	Client Security Software 5.4x	• Deinstallieren Sie Client Security Solution Version 6.0. • Installieren Sie Client Security Software Version 5.4ix.	• Client Security Solution Version 5.4x kann nicht über eine andere Produktinstallation installiert werden. • Bei der Deinstallation von Client Security Solution Version 6.0 erfolgt eine Aufforderung zum Löschen von Datendateien und Einstellungen. Die hier ausgewählte Option hat keine Auswirkungen auf den Betrieb von Client Security Software Version 5.4x.	011
Client Security Solution Version 6.0 Standalone	Rescue and Recovery Version 3.0	• Deinstallieren Sie Client Security Solution Version 6.0 • Installieren Sie das Produkt, und wählen Sie nur Rescue and Recovery aus.	• Bei der Deinstallation von Client Security Solution Version 6.0 erfolgt eine Aufforderung zum Löschen der Benutzerdateien und Einstellungen der Client Security Solution-Version. • Bei der Installation von Rescue and Recovery 3.0 wird der Benutzer aufgefordert, alle vorhandenen Benutzerdateien und Einstellungen von Client Security Solution zu entfernen. Wenn der Benutzer nicht die Auswahl zum Entfernen der Dateien trifft, wird die Installation abgebrochen.	012

Tabelle 35. (Forts.)

Ist die installierte Software ...	Und Sie möchten wechseln zu ...	Gehen Sie wie folgt vor ...	Bemerkungen	Build
Client Security Solution Version 6.0 Standalone	Rescue and Recovery Version 3.0 und Client Security Solution Version 6.0	• Führen Sie die Produktinstallation aus. • Die Auswahl der Optionen zu Rescue and Recovery und Client Security Solution kann nicht aufgehoben werden. • Die zuvor installierten Client Security Solution-Komponenten (Password Manager und Private Disk) sind standardmäßig ausgewählt, können aber abgewählt werden. Komponenten, die zuvor nicht installiert wurden, werden standardmäßig abgewählt, können aber auch ausgewählt werden.	• Client Security Solution Version 6.0 Standalone wird im Hintergrund (unbeaufsichtigt) deinstalliert. • Die Datendateien und Einstellungen zu Client Security Solution Version 6.0 werden beibehalten. • Der Emulations-/Nicht-Emulationsstatus bleibt erhalten. • Der Assistent zu Client Security Solution wird nach Abschluss der Produktinstallation nicht ausgeführt, da Client Security Solution zuvor konfiguriert wurde. • Die Option zum Schützen von Rescue and Recovery-Sicherungen mit Hilfe von Client Security Solution muss über die Rescue and Recovery-GUI ausgeführt werden. In der letzten Installationsanzeige steht eine Option zur Verfügung, mit der die Rescue and Recovery-GUI nach dem Neustart ausgeführt werden kann. • Nach der Installation des Produkts stehen unter ″Software″ die Optionen ‘Entfernen’, ‘Reparieren’ und ‘Ändern’ zur Verfügung. • Die installierte Version von Client Security Solution Version 6.0 muss gleich oder kleiner sein als die Version des gerade installierten Produkts, da dem Benutzer anderenfalls eine Nachricht angezeigt wird, dass das Produkt nicht installiert werden kann.	012

Anmerkungen:

1. Wenn der Benutzer Rescue and Recovery 3.0 unbeaufsichtigt installiert, werden die Benutzerdateien und Einstellungen von Client Security Solution während der Installation automatisch gelöscht.
2. Bei diesem Szenario wird durch Aus- oder Abwählen von Password Manager und Private Disk bei der Installation des Produkts (Rescue and Recovery 3.0 und Client Security Solution 6.0) der Endstatus der Komponente nach der Installation des Produkts festgelegt. Wenn z. B. Password Manager mit Client Security Solution 6.0 installiert wurde und der Benutzer Password Manager während der Produktinstallation abwählt, ist dieser nicht mehr installiert, wenn die Installation abgeschlossen ist. Wenn die Installation des Produkts (Rescue and Recovery und Client Security Solution) unbeaufsichtigt durchgeführt wird, werden sowohl Password Manager als auch Private Disk installiert, es sei denn, die entsprechenden Merkmale NOPRVDISK=1 oder NOPWMANAGER=1 sind im Installationsbefehl festgelegt.

Tabelle 36.

Ist die installierte Software ...	**Und Sie möchten wechseln zu ...**	**Gehen Sie wie folgt vor ...**	**Bemerkungen**	**Build**
Rescue and Recovery Version 3.0 und Client Security Solution Version 6.0	Client Security Software 5.4x	• Deinstallieren Sie das Produkt. • Installieren Sie Client Security Solution Version 5.4x.	• Client Security Software Version 5.4x kann nicht über eine andere Produktinstallation installiert werden. • Bei der Deinstallation des Produkts erfolgt eine Aufforderung zum Löschen von Datendateien und Einstellungen. Die hier ausgewählte Option hat keine Auswirkungen auf den Betrieb von Client Security Software Version 5.4x.	011

Tabelle 36. (Forts.)

Ist die installierte Software ...	Und Sie möchten wechseln zu ...	Gehen Sie wie folgt vor ...	Bemerkungen	Build
Rescue and Recovery Version 3.0 und Client Security Solution Version 6.0	Rescue and Recovery Version 3.0	• Wählen Sie unter ″Software″ die Option ‘Ändern’ aus. • Entfernen Sie Client Security Solution.	• Lokale Sicherungen werden gelöscht, wenn Client Security Solution entfernt wird. • Bei der Deinstallation von Client Security Solution erfolgt eine Warnung, dass PrivateDisk und Password Manager verloren gehen können. • Sicherungen von Rescue and Recovery Version 3.0, die mit Client Security Solution geschützt sind, sind nicht länger zugänglich. • Die Einstellungen und Datendateien von Client Security Solution werden gelöscht, wenn Client Security Solution unter ‘Ändern’ entfernt wird.	TBD nicht in Build 12 enthalten
Rescue and Recovery Version 3.0 und Client Security Solution Version 6.0	Client Security Solution Version 6.0	• Deinstallieren Sie das Produkt. • Bei der Deinstallation erfolgt eine Aufforderung zum Löschen der Dateien und Einstellungen von Client Security Solution. Die Dateien und Einstellungen können beibehalten werden, wenn der Benutzer weiterhin die vorhandene Client Security Solution-Konfiguration verwenden möchte. • Installieren Sie Client Security Solution Version 6.0 Standalone	• Deinstallieren Sie das Produkt. • Bei der Deinstallation erfolgt eine Aufforderung zum Löschen der Dateien und Einstellungen von Client Security Solution. Die Dateien und Einstellungen können beibehalten werden, wenn der Benutzer weiterhin die vorhandene Client Security Solution-Konfiguration verwenden möchte. • Installieren Sie Client Security Solution Version 6.0 Standalone	012

Anmerkungen:

1. Bei einer Deinstallation von Client Security Solution 6.0 über ″Software″ oder über eine Benutzerschnittstelle von der ursprünglichen Quelle aus wird der Benutzer dazu aufgefordert, die Datendateien und Einstellungen von CSS zu löschen. Wenn die Deinstallation über die Befehlszeile unbeaufsichtigt ausgeführt wird, werden standardmäßig die Einstellungen und Datendateien von CSS gelöscht. Dieser Vorgang kann jedoch auch umgangen werden, wenn das Merkmal NOCSSCLEANUP=1 im Befehl zum Deinstallieren festgelegt wird.
2. Bei einer Deinstallation des Produkts (Rescue and Recovery und Client Security Solution 6.0) über ″Software″ oder über eine Benutzerschnittstelle von der ursprünglichen Quelle aus, wird der Benutzer dazu aufgefordert, die Datendateien und Einstellungen von Client Security Solution zu löschen. Wenn die Deinstallation über die Befehlszeile unbeaufsichtigt ausgeführt wird, werden standardmäßig die Einstellungen und Datendateien von Client Security Solution gelöscht. Dieser Vorgang kann jedoch auch umgangen werden, wenn das Merkmal NOCSSCLEANUP=1 im Befehl zum Deinstallieren festgelegt wird.

Kapitel 7. Antidote Delivery Manager-Infrastruktur

Der Antidote Delivery Manager stellt Anweisungen eines Administrators an die einzelnen Systeme bereit und unterstützt Befehle zur Bekämpfung von Viren oder Würmern. Der Administrator erstellt ein Script mit den erforderlichen Aktionen für die einzelnen Systeme. Über die Repository-Funktion wird das Script dem System sicher innerhalb weniger Minuten zugestellt, und die Befehle werden über diese Funktion ebenfalls ausgeführt. Zur Funktionalität der Befehle gehören die Einschränkung von Netzverbindungen, die Anzeige von Nachrichten für Endbenutzer, die Wiederherstellung von Dateien aus Sicherungskopien, das Herunterladen von Dateien, die Ausführung sonstiger Systembefehle und der Neustart des Systems mit demselben Betriebssystem oder mit einem Wechsel in die Umgebung von Rescue and Recovery. Sowohl die Repository-Funktion als auch die Befehle funktionieren entweder unter dem normalen Betriebssystem (wie z. B. Windows XP) oder auch in der Umgebung von Rescue and Recovery.

Die Gesamtstrategie zur Bekämpfung eines Virus besteht in der Verringerung seiner Verbreitung und des vom zerstörerischen Programmcode verursachten Schadens, in der Anwendung von Programmkorrekturen und der Bereinigung auf den einzelnen Systemen sowie im anschließenden Verfügbarmachen der wiederhergestellten Systeme im Netzwerk. Bei Viren, die sehr zerstörerisch sind und sich schnell verbreiten, kann es erforderlich sein, Systeme aus dem Netzwerk zu entfernen und alle Reparaturoperationen in der Umgebung von Rescue and Recovery auszuführen. Obwohl dies die sicherste Methode ist, wird dadurch während der regulären Arbeitszeit die Arbeit der Endbenutzer unterbrochen. In einigen Situationen kann der Wechsel in die Umgebung von Rescue and Recovery verzögert oder vermieden werden, indem die Funktionen des Netzwerks eingeschränkt werden. Im nächsten Schritt werden Programmkorrekturen und Bereinigungscode heruntergeladen, der Bereinigungscode wird ausgeführt, und für die Installation werden die Programmkorrekturen eingerichtet. Im Allgemeinen sind Programmkorrekturen so konzipiert, dass sie bei aktivem Betriebssystem installiert werden. Für die Bereinigung und für andere Operationen ist jedoch möglicherweise die Umgebung von Rescue and Recovery besser geeignet. Wenn die Fehlerberichtigungen abgeschlossen sind, kann der normale Systembetrieb unter Windows XP mit der wiederhergestellten Netzkonfiguration wieder aufgenommen werden.

In den nächsten zwei Abschnitten werden die Funktionsweise des Repository und die Befehle detailliert beschrieben. Anschließend wird die Installation und Konfiguration der Funktion behandelt. Die folgenden Abschnitte enthalten Beispiele für die Verwendung des Systems für allgemeine Tasks wie das Testen, die Reaktion auf zerstörerische Viren, Systeme, die drahtlos oder über virtuelle private Netze (VPNs - Virtual Private Networks) verbunden sind, und die Behebung von weniger zerstörerischen Fehlern.

Repository

Die Repository-Funktion wird auf den einzelnen Systemen ausgeführt. Sie prüft in regelmäßigen Abständen, ob neue Nachrichten vom Administrator vorliegen. Sie prüft in einem geplanten Intervall oder bei Auftreten einiger besonderer Ereignisse (z. B. Booten, Fortsetzung nach dem Aussetzen des Betriebs oder Rückkehr aus dem Hibernationsmodus, Erkennung neuer Netzwerkadapter und Zuordnung einer neuen IP-Adresse). Die Repository-Funktion sucht in einer Reihe von Verzeichnissen, in einem freigegebenen Windows-Verzeichnis, wie z. B.

\\machine\share\directory, in HTTP-URLs und in FTP-URLs nach Nachrichten. Wenn mehrere Nachrichten gefunden werden, verarbeitet sie diese in der Reihenfolge, wie sie im Verzeichnis nach “Name” sortiert sind. Es wird immer nur eine Nachricht zur gleichen Zeit verarbeitet. Eine Nachricht wird zudem nur ein einziges Mal verarbeitet. Wenn die Verarbeitung einer Nachricht fehlschlägt, wird standardmäßig kein neuer Versuch unternommen. Ein erneuter Versuch kann jedoch in der Nachricht selbst angegeben werden.

Eine Nachricht muss von einem Administrator gepackt werden, bevor sie zur Verarbeitung durch die Repository-Funktion in ein Verzeichnis gestellt wird. Zur Erstellung des Pakets stellt der Administrator alle Dateien, aus denen die Nachricht besteht, in ein Verzeichnis (oder in zugehörige Unterverzeichnisse). Eine dieser Dateien muss den Namen “GO.RRS” haben. Dies ist das Primärbefehlsscript. Der Administrator kann für diese Nachricht optional einen Signaturschlüssel verwenden, dann muss jedoch der Schlüssel für alle Zielsysteme verfügbar sein. Die Repository-Funktion prüft das Paket auf Integrität, prüft ggf. die Signatur und entpackt alle Dateien in ein lokales Verzeichnis, bevor die Funktion die Datei GO.RRS ausführt.

Die Datei mit dem Primärbefehlsscript (GO.RRS) entspricht der Syntax einer Windows-Befehlsdatei. Sie darf zulässige Windows-Befehle und alle Befehle enthalten, die im folgenden Abschnitt aufgeführt sind. Darüber hinaus ist ein Python-Befehlsinterpreter als Teil der Umgebung von Rescue and Recovery installiert, so dass Sie vom Script GO.RRS aus auch Python-Scripts aufrufen können.

Nach der Ausführung des Scripts werden alle aus der Nachricht entpackten Dateien gelöscht. Daher müssen Sie, wenn Sie die Dateien nach Beenden des Scripts noch benötigen (z. B. bei der Installation einer Programmkorrektur nach einem Neustart), diese Dateien aus dem Nachrichtenverzeichnis verschieben.

Jedes System weist eine Konfiguration von zu überprüfenden Repositorys auf. Für den IT-Administrator kann es nützlich sein, die Systeme in Gruppen aufzuteilen und den einzelnen Gruppen unterschiedliche Repositorys (freigegebene Netzverzeichnisse) zuzuordnen. Die Systeme können z. B. nach räumlicher Nähe zum Dateiserver in Gruppen eingeteilt werden. Oder die Systeme können nach Funktionen eingeteilt werden, z. B. in ″Entwicklung″, ″Verkauf″ oder ″Technische Unterstützung″.

Antidote Delivery Manager-Befehle und verfügbare Windows-Befehle

Das Antidote Delivery Manager-System bietet verschiedene Befehle, um den Betrieb eines Systems zu vereinfachen. Zusätzlich zum Befehl zur Erstellung von Nachrichten und zur Anpassung von Einstellungen gibt es Befehle zur Steuerung des Netzwerks, zur Bestimmung und Steuerung des Betriebssystemstatus, zur Analyse von XML-Dateien aus Systembeständen und zur Benachrichtigung des Endbenutzers über den Fortschritt des Antidote Delivery Manager-Scripts auf dem Clientsystem. Der Befehl NETWK aktiviert bzw. inaktiviert den Netzbetrieb oder schränkt den Netzbetrieb auf eine Gruppe von Netzadressen ein. Mit dem Befehl INRR kann auch bestimmt werden, ob das Betriebssystem Windows XP aktiv ist oder ob der Computer mit der Umgebung von Rescue and Recovery ausgeführt wird. Mit dem Befehl REBOOT kann der Computer heruntergefahren werden, und es kann angegeben werden, dass er entweder mit Windows XP oder mit der Umgebung von Rescue and Recovery gestartet werden soll. Die Anwendung MSGBOX ermöglicht die Kommunikation mit dem Endbenutzer, indem eine Nachricht in einem Dialogfenster angezeigt wird. Dieses Nachrichtenfenster kann optional

die Schaltflächenn ″OK″ und ″Cancel″ enthalten, so dass die Nachricht in Abhängigkeit von der Eingabe des Endbenutzers unterschiedlich reagiert.

Bestimmte Microsoft-Befehle sind auch in Antidote Delivery Manager verfügbar. Zu den zulässigen Befehlen gehören alle in die Befehlsshell integrierten Befehle, z. B. die Befehle DIR und CD. Weitere nützliche Befehle wie REG.EXE, womit die Registrierungsdatenbank geändert werden kann, sowie CHKDSK.EXE zur Überprüfung der Integrität von Festplatten, sind ebenfalls verfügbar.

Typische Verwendung von Antidote Delivery Manager

Sie können das Antidote Delivery Manager-System für eine Vielzahl von Aufgaben einsetzen. Die folgenden Beispiele zeigen, wie Sie das System verwenden können.

- **Einfacher Systemtest - Benachrichtigung in der Anzeige**

  Die einfachste Verwendung des Systems besteht darin, dem Endbenutzer eine einzelne Nachricht anzuzeigen. Sie können diesen Test am einfachsten ausführen und auch andere Scripts vor der Implementierung testen, indem Sie die Nachricht in ein Repository stellen. Wählen Sie ein lokales Verzeichnis auf dem PC des Administrators als Repository aus. Diese Position ermöglicht das schnelle Testen des Scripts, ohne dass es sich auf andere Computer auswirkt.

- **Script vorbereiten und packen**

  Schreiben Sie auf einem beliebigen System, auf dem Antidote Delivery Manager installiert ist, ein Script mit dem Namen GO.RRS. Fügen Sie darin die folgende Zeile ein: `MSGBOX /MSG "Hello World" /OK`. Führen Sie im Verzeichnis, das die Datei GO.RRS enthält, den Befehl APKGMSG aus, um eine Nachricht zu erstellen.

- **Script ausführen**

  Stellen Sie die Nachrichtendatei in eines der Repository-Verzeichnisse Ihres Systems, und überprüfen Sie die korrekte Ausführung. Wenn der Mailagent das nächste Mal ausgeführt wird, wird ein Nachrichtenfenster mit dem Text “Hello World” angezeigt. Ein solches Script ist auch eine gute Möglichkeit, Netzrepositorys zu überprüfen, wenn nach dem Aussetzen der Betrieb fortgesetzt wird.

Angriff eines gefährlichen Virus oder Wurms

Im folgenden Beispiel wird das mögliche Vorgehen bei der Bekämpfung eines gefährlichen Virus oder Wurms veranschaulicht. Das grundlegende Vorgehen besteht darin, den Netzbetrieb auszuschalten, anschließend mit Rescue and Recovery zu booten, Fixes abzurufen, Reparaturen durchzuführen und anschließend wieder mit Windows XP zu booten, die Programmkorrekturen zu installieren und den Netzbetrieb wiederherzustellen. Zur Ausführung aller genannten Funktionen kann durch den Einsatz von Flagdateien und durch die Verwendung des Befehls RETRYONERROR eine einzige Nachricht verwendet werden.

1. **Phase für das Herunterfahren**

   Zuerst müssen die Endbenutzer darüber informiert werden, was geschieht. Wenn der Angriff nicht sehr schwerwiegend ist, kann der Administrator dem Endbenutzer die Möglichkeit geben, die Korrektur auf einen späteren Zeitpunkt zu verschieben. Beim konservativsten Szenario wird in dieser Phase der Netzbetrieb inaktiviert, und die Endbenutzer erhalten ein kurzes Zeitfenster von z. B. 15 Minuten, um ihre aktuelle Arbeit zu speichern. Mit RETRYONERROR wird das Script weiterhin ausgeführt, und anschließend kann das System in der Umgebung von Rescue and Recovery erneut gestartet werden.

2. **Phase für die Codeverteilung und für die Reparatur**

   Sobald die Bedrohung durch ein infiziertes System durch Inaktivieren des Netzwerks und Neustart mit Rescue and Recovery abgewendet ist, kann zusätzlicher Code abgerufen werden und es können Reparaturen durchgeführt werden. Das Netzwerk kann aktiv bleiben, oder es können während der zum Abruf zusätzlicher Dateien erforderlichen Zeit nur bestimmte Adressen zugelassen werden. In der Umgebung von Rescue and Recovery können Virusdateien entfernt werden, und die Registrierungsdatenbank kann bereinigt werden. Leider ist die Installation von Programmkorrekturen und neuer Software nicht möglich, da die Programmkorrekturen voraussetzen, dass Windows XP ausgeführt wird. Während der Netzbetrieb weiterhin inaktiviert ist und der gesamte Virencode entfernt wird, ist es sicher, mit Windows XP erneut zu starten, um Reparaturen durchzuführen. Eine geschriebene Befehlsdatei verweist nun das Script nach dem Neustart auf den Abschnitt mit der Programmkorrektur.

3. **Phase für die Programmkorrektur und die Wiederherstellung**

   Wenn das System mit Windows XP erneut gestartet wird, beginnt Antidote Delivery Manager erneut mit der Verarbeitung, bevor sich der Endbenutzer anmelden kann. Programmkorrekturen sollten zu diesem Zeitpunkt installiert werden. Das System kann schließlich ein letztes Mal erneut gestartet werden, falls dies die neu installierten Programmkorrekturen erfordern. Sobald die gesamte Bereinigung und Installation von Korrekturen beendet ist, kann das Netzwerk aktiviert und der Endbenutzer über den normalen Betrieb informiert werden.

Nicht dringend erforderliche Aktualisierung einer Anwendung

Nicht jede Wartungsarbeit erfordert die oben beschriebenen drastischen Maßnahmen. Wenn eine Programmkorrektur verfügbar ist, jedoch derzeit kein Virenangriff stattfindet, kann eine einfachere Vorgehensweise angemessen sein.

Ein einzelnes Script kann den Betrieb unter Verwendung von RETRYONERROR und über Befehlsdateien steuern.

1. **Phase des Herunterladens**

   Der Prozess beginnt mit einem Nachrichtenfenster, in dem der Endbenutzer darüber informiert wird, dass eine Programmkorrektur zur späteren Installation heruntergeladen wird. Anschließend kann die Programmkorrektur vom Server kopiert werden.

2. **Phase für die Programmkorrektur**

   Nachdem der Patch-Code zur Installation bereitgestellt wurde, sollte der Endbenutzer gewarnt und mit der Installation begonnen werden. Wenn der Endbenutzer eine Verzögerung anfordert, kann diese unter Verwendung einer Befehlsdatei verfolgt werden. Spätere Anforderungen, die Programmkorrektur zu installieren, können in dringenderem Ton formuliert werden. Beachten Sie, dass Antidote Delivery Manager diesen Status selbst dann beibehält, wenn der Endbenutzer sein System ausschaltet oder erneut startet. Wenn der Endbenutzer über eine entsprechende Berechtigung verfügt, kann erforderlichenfalls die Programmkorrektur installiert und das System erneut gestartet werden.

VPNs und Sicherheit bei drahtlosen Verbindungen

Die Umgebung von Rescue and Recovery unterstützt derzeit weder den Fernzugriff über virtuelle private Netze (VPNs - Virtual Private Networks) noch drahtlose Netzverbindungen. Wenn ein Computer eine dieser Netzverbindungen unter Windows XP verwendet und anschließend mit Rescue and Recovery erneut startet, geht die Netzkonnektivität verloren. Daher funktioniert ein Script nicht, das dem oben beschriebenen Script ähnelt, da der Netzbetrieb zum Herunterladen von Dateien und Korrekturen in Rescue and Recovery nicht verfügbar ist.

Sie können jedoch alle erforderlichen Dateien in der ursprünglichen Nachricht zusammenpacken oder die erforderlichen Dateien vor dem Neustart herunterladen. Dazu stellen Sie alle erforderlichen Dateien in das Verzeichnis, in dem sich die Datei GO.RRS befindet. In der Scriptdatei muss berücksichtigt werden, dass die erforderlichen Dateien an deren endgültige Positionen verschoben werden, bevor das Script beendet wird (beim Löschen des Clientverzeichnisses, das die Datei GO.RRS enthält). Wenn die Programmkorrekturen sehr umfangreich sind, ist es möglicherweise nicht zweckmäßig, sie in die Nachrichtendatei zu packen. In diesem Fall sollte der Endbenutzer informiert und anschließend der Netzbetrieb auf lediglich den Server eingeschränkt werden, auf dem sich die Programmkorrektur befindet. Anschließend können Sie die Programmkorrektur unter Windows XP herunterladen. Auch wenn Windows XP somit länger durch einen Virus gefährdet ist, ist dies mit hoher Wahrscheinlichkeit nicht von Bedeutung.

Kapitel 8. Bewährte Verfahren

In diesem Kapitel werden Einsatzszenarios zur Veranschaulichung von Empfehlungen für die Verwendung von Rescue and Recovery, Client Security Solution und der ThinkVantage Fingerprint Software dargestellt. Das vorliegende Beispielszenario beginnt mit der Konfiguration des Festplattenlaufwerks, erläutert verschiedene Aktualisierungen und beschreibt den gesamten Lebenszyklus einer Implementierung. Es wird die Installation auf IBM Computern und auf Computern anderer Hersteller beschrieben.

Implementierungsbeispiele für die Installation von Rescue and Recovery und Client Security Solution

In diesem Abschnitt finden Sie eine Reihe von Beispielen zur Installation von Rescue and Recovery und Client Security Solution auf Maschinen vom Typ ThinkCentre und ThinkPad.

Implementierungsbeispiel für ThinkCentre

Hierbei handelt es sich um ein Beispiel einer Installation auf einem ThinkCentre unter Verwendung der folgenden hypothetischen Kundenanforderungen:

- **Verwaltung**
  - Sysprep-Basissicherung mit Hilfe von Rescue and Recovery erstellen
  - Lokales Administratorkonto für die Verwaltung des Computers verwenden
- **Rescue and Recovery**
  - Client Security-Verschlüsselungstext verwenden, um den Zugriff auf den Arbeitsbereich von Rescue and Recovery zu schützen
    - Die Benutzer müssen sich mit ihrem Verschlüsselungstext anmelden und können so ihre SafeGuard PrivateDisk-Datenträgerdatei zum Sichern von Dateien verwenden
- **Client Security Solution**
  - Installation und Ausführung im Emulationsmodus
    - Nicht alle IBM Systeme verfügen über ein Trusted Platform Module (TPM, Sicherheitschip)
  - Kein Password Manager
    - Der Kunde verwendet stattdessen eine unternehmensweite SSO-Lösung (SSO - Single-Sign On, Einzelanmeldung)
  - Client Security-Verschlüsselungstext aktivieren
    - Client Security Solution-Anwendungen mit Hilfe eines Verschlüsselungstexts schützen
  - Client Security-Anmeldung bei Windows aktivieren
    - Anmeldung bei Windows mit Client Security-Verschlüsselungstext
  - SafeGuard PrivateDisk mit einer Größe von 500 MB für alle Benutzer erstellen
    - Jeder Benutzer benötigt 500 MB Speicherplatz, um Daten sicher zu speichern
  - Wiederherstellungsfunktion für Verschlüsselungstext von Endbenutzern aktivieren

- Benutzern die Wiederherstellung ihres Verschlüsselungstexts durch drei benutzerdefinierte Fragen und Antworten ermöglichen

– Client Security Solution-XML-Script mit Kennwort verschlüsseln = "XML-scriptPW"
  - Client Security Solution-Konfigurationsdatei mit Kennwort schützen

Auf der Erstellungsmaschine:

1. Melden Sie sich mit dem lokalen Administratorkonto unter Windows an.
2. Installieren Sie das Programm "Rescue and Recovery and Client Security Solution" mit den folgenden Optionen:

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

   Anmerkungen:

   a. Stellen Sie sicher, dass sich Dateien mit der Erweiterung .tvt, wie z. B. z062zaa1025us00.tvt, in demselben Verzeichnis wie die ausführbare Datei befinden. Andernfalls schlägt die Installation fehl.

   b. Wenn Ihre Datei mit setup_tvtrnr3_1027c.exe benannt ist, haben Sie das kombinierte Paket heruntergeladen. Diese Anweisungen gelten für die Dateien, die einzeln von der Downloadseite "Large Enterprise individual language files" heruntergeladen werden können.

   c. Wenn Sie eine administrative Installation durchführen, finden Sie weitere Informationen unter „Installation von Rescue and Recovery in einer neuen Implementierung auf Lenovo und IBM Computern" auf Seite 133.

3. Melden Sie sich nach dem Neustart mit dem lokalen Administratorkonto unter Windows an, und bereiten Sie das XML-Script für die Implementierung vor. Führen Sie über die Befehlszeile den folgenden Befehl aus:

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

   Wählen Sie im Assistenten die folgenden Optionen aus:

   - Wählen Sie die Option für "Erweitert" (Advanced) und anschließend "Weiter" (Next) aus.
   - Wählen Sie die Option für den Client Security-Verschlüsselungstext (Client Security passphrase) und anschließend "Weiter" (Next) aus.
   - Wählen Sie die Option für die Anmeldung über die Anmeldeanzeige von Client Security (Log on with the Client Security Login Screen) und anschließend "Weiter" (Next) aus.
   - Geben Sie das Windows-Kennwort für das Administratorkonto ein, und klicken Sie auf "Weiter" (Next).

     (z. B. WPW4Admin)
   - Geben Sie den Client Security-Verschlüsselungstext für das Administratorkonto ein, aktivieren Sie das Markierungsfeld, um den Client Security-Verschlüsselungstext zum Schützen des Zugriffs auf den Arbeitsbereich von Rescue and Recovery zu verwenden (Use the Client Security passphrase to protect access to the Rescue and Recovery workspace), und klicken Sie auf "Weiter" (Next).

     (z. B. CSPP4Admin)
   - Aktivieren Sie das Feld zur Aktivierung der Kennwortwiederherstellung (**Enable Password Recovery**), und wählen Sie drei Fragen und die zugehörigen Antworten für das Administratorkonto aus **-> Next**

     a. Wie heißt Ihr Haustier?

(z. B. Hasso)

b. Was ist Ihr Lieblingsfilm?

(z. B. Vom Winde verweht)

c. Welche ist Ihre Lieblingsmannschaft?

(z. B. VfB Stuttgart)

- Wählen Sie nicht die Option zum Erstellen eines PrivateDisk-Datenträgers für jeden Benutzer mit der unten ausgewählten Größe aus (Create a Private-Disk volume for each user, with the size selected below), und klicken Sie auf ″Weiter″ (Next).
- Überprüfen Sie die Zusammenfassung, und wählen Sie die Option zum Übernehmen (Apply) aus, um die xml-Datei in der folgenden Position zu schreiben C:\ThinkCentre.xml **-> Apply**.
- Wählen Sie die Option zum Fertigstellen (Finish) aus, um den Assistenten zu schließen.

4. Öffnen Sie die folgende Datei in einem Texteditor (der XML-Scripteditor oder Microsoft Word 2003 verfügen über integrierte XML-Formatierungsfunktionen), und ändern Sie die folgenden Einstellungen:
   - Entfernen Sie alle Verweise auf die Einstellung für die Domäne. Dadurch wird das Script angewiesen, den Namen der lokalen Maschine auf den einzelnen Systemen zu verwenden. Speichern Sie die Datei.
5. Verschlüsseln Sie das XML-Script mit Hilfe des Tools unter C:\Program Files\IBM ThinkVantage\Client Security Solution\xml_crypt_tool.exe mit einem Kennwort. Führen Sie die Datei über eine Eingabeaufforderung aus. Verwenden Sie dazu die folgende Syntax:
   a. xml_crypt_tool.exe C:\ThinkCentre.xml /encrypt XMLScriptPW
   b. Die Datei heißt jetzt C:\ThinkCentre.xml.enc und wird durch das Kennwort = XMLScriptPW geschützt.

Die Datei C:\ThinkCentre.xml.enc kann nun zu der Implementierungsmaschine hinzugefügt werden.

Auf der Implementierungsmaschine:

1. Melden Sie sich mit dem lokalen Administratorkonto unter Windows an.
2. Installieren Sie die Programme ″Rescue and Recovery and Client Security Solution″ mit den folgenden Optionen:

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

   Anmerkungen:

   a. Stellen Sie sicher, dass sich Dateien mit der Erweiterung .tvt, wie z. B. z062zaa1025us00.tvt, in demselben Verzeichnis wie die ausführbare Datei befinden. Andernfalls schlägt die Installation fehl.

   b. Wenn Ihre Datei mit setup_tvtrnr3_1027c.exe benannt ist, haben Sie das kombinierte Paket heruntergeladen. Diese Anweisungen gelten für die Dateien, die einzeln von der Downloadseite mit den Dateien mit sprachabhängigen Anweisungen für Großunternehmen heruntergeladen werden können.

   c. Wenn Sie eine administrative Installation durchführen, finden Sie weitere Informationen unter „Installation von Rescue and Recovery in einer neuen Implementierung auf Lenovo und IBM Computern” auf Seite 133.
3. Melden Sie sich nach dem Neustart mit dem lokalen Administratorkonto unter Windows an.

4. Fügen Sie die zuvor vorbereitete Datei ThinkCentre.xml.enc zum Verzeichnis C:\ root hinzu.
5. Ändern Sie die Registrierungsdatenbank so, dass die Standarddatenträgergröße für SafeGuard PrivateDisk = 500 MB für alle Benutzer ist. Dies kann ohne großen Aufwand durch das Importieren einer *reg*-Datei vorgenommen werden.
   a. Rufen Sie HKEY_LOCAL_MACHINE\SOFTWARE\IBM ThinkVantage\Client Security Software auf.
   b. Erstellen Sie einen neuen Zeichenfolgewert mit dem Wertnamen: = PrivateDiskSize und dem Wert: = 500
   c. Erstellen Sie einen Wert DWORD mit dem Wertnamen: = UsingPrivateDisk und dem Wert: = 1
6. Bereiten Sie den Befehl RunOnceEx mit den folgenden Parametern vor.
   - Fügen Sie einen neuen Schlüssel mit dem Namen "0001" zu RunonceEx hinzu. Das sollte wie folgt aussehen: HKEY_LOCAL_MACHINE \Software\Microsoft\Windows\Current Version\RunOnceEx\0001
   - Fügen Sie zu diesem Schlüssel einen Zeichenfolgewert mit dem Namen "CSSEnroll" mit dem folgenden Wert hinzu: ″c:\program files\IBM ThinkVantage\Client Security Solution\vmservere.exe" C:\ThinkCenter.xml.enc XMLscriptPW
7. Führen Sie "%rr%\rrcmd.exe sysprepbackup location=L name="Sysprep Backup" aus. Nachdem das System entsprechend vorbereitet wurde, wird die folgende oder eine ähnliche Ausgabe angezeigt:

```
**********************************************************************
** Für Sysprep-Sicherung bereit.                                    **
**                                                                  **
** FÜHREN SIE SYSPREP JETZT AUS, UND FAHREN SIE DAS SYSTEM HERUNTER.**
**                                                                  **
** Beim nächsten Booten der Maschine wird die                       **
** Predesktop Area aufgerufen und eine Sicherung erstellt.          **
**********************************************************************
```

8. Führen Sie jetzt die Sysprep-Implementierung aus.
9. Führen Sie einen Systemabschluss durch, und starten Sie das System erneut. Dadurch wird der Sicherungsprozess unter Windows PE gestartet.

   Anmerkung: Sie erhalten die Nachricht, dass die Verarbeitung, aber auch eine Sicherung stattfindet. SCHALTEN SIE das System nach der Sicherung AUS, und starten Sie es nicht erneut.

Die Sysprep-Basissicherung ist nun abgeschlossen.

Implementierungsbeispiel für Thinkpad

Hierbei handelt es sich um ein Beispiel einer Installation auf einem ThinkPad unter Verwendung der folgenden hypothetischen Kundenanforderungen:

- **Verwaltung**
  - Installation auf Systemen, auf denen bereits Image und Implementierung vorhanden sind
  - Administratorkonto der Domäne für die Verwaltung des Computers verwenden
  - Alle Computer verfügen über das BIOS-Administratorkennwort ″BIOSpw″
- **Client Security Solution**
  - Trusted Platform Module (TPM, Sicherheitschip) nutzen
    - Alle Maschinen verfügen über den Sicherheitschip

  - Password Manager aktivieren
  - SafeGuard PrivateDisk inaktivieren
    - Stattdessen vollständige Verschlüsselung des Festplattenlaufwerks mit Utimaco SafeGuard Easy nutzen
  - Windows-Kennwort des Benutzers als Authentifizierung bei Client Security Solution verwenden
    - Einfaches Windows-Kennwort für die Authentifizierung bei Utimaco SafeGuard Easy, Client Security Solution und der Windows-Domäne zulassen
  - Verschlüsselung des Client Security Solution-XML-Scripts mit einem Kennwort = ″XMLscriptPW″
    - Das Kennwort schützt die Client Security Solution-Konfigurationsdatei
- **ThinkVantage Fingerprint Software**
  - BIOS- und Festplattenkennwörter sollen nicht verwendet werden
  - Anmeldung über Fingerabdruck
    - Nachdem sich der Benutzer anfangs über die Selbstregistrierung angemeldet hat, wechselt er später in den Modus der sicheren Anmeldung, für die bei Benutzern ohne Administratorberechtigung ein Fingerabdruck erforderlich ist. Auf diese Weise erfolgt eine 2-Wege-Authentifizierung.
  - Fingerprint Tutorial integrieren (Lernprogramm für elektronischen Fingerabdruck)
    - Die Endbenutzer lernen, wie sie ihren Finger richtig über das Lesegerät für Fingerabdrücke ziehen und erhalten ein grafisch unterstütztes Feedback darüber, was sie möglicherweise falsch gemacht haben.

Auf der Erstellungsmaschine:

1. Starten Sie den Computer aus dem ausgeschalteten Status heraus, und drücken Sie die Taste **F1**, um das BIOS aufzurufen. Navigieren Sie zum Menü für Sicherheit, und löschen Sie den Sicherheitschip. Speichern Sie, und verlassen Sie das BIOS.
2. Melden Sie sich mit dem Administratorkonto für die Windows-Domäne an.
3. Installieren Sie die ThinkVantage Fingerprint Software. Führen Sie dazu f001zpz2001us00.exe aus, um die Datei ″setup.exe″ aus dem Webpaket zu extrahieren. Dadurch wird die Datei ″setup.exe″ automatisch in folgendes Verzeichnis entpackt: C:\IBMTOOLS\APPS\TFS4.6-Build1153\Application\0409\setup.exe.
4. Installieren Sie das ThinkVantage Fingerprint Tutorial (Lernprogramm für Fingerabdrücke), indem Sie die Datei f001zpz7001us00.exe ausführen, um die Datei ″tutess.exe″ aus dem Webpaket zu extrahieren. Dadurch wird die Datei ″setup .exe″ automatisch in folgendes Verzeichnis entpackt: C:\IBMTOOLS\APPS\tutorial\TFS4.6-Build1153\Tutorial\0409\tutess.exe.
5. Installieren Sie die ThinkVantage Fingerprint Console, indem Sie die Datei ″f001zpz5001us00.exe″ ausführen, um die Datei fprconsole.exe aus dem Webpaket zu extrahieren. Durch die Ausführung von f001zpz5001us00.exe wird die Datei ″setup.exe″ automatisch in folgendes Verzeichnis entpackt: C:\IBMTOOLS\APPS\fpr_con\APPS\UPEK\FPR Console\TFS4.6-Build1153\Fprconsole\fprconsole.exe.
6. Installieren Sie das Programm ″Client Security Solution″ mit den folgenden Optionen:

   ```
   setup_tvtcss6_1027.exe /s /v"/qn NOPRVDISK=1 NOCSSWIZARD=1 SUPERVISORPW=
   "BIOSpw""
   ```

7. Melden Sie sich nach dem Neustart mit dem Administratorkonto für die Windows-Domäne an, und bereiten Sie das XML-Script für die Implementierung vor. Führen Sie über die Befehlszeile den folgenden Befehl aus:

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

   Wählen Sie im Assistenten die folgenden Optionen aus, um eine Übereinstimmung mit dem Beispielscript zu erzielen:

   - Wählen Sie die Option für Erweitert (Advanced) und anschließend ″Weiter″ (Next) aus.
   - Wählen Sie die Option für das Windows-Kennwort (Windows password) und anschließend ″Weiter″ (Next) aus.
   - Wählen Sie die Option zur Anmeldung über den Sensor für Fingerabdrücke (Log on with the fingerprint sensor) und anschließend ″Weiter″ (Next) aus.
   - Geben Sie das Windows-Kennwort für das Administratorkonto für die Domäne ein, und klicken Sie auf ″Weiter″ (Next)

     (z. B. WPW4Admin).
   - • Heben Sie die Markierung für die Option zur Aktivierung der Kennwortwiederherstellung (Enable Password Recovery) auf, und klicken Sie auf ″Weiter″ (Next).
   - • Überprüfen Sie die Zusammenfassung, und wählen Sie die Option zum Übernehmen (Apply) aus, um die xml-Datei in die folgende Position zu schreiben C:\ThinkPad.xml
   - • Wählen Sie die Option zum Beenden (Finish) aus, um den Assistenten zu schließen.

8. Verschlüsseln Sie das XML-Script mit Hilfe des Tools unter C:\Program Files\IBM ThinkVantage\Client Security Solution\xml_crypt_tool.exe mit einem Kennwort. Führen Sie die Datei über eine Eingabeaufforderung aus. Verwenden Sie dazu die folgende Syntax:
   a. xml_crypt_tool.exe C:\ThinkPad.xml /encrypt XMLScriptPW
   b. Die Datei heißt jetzt C:\ThinkPad.xml.enc und wird durch das Kennwort = XMLScriptPW geschützt.

Auf der Implementierungsmaschine:

1. Implementieren Sie mit Hilfe der Softwareverteilungstools Ihres Unternehmens die ausführbare Datei ″setup.exe″ für die ThinkVantage Fingerprint Software, die von der Erstellungsmaschine auf alle Implementierungsmaschinen entpackt wurde. Wenn die Datei ″setup.exe″ auf die Maschine übertragen wurde, installieren Sie sie unter Verwendung des folgenden Befehls:

   ```
   setup.exe CTLCNTR=0 /q /i
   ```

2. Implementieren Sie mit Hilfe der Softwareverteilungstools Ihres Unternehmens die ausführbare Datei ″tutess.exe″ für das ThinkVantage Fingerprint Tutorial, die von der Erstellungsmaschine auf alle Implementierungsmaschinen entpackt wurde. Wenn die Datei ″tutess.exe″ auf die Maschine übertragen wurde, installieren Sie sie unter Verwendung des folgenden Befehls:

   ```
   tutess.exe /q /i
   ```

3. Implementieren Sie mit Hilfe der Softwareverteilungstools Ihres Unternehmens die ausführbare Datei ″fprconsole.exe″ für die ThinkVantage Fingerprint Console, die von der Erstellungsmaschine auf alle Implementierungsmaschinen entpackt wurde.
   - Stellen Sie die Datei ″fprconsole.exe″ in das Verzeichnis “C:\Program Files\ThinkVantage Fingerprint Software\”.

- Schalten Sie die Unterstützung für das Einschalten von Sicherheitsfunktionen des BIOS durch Ausführen des folgenden Befehls aus: fprconsole.exe settings TBX 0

4. Implementieren Sie mit Hilfe der Softwareverteilungstools Ihres Unternehmens die ausführbare Datei “setup_tvtcss6_1027.exe” für ThinkVantage Client Solution.
   - Wenn die Datei "setup_tvtcss6_1027.exe" auf dem System gespeichert ist, nehmen Sie die Installation über den folgenden Befehl vor: setup_tvtcss6_1027.exe /s /v"/qn NOPRVDISK=1 NOCSSWIZARD=1 SUPERVISORPW="BIOSpw""
   - Durch die Installation der Software wird automatisch die Hardware für das Trusted Platform Module (TPM, Sicherheitschip) aktiviert.
5. Konfigurieren Sie das System nach einem Neustart über die XML-Scriptdatei mit Hilfe der folgenden Prozedur:
   - Kopieren Sie die zuvor erstellte Datei ThinkPad.xml.enc in das Verzeichnis C:\.
   - Führen Sie C:\Program Files\IBM ThinkVantage\Client Security Solution\vmserver.exe C:\ThinkPad.xml.enc XMLScriptPW aus.
6. Nach einem Neustart ist das System nun bereit für die Client Security Solution-Benutzerregistrierung. Jeder Benutzer kann sich nun mit seiner Benutzer-ID und dem Windows-Kennwort am System anmelden. Jeder Benutzer, der sich am System anmeldet, wird automatisch dazu aufgefordert, sich bei Client Security Solution zu registrieren und kann sich dann beim Lesegerät für Fingerabdrücke registrieren.
7. Nachdem sich alle Benutzer für das System bei der ThinkVantage Fingerprint Software registriert haben, kann die Einstellung für den sicheren Modus aktiviert werden, durch den alle Windows-Benutzer ohne Administratorberechtigung gezwungen werden, sich über ihren Fingerabdruck anzumelden.
   - Führen Sie den folgenden Befehl aus: C:\Program Files\ThinkVantage Fingerprint Software\fprconsole.exe settings securemode 1
   - Drücken Sie die Tastenkombination Strg + ALT + Entf, um die Nachricht zu entfernen und die Anmeldung über ein Kennwort vorzunehmen. Führen Sie von der Anmeldeanzeige aus den folgenden Befehl aus:

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

Die Implementierung von Client Security Solution 6.0 und ThinkVantage Fingerprint Software ist nun abgeschlossen.

Installation von Rescue and Recovery in einer neuen Implementierung auf Lenovo und IBM Computern

In diesem Abschnitt wird die Installation von Rescue and Recovery in einer neuen Implementierung beschrieben.

Festplattenlaufwerk vorbereiten

Bei der Implementierung eines Systems muss zunächst das Festplattenlaufwerk des Donatorsystems vorbereitet werden. Um sicherzustellen, dass Sie mit einer leeren Festplatte beginnen, müssen Sie den Master-Bootsatz der primären Festplatte bereinigen.

1. Entfernen Sie aus dem Donatorsystem alle Speichereinheiten, wie z. B. zusätzliche Festplatten, USB-Festplatten, USB-Memory-Keys, PC-Karten usw. außer dem primären Festplattenlaufwerk, auf dem Sie Windows installieren.

   Achtung: Mit dem nachfolgenden Befehl wird der gesamte Inhalt des Zielplattenlaufwerks gelöscht. Nach Ausführung dieses Befehls können keine Daten des Zielplattenlaufwerks wiederhergestellt werden.
2. Erstellen Sie eine DOS-Bootdiskette, und kopieren Sie die Datei CLEANDRV.EXE auf diese Diskette.
3. Booten Sie mit dieser Diskette (mit nur einer angeschlossenen Speichereinheit). Geben Sie an der DOS-Eingabeaufforderung den folgenden Befehl ein:

   ```
   CLEANDRV /HDD=0
   ```
4. Installieren Sie das Betriebssystem und die zugehörigen Anwendungen. Erstellen Sie das Donatorsystem, ohne die Installation von Rescue and Recovery zu berücksichtigen. Installieren Sie anschließend Rescue and Recovery.

Installation

Bei der Installation muss zunächst die ausführbare Datei von InstallShield in das Verzeichnis C:\RRTEMP extrahiert werden. Wenn Sie eine Installation von Rescue and Recovery auf mehreren Systemen planen, können Sie durch das einmalige Ausführen dieses Prozesses die Installationszeit ungefähr um die Hälfte reduzieren.

1. Wenn sich die Installationsdatei beispielsweise im Hauptverzeichnis des Laufwerks C befindet, erstellen Sie eine Datei mit dem Namen EXE_EXTRACT.CMD. Diese extrahiert die Datei C:\SETUP_TVTRNR3_*XXXX*.EXE (wobei *XXXX* für die Build-ID steht) in das Verzeichnis C:\RRTEMP:

   ```
   :: This package will extract the WWW EXE to the directory c:\RRTemp for an
   :: administrative install.
   @ECHO OFF
   :: This is the name of the EXE (Without the .EXE)
   set BUILDID=setup_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"
    TARGETDIR=c:\RRTemp"
   Copy Z062ZAA1025US00.TVT C:\rrtemp\
   ```
2. Sie können Anpassungen vornehmen, bevor Sie Rescue and Recovery installieren. Dazu erhalten Sie hier im Rahmen dieses Szenarios einige Beispiele:
   - Die maximale Anzahl von inkrementellen Sicherungen soll in den Wert von 4 geändert werden.
   - Rescue and Recovery soll so konfiguriert werden, dass täglich um 13.59 Uhr eine inkrementelle Sicherung auf der lokalen Festplatte ausgeführt wird. Für diese Sicherungen wird die Bezeichnung ″Geplant″ verwendet.
   - Die Benutzerschnittstelle von Rescue and Recovery soll für alle Benutzer ausgeblendet werden, die nicht der Gruppe ″Administratoren″ angehören.
3. Erstellen Sie eine angepasste TVT.TXT-Datei. Einige Parameter können geändert werden. Weitere Informationen hierzu finden Sie unter Anhang B, „Einstellungen und Werte für die Datei TVT.TXT”, auf Seite 155.

```
[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="Geplant" geplant
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. Erstellen Sie in dem Verzeichnis, in dem sich auch die angepasste Datei TVT-.TXT befindet, eine Datei mit dem Namen INSTALL.CMD, mit der verschiedene Aktionen ausgeführt werden können:
   - Kopieren Sie die angepasste Datei TVT.TXT in das Installationspaket, das im Verzeichnis C:\RRTemp erstellt wurde:
   - Führen Sie eine unbeaufsichtigte Installation von Rescue and Recovery ohne einen Neustart am Ende durch.
   - Starten Sie Rescue and Recovery, so dass eine Basissicherung durchgeführt werden kann.
   - Nach dem Start des Service wird die Umgebung zum Erstellen eines ISO-Image von der Rescue and Recovery-CD eingerichtet. (Dies erfolgt normalerweise beim Neustart.)
   - Erstellen Sie das ISO-Image.
   - Erstellen Sie die Basissicherung, und führen Sie einen Neustart durch.
5. Ändern Sie den Code in der Datei INSTALL.CMD. Die Datei INSTALL.CMD enthält folgenden Code:

```
:: 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 Recoveery\rrcd
```

   Anmerkung: Sie müssen die Umgebung nicht einrichten, wenn das System erneut gebootet wird.

```
:: 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
```

Anpassung

Angenommen, Sie haben Rescue and Recovery in Ihrer Umgebung implementiert. Nun können Sie für Rescue and Recovery die folgenden Einstellungen ändern:

- Sie möchten nicht mehr 4, sondern 10 inkrementelle Sicherungen ausführen lassen.
- Die für die Sicherung festgelegte Uhrzeit von 13.59 Uhr ist für Ihre Umgebung eher ungünstig. Die Sicherung soll stattdessen um 10.24 Uhr erfolgen.
- Sie möchten allen Benutzern Ihrer Systeme einen Zugriff auf die Benutzerschnittstelle von Rescue and Recovery 3.0 ermöglichen.
- Während der geplanten Sicherungen soll das System auch für andere Zwecke zur Verfügung stehen. Nach verschiedenen Tests ergibt sich als günstigster Wert für `Yield=` in Ihrer Umgebung ein Wert von `2` (Standardwert: `0`).

Gehen Sie wie folgt vor, um diese Änderungen auf mehreren Systemen vorzunehmen:

1. Erstellen Sie eine MOD-Datei mit dem Namen UPDATE.MOD (in einem Texteditor). Diese Datei soll folgenden Inhalt haben:

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

2. Sie können anschließend eine Datei mit dem Namen INSTALL.CMD erstellen und die Dateien INSTALL.CMD und UPDATE.MOD mit einem Systemverwaltungstool Ihrer Wahl auf den Zielsystemen speichern. Nach der Ausführung der Datei INSTALL.CMD sind die Aktualisierungen wirksam. Die Datei INSTALL.CMD enthält folgenden Code:

   ```
   :: 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"
   ```

Aktualisierung

Im Folgenden wird angenommen, dass Sie größere Änderungen an Ihrem System durchführen möchten, z. B. eine Aktualisierung mit einem Service-Pack für Windows. Gehen Sie wie folgt vor, um vor der Installation des Service-Packs eine inkrementelle Sicherung auszuführen und diese mit einem eigenen Namen zu kennzeichnen:

1. Erstellen Sie die Datei FORCE_BU.CMD, und speichern Sie sie auf den Zielsystemen.
2. Rufen Sie die Datei FORCE_BU.CMD auf, wenn sie sich auf dem Zielsystem befindet.

Die Datei FORCE_BU.CMD enthält folgenden Inhalt:

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

Arbeitsoberfläche von Rescue and Recovery aktivieren

Wenn Sie nach einer gewissen Zeit die Vorteile von Rescue and Recovery kennen gelernt haben, können Sie die Umgebung von Rescue and Recovery nutzen. Zu Demonstrationszwecken wird im folgenden Abschnitt das Beispielscript UPDATE_RRE.CMD vorgestellt. Es extrahiert die Steuerdatei für die Umgebung von Rescue and Recovery. Anschließend können Sie diese Steuerdatei mit Hilfe der Datei RRUTIL.exe bearbeiten und zurück in die Umgebung von Rescue and Recovery stellen. Weitere Informationen hierzu finden Sie im Abschnitt „RRUTIL.EXE verwenden” auf Seite 21.

Für das Ändern der Predesktop Area veranschaulicht das Script UPDATE_RRE.CMD mehrere Vorgänge:

- Mit RRUTIL.exe wird eine Datei aus der Umgebung von Rescue and Recovery abgerufen. Die aus der Umgebung von Rescue and Recovery zu extrahierenden Dateien sind in der Datei GETLIST.TXT definiert.
- Es wird eine Verzeichnisstruktur erstellt, über die Dateien nach der Bearbeitung der entsprechenden Datei zurück in die Predesktop Area gestellt werden.
- Zur Sicherheit wird eine Kopie der Datei erstellt. Diese wird anschließend bearbeitet.

In diesem Beispiel soll eine Homepage geändert werden, die beim Klicken auf **Browser öffnen** in der Umgebung von Rescue and Recovery aufgerufen wird. Die Webseite `http://www.lenovo.com/thinkvantage` wird geöffnet.

Wenn Notepad mit der Datei PEACCESSIBMEN.INI geöffnet wird, gehen Sie wie folgt vor, um die Änderung durchzuführen:

1. Ändern Sie die folgende Zeile:

```
button13 = 8, "Browser öffnen",
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__
```

   IN

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

2. Stellen Sie die neue Version in die Verzeichnisstruktur, über die Dateien in die Umgebung von Rescue and Recovery gestellt werden sollen. Weitere informationen hierzu finden Sie unter „RRUTIL.EXE verwenden" auf Seite 21.
3. Führen Sie einen Neustart des Systems mit der Umgebung von Rescue and Recovery durch.
4. Beim vorliegenden Beispiel wird nun davon ausgegangen, dass Sie nach einigen Analysen festgestellt haben, dass bestimmte Dateien unbedingt gesichert werden müssen, während dies bei anderen Dateien nicht erforderlich ist, da sie sich auf dem Server befinden und nach einer Systemwiederherstellung wieder verfügbar sind. Passen Sie dazu die Datei IBMFILTER.TXT an. Diese Datei wird in das Verzeichnis mit der Datei NSF.CMD gestellt, von der sie wie im folgenden Beispiel in die richtige Position kopiert wird:

   NSF.CMD:

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

   IBMFILTER.TXT:

   ```
   x=*.nsf
   ```

Tabelle 37. Script für die Datei UPDATE_RR.CMD

```
@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

Die Datei wird automatisch geöffnet
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

Die Datei GETLIST.TXT wird erstellt:
\preboot\usrintfc\PEAccessIBMen.ini
```

Rescue and Recovery auf Computern anderer Hersteller installieren

Zur Installation von Rescue and Recovery müssen im Master-Bootsatz auf der Festplatt acht freie Sektoren verfügbar sein. Rescue and Recovery verwendet einen angepassten Boot-Manager zum Aufrufen des Wiederherstellungsbereichs.

Einige OEM-Hersteller speichern Zeiger zu einem eigenen Wiederherstellungscode im Sektor mit dem Master-Bootsatz. Dieser OEM-Wiederherstellungscode führt möglicherweise zu Konflikten mit der Installation des Boot-Managers für Rescue and Recovery.

Orientieren Sie sich an den nachfolgenden Szenarios und Empfehlungen, und stellen Sie so sicher, dass Rescue and Recovery die gewünschten Funktionen und Einrichtungen bereitstellt:

Empfehlungen zur Festplattenkonfiguration: Szenario 1

Im folgenden Szenario wird die Implementierung eines neuen Images erläutert, das Rescue and Recovery enthält. Wenn Sie Rescue and Recovery auf vorhandenen OEM-Clients implementieren, auf denen ein OEM-Code für Produktwiederherstellung gespeichert ist, müssen Sie durch den nachfolgenden Test sicherstellen, dass dieser Code Rescue and Recovery nicht beeinträchtigt:

1. Richten Sie einen Testclient mit dem Image ein, das den OEM-Wiederherstellungscode enthält.
2. Installieren Sie Rescue and Recovery. Wenn auf dem Master-Bootsatz wegen des OEM-Wiederherstellungscodes weniger als acht freie Sektoren verfügbar sind, wird eine Fehlernachricht mit dem folgenden oder einem ähnlichen Inhalt angezeigt:

   ```
   Fehler 1722. Bei diesem Windows
   -Installationspaket liegt ein Fehler vor. Ein im Rahmen des
   Setup
   ausgeführtes Programm konnte nicht wie erwartet beendet werden. Wenden Sie sich an
   den zuständigen Mitarbeiter oder den Hersteller.
   ```

Wenn Sie ein OEM-Image für das Basisbetriebssystem verwenden, müssen Sie sicherstellen, dass der Master-Bootsatz keine Produktwiederherstellungsdaten enthält. Dazu können Sie wie folgt vorgehen:

Achtung: Mit dem nachfolgenden Befehl wird der gesamte Inhalt des Zielplattenlaufwerks gelöscht. Nach Ausführung dieses Befehls können keine Daten des Zielplattenlaufwerks wiederhergestellt werden.

1. Verwenden Sie die Datei CLEANDRV.EXE aus dem Abschnitt mit den Verwaltungstools auf der Website unter der Adresse:

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

   um sicherzustellen, dass auf der Festplatte, auf der das Basisimage erstellt werden soll, alle Sektoren des Master-Bootsatzes gelöscht wurden.
2. Erstellen Sie gemäß den Anforderungen für Ihre Implementierung ein Paket mit dem Image.

Empfehlungen zur Festplattenkonfiguration: Szenario 2

Die Implementierung von Rescue and Recovery auf vorhandenen Clients setzt eine gewisse Planung und Vorbereitung voraus.

Wenden Sie sich an den IBM Help-Desk, wenn die Fehlernachricht 1722 angezeigt wird und Sie acht freie Sektoren erstellen müssen.

Bootfähige CD von Rescue and Recovery erstellen

Die Wiederherstellungs-CD wird von Rescue and Recovery standardmäßig anhand der Daten im aktuellen Wartungsbereich erstellt und gebrannt, und nicht anhand eines vorprogrammierten ISO-Images. Wenn jedoch ein geeignetes ISO-Image vorliegt, das zuvor geladen oder erstellt wurde, wird die CD mit diesem Image gebrannt. In diesem Fall wird kein neues Image erstellt.

Aufgrund der Ressourcenanforderungen können nicht mehrere CDs gleichzeitig gebrannt werden. Ist eine Sitzung zum Brennen einer CD gestartet, löst der Versuch, eine weitere Sitzung zum Brennen zu starten, einen Fehler aus. Die zweite Sitzung wird daraufhin abgebrochen. Darüber hinaus gilt, dass aufgrund der Sicherheitsanforderungen für geschützte Festplattenbereiche nur Administratoren das ISO-Image erstellen können. Benutzer mit eingeschränkter Berechtigung können das ISO-Image jedoch auf CD brennen. Die folgenden Dateien und Verzeichnisse werden der Wiederherstellungs-CD hinzugefügt:

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

Anmerkung: Auf dem Systemlaufwerk müssen für das Kopieren der Verzeichnisstrukturen und das Erstellen des ISO-Images mindestens 400 MB freier Speicherbereich verfügbar sein. Das Verarbeiten dieser Datenmenge erfordert viele Festplattenoperationen und kann bei einigen Computern mehr als 15 Minuten in Anspruch nehmen.

ISO-Wiederherstellungsdatei erstellen und CD mit Beispielscriptdatei brennen: Erstellen Sie den folgenden Code:

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

Anmerkung: Die sieben nachfolgenden Zeilen (fett gedruckt) sind nur erforderlich, wenn das System nach der Installation nicht erneut gebootet wird.

```
:: 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
```

Rescue and Recovery auf einer Servicepartition vom Typ 12 installieren

Für die Installation von Rescue and Recovery auf einer Servicepartition vom Typ 12 müssen Sie über Folgendes verfügen:

- Datei SP.PQI. Diese Datei enthält die wichtigsten bootfähigen Dateien zum Erstellen einer Servicepartition.
- PowerQuest PQDeploy
- Aktuelles Installationsprogramm für Rescue and Recovery

Bei einer Installation der Umgebung von Rescue and Recovery auf einer Servicepartition sind verschiedene Optionen verfügbar.

Anmerkung: Die Servicepartition vom Typ 12 muss sich im zuletzt verwendeten Eintrag in der Partitionstabelle auf dem Laufwerk befinden, das auch Windows (in der Regel Laufwerk C:\) enthält. Sie können mit Hilfe von bmgr32 /info bestimmen, wo sich die Partition vom Typ 12 auf dem Festplattenlaufwerk befindet. Weitere Informationen hierzu finden Sie unter „Boot-Manager von Rescue and Recovery (BMGR32) steuern" auf Seite 178.

Gehen Sie wie folgt vor, um die Installation durchzuführen:

1. Lassen Sie mindestens 700 MB nicht zugeordneten freien Speicherbereich am Ende des Laufwerks frei.
2. Stellen Sie die Datei SP.PQI mit Hilfe von PowerQuest in diesem nicht zugeordneten freien Speicherbereich wieder her.
3. Löschen Sie die in Schritt 1 erstellten primären Partitionen mit Ausnahme von Laufwerk C, und booten Sie das System erneut.

   Anmerkung: Auf der neu erstellten Servicepartition sind möglicherweise Systemdatenträgerinformationen gespeichert. Diese Daten müssen über eine Windows-Systemwiederherstellung gelöscht werden.
4. Installieren Sie Rescue and Recovery, und starten Sie das System bei entsprechender Aufforderung erneut.

Sicherung/Wiederherstellung mit Hilfe von Sysprep

Beachten Sie, dass die Kennwortpersistenz bei der Sicherung/Wiederherstellung mit Sysprep nicht funktioniert.

Nach einem Sicherungsvorgang mit dem Dienstprogramm ″Sysprep″ sollten Sie das System ausschalten und anschließend erneut starten.

Computrace und Rescue and Recovery

Rescue and Recovery kann nicht auf Systemen ohne BIOS deinstalliert werden, wenn Computrace installiert ist.

Kapitel 9. Fingerprint Software

Die Fingerprint Console muss vom Installationsordner der Fingerprint Software aus ausgeführt werden. Die grundlegende Syntax lautet FPRCONSOLE [USER | SETTINGS]. Dabei gibt der Befehl USER oder SETTINGS an, welche Operationsgruppe verwendet wird. Der vollständige Befehl lautet z. B. “fprconsole user add TestUser /FORCED”. Wenn der Befehl unbekannt ist oder nicht alle Parameter angegeben wurden, wird eine kurze Befehlsliste zusammen mit den Parametern angezeigt.

Verwenden Sie den folgenden Link, um die Fingerprint Software und Management Console herunterzuladen:

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

Benutzerspezifische Befehle

Zum Registrieren und Bearbeiten von Benutzern wird der Abschnitt USER verwendet. Wenn der aktuelle Benutzer nicht über Administratorberechtigung verfügt, richtet sich das Verhalten der Console nach dem Sicherheitsmodus der Fingerprint Software. Im komfortablen Modus können Standardbenutzer die Befehle ADD, EDIT und DELETE ausführen. Jedoch kann ein Benutzer nur das ihm zugeordnete Kennwort (das mit seinem Benutzernamen registriert ist) ändern. Im sicheren Modus sind keine Befehle zulässig. Syntax:

`FPRCONSOLE USER` *`Befehl`*

wobei *Befehl* für einen der folgenden Befehle steht: ADD, EDIT, DELETE, LIST, IMPORT, EXPORT.

Tabelle 38.

Befehl	Syntax	Beschreibung	Beispiel

Neuen Benutzer registrieren	`ADD [`*`Benutzername`*
	`[| `*`Domäne`*`\`*`Benutzername`*`]]`
	`[/FORCED]`
		Das Flag /FORCED inaktiviert die Schaltfläche zum Abbrechen innerhalb des Assistenten, so dass die Registrierung erfolgreich abgeschlossen werden muss. Wird kein Benutzername angegeben, wird der aktuelle Benutzername verwendet.	`fprconsole add domain0\testuser`
			`fprconsole add testuser`
			`fprconsole add testuser /FORCED`

Registrierten Benutzer bearbeiten	`EDIT [`*`Benutzername`* `[| `*`Domäne`*`\`*`Benutzername`*`]]`	Wird kein Benutzername angegeben, wird der aktuelle Benutzername verwendet. **Anmerkung:** Der Benutzer, für den Änderungen vorgenommen werden, muss zuerst seinen Fingerabdruck bestätigen.	`fprconsole edit domain0\testuser` `fprconsole edit testuser`

Tabelle 38. (Forts.)

Befehl	Syntax	Beschreibung	Beispiel

Benutzer löschen	`DELETE [Benutzername [| Domäne\Benutzername | /ALL]]`	Das Flag /ALL löscht alle auf diesem Computer registrierten Benutzer. Wird kein Benutzername angegeben, wird der aktuelle Benutzername verwendet.	`fprconsole delete domain0\testuser`
			`fprconsole delete testuser`
			`fprconsole delete /ALL`

Registrierte Benutzer aufzählen	`List`		
Registrierten Benutzer in Datei exportieren	`Syntax: EXPORT Benutzername [| Domäne\Benutzername] Datei`	Dieser Befehl exportiert einen registrierten Benutzer in eine Datei auf dem Festplattenlaufwerk. Der Benutzer kann anschließend über den Befehl IMPORT auf einen anderen Computer oder auf denselben Computer importiert werden, wenn der Benutzer auf diesem gelöscht wurde.	
Registrierten Benutzer importieren	`Syntax: IMPORT Datei`	Beim Import wird der Benutzer aus der angegebenen Datei importiert. **Anmerkung:** Wenn der Benutzer in der Datei bereits auf demselben Computer mit denselben Fingerabdrücken registriert ist, ist nicht sichergestellt, welcher Benutzer bei der Identifikation Vorrang hat.	

Befehle zu globalen Einstellungen

Die globalen Einstellungen der Fingerprint Software können über den Abschnitt SETTINGS geändert werden. Für alle Befehle in diesem Abschnitt ist eine Administratorberechtigung erforderlich. Syntax:

`FPRCONSOLE SETTINGS Befehl`

wobei *Befehl* für einen der folgenden Befehle steht: SECUREMODE, LOGON, CAD, TBX, SSO.

Tabelle 39.

Befehl	Beschreibung	Syntax	Beispiel
Sicherheitsmodus	Diese Einstellung wechselt zwischen dem komfortablen und dem sicheren Modus der Fingerprint Software.	`SECUREMODE 0|1`	Zum Einstellen des komfortablen Modus: `fprconsole settings securemode 0`

Tabelle 39. (Forts.)

Befehl	Beschreibung	Syntax	Beispiel
Art der Anmeldung	Diese Einstellung aktiviert (1) oder inaktiviert (0) die Anmeldeanwendung. Wird der Parameter /FUS verwendet, ist für die Anmeldung der Modus zum schnellen Wechseln zwischen Benutzern (FUS - Fast User Switching) aktiviert, wenn die Computerkonfiguration dies zulässt.	`LOGON 0|1 [/FUS]`	
Strg+Alt+Entf-Nachricht	Diese Einstellung aktiviert (1) oder inaktiviert (0) den Text zum Drücken der Tastenkombination Strg+Alt+Entf während der Anmeldung.	`CAD 0|1`	
Sicherheitsfunktionen beim Einschalten	Diese Einstellung schaltet bei der Einstellung 0 global die Unterstützung für die Sicherheitsfunktionen beim Einschalten in der Fingerprint Software aus. Wenn die Unterstützung für die Sicherheitsfunktionen beim Einschalten ausgeschaltet ist, werden keine Sicherheitsassistenten oder -seiten beim Einschalten angezeigt. Außerdem sind in diesem Fall die BIOS-Einstellungen bedeutungslos.	`TBX 0|1`	
Sicherheitsfunktionen beim Einschalten - SSO (Single Sign-On)	Diese Einstellung aktiviert (1) oder inaktiviert (0) die Verwendung der im BIOS für die Anmeldung verwendeten Fingerabdrücke, um einen Benutzer automatisch anzumelden, wenn dieser im BIOS bestätigt ist.	`SSO 0|1`	

Sicherer Modus vs. komfortabler Modus

Die ThinkVantage Fingerprint Software kann in zwei Sicherheitsmodi ausgeführt werden: dem komfortablen Modus und dem sicheren Modus.

Der komfortable Modus wurde für Heimcomputer entwickelt, bei denen ein hohes Sicherheitsniveau nicht unbedingt erforderlich ist. Alle Benutzer dürfen alle Operationen ausführen, einschließlich dem Bearbeiten von Berechtigungsnachweisen anderer Benutzer und der Möglichkeit, sich am System mit dem Kennwort (ohne Authentifizierung über Fingerabdruck) anzumelden.

Der sichere Modus wurde für Situationen entwickelt, in denen ein hohes Sicherheitsniveau wichtig ist. Besondere Funktionen sind ausschließlich für den

Administrator reserviert. Nur Administratoren können sich ohne zusätzliche Authentifizierung und nur mit dem Kennwort anmelden.

Ein *Administrator* ist ein Mitglied der lokalen Administratorgruppe. Wenn Sie den sicheren Modus einstellen, kann nur ein Administrator wieder in den komfortablen Modus wechseln.

Sicherer Modus – Administrator

Bei der Anmeldung wird im sicheren Modus die folgende Nachricht angezeigt, wenn der falsche Benutzername oder das falsche Kennwort eingegeben wurde: ″Only administrators can log on this computer with user name and password.″ (Nur Administratoren dürfen sich an diesem Computer mit Benutzername und Kennwort anmelden.) Dadurch soll die Sicherheit erhöht und gleichzeitig vermieden werden, dass Hacker Informationen dazu erhalten, warum sie sich nicht anmelden können.

Tabelle 40.

Fingerprints (Fingerabdrücke)	**Beschreibung**
Create a new passport (Neuen Berechtigungsnachweis erstellen)	Administratoren können ihren eigenen Berechtigungsnachweis und den Berechtigungsnachweis für einen Benutzer mit eingeschränkter Berechtigung erstellen.
Edit Passports (Berechtigungsnachweise bearbeiten)	Administratoren können *nur* ihren eigenen Berechtigungsnachweis bearbeiten.
Delete Passport (Berechtigungsnachweis löschen)	Administratoren können die Berechtigungsnachweise von allen Benutzern mit eingeschränkter Berechtigung und anderen Administratoren löschen. Wenn andere Benutzer Sicherheitsfunktionen beim Einschalten verwenden, hat der Administrator die Möglichkeit, Benutzervorlagen zu diesem Zeitpunkt von den Sicherheitsfunktionen beim Einschalten zu entfernen.
Power-on Security (Sicherheitsfunktionen beim Einschalten)	Administratoren können die beim Starten verwendeten Fingerabdrücke von Benutzern mit eingeschränkter Berechtigung und von Administratoren löschen. **Anmerkung:** Bei aktiviertem Startmodus muss mindestens ein Fingerabdruck vorhanden sein.
Settings (Einstellungen)	
Logon settings (Anmeldeeinstellungen)	Administratoren können an allen Anmeldeeinstellungen Änderungen vornehmen.
Protected screen saver (Geschützter Bildschirmschoner)	Administratoren haben Zugriff.
Passport type (Typ des Berechtigungsnachweises)	Administratoren haben Zugriff. - Nur in Verbindung mit Servern relevant.
Security mode (Sicherheitsmodus)	Administratoren können zwischen dem sicheren und dem komfortablen Modus wechseln.
Pro Servers (Pro Server)	Administratoren haben Zugriff. - Nur in Verbindung mit Servern relevant.

Sicherer Modus - Benutzer mit eingeschränkter Berechtigung

Bei einer Windows-Anmeldung müssen sich Benutzer mit eingeschränkter Berechtigung mit ihrem Fingerabdruck anmelden. Wenn das Lesegerät für Fingerabdrücke nicht funktioniert, muss ein Administrator die Einstellung der Fingerprint Software ändern und den komfortablen Modus einstellen, damit der Zugriff über Benutzername und Kennwort möglich wird.

Tabelle 41.

Fingerprints (Fingerabdrücke)	
Create a new passport (Neuen Berechtigungsnachweis erstellen)	Benutzer mit eingeschränkter Berechtigung haben keinen Zugriff.
Edit Passports (Berechtigungsnachweise bearbeiten)	Benutzer mit eingeschränkter Berechtigung können nur ihren eigenen Berechtigungsnachweis bearbeiten.
Delete Passport (Berechtigungsnachweis löschen)	Benutzer mit eingeschränkter Berechtigung können nur ihren eigenen Berechtigungsnachweis löschen.
Power-on Security (Sicherheitsfunktionen beim Einschalten)	Benutzer mit eingeschränkter Berechtigung haben keinen Zugriff.
Settings (Einstellungen)	
Logon settings (Anmeldeeinstellungen)	Benutzer mit eingeschränkter Berechtigung können die Anmeldeeinstellungen nicht ändern.
Protected screen saver (Geschützter Bildschirmschoner)	Benutzer mit eingeschränkter Berechtigung haben Zugriff.
Passport type (Typ des Berechtigungsnachweises)	Benutzer mit eingeschränkter Berechtigung haben keinen Zugriff.
Security mode (Sicherheitsmodus)	Benutzer mit eingeschränkter Berechtigung können die Sicherheitsmodi nicht ändern.
Pro Servers (Pro Server)	Benutzer mit eingeschränkter Berechtigung haben Zugriff. - Nur in Verbindung mit Servern relevant.

Komfortabler Modus - Administrator

Bei einer Windows-Anmeldung können sich Administratoren entweder mit ihrem Benutzernamen und Kennwort oder ihrem Fingerabdruck anmelden.

Tabelle 42.

Fingerprints (Fingerabdrücke)	
Create a new passport (Neuen Berechtigungsnachweis erstellen)	Administratoren können *nur* ihren eigenen Berechtigungsnachweis erstellen.
Edit Passports (Berechtigungsnachweise bearbeiten)	Administratoren können *nur* ihren eigenen Berechtigungsnachweis bearbeiten.
Delete Passport (Berechtigungsnachweis löschen)	Administratoren können *nur* ihren eigenen Berechtigungsnachweis löschen.

Tabelle 42. (Forts.)

Fingerprints (Fingerabdrücke)	
Power-on Security (Sicherheitsfunktionen beim Einschalten)	Administratoren können die beim Starten verwendeten Fingerabdrücke von Benutzern mit eingeschränkter Berechtigung und von Administratoren löschen. **Anmerkung:** Bei aktiviertem Startmodus muss mindestens ein Fingerabdruck vorhanden sein.
Settings (Einstellungen)	
Logon settings (Anmeldeeinstellungen)	Administratoren können an allen Anmeldeeinstellungen Änderungen vornehmen.
Protected screen saver (Geschützter Bildschirmschoner)	Administratoren haben Zugriff.
Passport type (Typ des Berechtigungsnachweises)	Administratoren haben Zugriff. - Nur in Verbindung mit Servern relevant.
Security mode (Sicherheitsmodus)	Administratoren können zwischen dem sicheren und dem komfortablen Modus wechseln.
Pro Servers (Pro Server)	Administratoren haben Zugriff. - Nur in Verbindung mit Servern relevant.

Komfortabler Modus - Benutzer mit eingeschränkter Berechtigung

Bei einer Windows-Anmeldung können sich Benutzer mit eingeschränkter Berechtigung entweder mit ihrem Benutzernamen und Kennwort oder ihrem Fingerabdruck anmelden

Tabelle 43.

Fingerprints (Fingerabdrücke)	
Create a new passport (Neuen Berechtigungsnachweis erstellen)	Benutzer mit eingeschränkter Berechtigung können nur ihren eigenen Berechtigungsnachweis erstellen.
Edit Passports (Berechtigungsnachweise bearbeiten)	Benutzer mit eingeschränkter Berechtigung können nur ihren eigenen Berechtigungsnachweis bearbeiten.
Delete Passport (Berechtigungsnachweis löschen)	Benutzer mit eingeschränkter Berechtigung können nur ihren eigenen Berechtigungsnachweis löschen.
Power-on Security (Sicherheitsfunktionen beim Einschalten)	Benutzer mit eingeschränkter Berechtigung können nur ihre eigenen Fingerabdrücke erstellen.
Settings (Einstellungen)	
Logon settings (Anmeldeeinstellungen)	Benutzer mit eingeschränkter Berechtigung können die Anmeldeeinstellungen nicht ändern.

Tabelle 43. (Forts.)

Fingerprints (Fingerabdrücke)	
Protected screen saver (Geschützter Bildschirmschoner)	Benutzer mit eingeschränkter Berechtigung haben Zugriff.
Passport type (Typ des Berechtigungsnachweises)	Benutzer mit eingeschränkter Berechtigung haben keinen Zugriff. - Nur in Verbindung mit Servern relevant.
Security mode (Sicherheitsmodus)	Benutzer mit eingeschränkter Berechtigung können die Sicherheitsmodi nicht ändern.
Pro Servers (Pro Server)	Benutzer mit eingeschränkter Berechtigung haben Zugriff. - Nur in Verbindung mit Servern relevant.

ThinkVantage Fingerprint Software und Novell Netware Client

Die Benutzernamen und Kennwörter für die ThinkVantage Fingerprint Software und Novell müssen übereinstimmen.

Wenn auf Ihrem Computer die ThinkVantage Fingerprint Software installiert ist und Sie anschließend den Novell Netware Client installieren, werden möglicherweise einige Einträge in der Registrierungsdatenbank überschrieben. Wenn Sie Probleme bei der Anmeldung der ThinkVantage Fingerprint Software feststellen, rufen Sie das Fenster mit den Einstellungen für die Anmeldung auf, und aktivieren Sie den Logon Protector wieder.

Wenn auf Ihrem Computer der Novell Netware Client installiert ist, Sie sich aber vor der Installation der ThinkVantage Fingerprint Software beim Client angemeldet haben, wird das Fenster für die Novell-Anmeldung angezeigt. Geben Sie die angeforderten Informationen ein.

Gehen Sie wie folgt vor, um die Einstellung für den Logon Protector zu ändern:

- Starten Sie das Control Center (Steuerzentrale).
- Klicken Sie auf **Settings** (Einstellungen).
- Klicken Sie auf **Logon settings** (Anmeldeeinstellungen).
- Aktivieren oder inaktivieren Sie den Logon Protector.

  Wenn Sie die Anmeldung mit Fingerabdrücken verwenden möchten, aktivieren Sie das Markierungsfeld ″Replace Windows logon with fingerprint-protected logon″ (Windows-Anmeldung durch Anmeldung mit Fingerabdrücken ersetzen). Beachten Sie, dass das Aktivieren und Inaktivieren des Logon Protector einen Neustart erfordert.
- Aktivieren oder inaktivieren Sie das schnelle Wechseln zwischen Benutzern, wenn dies vom System unterstützt wird.
- (Optionale Funktion) Aktivieren oder inaktivieren Sie die automatische Anmeldung für Benutzer, die über die Bootsicherheitsfunktionen beim Einschalten authentifiziert sind.

- Legen Sie die Novell-Anmeldeeinstellungen fest. Die folgenden Einstellungen stehen bei der Anmeldung an einem Novell-Netzwerk zur Verfügung:
  - **Activated** (Aktiviert)

    Die ThinkVantage Fingerprint Software stellt automatisch bekannte Berechtigungsnachweise zur Verfügung. Schlägt die Novell-Anmeldung fehl, wird das Fenster für die Novell Client-Anmeldung mit der Aufforderung, die richtigen Daten einzugeben, angezeigt.
  - **Ask during logon** (Während Anmeldung abfragen)

    Die ThinkVantage Fingerprint Software zeigt das Fenster für die Novell Client-Anmeldung mit der Aufforderung, die Anmeldedaten einzugeben, an.
  - **Disabled** (Inaktiviert)

    Die ThinkVantage Fingerprint Software versucht keine Novell-Anmeldung.

Anhang A. Befehlszeilenparameter für die Installation

Das Microsoft Windows-Installationsprogramm bietet mehrere Administratorfunktionen über Befehlszeilenparameter.

Verfahren und Befehlszeilenparameter für die administrative Installation

Das Windows-Installationsprogramm kann eine administrative Installation einer Anwendung oder eines Produkts in einem Netz zur Verwendung durch eine Arbeitsgruppe oder zu Anpassungszwecken ausführen. Beim Installationspaket für Rescue and Recovery werden bei einer administrativen Installation die Installationsquellendateien an einer bestimmten Speicherposition entpackt.

- Um eine administrative Installation auszuführen, führen Sie das Installationspaket über die Befehlszeile mit dem Parameter `/a` aus:

  ```
  Setup.exe /a
  ```

Eine administrative Installation stellt einen Assistenten bereit, der den Administrator auffordert, die Speicherpositionen zum Entpacken der Installationsdateien anzugeben. In der Standardeinstellung werden die Dateien auf Laufwerk C:\ extrahiert. Sie können eine andere Position auf anderen Laufwerken als C:\ auswählen (andere lokale Laufwerke, zugeordnete Netzlaufwerke usw.). Sie können in diesem Schritt auch neue Verzeichnisse erstellen.

- Um eine administrative Installation unbeaufsichtigt auszuführen, können Sie das öffentliche Merkmal TARGETDIR in der Befehlszeile festlegen, um folgende Position für die Extraktion anzugeben:

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

  Oder

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

Nachdem eine administrative Installation ausgeführt wurde, kann der Administrator die Quellendateien anpassen, wie z. B. in der Datei TVT.TXT Einstellungen hinzufügen.

MSIEXEC.EXE verwenden

Um nach dem Vornehmen von Anpassungen eine Installation mit Hilfe der entpackten Quellendatei auszuführen, muss der Benutzer das Programm MSIEXEC.EXE über die Befehlszeile aufrufen und den Namen der entpackten *.MSI-Datei angeben. MSIEXEC.EXE ist das ausführbare Programm des Installationsprogramms, das verwendet wird, um die Installationspakete zu interpretieren und die Produkte auf Zielsystemen zu installieren.

```
msiexec /i "C:\Windows-Ordner\Profiles\Benutzername\
Personal\MySetups\Projektname\Produktkonfiguration\Releasename\
DiskImages\Disk1\Produktname.msi"
```

Anmerkung: Geben Sie den oben angegebenen Befehl in eine einzige Zeile ein, ohne Leerzeichen nach den Schrägstrichen.
Tabelle 44 auf Seite 152 enthält eine Beschreibung der verfügbaren Befehlszeilenparameter, die mit dem Programm MSIEXEC.EXE verwendet werden können, sowie Beispiele zur Verwendung.

Tabelle 44. Befehlszeilenparameter

Parameter	Beschreibung
/I *Paket* oder *Produktcode*	Verwenden Sie zur Installation des Produkts folgendes Format: `Othello:msiexec /i "C:\ Windows-Ordner\Profiles\ Benutzername\Personal\MySetups \Othello\Trial Version\ Release\DiskImages\Disk1\ Othello Beta.msi"` Der Produktcode verweist auf die GUID, die im Produktcodemerkmal in der Projektansicht für das Produkt automatisch generiert wird.
/a *Paket*	Mit dem Parameter **/a** können Benutzer mit Administratorrechten ein Produkt im Netzwerk installieren.
/x *Paket* oder *Produktcode*	Mit dem Parameter **/x** wird ein Produkt deinstalliert.
/L [i|w|e|a|r|u|c|m|p|v|+] *Protokolldatei*	Mit dem Parameter **/L** wird der Pfad zur Protokolldatei angegeben. Die folgenden Flags geben an, welche Informationen in der Protokolldatei gespeichert werden sollen: • **i** protokolliert Statusnachrichten • **w** protokolliert nicht schwerwiegende Warnungen • **e** protokolliert Fehlernachrichten • **a** protokolliert den Beginn von Aktionsfolgen • **r** protokolliert aktionsspezifische Aufzeichnungen • **u** protokolliert Benutzeranforderungen • **c** protokolliert die Schnittstellenparameter für den Erstbenutzer • **m** protokolliert Nachrichten zur Überschreitung der Speicherkapazität • **p** protokolliert Terminaleinstellungen • **v** protokolliert die Einstellung für ausführliche Ausgabe • **+** wird einer vorhandenen Datei hinzugefügt • * ist ein Platzhalterzeichen, mit dem Sie alle Informationen protokollieren können (außer der Einstellung für ausführliche Ausgabe)
/q [n|b|r|f]	Mit dem Parameter /q wird die Stufe der Benutzerschnittstelle in Verbindung mit den folgenden Flags angegeben: • mit **q** oder qn wird keine Benutzerschnittstelle erstellt • mit **qb** wird eine Basisbenutzerschnittstelle erstellt Mit den folgenden Benutzerschnittstelleneinstellungen wird am Ende der Installation ein Modaldialogfenster angezeigt: • mit **qr** wird die Benutzerschnittstelle verkleinert angezeigt • mit **qf** wird die Benutzerschnittstelle in Vollgröße angezeigt • mit **qn+** wird die Benutzerschnittstelle nicht angezeigt • mit **qb+** wird eine Basisbenutzerschnittstelle angezeigt
/? oder /h	Mit einem dieser beiden Befehle wird der Copyrightvermerk zum Windows-Installationsprogramm angezeigt.

Tabelle 44. Befehlszeilenparameter (Forts.)

Parameter	Beschreibung

TRANSFORMS	Mit dem Befehlszeilenparameter **TRANSFORMS** können Sie Umsetzungen angeben, die Sie für Ihr Basispaket anwenden möchten. Ihr Umsetzungsaufruf für die Befehlszeile könnte etwa die folgende Form aufweisen:
	`msiexec /i "C:\Windows-Ordner\`
	`Profiles\Benutzername\Personal \MySetups\`
	`Your Project Name\Trial Version\`
	`My Release-1 \DiskImages\Disk1\`
	`ProductName.msi" TRANSFORMS="New Transform 1.mst"`
	
	Sie können mehrere Umsetzungen mit einem Semikolon trennen. Verwenden Sie daher keine Semikolons in den Namen Ihrer Umsetzungen, da das Windows-Installationsprogramm diese Zeichen nicht richtig interpretiert.

Merkmale	Alle öffentlichen Merkmale können über die Befehlszeile festgelegt oder geändert werden. Öffentliche Merkmale unterscheiden sich von privaten Merkmalen dadurch, dass sie in Großbuchstaben angegeben sind. *FIRMENNAME* ist zum Beispiel ein öffentliches Merkmal.
	
	Zum Festlegen eines Merkmals über die Befehlszeile verwenden Sie die folgende Syntax:
	`MERKMAL=WERT`
	
	Wenn Sie den Wert von *FIRMENNAME* ändern möchten, geben Sie Folgendes ein:
	`msiexec /i "C:\Windows-Ordner\`
	`Profiles\Benutzername\Personal \`
	`MySetups\Projektname\`
	`Trial Version\My Release-1 \`
	`DiskImages\Disk1\Produktname.msi"`
	`FIRMENNAME="InstallShield"`

Anhang B. Einstellungen und Werte für die Datei TVT.TXT

Die im Folgenden angegebenen Standardwerte sind die empfohlenen Einstellungen. Bei anderen Konfigurationen können diese Werte abweichen (z. B. bei vorinstallierten Konfigurationen, Web-Downloads oder OEM-Versionen). Für die Installation sind folgende Konfigurationseinstellungen verfügbar:

Tabelle 45. Einstellungen und Werte für die Datei TVT.TXT

Einstellung	**Werte**
AccessFile (siehe auch GUIGroup)	*Dateiname*, wobei *Dateiname* der vollständig qualifizierte Pfad zu einer Datei ist, die die Namen von lokalen Windows-Gruppen (keine Domänennamen) enthält, die Operationen mit Rescue and Recovery ausführen dürfen. Wenn diese Datei leer ist oder fehlt, können alle Benutzer, die sich am Computer anmelden können, die GUI aufrufen und Befehlszeilenoperationen ausführen. In der Standardeinstellung ist diese Datei leer.
BackupPartition	0 = Erste Partition auf dem angegebenen Laufwerk 1 = Zweite Partition auf dem angegebenen Laufwerk 2 = Dritte Partition auf dem angegebenen Laufwerk 3 = Vierte Partition auf dem angegebenen Laufwerk Die Laufwerke werden in folgenden Abschnitten angegeben: [BackupDisk] = das lokale Festplattenlaufwerk [SecondDisk] = das zweite lokale Festplattenlaufwerk [USBDisk] = USB-Festplattenlaufwerk **Anmerkung:** Die Partitionen müssen bereits vorhanden sein. Wenn nicht, wird der Benutzer aufgefordert, die Partition zu erstellen (wenn auf dem in der Benutzerschnittstelle ausgewählten Ziellaufwerk mehrere Partitionen vorhanden sind).
BatteryPercentRequired	Umfasst den Bereich 0 bis 100. Der Standardwert ist 100.
CPUPriority	*n*, wobei *n* = 1 bis 5. 1 steht für die niedrigste Priorität und 5 für die höchste Priorität. Der Standardwert ist 3.
CustomPartitions	0 = Jede Partition sichern 1 = In jeder Partition nach ″IncludeInBackup″ suchen
DisableAnalyze	0 = Das Archiv ″optionEnable″ zur Optimierung von Sicherungsspeicher anzeigen 1 = Diese Option ausblenden Der Standardwert ist 0.
DisableArchive	0 = Archiv aktivieren 1 = Archiv ausblenden Der Standardwert ist 0.

Tabelle 45. Einstellungen und Werte für die Datei TVT.TXT (Forts.)

Einstellung	Werte
DisableBackupLocation	0 = Alle Ziele aktivieren 0x01 = Lokales Ziel inaktivieren 0x02 = CD-/DVD-Laufwerk inaktivieren 0x08 = USB-Festplattenlaufwerk inaktivieren 0x10 = Netzwerk inaktivieren 0x20 = Zweites Festplattenlaufwerk inaktivieren 1 = Archiv ausblenden Sie können diese Werte kombinieren, um mehrere Positionen zu inaktivieren. Der Wert 0x0A inaktiviert z. B. das CD-/DVD- und das USB-Festplattenlaufwerk, und der Wert 0x38 inaktiviert das USB-Festplattenlaufwerk, das Netzwerk und das zweite Festplattenlaufwerk. Wenn Sie nur die Sicherung auf dem lokalen Festplattenlaufwerk zulassen möchten, können Sie 0x3A (oder 0xFE) verwenden.
DisableBootDisc	0 = Bei der Erstellung von CD-/DVD-Sicherungen eine bootfähige CD erstellen 1 = Keine bootfähige CD erstellen Die Funktion ″DisableBootDisc″ ist nur für Sicherungen vorgesehen, und nicht zur Archivierung.
DisableDelete	0 = Option zum Löschen von Sicherungen anzeigen 1 = Diese Option ausblenden Der Standardwert ist 0.
DisableExclude	0 = Option zum Ausschließen von Dateien/Ordnern anzeigen 1 = Option zum Ausschließen von Dateien/Ordnern ausblenden Der Standardwert ist 0.
DisableLiveUpdate	0 = Option ″LiveUpdate″ anzeigen 1 = Diese Option ausblenden Der Standardwert ist 0.
DisableMigrate	0 = Datei zum Erstellen einer Migrationsdatei aus einer Sicherung anzeigen 1 = Diese Option ausblenden Der Standardwert ist 0.
DisableRestore	0 = Wiederherstellung aktivieren 1 = Wiederherstellung ausblenden Der Standardwert ist 0.

Tabelle 45. Einstellungen und Werte für die Datei TVT.TXT (Forts.)

Einstellung	Werte
DisableSchedule	0 = Option für Sicherungszeitplan anzeigen 1 = Option für Sicherungszeitplan ausblenden Der Standardwert ist 0.
DisableSFR	0 = Wiederherstellung von einzelnen Dateien aktivieren 1 = Wiederherstellen von einzelnen Dateien ausblenden Der Standardwert ist 0.
DisableSingleStorage	0 = Option für Einzelspeicherung anzeigen 1 = Diese Option ausblenden Der Standardwert ist 0.
DisableViewBackups	0 = Option zum Anzeigen von Sicherungen anzeigen 1 = Diese Option ausblenden Der Standardwert ist 0.
DisableVerifyDisc	0 = Optische Schreiboperationen prüfen 1 = Optische Schreiboperationen nicht prüfen Der Standardwert ist 0.
Exclude (siehe auch Include)	0 = GUIEXCLD.TXT nicht anwenden 1 = GUIEXCLD.TXT.txt anwenden **Anmerkungen:** 1. Das Ausschließen (″Exclude″) und Auswählen von Dateien kann vor der Installation definiert und während des Installationsprozesses angewendet werden. 2. ″Exclude″ und ″Include″ können nicht beide den Wert ″1″ aufweisen.
GUIGroup (siehe auch AccessFile)	*Gruppe*, wobei *Gruppe* eine lokale Windows-Gruppe (keine Domänengruppe) ist, die Operationen mit Rescue and Recovery ausführen darf. Die Liste der Berechtigungsgruppen wird in einer Datei gespeichert, die durch den Eintrag ″AccessFile″ definiert ist.
HideAdminBackups	0 = Administratorsicherungen in Liste anzeigen 1 = Administratorsicherungen ausblenden Der Standardwert ist 0.
HideBaseFromDelete	0 = Im Dialog zum Löschen von Sicherungen Basissicherung anzeigen 1 = Im Dialog für das Löschen von Sicherungen Basissicherung ausblenden Der Standardwert ist 0.

Tabelle 45. Einstellungen und Werte für die Datei TVT.TXT (Forts.)

Einstellung	Werte
HideBootUSBDialog	0 = Eingabeaufforderung anzeigen, wenn auf ein nicht bootfähiges USB-Festplattenlaufwerk gesichert wird 1 = Eingabeaufforderung ausblenden Der Standardwert ist 0.
HideDiffFileSystems	0 = FAT-/FAT32-Partitionen beim Wiederherstellen/Sichern von Dateien anzeigen 1 = FAT-/FAT32-Partitionen beim Wiederherstellen/Sichern von Dateien ausblenden Der Standardwert ist 0.
HideCSSEncrypt	0 = Option zum Verschlüsseln von Sicherungen mit Client Security Solution anzeigen 1 = Option zum Verschlüsseln von Sicherungen mit Client Security Solution ausblenden Der Standardwert ist 0.
HideGUI	0 = GUI für berechtigte Benutzer anzeigen 1 = GUI für alle Benutzer ausblenden
HideLocationNotFoundMessage	0 = Dialognachricht anzeigen 1 = Dialognachricht ausblenden Der Standardwert ist 0.
HideLockHardDisk	0 = Option zum Schützen der Festplatte vor einer Beschädigung des Master-Bootsatzes anzeigen 1 = Diese Option ausblenden Der Standardwert ist 1.
HideMissedBackupMessages	0 = Dialogfenster anzeigen 1 = Dialogfenster ausblenden Der Standardwert ist 1.
HideNoBatteryMessage	0 = Nachricht anzeigen 1 = Nachricht ausblenden Der Standardwert ist 1.
HideNumBackupsDialog	0 = Dialogfenster, in dem die Benutzer angezeigt werden, die eine bestimmte maximale Anzahl von Sicherungen ausgeführt haben, anzeigen 1 = Dialogfenster, in dem die Benutzer angezeigt werden, die eine bestimmte maximale Anzahl von Sicherungen ausgeführt haben, ausblenden Der Standardwert ist 1.

Tabelle 45. Einstellungen und Werte für die Datei TVT.TXT (Forts.)

Einstellung	Werte
HidePowerLossBackupMessage	0 = Nachricht über Spannungsverlust bei der Sicherung anzeigen 1 = Nachricht ausblenden Der Standardwert ist 0.
HidePasswordPersistence	0 = GUI ausblenden 1 = GUI anzeigen Der Standardwert ist 0.
HidePasswordProtect	0 = Markierungsfeld für Kennwortschutz anzeigen 1 = Markierungsfeld für Kennwortschutz ausblenden Der Standardwert ist 0.
HideSuspendCheck	0 = Markierungsfeld zur Wiederaufnahme des Betriebs aus dem Bereitschaftsmodus oder aus dem Hibernationsmodus anzeigen 1 = Markierungsfeld ausblenden Der Standardwert ist 1.
Include (siehe auch Exclude)	0 = GUIINCLD.TXT nicht anwenden 1 = GUIINCLD.TXT anwenden und die Option zum Festlegen der einzuschließenden (″Include″) Dateien und Ordner anzeigen **Anmerkungen:** 1. Das Ausschließen (″Exclude″) und Auswählen von Dateien kann vor der Installation definiert und während des Installationsprozesses angewandt werden. 2. ″Exclude″ und ″Include″ können nicht beide den Wert ″1″ aufweisen.
LocalBackup2Location	*x**Ordnername*, wobei *x* der Laufwerkbuchstabe und *Ordnername* der vollständig qualifizierte Name eines Ordners ist. Der Standardwert lautet: *Erste Partition auf dem zweiten Laufwerk*:\IBMBackupData **Anmerkungen:** 1. Da der Laufwerkbuchstabe sich ändern kann, ordnet Rescue and Recovery einer Partition bei der Installation einen Laufwerkbuchstaben zu und verwendet anschließend die Partitionsinformationen, und nicht den Laufwerkbuchstaben. 2. Dies ist das Adressfeld des Eintrags `TaskParameters`.
LockHardDisk	0 = Festplatte nicht sperren, um den Master-Bootsatz zu schützen 1 = Festplatte sperren Der Standardwert ist 0.
MaxBackupSizeEnforced	*x*, wobei *x* die Speicherkapazität in GB ist. Dieser Wert bedeutet nicht, dass eine Sicherung diesen Schwellenwert nicht überschreiten kann. Wenn der Schwellenwert überschritten wird, wird der Benutzer allerdings bei der nächsten On Demand Sicherung in Bezug auf die Größe der Datei gewarnt. Der Standardwert ist 0.

Tabelle 45. Einstellungen und Werte für die Datei TVT.TXT (Forts.)

Einstellung	Werte
MaxNumberOf IncrementalBackups	Standardwert = 5, Mindestwert = 2, Höchstwert = 32
MinAnalyzeFileSize *n*	Hierbei ist *n* die Mindestgröße für Dateien in MB, die dem Benutzer in der Anzeige zur Optimierung des Sicherungsspeicherbereichs angezeigt werden. Der Standardwert ist 20.
NetworkUNCPath	Ein freigegebenes Netzwerkverzeichnis im folgenden Format: *\\Computername\freigegebener Ordner* Kein Standardwert vorhanden. **Anmerkung:** Diese Position wird nicht durch den Dateifiltertreiber geschützt.
NetworkUNCPath	*freigegebenes Serververzeichnis*, zum Beispiel \\SERVER\FREIGABEVERZ\ORDNER
NumMinutes	*x*, das heißt, die Task wird nach *x* Minuten ausgeführt.
PasswordRequired	0 = Kein Kennwort zum Aufrufen der Umgebung von Rescue and Recovery erforderlich 1 = Kennwort zum Aufrufen der Umgebung von Rescue and Recovery erforderlich
PDAPreRestore	*cmd*, wobei *cmd* ein vollständig qualifizierter Pfad zu dem Programm ist, das vor einer Wiederherstellungsoperation in der Umgebung von Rescue and Recovery ausgeführt werden soll.
PDAPreRestore *n*	*cmd*, wobei *cmd* ein vollständig qualifizierter Pfad zu dem Programm ist, das vor einer Wiederherstellungsoperation in der Umgebung von Rescue and Recovery ausgeführt werden soll.
PDAPreRestoreParameters	Die in dem Programm "PDARestore" zu verwendenden Parameter.
PDAPreRestoreParameters *n*	Die in dem Programm "PDARestore" zu verwendenden Parameter.
PDAPreRestoreShow	0 = Task ausblenden 1 = Task anzeigen
PDAPreRestoreShow *n*	0 = Task ausblenden 1 = Task anzeigen
PDAPostRestore	*cmd*, wobei *cmd* ein vollständig qualifizierter Pfad zu dem Programm ist, das vor einer Wiederherstellungsoperation in der Umgebung von Rescue and Recovery ausgeführt werden soll.
PDAPostRestore *n*	*cmd*, wobei *cmd* ein vollständig qualifizierter Pfad zu dem Programm ist, das vor einer Wiederherstellungsoperation in der Umgebung von Rescue and Recovery ausgeführt werden soll.
PDAPostRestoreParameters	Die in dem Programm "PDARestore" zu verwendenden Parameter.
PDAPostRestoreParameters *n*	Die in dem Programm "PDARestore" zu verwendenden Parameter.
PDAPostRestoreShow	0 = Task ausblenden 1 = Task anzeigen
PDAPostRestoreShow *n*	0 = Task ausblenden 1 = Task anzeigen

Tabelle 45. Einstellungen und Werte für die Datei TVT.TXT (Forts.)

Einstellung	Werte
Post (siehe auch PostParameters)	*cmd*, wobei *cmd* ein vollständig qualifizierter Pfad zu einer ausführbaren Datei ist, die nach der primären Task ausgeführt werden soll.
Post (siehe auch PostParameters) *n*	Hierbei ist *n* die Sicherungsnummer: 0, 1, 2, 3 ... 32. *cmd*, wobei *cmd* ein vollständig qualifizierter Pfad zu einer ausführbaren Datei ist, die nach der primären Task ausgeführt werden soll. Zum Beispiel: • Post0=command.bat *Pfad* Diese Datei wird nach der Basissicherung ausgeführt • Post1=command.bat *Pfad* Diese Datei wird nach einer inkrementellen Sicherung ausgeführt **Anmerkung:** Diese Einstellung gilt nur für Sicherungen.
PostParameters (siehe auch Post)	*cmd*, wobei *cmd* ein vollständig qualifizierter Pfad zu einer ausführbaren Datei ist, die nach der primären Task ausgeführt werden soll. Diese Einstellung gilt nur für Sicherungen.
PostParameters *n* (siehe auch Post)	*parms*, wobei *parms* die in der Post-Task zu verwendenden Parameter sind.
	parms, wobei *parms* die in der Post-Task zu verwendenden Parameter sind. **Anmerkung:** Diese Einstellung gilt nur für Sicherungen.
PostRestore	*cmd*, wobei *cmd* ein vollständig qualifizierter Pfad zu dem Programm ist, das nach einer Wiederherstellungsoperation unter Windows ausgeführt werden soll.
PostRestore *n*	*cmd*, wobei *cmd* ein vollständig qualifizierter Pfad zu dem Programm ist, das nach einer Wiederherstellungsoperation unter Windows ausgeführt werden soll.
PostRestoreParameters	Die in dem Programm "PostRestore" zu verwendenden Parameter.
PostRestoreParameters *n*	Die in dem Programm "PostRestore" zu verwendenden Parameter.
PostRestoreShow	0 = Wiederherstellungstask ausblenden 1 = Wiederherstellungstask anzeigen
PostRestoreShow *n*	0 = Wiederherstellungstask ausblenden 1 = Wiederherstellungstask anzeigen
PostShow	0 = Post-Task ausblenden 1 = Post-Task anzeigen Der Standardwert ist 0.

Tabelle 45. Einstellungen und Werte für die Datei TVT.TXT (Forts.)

Einstellung	Werte
PostShow *n*	0 = Post-Task ausblenden 1 = Post-Task anzeigen Der Standardwert ist 0. Hierbei ist *n* die Sicherungsnummer: 0, 1, 2, 3 ... 32. **Anmerkung:** Diese Einstellung gilt nur für Sicherungen.
Pre (siehe auch PreParameters)	*cmd*, wobei *cmd* ein vollständig qualifizierter Pfad zu einer ausführbaren Datei ist, die vor der primären Task ausgeführt werden soll.
Pre (siehe auch PreParameters) *n*	Hierbei ist *n* die Sicherungsnummer: 0, 1, 2, 3 ... 32. *cmd*, wobei *cmd* ein vollständig qualifizierter Pfad zu einer ausführbaren Datei ist, die vor der primären Task ausgeführt werden soll. Zum Beispiel: • Pre0=command.bat *Pfad* Diese Datei wird vor der Basissicherung ausgeführt • Pre1=command.bat *Pfad* Diese Datei wird vor einer inkrementellen Sicherung ausgeführt **Anmerkung:** Diese Einstellung gilt nur für Sicherungen.
PreParameters (siehe auch Pre)	Hierbei sind *parms* die in der Pre-Task zu verwendenden Parameter.
PreRejuvenate *cmd*	Hierbei ist *cmd* der vollständig qualifizierte Pfad zu dem Programm, das vor einer Erneuerungsoperation unter Windows ausgeführt werden soll.
PreRejuvenateParameters *parms*	Hierbei sind *parms* die im Programm "PreRejuvenate" zu verwendenden Parameter.
PreRejuvenateShow	0 = Task ausblenden 1 = Task anzeigen
PostRejuvenate *cmd*	*cmd*, wobei *cmd* ein vollständig qualifizierter Pfad zu dem Programm ist, das nach einer Erneuerungsoperation unter Windows ausgeführt werden soll.
PostRejuvenateParameters *parms*	Hierbei sind *parms* die im Programm "PostRejuvenate" zu verwendenden Parameter.
PostRejuvenateShow	0 = Task ausblenden 1 = Task anzeigen
PreShow	0 = Pre-task ausblenden 1 = Pre-task anzeigen Der Standardwert ist 1.
PreShow *n*	Hierbei ist *n* die Sicherungsnummer: 0, 1, 2, 3 ... 32. *cmd*, wobei *cmd* ein vollständig qualifizierter Pfad zu einer ausführbaren Datei ist, die vor der primären Task ausgeführt werden soll. **Anmerkung:** Diese Einstellung gilt nur für Sicherungen.

Tabelle 45. Einstellungen und Werte für die Datei TVT.TXT (Forts.)

Einstellung	Werte
PreWinRestore	*cmd*, wobei *cmd* ein vollständig qualifizierter Pfad zu dem Programm ist, das vor einer Wiederherstellungsoperation unter Windows ausgeführt werden soll.
PreWinRestore *n*	*cmd*, wobei *cmd* ein vollständig qualifizierter Pfad zu dem Programm ist, das vor einer Wiederherstellungsoperation unter Windows ausgeführt werden soll.
PreWinRestoreParameters	Die in dem Programm "PreWinRestore" zu verwendenden Parameter.
PreWinRestoreParameters *n*	Die in dem Programm "PreWinRestore" zu verwendenden Parameter.
PreWinRestoreShow	0 = Post-Task ausblenden 1 = Post-Task anzeigen
PreWinRestoreShow *n*	0 = Post-Task ausblenden 1 = Post-Task anzeigen
ResumePowerLossBackup	0 = Den Sicherungsvorgang nicht wieder aufnehmen, wenn während der letzten Sicherung der Netzstrom ausgefallen ist. 1 = Sicherung wieder aufnehmen Der Standardwert ist 1.
RunBaseBackup	0 = Basissicherung nicht ausführen 1 = Basissicherung ausführen Der Standardwert ist 0. `runbasebackuplocation=(Position)` Gültige Werte sind: L = Lokal U = USB N = Netzwerk S = Zweites Festplattenlaufwerk C = CD
ScheduleDayOfTheMonth	*x*, wobei *x* = 1 bis 28 oder 35 (nur für monatliche Sicherungen). 35 = der letzte Tag im Monat.

Tabelle 45. Einstellungen und Werte für die Datei TVT.TXT (Forts.)

Einstellung	Werte
ScheduleDayOfTheWeek	Nur für wöchentliche Sicherungen 0 = Sonntag 1 = Montag 2 = Dienstag 3 = Mittwoch 4 = Donnerstag 5 = Freitag 6 = Samstag Der Standardwert ist 0 (Sonntag).
ScheduleFrequency	0 = Nicht geplant 1 = Täglich 2 = Wöchentlich 3 = Monatlich Der Standardwert ist 2 (wöchentlich).
ScheduleHour	*x*, wobei *x* = 0 bis 23, und 0 = 12.00 Uhr, 12 = mittags und 23 = 23.00 Uhr. Der Standardwert ist 0.
ScheduleMinute	*x*, wobei *x* = 0 bis 59; diese inkrementelle Zahl steht für die Minute, zu der die inkrementelle Sicherung gestartet wird. Der Standardwert ist 0.
ScheduleWakeForBackup	0 = Computer nicht für geplante Sicherungen starten 1 = Desktop-Computer für geplante Sicherungen starten, Notebook-Computer nicht starten 2 = Computer immer starten, unabhängig davon, ob es sich um einen Desktop- oder um einen Notebook-Computer handelt Der Standardwert ist 2. **Anmerkung:** Wenn ein Notebook-Computer für eine Sicherung gestartet wird, jedoch keine Stromversorgung festgestellt wird, wird er wieder in den Bereitschaftsmodus oder in den Hibernationsmodus versetzt, bevor der Sicherungsvorgang beginnt.

Tabelle 45. Einstellungen und Werte für die Datei TVT.TXT (Forts.)

Einstellung	Werte
ScheduleMode	*x*, wobei *x* eine Bitmaske mit einem der folgenden Werte ist: • 0 = Nicht geplant • 0x01 = Minütlich • 0x04 = Wöchentlich • 0x08 = Monatlich • 0x10 = Jedes Mal, wenn ein Service gestartet wird (in der Regel bei jedem Bootvorgang) • 0x20 = Das System nimmt den Betrieb aus dem Bereitschaftsmodus/Hibernationsmodus wieder auf • 0x40 = Ein USB-Festplattenlaufwerk wird angeschlossen • 0x80 = Ein Netzwerk wird angeschlossen • 0x100 = Die Verbindung zu einem Netzwerk wird getrennt • 0x200 = Das BIOS-Kennwort wird zurückgesetzt • 0x400 = Die Steuerplatine wird ersetzt Dieser Parameter wird automatisch aktualisiert, wenn der Benutzer in der GUI Werte ändert. Wenn der Wert für ″ScheduleFrequency″ entweder durch manuelle Änderungen der Datei TVT.TXT oder durch Scripterstellung geändert wird, wird dieser Parameter mit dem Befehl RELOADSCHED aktualisiert. **Anmerkung:** Die Bits `USB-Festplattenlaufwerk wird angeschlossen` oder `Netzwerk wird angeschlossen` müssen für die automatische Synchronisation von Sicherungen auf einem lokalen Festplattenlaufwerk mit einem USB-Festplattenlaufwerk oder mit einem Netzwerk nicht festgelegt sein.
SkipLockedFiles	0 = Dialogfenster anzeigen, wenn eine gesperrte oder beschädigte Datei erkannt wird 1 = Gesperrte oder beschädigte Dateien immer überspringen
SPBackupLocation=2	Dient zur Bestimmung der Sicherung der Servicepartition. Wenn diese Einstellung nicht vorgenommen wird, wird die Standardservicepartition mit einer Speicherkapazität von 500 MB wiederhergestellt, wenn von einer CD gebootet wird oder wenn von einer CD wiederhergestellt wird, und andere Daten werden von der Servicepartition gelöscht.
Task	*cmd*, wobei *cmd* ein vollständig qualifizierter Pfad zu dem Programm ist, das als primäre Task ausgeführt werden soll. **Anmerkung:** Die Höchstanzahl der Tasks ist 50.
TaskParameter	*parms* sind die in der Task zu verwendenden Parameter.
TaskShow	0 = Task ausblenden 1 = Task anzeigen Der Standardwert ist 0.
UUIDMatchRequired	0 = Keine übereinstimmende Computer-UUID erforderlich 1 = Übereinstimmende Computer-UUID erforderlich **Anmerkung:** Für Sicherungen, die erstellt wurden, als der Wert für UUIDMatchRequired ″1″ betrug, ist weiterhin eine UUID-Übereinstimmung erforderlich, auch wenn diese Einstellung später geändert wird.

Tabelle 45. Einstellungen und Werte für die Datei TVT.TXT (Forts.)

Einstellung	Werte
Yield	*n*, wobei *n* ein Wert von 0 bis 8 ist. Der Wert 0 bedeutet, dass Rescue and Recovery keinen Yield-Wert verwendet. Der Wert 8 bedeutet, dass Rescue and Recovery den höchsten Yield-Wert verwendet. **Anmerkung:** Bei einem höheren Yield-Wert sinkt die Sicherungsleistung schrittweise; die interaktive Leistung wird hingegen besser. Der Standardwert ist 0.

Nach der Installation von Rescue and Recovery können folgende Konfigurationseinstellungen in der Datei TVT.TXT geändert werden, die sich im Installationsverzeichnis befindet. Die Einstellungen werden mit den während der Installation zugeordneten Werten initialisiert.

Sicherung und Wiederherstellung mit der Datei TVT.TXT

Zur Unterstützung der unbeaufsichtigten Installation ist die Konfiguration der Sicherung und der Wiederherstellung bei Rescue and Recovery in einer externen Datei (*TVT.TXT*) definiert, die vor der Installation bearbeitet wird. Die Datei TVT-.TXT entspricht dem Windows-Standardformat für INI-Dateien, das heißt, die Daten sind in Abschnitte gegliedert, die durch eckige Klammern (″[]″) begrenzt sind und die in jeder Zeile einen Eintrag im Format “Einstellung=Wert” enthalten. Rescue and Recovery verwendet den Produktnamen als Abschnittsüberschrift (z. B. Rapid Restore Ultra). Darüber hinaus kann die Datei zum Ein-/Ausschließen durch Filter vor der Installation definiert und während der Installation angewandt werden.

Wenn der IT-Administrator Sicherungen mit Einstellungen anpassen möchte, muss er die Datei TVT.TXT bearbeiten, die sich im Installationsverzeichnis befindet. Der günstigste Zeitpunkt dazu ist vor der Installation von Rescue and Recovery oder aber nach dieser Installation, jedoch vor der ersten Sicherung. An jeder Sicherungsposition befindet sich eine TVT.TXT-Datei. Vor der ersten Sicherung ist nur eine einzige TVT.TXT-Datei vorhanden. Wenn Sie so vorgehen, enthalten alle Sicherungen alle Änderungen, ohne dass Probleme mit der Version der TVT.TXT-Dateien und mit der Synchronisation auftreten. Manchmal muss die TVT.TXT-Datei nach einer Sicherung bearbeitet werden. In diesem Fall haben Sie zwei Möglichkeiten, um alle TVT.TXT-Dateien unter Berücksichtigung der letzten Änderungen zu aktualisieren. Der IT-Administrator kann entweder die TVT.TXT-Datei aus dem Installationsverzeichnis in alle Sicherungsordner kopieren, oder er kann eine weitere Sicherung starten, so dass alle Versionen der TVT.TXT-Dateien automatisch mit der Version im Installationsverzeichnis synchronisiert werden. Die zweite Methode ist vorzuziehen.

Sicherungen und zugehörige Aufgaben planen

Der Scheduler wurde nicht speziell für Rescue and Recovery entwickelt. Die Konfiguration ist jedoch ebenfalls in der Datei TVT.TXT gespeichert. Bei der Installation von Rescue and Recovery werden die entsprechenden Einstellungen für den Scheduler übernommen.

Der Scheduler weist folgende Struktur auf:
- Position: Installationsordner
- Einträge für die einzelnen geplanten Jobs
- Auszuführendes Script
- Benannte Pipe für Fortschrittsbenachrichtigungen (optional)
- Planungsinformationen: monatlich, wöchentlich, täglich, wochentags, am Wochenende, Verwendung mehrerer Zeitpläne (z. B. zur Unterstützung von Dienstagen und Freitagen durch das Erstellen von zwei Zeitplänen)
- Variablen, die an Funktionen übergeben werden

In folgendem Beispiel soll Rescue and Recovery nach einem Zeitplan inkrementelle Sicherungen mit Callbacks vor und nach der Sicherung durchführen. Durch den folgenden Eintrag erhält die Anwendung die entsprechenden Anweisungen:

```
[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"
```

Unterschiedliche TVT.TXT-Dateien verwalten

Da Festplattenlaufwerke mehrere Partitionen aufweisen können, muss dem Programm zur Sicherung und zur Wiederherstellung angegeben werden, auf welcher Partition die Sicherungsdaten gespeichert werden sollen. Wenn ein bestimmtes Ziel mehrere Partitionen aufweist und Sicherungsoperationen über ein Script gesteuert werden, müssen Sie vor der Sicherungsoperation die folgende Einstellung konfigurieren. Wenn die Sicherungsoperation vom Benutzer eingeleitet werden kann, können Sie diesen Abschnitt ignorieren.

Für Sicherungen auf dem lokalen Festplattenlaufwerk befindet sich die Einstellung in der Datei TVT.TXT im Abschnitt "BackupDisk". Sicherungen auf dem zweiten lokalen Festplattenlaufwerk verwenden den Abschnitt "SecondDisk", und Sicherungen auf dem USB-Festplattenlaufwerk verwenden den Abschnitt "USBDisk", und zwar wie folgt:

```
BackupPartition=x
```

Hierbei steht *x* für den Bereich von 0 bis 3, wobei 0 für die erste Partition auf dem entsprechenden Laufwerk steht.

Anmerkung: Die Partitionen müssen bereits vorhanden sein. Wenn sie nicht konfiguriert sind und wenn mehrere Partitionen vorhanden sind, wird der Benutzer zu einer Eingabe aufgefordert, wenn er in der grafischen Benutzerschnittstelle das entsprechende Ziel auswählt. Wenn die Sicherung zum Beispiel auf der zweiten Partition des USB-Festplattenlaufwerks vorgenommen werden soll, lautet der Eintrag in der Datei TVT.TXT wie folgt:

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

Netzlaufwerke für Sicherungen zuordnen

Die Funktion zum Zuordnen des Netzlaufwerks basiert auf der Datei MAPDRV.INI, die sich im Verzeichnis C:\Program Files\IBM ThinkVantage\Common\MND befindet. Alle Informationen sind im Abschnitt ″DriveInfo″ gespeichert.

Der Eintrag ″UNC″ (Universal Naming Convention) enthält den Namen des Computers und den Namen des freigegebenen Verzeichnisses, zu dem eine Verbindung hergestellt werden soll.

Der Eintrag ″NetPath″ ist eine Ausgabe der Datei ″mapdrv.exe″. Er enthält den Namen, der zum Herstellen der Verbindung verwendet wurde.

Die Einträge ″User″ und ″Pwd″ enthalten die Einträge für den Benutzernamen und das Kennwort. Sie sind verschlüsselt.

Im folgenden Beispiel sind die Einträge zum Zuordnen eines Netzlaufwerks dargestellt:

```
[DriveInfo]
UNC=\\server\share
NetPath=\\9.88.77.66\share
User=116226064151192077230149185054220105210064012092037082020 15...
Pwd=1162260641510000000001491850542201052100640120920370820201 5...
```

Für die Implementierung kann diese Datei auf mehrere Computer kopiert werden, die denselben Benutzernamen und dasselbe Kennwort verwenden. Der Eintrag ″UNC″ wird von Rapid Restore Ultra entsprechend einem Wert in der Datei TVT.TXT überschrieben.

Benutzereinträge für Netzwerksicherungen konfigurieren

Wenn das Verzeichnis RRUBACKUPS auf dem freigegebenen Netzlaufwerk erstellt wird, wird das Verzeichnis in einen schreibgeschützten Ordner geändert. Die Zugriffsberechtigung wird so festgelegt, dass *nur* der Benutzer, der den Ordner erstellt hat, über die vollständige Zugriffsberechtigung für den Ordner verfügt.

Für die Ausführung von Mischoperationen sind die entsprechenden MOVE-Berechtigungen für den Benutzereintrag vorhanden. Wenn ein anderer Benutzer als der Benutzer, der den Ordner ursprünglich erstellt hat (z. B. der Administrator), angemeldet ist, schlägt der Mischvorgang fehl.

Anhang C. Befehlszeilentools

Die Funktionen von ThinkVantage Technologies können auch lokal oder über Remotezugriff von einem IT-Administrator des Unternehmens über die Befehlszeilenschnittstelle aufgerufen werden. Die Konfigurationseinstellungen können dabei über die Einstellungen einer fernen Textdatei verwaltet werden.

Antidote Delivery Manager

Mailman

Hierfür wird der Befehl C:\Program Files|IBM ThinkVantage\Rescue and Recovery\ADM\mailman.exe verwendet. Dieses Programm durchsucht das Antidote Repository auf auszuführende Tasks. Hierfür gibt es keine Befehlszeilenargumente.

Antidote-Assistent

Der Befehl hierfür, AWizard.exe, wird dort gespeichert, wo er vom Administrator installiert wird. Hierfür gibt es keine Befehlszeilenargumente.

Kennwörter festlegen

Informationen zum Festlegen von Kennwörtern finden Sie im Abschnitt „Kennwörter" auf Seite 36.

CFGMOD

Der Befehl CFGMOD bietet die Möglichkeit, die Datei TVT.TXT über ein Script zu aktualisieren. Die Befehlsdatei des Befehls CFGMOD befindet sich im Verzeichnis C:\Program Files\IBM ThinkVantage\Rescue and Recovery\. Wenn Sie den Sicherungsplan ändern, muss dieser Befehl von dem Befehl RELOADSCHED gefolgt sein. Dieses Dienstprogramm kann nur von einem Benutzer mit Administratorberechtigung ausgeführt werden.

Syntax:

```
cfgmod TVT.TXT mod-Datei
```

Das Format der mod-Datei sieht nur eine Zeile pro Eintrag vor. Jeder Eintrag besteht aus einer Abschnittsnummer (abgegrenzt von [und]), gefolgt von einem Parameternamen, dem Gleichheitszeichen (=) und dem entsprechenden Wert. Zum Anpassen des Sicherungsplans könnten folgende Einträge in der mod-Datei enthalten sein:

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

Client Security Solution

Client Security Solution verfügt über die folgenden Befehlszeilentools:

SafeGuard PrivateDisk

Die Befehlszeilenschnittstelle befindet sich in dem Ordner C:\Program Files\IBM ThinkVantage\SafeGuard PrivateDisk\. Die Syntax lautet:

```
PDCMD
 [ADDCERT Datenträgername /pw Administratorkennwort /sn ZertSN [/acc Zugriff]]  |
 [LIST]  |
 [MOUNT Datenträgername [/pw Benutzerkennwort [/pt Authentifizierungsmodus]] [/ro]]  |
 [NEW Datenträgername [/sz Größe] [/dl Laufwerkbuchstabe] [/fs Dateisystem]
   [/pw Administratorkennwort] [/pwu Benutzerkennwort]]  |
 [UNMOUNT Datenträgername /f]  |
 [UNMOUNTALL [/f]]  |
 [SETPASSWORD Datenträgername /pw Administratorkennwort /pwu Benutzerkennwort [/ro]]
```

Die Parameter sind in Tabelle 46 aufgeführt:

Tabelle 46.

Parameter	Ergebnis
ADDCERT	Fügt dem PrivateDisk-Datenträger ein Zertifikat hinzu
LIST	Listet die PrivateDisk-Datenträger für diesen Benutzer auf
MOUNT	Hängt einen bestimmten PrivateDisk-Datenträger an
NEW	Erstellt einen neuen PrivateDisk-Datenträger
UNMOUNT	Hängt einen bestimmten PrivateDisk-Datenträger ab
UNMOUNTALL	Hängt alle PrivateDisk-Datenträger ab
SETPASSWORD	Legt ein Benutzerkennwort für einen PrivateDisk-Datenträger fest
Datenträgername	Der Name der Datei, die die PrivateDisk-Dateien enthält
pw	Das Kennwort
sn	Die Seriennummer des Zertifikats
acc	Der Zugriffstyp für das Zertifikat, das hinzugefügt werden soll. Gültige Werte sind: • **adm** Administratorzugriff • **uro** schreibgeschützter Lesezugriff für Benutzer • **usr** Schreibzugriff für Benutzer (Standardwert)

Tabelle 46. (Forts.)

Parameter	Ergebnis
pt	Authentifizierungsmethode. Gültige Werte sind: • **0** Administratorzugriff (Standardwert) • **1** Benutzerkennwort • **2** PIN für eine zertifikatbasierte Anmeldung
ro	Lesezugriff
sz	Größe (in Kilobytes)
dl	Laufwerkbuchstabe für den PrivateDisk-Datenträger (Standardwert: der nächste verfügbare Laufwerkbuchstabe)
fs	Das Dateisystem. Gültige Werte sind: • FAT (Standardwert) • NTFS
pwu	Benutzerkennwort
f	Verarbeitung erzwingen

Security Advisor

Um dieses Programm über die GUI auszuführen, klicken Sie auf **Start -> Programme -> ThinkVantage -> Client Security Solution**. Klicken Sie auf **Advanced**, und wählen Sie **Audit Security Settings** aus. Die Datei C:\Program Files\IBM ThinkVantage\Common\WST\wst.exe wird für eine Standardinstallation ausgeführt.

Die Parameter lauten:

Tabelle 47.

Parameter	Beschreibung
HardwarePasswords	Der Wert ist 1 oder 0. Dabei dient 1 zum Anzeigen und 0 zum Ausblenden dieses Abschnitts. Ist dieser Parameter nicht vorhanden, wird der Abschnitt standardmäßig angezeigt.
PowerOnPassword	Legt fest, dass ein Kennwort zum Einschalten aktiviert wird, oder die Einstellung wird markiert.
HardDrivePassword	Legt fest, dass ein Kennwort für das Festplattenlaufwerk aktiviert wird, oder die Einstellung wird markiert.
AdministratorPassword	Legt fest, dass ein Administratorkennwort aktiviert wird, oder die Einstellung wird markiert.

Tabelle 47. (Forts.)

Parameter	Beschreibung
WindowsUsersPasswords	Der Wert ist 1 oder 0. Dabei dient 1 zum Anzeigen und 0 zum Ausblenden dieses Abschnitts. Ist dieser Parameter nicht vorhanden, wird der Abschnitt standardmäßig angezeigt.
Password	Legt fest, dass das Benutzerkennwort aktiviert wird, oder die Einstellung wird markiert.
PasswordAge	Legt die Gültigkeitsdauer des Windows-Kennworts für die betreffende Maschine fest, oder die Einstellung wird markiert.
PasswordNeverExpires	Legt fest, dass die Gültigkeit des Windows-Kennworts nie abläuft, oder die Einstellung wird markiert.
WindowsPasswordPolicy	Der Wert ist 1 oder 0. Dabei dient 1 zum Anzeigen und 0 zum Ausblenden dieses Abschnitts. Ist dieser Parameter nicht vorhanden, wird der Abschnitt standardmäßig angezeigt.
MinimumPasswordLength	Legt die Kennwortlänge für die betreffende Maschine fest, oder die Einstellung wird markiert.
MaximumPasswordAge	Legt die Gültigkeitsdauer des Kennworts für die betreffende Maschine fest, oder die Einstellung wird markiert.
ScreenSaver	Der Wert ist 1 oder 0. Dabei dient 1 zum Anzeigen und 0 zum Ausblenden dieses Abschnitts. Ist dieser Parameter nicht vorhanden, wird der Abschnitt standardmäßig angezeigt.
ScreenSaverPasswordSet	Legt fest, dass der Bildschirmschoner kennwortgeschützt ist, oder die Einstellung wird markiert.
ScreenSaverTimeout	Legt das Zeitlimit für den Bildschirmschoner für die betreffende Maschine fest, oder die Einstellung wird markiert.
FileSharing	Der Wert ist 1 oder 0. Dabei dient 1 zum Anzeigen und 0 zum Ausblenden dieses Abschnitts. Ist dieser Parameter nicht vorhanden, wird der Abschnitt standardmäßig angezeigt.
AuthorizedAccessOnly	Legt fest, dass für den gemeinsamen Dateizugriff eine entsprechende Berechtigung erforderlich ist, oder die Einstellung wird markiert.
ClientSecurity	Der Wert ist 1 oder 0. Dabei dient 1 zum Anzeigen und 0 zum Ausblenden dieses Abschnitts. Ist dieser Parameter nicht vorhanden, wird der Abschnitt standardmäßig angezeigt.
EmbeddedSecurityChip	Legt fest, dass der Sicherheitschip aktiviert wird, oder die Einstellung wird markiert.

Tabelle 47. (Forts.)

Parameter	Beschreibung
ClientSecuritySolution	Legt die CSS-Version für die betreffende Maschine fest, oder die Einstellung wird markiert.

Eine andere Option für alle diese Werte ist ″ignore″ (ignorieren), das heißt, der Wert wird angezeigt, aber beim Abgleich nicht eingeschlossen. Während der Security Advisor ausgeführt wird, wird eine HTML-Datei in das Verzeichnis c:\ibmshare\wst.html und eine XML-Datei mit Rohdaten in das Verzeichnis c:\ibmshare\wst.xml geschrieben.

Beispiel

Es folgt ein [WST]-Abschnitt, bei dem alle Abschnitte vorhanden sind und alle Einstellungen auf die Standardwerte gesetzt sind:

```
[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
```

Um den Security Advisor auszublenden oder anzupassen, fügen Sie in der TVT.TXT-Datei einen Abschnitt mit dem Namen WST hinzu. Verschiedene Werte können ausgeblendet oder angepasst werden, müssen jedoch in der TVT.TXT-Datei hinzugefügt werden.

Wenn Sie den Security Advisor nicht verwenden möchten und nicht wünschen, dass er in der GUI als aktiviert angezeigt wird, löschen Sie die folgende ausführbare Datei:

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

Assistent zur Übertragung von Zertifikaten

Wenn Sie den Assistenten zur Übertragung von Zertifikaten nicht verwenden möchten und nicht wünschen, dass er in der GUI als aktiviert angezeigt wird, löschen Sie die folgende ausführbare Datei:

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

Client Security-Assistent

Mit diesem Assistenten können Sie das Eigentumsrecht für Hardware übernehmen, die Software konfigurieren und Benutzer registrieren. Darüber hinaus können Sie damit Implementierungsscripts über XML-Dateien generieren. Um die Funktionen dieses Assistenten besser kennen zu lernen, führen Sie den folgenden Befehl aus:

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

Tabelle 48.

Parameter	Ergebnis
/h oder /?	Zeigt das Feld mit Hilfenachrichten an.
/name:*DATEINAME*	Steht vor dem vollständig qualifizierten Pfad und dem Dateinamen der generierten Implementierungsdatei. Die Datei weist die Erweiterung .xml auf.
/encrypt	Verschlüsselt die Scriptdatei durch AES-Verschlüsselung. Der Dateiname wird nach der Verschlüsselung mit der Erweiterung .enc hinzugefügt. Wenn der Befehl /pass nicht verwendet wird, wird ein statischer Verschlüsselungstext verwendet, um die Datei unkenntlich zu machen.
/pass:	Steht vor dem Verschlüsselungstext zum Schutz der verschlüsselten Implementierungsdatei.
/novalidate	Inaktiviert die Überprüfungsfunktionen für das Kennwort und für den Verschlüsselungstext des Assistenten, so dass eine Scriptdatei auf einer bereits konfigurierten Maschine erstellt werden kann. Zum Beispiel ist das Administratorkennwort für die aktuelle Maschine möglicherweise nicht das gewünschte Kennwort für das gesamte Unternehmen. Mit dem Befehl /novalidate können Sie ein anderes Administratorkennwort eingeben (in der GUI von css_wizard während der Erstellung der xml-Datei).

Es folgt ein Beispiel für diesen Befehl:

```
css_wizarde.exe /encrypt /pass:geheimer Schlüssel /name:C:\DeployScript /novalidate
```

Anmerkung: Wenn das System im Emulationsmodus ausgeführt wird, lautet der Name der ausführbaren Datei "css_wizard.exe".

Tool zur Verschlüsselung und Entschlüsselung der Implementierungsdatei

Dieses Tool dient zum Verschlüsseln und Entschlüsseln der XML-Implementierungsdateien von Client Security. Um die Funktionen dieses Tools besser kennen zu lernen, führen Sie den folgenden Befehl aus:

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

Die Parameter sind in Tabelle 49 aufgeführt:

Tabelle 49.

Parameter	Ergebnis
/h oder /?	Anzeige von Hilfenachrichten
DATEINAME	Der vollständig qualifizierte Pfadname und der Dateiname mit der Erweiterung .xml oder .enc
/encrypt oder /decrypt	Wählen Sie "/encrypt" für .xml-Dateien und "/decrypt" für .enc-Dateien aus.
VERSCHLÜSSELUNGSTEXT	Ein optionaler Parameter, der erforderlich ist, wenn ein Verschlüsselungstext verwendet wird, um die Datei zu schützen.

Beispiele:

```
xml_crypt_tool.exe "C:\Implementierungsscript.xml"  /encrypt "geheimer Schlüssel"
```

und

```
xml_crypt_tool.exe "C:\Implementierungsscript.xml.enc"  /decrypt "geheimer Schlüssel"
```

Tool zur Verarbeitung der Implementierungsdatei

Mit dem Tool "vmserver.exe" werden die XML-Implementierungsscripts von Client Security verarbeitet. Um die Funktionen dieses Assistenten besser kennen zu lernen, führen Sie den folgenden Befehl aus:

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

Tabelle 50.

Parameter	Ergebnis
DATEINAME	Der Parameter DATEINAME muss die Dateierweiterung .xml oder .enc aufweisen.
VERSCHLÜSSELUNGSTEXT	Der Parameter VERSCHLÜSSELUNGSTEXT dient zum Entschlüsseln einer Datei mit der Erweiterung .enc.

Es folgt ein Beispiel für diesen Befehl:

```
Vmservere.exe  C:\Implementierungsscript.xml.enc  "geheimer Schlüssel"
```

Anmerkung: Wenn das System im Emulationsmodus ausgeführt wird, lautet der Name der ausführbaren Datei "vmserver.exe".

TPMENABLE.EXE

Die Datei TPMENABLE.EXE dient zum Ein- und Ausschalten des Sicherheitschips.

Tabelle 51.

Parameter	Beschreibung
/enable oder /disable	Zum Ein- oder Ausschalten des Sicherheitschips
/quiet	Zum Ausblenden von Eingabeaufforderungen für das BIOS-Kennwort oder von Fehlermeldungen
sp:*Kennwort*	BIOS-Administratorkennwort; nicht in Anführungszeichen setzen

Beispiel:

```
tpmenable.exe /enable /quiet /sp: Kennwort für eigenes BIOS
```

eGatherer

Der Befehl "eGatherer" befindet sich im Verzeichnis C:\Program Files\IBM ThinkVantage\common\egatherer\egather2.exe.

Die Befehlsdatei "egathere2.exe" erstellt eine EG2-Ausgabe mit den erfassten Daten. Es kann auch eine lokale XML-Ausgabedatei erstellt werden, die im Ausgangsverzeichnis gespeichert wird. Beachten Sie, dass die EG2-Datei ein internes Format aufweist.

Zwei XML-Dateien werden erstellt, eine für die Systeminformationen und eine andere für demographische Informationen. Der Name der XML-Datei besteht aus einer Kombination des Namens des Herstellers, des Modelltyps und der Seriennummer, wie zum Beispiel: IBM-2373Q1U-99MA4L7.XML, IBM-2373Q1U-99MA4L7.DEMOGRAPHICS.XML.

Die Suchsoftware kann über eine Befehlszeile mit der folgenden Syntax ausgeführt werden:

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

- **-help**

  Eine kurze Hilfenachricht anzeigen.
- **-batch**

  Haftungsausschluss nicht anzeigen.
- **-silent**

  Während des Betriebs nichts anzeigen.
- **-nolimit**

  Das gesamte Ereignisprotokoll erfassen. In der Standardeinstellung werden nur die letzten 500 Einträge erfasst.

- **-local**
  Eine lokale XML-Datei erstellen.
- **-listprobes**
  Die verfügbaren Proben auflisten.
- **-probe**
  Die angegebenen Proben ausführen.

MAPDRV

Mit dem Befehl MAPDRV können Sie die Benutzerschnittstelle zum Zuordnen eines Netzlaufwerks aufrufen. Die Befehlsdatei MAPDRV.EXE befindet sich im Verzeichnis C:\Program Files\IBM ThinkVantage\Common\MND. Die Schnittstelle zum Zuordnen eines Netzlaufwerks unterstützt die folgenden Parameter.

Syntax:

```
mapdrv [Schalter]
```

Bei Eingabe des Befehls ohne Parameter wird die Anwendung gestartet, und die Informationen müssen manuell eingegeben werden.

Die Rückkehrcodes für alle Parameter lauten:

- **0** = erfolgreich
- **> 0** = fehlgeschlagen

Tabelle 52. Parameter für MAPDRV

Parameter	Ergebnis
/nodrive	Erstellt eine Netzverbindung, ohne der Verbindung einen Laufwerkbuchstaben zuzuordnen.
/pwd	Das Kennwort des betreffenden Benutzers für dieses freigegebene Verzeichnis.
/set	Legt das freigegebene Verzeichnis, den Benutzer und das Kennwort fest, die zum Sichern und Wiederherstellen verwendet werden. Die Rückkehrcodes lauten:
/s	Unbeaufsichtigt. Es wird keine Eingabeaufforderung für den Benutzer angezeigt, unabhängig davon, ob die Verbindung hergestellt werden konnte.
/timeout	Legt den Zeitlimitwert fest.
/unc	Der Freigabename in der Form \\server\share.
/user	Der Benutzername für das betreffende freigegebene Verzeichnis.

Wenn der Befehl /SET verwendet wird, wird der folgende Abschnitt in der Datei TVT.TXT hinzugefügt. Dies wird im folgenden Beispiel veranschaulicht, in dem die Parameter /UNC/USER und PWD verwendet werden:

```
mapdrv /set /unc Freigabename /user  Benutzername /pwd Kennwort
[mapdrv]
UNC=\\test\test
User=1EE22597AE4D
PWD=04E22197B34D95943ED5A169A0407C5C
```

Boot-Manager von Rescue and Recovery (BMGR32) steuern

Die Befehlszeilenschnittstelle für den Boot-Manager ist BMGR32. Der Boot-Manager befindet sich im Verzeichnis C:\Program Files\IBM ThinkVantage\Common \BMGR. In der folgenden Tabelle werden die Schalter und die jeweiligen Ergebnisse für BMGR32 beschrieben.

Tabelle 53. Parameter für BMGR32

bmgr32	**Ergebnis**
/B0	Booten in Partition 0 (entsprechend der Reihenfolge in der Partitionstabelle)
/B1	Booten in Partition 1
/B2	Booten in Partition 2
/B3	Booten in Partition 3
/BS	Booten in die Servicepartition
/BW	Booten in die geschützte Partition von Rescue and Recovery
/BWIN	Zurücksetzen der Anforderung zum Booten in WINPE. Dieser Befehl muss vor dem Booten ausgegeben werden.
/CFG*Datei*	Übernahme der Parameter aus der Konfigurationsdatei. Weitere Informationen zur Konfigurationsdatei finden Sie im Abschnitt „Befehlszeilenschnittstelle RRCMD" auf Seite 181.
/DS	Rückgabe des Master-Bootsatz-Datensektors (mit der Basis 0)
/D*n*	Übernahme der Änderungen für Platte n, wobei n die Basis 0 hat (Standardwert: die Umgebungsvariable, die die Platte angibt, "SystemDrive" oder "C:\", wenn "SystemDrive" nicht definiert ist)
/H0	Partition 0 verdecken
/H1	Partition 1 verdecken
/H2	Partition 2 verdecken
/H3	Partition 3 verdecken
/HS	Servicepartition verdecken
/P12	Servicepartition verdecken, indem der Partitionstyp auf 12 gesetzt wird
/INFO	Informationen zum Festplattenlaufwerk anzeigen (Suche nach 8 freien Sektoren)
/INFOP	Informationen zum Festplattenlaufwerk anzeigen (Suche nach 16 freien Sektoren)
/M0	Die Umgebung von Rescue and Recovery befindet sich auf der Servicepartition
/M1	Die Umgebung von Rescue and Recovery befindet sich im Verzeichnis C:\PARTITION (doppeltes Booten in Windows und Windows PE)
/M2	Die Umgebung von Rescue and Recovery befindet sich auf der Servicepartition mit DOS (doppeltes Booten in Windows PE und DOS; nur für Lenovo oder IBM Systeme mit werkseitig vorinstalliertem Programm)

Tabelle 53. Parameter für BMGR32 (Forts.)

bmgr32	**Ergebnis**
/OEM	Der Computer ist kein IBM oder Lenovo Produkt. Dieser Befehl erzwingt eine zweite Überprüfung für das Drücken der Taste F11 (Standardwert) nach dem POST. Dies ist möglicherweise auch bei älteren IBM Systemen erforderlich. Dies ist außerdem die Standardeinstellung für die OEM-Version von Rescue and Recovery.
/Patch*n*	Wird für das Installationsprogramm nur verwendet, um eine Variable festzulegen, auf die ein Korrekturprogramm für den Master-Bootsatz zugreifen kann.
Patchfile*Dateiname*	Wird für das Installationsprogramm nur zur Installation einer Programmkorrektur für den Master-Bootsatz verwendet.
/PRTC	Wird für das Installationsprogramm nur zum Abrufen eines Rückkehrcodes für eine Programmkorrektur verwendet.
/IBM	Das System ist ein Computer von IBM oder Lenovo.
/Q	unbeaufsichtigt
/V	ausführlich
/R	Computer neu starten
/REFRESH	Partitionstabelleneinträge im Datensektor zurücksetzen
/TOC *TOC-Wert*	Festlegen des BIOS-TOC-Standorts (16 Zeichen für 8 Bytes an Daten)
/U0	Partition 0 anzeigen
/U1	Partition 1 anzeigen
/U2	Partition 2 anzeigen
/U3	Partition 3 anzeigen
/US	Servicepartition anzeigen
/F*Master-Bootsatz*	Lädt das Programm für den Master-Bootsatz für die Umgebung von Rescue and Recovery.
/U	Entlädt das Programm für den Master-Bootsatz für die Umgebung von Rescue and Recovery.
/UF	Installation oder Deinstallation des Programms für den Master-Bootsatz erzwingen
/?	Auflisten der Befehlszeilenoptionen

Wenn Sie die Datei "bmgr.exe" mit einem /info-Attribut aufrufen, wird von den folgenden Informationen ein Speicherauszug erstellt:

- **Additional MBR**

  Die Nummern der Sektoren, die den Master-Bootsatz enthalten, falls dies nicht der erste Sektor ist.
- **Data**

  Die Nummer des vom Master-Bootsatz verwendeten Datensektors.
- **Patch indices**

  Die Nummern der Sektoren mit Patches, die mit Hilfe des Master-Bootsatzes angewandt wurden.
- **Checksum return**

  Dieser Wert beträgt 0, wenn keine Kontrollsummenfehler vorliegen.
- **Boot Partition**

  Der Partitionstabellenindex der Partitionstabelle mit der Basis 1.
- **Alt Partition**

  Der Partitionstabellenindex, der auf den in DOS bootfähigen Bereich verweist, falls vorhanden.
- **Original MBR**

  Die Nummer des Sektors, in dem der ursprüngliche Master-Bootsatz der Maschine gespeichert ist.
- **IBM Flag**

  Wert aus dem Datensektor (1 für Systeme von IBM oder Lenovo, 0 für andere Systeme).
- **Boot Config**

  Beschreibung der Installationsoption, die zur Beschreibung des Maschinenlayouts verwendet wird; ob eine Servicepartition oder eine virtuelle Partition verwendet wurde.
- **Signature**

  Signaturwert aus dem Datensektor und dem ersten Sektor; sollte “NP” enthalten.
- **Pause Duration**

  Die Anzahl an ¼-Sekunden, die gewartet wird, wenn die F11-Nachricht auf dem Bildschirm angezeigt wird.
- **Scan Code**

  Welche Taste beim Booten in den Servicebereich verwendet wird. "85" steht für die Taste F11.
- **RR**

  Wird vom Boot-Manager nicht verwendet, sondern von Rescue and Recovery festgelegt.
- **Prev Active Part**

  Beim Booten in den Servicebereich enthält dieser Wert den Partitionstabellenindex der zuletzt aktiven Partition.

- **Boot State**

  Wird vom Master-Bootsatz verwendet, um den aktuellen Zustand der Maschine zu ermitteln. 0 – Normales Booten in das Betriebssystem, 1 – Booten in das Servicebetriebssystem, 2 – Aus dem Servicebetriebssystem zurück in das normale Betriebssystem booten.
- **Alt Boot Flag**

  Booten in ein alternatives Betriebssystem, zum Beispiel DOS.
- **Previous Partition type**

  Beim Booten in den Servicebereich enthält dieser Wert den Partitionstyp, der für die Servicepartition vor dem Booten festgelegt war.
- **Prior IBM MBR Index**

  Wird vom Installationsprogramm verwendet.
- **Patch IN: OUT**

  Eingabe- und Ausgabewerte aus des Patch-Codes, falls verwendet.
- **F11 Msg**

  Nachricht, die dem Benutzer angezeigt wird, wenn ordnungsgemäße BIOS-Aufrufe nicht unterstützt werden.

RELOADSCHED

Mit diesem Befehl werden die geplanten Einstellungen, die in der Datei TVT.TXT definiert sind, erneut geladen. Wenn Sie Änderungen an dem Zeitplan in der Datei TVT.TXT vornehmen, müssen Sie diesen Befehl ausführen, um die Änderungen zu aktivieren.

Beispiel:

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

Befehlszeilenschnittstelle RRCMD

RRCMD ist die primäre Befehlszeilenschnittstelle von Rescue and Recovery. Der Befehl befindet sich im Unterverzeichnis C:\Program Files\IBM ThinkVantage\Rescue and Recovery\reloadsched.exe. Im Folgenden erhalten Sie Informationen zur Verwendung der Befehlszeilenschnittstelle für Rescue and Recovery.

Syntax:

```
RRcmd Befehl filter=Filterdatei  location=c [name=abc | level=x] [silent]
```

Tabelle 54. Parameter für RRCMD

Befehl	Ergebnis
`Backup`	Einleiten einer normalen Sicherungsoperation (die Parameter ″location″ und ″name″ sind erforderlich).
`Restore`	Einleiten einer normalen Wiederherstellungsoperation (die Parameter ″location″ und ″level″ sind erforderlich).
`List`	Auflisten der Dateien, die in der Sicherungsstufe enthalten sind (die Parameter ″location″ und ″level″ sind erforderlich).

Tabelle 54. Parameter für RRCMD (Forts.)

Befehl	Ergebnis
`Basebackup`	Einleiten einer alternativen Basissicherung. Dieser Befehl darf nicht als Basis für inkrementelle Sicherungen verwendet werden, und die Parameter "location", "name" und "level" sind erforderlich. Der Wert für den Parameter "level" muss weniger als 99 betragen. Wenn eine andere Basissicherung mit demselben Parameter "level" vorhanden ist, wird sie überschrieben.
`Sysprepbackup`	Ausführen in Stufen einer Sicherungsoperation in der Predesktop Area nach einem Neustart des Computers. Dieser Befehl wird vor allem zur Erfassung einer Sicherung mit dem Befehl "Sysprep" verwendet. **Anmerkungen:** 1. In einigen Fällen bewegt sich der Fortschrittsanzeiger nicht. Sie können in diesem Fall überprüfen, ob die Sicherung im Gange ist, indem Sie auf Betriebsgeräusche des Festplattenlaufwerks achten. Wenn die Sicherung beendet ist, wird eine entsprechende Nachricht angezeigt. 2. Wenn Sie bei der Erstellung einer Sicherung mit dem Befehl "Sysprepbackup" im Netzwerk ein Kennwort festlegen, wird die Kennwortdatei erst in die Sicherungsposition geschrieben, wenn eine inkrementelle Sicherung vorgenommen wurde. Zur Behebung dieses Problems gibt es zwei Strategien: a. Erstellen Sie eine lokale Sicherung mit dem Befehl "Sysprep", und kopieren Sie die Sicherungen entweder ins Netzwerk oder auf das USB-Laufwerk. b. Erstellen Sie nach der Sicherung mit dem Befehl "Sysprep", eine inkrementelle Sicherung im Netzwerk oder auf dem USB-Laufwerk, wobei Sie die inkrementelle Sicherung anschließend beibehalten oder löschen können.
`Copy`	Kopieren von Sicherungen aus einer Position in eine andere. Dies wird auch als Archivierung bezeichnet, und der Parameter "location" ist erforderlich.
`Rejuvenate`	Erneuern des Betriebssystems anhand der angegebenen Sicherung.
`Delete`	Löschen von Sicherungen. Der Parameter "location" ist erforderlich.
`Changebase`	Ändern von Dateien in allen Sicherungen auf der Grundlage des Inhalts der Datei "file.txt". Die Optionen in der Datei "file.txt" lauten: **A** Hinzufügen **D** Löschen **RS** Ersetzen
`migrate`	Erstellen einer Migrationsdatei aus einer Sicherung.
`filter=`*`Filterdatei`*	Gibt an, welche Dateien und Ordner wiederhergestellt werden und ändert keine anderen Dateien. Dieser Parameter wird nur mit dem Befehl **restore** verwendet.

Tabelle 54. Parameter für RRCMD (Forts.)

Befehl	Ergebnis
`Location=c`	Folgende Optionen mit den jeweiligen Ergebnissen können einzeln oder kombiniert ausgewählt werden. **L** Für das primäre lokale Festplattenlaufwerk **U** Für ein USB-Festplattenlaufwerk **S** Für ein sekundäres lokales Festplattenlaufwerk **N** Für das Netzwerk **C** Für CD-/DVD-Wiederherstellung
`name=abc`	*abc* steht für den Namen der Sicherung.
`level=x`	*x* steht dabei für eine Zahl zwischen 0 (für die Basissicherung) und der maximalen Anzahl an inkrementellen Sicherungen (wird nur zusammen mit der Wiederherstellungsoption verwendet). Für Sicherungsbefehle ist der Parameter "level=*x*" nur erforderlich, wenn eine Administratorsicherung ausgeführt wird (z. B. größer oder gleich 100). **Anmerkungen:** 1. Um eine Wiederherstellung anhand der letzten Sicherung auszuführen, geben Sie diesen Parameter nicht an. 2. Alle Funktionen für Sicherung und Wiederherstellung werden über den Service geleitet, damit die richtige Reihenfolge beibehalten wird, z. B. beim Ausführen von Callbacks. Der Sicherungsbefehl wird durch die Befehlszeilenoptionen ersetzt.

Format der Konfigurationsdatei des Boot-Managers	Das Format der Konfigurationsdatei des Boot-Managers ist abwärtskompatibel mit der letzten Version des Boot-Managers. Schalter, die unten nicht aufgeführt sind, werden nicht unterstützt. Die Datei ist eine Textdatei, in der jeder Eintrag in einer separaten Zeile steht.
	
	`<PROMPT1=der Text für die F11-Eingabeaufforderung>`
	`<KEY1=F11>`
	`<WAIT=40>`

System Migration Assistant

Dieses Modul ist ein Befehlszeilenprogramm, das mit dem älteren Programm "SMA4.2 SMABAT.EXE" kompatibel ist. Die Befehlsparameter und die Steuerkarte (Commands.TXT) für das Modul sollten mit SMA 4.2 kompatibel sein.

Active Update

Active Update ist eine eSupport-Technologie, die die Aktualisierungsclients auf dem lokalen System verwendet, um die gewünschten Pakete im Web zu liefern, ohne dass eine Benutzerinteraktion nötig wäre. Active Update fragt die verfügbaren Aktualisierungsclients ab und verwendet den verfügbaren Aktualisierungsclient zum Installieren des gewünschten Pakets. Active Update startet ThinkVantage System Update oder das Programm "Software Installer" auf dem System.

Um zu bestimmen, ob das Programm "Active Update Launcher" installiert ist, suchen Sie nach dem folgenden Registrierungsschlüssel: HKLM\Software\Thinkvantage\ActiveUpdate.

Um zu bestimmen, ob das Programm ″Active Update Launcher″ konfiguriert ist, um Active Update zuzulassen, muss HKLM\Software\IBMThinkvantage\Rescue and Recovery in seinem eigenen Registrierungsschlüssel nach dem Wert für das Attribut ″EnableActiveUpdate″ suchen. Beim Wert ″EnableActiveUpdate=1″ wird der Menüpunkt ″Active Update″ im Hilfemenü angezeigt.

Active Update Launcher

Um zu bestimmen, ob das Programm ″Active Update Launcher″ installiert ist, suchen Sie nach dem folgenden Registrierungsschlüssel:

```
HKLM\Software\TVT\ActiveUpdate
```

Um zu bestimmen, ob die Datei TVT.TXT konfiguriert ist, um Active Update zuzulassen, muss die TVT im eigenen Registrierungsschlüssel nach dem Wert für das Attribut ″EnableActiveUpdate″ suchen. Beim Wert ″EnableActiveUpdate=1″ fügt die TVT den Menüpunkt ″Active Update″ im Hilfemenü hinzu.

Um Active Update aufzurufen, muss die aufrufende TVT das Programm ″Active Update Launcher″ starten und eine Parameterdatei übergeben (die Parameterdatei wird im Abschnitt ″Parameterdatei für Active Update″ beschrieben).

Gehen Sie wie folgt vor, um Active Update aufzurufen:

1. 1. Öffnen Sie den Registrierungsschlüssel des Programms ″Active Update Launcher″:

   ```
   HKLM\Software\TVT\ActiveUpdate
   ```

2. 2. Suchen Sie den Wert für das Attribut ″Path″.
3. 3. Suchen Sie den Wert für das Attribut ″Program″.
4. 4. Verknüpfen Sie die gefundenen Werte für die Attribute ″Path″ und ″Program″ zu einer Befehlszeichenfolge.
5. 5. Fügen Sie die Parameterdatei (siehe dazu den Abschnitt ″Parameterdatei für Active Update″) zur Befehlszeichenfolge hinzu.
6. 6. Führen Sie die Befehlszeichenfolge aus. Die sich ergebende Befehlszeichenfolge könnte etwa folgendermaßen lauten:

   ```
   C:\Program Files\ThinkVantage\ActiveUpdate\activeupdate.exe C:\Programme\
   ThinkVantage\RnR\tvtparms.xml
   ```

Es wird empfohlen, Active Update asynchron aufzurufen, damit die aufrufende TVT nicht blockiert wird. Wenn die aufrufende TVT beendet werden muss, bevor die Aktualisierung installiert wurde, muss das Installationsprogramm für die Aktualisierung die TVT beenden.

Parameterdatei für Active Update

Die Parameterdatei für Active Update enthält die Einstellungen, die Active Update übermittelt werden sollen. Zurzeit wird nur die Datei ″TargetApp″ (der Name der TVT) übermittelt, wie im folgenden Beispiel dargestellt:

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

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

Anhang D. Administrations-Tools

ThinkVantage Technologies bietet Tools für IT-Administratoren in Unternehmen.

Antidote-Assistent

Informationen zum Antidote-Assistenten finden Sie in Anhang F, „Befehlsreferenz und Beispiele für Antidote Delivery Manager", auf Seite 191.

BMGR CLEAN

Mit dem Programm "CleanMBR" wird der Master-Bootsatz gereinigt. Sie können dieses Programm verwenden, wenn ein Fehler bei der Installation von Rescue and Recovery auftritt, wie zum Beispiel, wenn es nicht möglich ist, Rescue and Recovery mit weniger freien Sektoren zu installieren, als erforderlich sind, um den Boot-Manager zu installieren.

Anmerkungen:

1. Nachdem Sie dieses Tool ausgeführt haben, sind Anwendungen, die den Master-Bootsatz verwenden, überflüssig, wie zum Beispiel SafeGuard Easy, SafeBoot, die Master-Bootsatz-Version von Computrace usw.
2. Das Tool sollte vor der Installation von Rescue and Recovery ausgeführt werden.
3. Verwenden Sie die Datei "cleanmbr.exe" unter DOS. "CleanMBR32.exe" kann unter Windows verwendet werden.
4. Nach der Ausführung von "CleanMBR" für DOS führen Sie den Befehl "FDISK /MBR" aus. Dadurch wird der Master-Bootsatz aktiviert.

Die Parameter für "CleanMBR32.exe" lauten:

Tabelle 55.

Parameter (erforderlich):	**Beschreibung**
/A	Master-Bootsatz löschen und PC-DOS-Master-Bootsatz installieren
Parameter (optional):	
/Dn	Änderungen auf das Laufwerk anwenden. Für das erste Laufwerk verwenden Sie *n*=0.
/Y	Alle bestätigen
/?	Hilfe anzeigen
/H	Hilfe anzeigen

CLEANDRV.EXE

Bereinigt das Laufwerk von allen Dateien. Nach Ausführen dieses Befehls ist kein Betriebssystem mehr vorhanden. Weitere Informationen hierzu finden Sie im Abschnitt „Rescue and Recovery auf einer Servicepartition vom Typ 12 installieren" auf Seite 142.

CONVDATE

Das Dienstprogramm "Convdate" ist Teil des Verwaltungstools "Rescue and Recovery". Es dient zur Bestimmung der Hexadezimalwerte für Datum und Uhrzeit sowie zum Konvertieren der Werte für Datum und Uhrzeit in Hexadezimalwerte und kann auch verwendet werden, um benutzerdefinierte Werte für Datum und Uhrzeit in einem Sicherungsfeld von TVT.TXT festzulegen.

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

Zum Ausführen des Dienstprogramms gehen Sie wie folgt vor:

1. Extrahieren Sie die Verwaltungstools von Rescue and Recovery aus dem Verzeichnis http://www.lenovo.com/thinkvantage.
2. Öffnen Sie ein Befehlsfenster.
3. Geben Sie "convdate" ein.

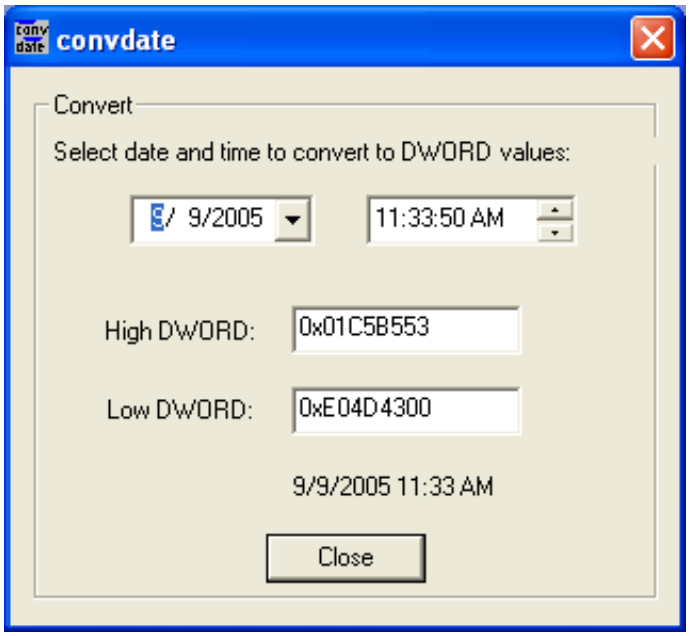

Abbildung 5. Fenster "convdate"

4. Geben Sie in den Feldern zum Auswählen von Datum und Uhrzeit zum Konvertieren der DWORD-Werte das Datum und die Uhrzeit ein.
5. Die entsprechenden Werte in der Datei TVT.TXT lauten:
   - High DWORD=StartTimeHigh
   - Low Dword=StartTimeLow

CREAT SP

Mit diesem Befehl wird eine Partition mit einer bestimmten Anzahl von Megabyte als Servicepartition erstellt. Die Angabe des Laufwerkbuchstaben ist optional.

Die Syntax lautet:

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

Die Parameter für CREAT SP lauten:

Tabelle 56.

Parameter	Beschreibung
size=*x*	Größe der zu erstellenden Servicepartition in Megabyte.
drive=*x*	Die Bezeichnung des Laufwerks, auf dem die Servicepartition erstellt werden soll. Wenn Sie kein Laufwerk angeben, wird das erste Nicht-USB-Laufwerk verwendet. Dieser Parameter ist optional.
/y	Unterdrückt die Aufforderung zum Bestätigen, dass das Laufwerk bereinigt werden soll. Dieser Parameter ist optional.

Anmerkung: Die Datei ″bmgr32.exe″ muss sich im selben Verzeichnis wie die Datei ″createsp.exe″ befinden und sollte unter Windows PE ausgeführt werden.

RRUTIL.EXE

Informationen zur Datei RRUTIL.EXE finden Sie im Abschnitt „Predesktop Area” auf Seite 20.

SP.PQI

Mit dieser Datei können Sie eine Servicepartition vom Typ 12 erstellen. Weitere Informationen hierzu finden Sie im Abschnitt „Rescue and Recovery auf einer Servicepartition vom Typ 12 installieren” auf Seite 142.

Anhang E. Benutzertasks

Je nach ihrer Berechtigung können Benutzer möglicherweise nicht alle Tasks ausführen. In den folgenden Tabellen sind die verfügbaren Basistasks für die unterschiedlichen Benutzer-ID-Berechtigungen in einem Standardbetriebssystem aufgeführt: Benutzer/Benutzer mit eingeschränkter Berechtigung, Hauptbenutzer und Administrator. Die Tasks und Möglichkeiten unterschieden sich je nach Windows-Betriebssystem.

Windows XP

In der folgenden Tabelle sind die Tasks aufgelistet, die Benutzer mit eingeschränkter Berechtigung, Hauptbenutzer und Benutzer mit Administratorberechtigung in Rescue and Recovery in einer Windows XP-Umgebung ausführen können.

Tabelle 57. Benutzertasks unter Windows XP

Benutzer von Windows XP können folgende Tasks ausführen:	**Benutzer mit eingeschränkter Berechtigung**	**Hauptbenutzer**	**Administrator**
ISO-Sicherungsdatenträger erstellen	Nein	Nein	Ja (über die unten angegebene Befehlszeile)
Bootfähige CD-Datenträger erstellen	Ja	Ja	Ja
Bootfähige USB-Festplattendatenträger erstellen	Nein	Nein	Ja
Sicherung einleiten	Ja	Ja	Ja
Wiederherstellung in der Umgebung von Rescue and Recovery (RRE) einleiten	Ja	Ja	Ja
Wiederherstellung einer Einzeldatei in der RRE ausführen	Nein (Windows) Ja (Preboot-Bereich von Windows)	Nein (Windows) Ja (Preboot-Bereich von Windows)	Ja
Optionen zum Einschließen und Ausschließen über die Schnittstelle von Rescue and Recovery festlegen	Ja	Ja	Ja
Sicherung auf ein Netzlaufwerk	Ja	Ja	Ja
Sicherungen zeitlich planen	Ja	Ja	Ja

Windows 2000

In der folgenden Tabelle sind die Tasks aufgelistet, die Benutzer mit eingeschränkter Berechtigung, Hauptbenutzer und Benutzer mit Administratorberechtigung in Rescue and Recovery in einer Windows 2000-Umgebung ausführen können.

Tabelle 58. Benutzertasks unter Windows 2000

Benutzer von Windows 2000 können folgende Tasks ausführen:	**Benutzer mit eingeschränkter Berechtigung**	**Hauptbenutzer**	**Administrator**
ISO-Sicherungsdatenträger erstellen	Nein	Nein	Ja (über die unten angegebene Befehlszeile)
Bootfähige CD-Datenträger erstellen	Ja	Ja	Ja
Bootfähige USB-Festplattendatenträger erstellen	Nein	Nein	Ja
Sicherung einleiten	Ja	Ja	Ja
Wiederherstellung in der Umgebung von Rescue and Recovery (RRE) einleiten	Ja	Ja	Ja
Wiederherstellung einer Einzeldatei in der RRE ausführen	Nein (Windows) Ja (Preboot-Bereich von Windows)	Nein	Ja
Optionen zum Einschließen und Ausschließen über die Schnittstelle von Rescue and Recovery festlegen	Ja	Ja	Ja
Sicherung auf Netzlaufwerk	Nein	Nein	Ja
Sicherungen zeitlich planen	Ja	Ja	Ja

Sicherungsdatenträger erstellen

Benutzer mit Administratorberechtigung können mit folgenden Befehlszeilen ISO-Sicherungsdatenträger erstellen. Diese Befehlszeilen ermöglichen Ihnen das Erstellen der erforderlichen ISO-Datei, die automatisch im Verzeichnis C:\Program Files\IBM ThinkVantage\Rescue and Recovery\rrcd\ gespeichert wird:

```
:: 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
```

Anhang F. Befehlsreferenz und Beispiele für Antidote Delivery Manager

Dem Administrator wird ein Befehlszeilentool zum Erstellen von Paketen zur Verfügung gestellt, damit er Nachrichten erstellen kann. Darüber hinaus bietet Antidote Delivery Manager einige besondere Befehlsfunktionen, die in den Nachrichten verwendet werden können.

Leitfaden für Antidote Delivery Manager-Befehle

Die Befehlszeilenschnittstelle für den Boot-Manager ist BMGR32. Sie befindet sich im Verzeichnis C:\Program Files\IBM ThinkVantage\Rescue and Recovery\ADM. In der folgenden Tabelle werden die Schalter und die jeweiligen Ergebnisse für BMGR32 beschrieben.

Tabelle 59. Befehle des Antidote Delivery Managers

Befehle	Beschreibung
APKGMES [/KEY *Schlüsseldatei*|/NEWKEY *Schlüsseldatei* |/NOSIG] *Nachrichtenverzeichnis Nachrichtenname*	Für APKGMES /KEY wird eine Nachrichtendatei auf der Basis des Inhalts des Verzeichnisses *Nachrichtenverzeichnis_von_TVT.TXT* erstellt. Das Verzeichnis muss eine Datei mit dem Namen GO.RRS enthalten. Wenn Sie den Parameter /KEY verwenden, wird aus der Datei "keyfile.prv" ein Signierschlüssel abgerufen, und der Schlüssel in "keyfile.pub" muss an alle Clients verteilt worden sein, die die Nachricht verarbeiten sollen. In der Standardeinstellung wird die Schlüsseldatei "KEYFILE.PRV" verwendet. Zur Erstellung eines Schlüssels kann der Parameter /NEWKEY verwendet werden. Wenn Sie das Signieren nicht wünschen, können Sie es mit dem Parameter /NOSIG verhindern. An das Ende des Nachrichtennamens wird ein Datumsstempel angehängt, der das Format *Nachrichtenname*JJMMTTSSmm.zap aufweist.
REBOOT [/*RR*|/Win] [/wait | /f]	Mit diesem Befehl wird ein Neustart des Systems ausgeführt. Ohne Angabe von Parametern wird das System in der normalen Startreihenfolge gebootet. Der Parameter RR bestimmt, dass ein Neustart in das Programm "Rescue and Recovery" ausgeführt wird, und der Parameter WIN, dass ein Neustart in das reguläre Betriebssystem ausgeführt wird. Der Neustart wird erst ausgeführt, wenn das Script beendet ist, so dass dies normalerweise der letzte Befehl in einem Script ist. Der optionale Befehl WAIT erzwingt beim nächsten Neustart (manuell oder auf andere Weise) das Booten des Systems in die angegebene Umgebung. Der Parameter /f erzwingt den sofortigen Neustart, und der Benutzer erhält keine Gelegenheit, Daten aus geöffneten Anwendungen zu speichern. Wenn keine Parameter angegeben werden, lautet der Standardparameter /win (ohne Angabe von /wait und /f).

Tabelle 59. Befehle des Antidote Delivery Managers (Forts.)

Befehle	Beschreibung
`RETRYONERROR [ON|OFF] Wiederholungen`	In der Standardeinstellung wird nur einmal versucht, ein Script auszuführen. Wenn es jedoch wichtig ist, die Ausführung eines Scripts so lange zu versuchen, bis es funktioniert, können Sie mit dem Befehl RETRYONERROR die Mailboxfunktion benachrichtigen, dass für die Ausführung dieses Scripts eine endliche Anzahl von Versuchen gelten soll, die im Parameter für Wiederholungen angegeben ist. Wenn Sie keine Zahl angeben, lautet der Standardwert 3. In der Datei TVT.TXT können Sie im Abschnitt für Sicherungen einen globalen Standardwert für `retries = Wiederholungen` festlegen. Sie können für Wiederholungen auch FOREVER festlegen. Dies führt zu einer Endlosschleife.
`MSGBOX /msg Nachrichtentext [/head Überschriftentext] [/OK] [/CANCEL]| [/TIMER Zeitlimit] /B3`	Mit dem Befehl MSGBOX wird angemeldeten Endbenutzern eine Nachricht angezeigt. Die Nachricht wird so lange angezeigt, und das Script wird so lange gesperrt, bis das Zeitlimit überschritten wird, die Schaltfläche für Abbruch oder (bei Angabe von "/OK") **OK** ausgewählt wird. Die Schaltfläche für Abbruch wird im Fenster nur angezeigt, wenn der Parameter "/CANCEL" festgelegt wurde. Das Entfernen dieser Anzeige ist schwierig. Der Befehl gibt folgende Meldungen zurück: • 0 = "OK" wurde ausgewählt • 1 = Abbruch • 2 = Zeitgeber abgelaufen Den Text in der Nachricht können Sie mit \n für eine neue Zeile und mit \t für Tabulator formatieren.
`NETWK [/D|/E|/A [/IP IP-Adresse | /DN Domänenname] [/NM Netzmaske]`	Der Befehl NETWK mit dem Parameter /D stoppt den gesamten Datenaustausch im Netz, indem alle Netzwerkadapter inaktiviert werden. Der Netzbetrieb bleibt so lange inaktiviert, bis der Befehl NETWK mit dem Parameter /E ausgeführt wird. Der Befehl NETWK /A schränkt den Netzbetrieb auf die angegebene IP-Adresse ein. Dabei können Sie entweder den Schalter /IP (Schreibweise mit Trennzeichen) oder /DN (Name der DNS) angeben. Der Schalter /NM gibt die Netzmaske an. Wenn Sie /NM nicht angeben, kann nur auf das System zugegriffen werden, das mit /IP oder mit /DN angegeben wurde. Der Status dieses Befehls wird nach einem Neustart beibehalten, so dass der Netzbetrieb explizit aktiviert werden muss.

Tabelle 59. Befehle des Antidote Delivery Managers (Forts.)

Befehle	Beschreibung
APUBKEY [/ADD|/DELETE] *ASN-1-codierter_öffentl_Schlüssel*	Mit dem Befehl APASSWD kann ein Administrator die Signierschlüssel für die Nachricht des Antidote Delivery Managers auf den einzelnen PCs fern verwalten. Auf jedem PC können mehrere Schlüssel gespeichert werden. Wenn eine signierte Nachricht verarbeitet wird, wird jeder Schlüssel probiert, bis ein Schlüssel passt. Schlüssel werden nicht separat benannt, müssen also über ihren Inhalt bestimmt werden. Mit dem Parameter ADD können Sie einen neuen Schlüssel hinzufügen und mit dem Parameter DELETE einen Schlüssel löschen. Beachten Sie, dass bei Angabe von Schlüsseln in der Datei TVT.TXT keine nicht signierten Nachrichten mehr verwendet werden können (also keine Nachrichten, die mit dem Parameter /NOSIG erstellt wurden).
AUNCPW [/Add|/CHANGE|/DELETE] *allgemeine_Namenskonvention* [/USER *Benutzer-ID*] [/PWD *Kennwort*] [/REF *Referenzname*]	Mit diesem Befehl können Sie ein Kennwort für ein Netzlaufwerk hinzufügen, ändern oder löschen. Den Referenznamen können Sie in einer Nachricht als Direktaufruf verwenden, statt die allgemeine Namenskonvention zu verwenden. Die Rückgabewerte lauten: • 0 = Erfolgreich • 1 = Einstellen mit den angegebenen Daten nicht möglich • 2 = Erfolgreich, es wurde jedoch bereits eine andere allgemeine Namenskonvention mit demselben Referenznamen definiert

Tabelle 59. Befehle des Antidote Delivery Managers (Forts.)

Befehle	Beschreibung
`XMLtool`	Bedingungsangaben (eGatherer, aktuelle Hardware-informationen) • **Verwendung:** xmltool.exe *Dateiname XPath Funktion Vergleichsoperator Wert*. Dabei gilt: – **Dateiname** Der Pfad und der Dateiname der XML-Datei. – **XPath** Der vollständig qualifizierte XPath zum Wert. – **Funktion** Muss einen der folgenden Werte aufweisen: - /C - zum Vergleichen der Werte (ein Vergleichsoperator und ein Wert müssen angegeben werden). - /F - zum Speichern des angegebenen Werts in der Datei %IBMSHARE%\RET.TXT. – **Vergleichsoperator:** Muss einen der folgenden Werte aufweisen: - LSS - LEQ - EQU - GTR - GEQ - NEW – **Wert:** Der Wert, mit dem der XML-Eintrag verglichen wird. • Rückgabewerte: – **0** Der Vergleich wird als wahr bewertet (/c). – **1** Der Vergleich wird als falsch bewertet. – **2** Falsche Befehlszeilenparameter. – **3** Fehler beim Öffnen einer XML-Datei (die Datei ist nicht vorhanden oder weist Fehler auf). – **4** Der angegebene XPath hat keinen Wert zurückgegeben. • **Beispiel:** `xmltool.exe %ibmshare%\\ibmegath.xml //system_summary/bios_version GEQ 1UET36WW`

Tabelle 59. Befehle des Antidote Delivery Managers (Forts.)

Befehle	Beschreibung
INRR	Mit dem Befehl INRR können Sie bestimmen, ob das Script in der Umgebung von Rescue and Recovery ausgeführt wird. Die Rückgabewerte lauten: • 0 = Das aktuelle Betriebssystem ist PE. • 1 = Das aktuelle Betriebssystem ist nicht PE. • >1 = Fehler.
STATUS [/QUERY *Position Nachrichtenname* | /CLEAR *Position]*	Mit dem Befehl STATUS /QUERY können Sie bestimmen, ob ein Script ausgeführt wurde oder ob es sich noch in der Warteschlange für die Ausführung befindet. Die Position muss einen der folgenden Werte aufweisen: • **FAIL** Die Nachricht wurde bereits ausgeführt und ist fehlschlagen. • **SUCCESS** Die Nachricht wurde erfolgreich abgeschlossen. • **WORK** Die Nachricht wird soeben oder bei der nächsten Ausführung von Antidote Delivery Manager aufgeführt. • **CACHE** Die Nachricht wird zur Ausführung in die Warteschlange gestellt. Mit dem Befehl STATUS/CLEAR wird die angegebene *Position* gelöscht. Die Rückgabewerte lauten: • 0 = Die angegebene Nachricht wurde gefunden, oder der Befehl wurde erfolgreich aufgeführt. • 1 = Die angegebene Nachricht wurde nicht gefunden, oder der Befehl ist fehlschlagen.

Unterstützte Microsoft-Befehle

Tabelle 60. Unterstützte Microsoft-Befehle

Befehle	Beschreibung
ATTRIB.EXE	Anzeigen oder Ändern von Dateiattributen.
CACLS.EXE	Anzeigen oder Ändern von Zugriffssteuerungslisten (ACLs).
CHKDSK.EXE	Überprüfung eines Datenträgers und Anzeige eines Statusberichts.
COMP.EXE	Vergleich des Inhalts zweier Dateien oder zweier Gruppen von Dateien.
COMPACT.EXE	Anzeigen oder Ändern der Komprimierung von Dateien auf NTFS-Partitionen.
CONVERT.EXE	Konvertieren von FAT-Datenträgern in NTFS-Datenträger. Das aktuelle Laufwerk kann nicht konvertiert werden.
DISKPART.EXE	Partitionieren eines Laufwerks.
FC.EXE	Vergleich zweier Dateien oder zweier Gruppen von Dateien und Anzeige der Unterschiede zwischen ihnen.

Tabelle 60. Unterstützte Microsoft-Befehle (Forts.)

Befehle	Beschreibung
FIND.EXE	Suche in einer Datei oder in mehreren Dateien nach einer Textzeichenfolge.
FINDSTR.EXE	Suche in Dateien nach Zeichenfolgen.
FORMAT.COM	Formatieren eines Datenträgers für Windows.
LABEL.EXE	Ändern oder Löschen der Datenträgerbezeichnung.
NET.EXE	Angeben der Befehle für den Netzbetrieb.
PING.EXE	Überprüfen, ob eine Netzressource erreicht werden kann.
RECOVER.EXE	Wiederherstellen der lesbaren Daten eines beschädigten oder fehlerhaften Datenträgers.
REG.EXE	Bearbeiten der Registrierungsdatenbank.
REPLACE.EXE	Ersetzen von Dateien.
RRCMD.EXE	Ausführen von Sicherungen über das Betriebssystem oder von Wiederherstellungen über das Betriebssystem oder Rescue and Recovery; Sortieren von Eingabedaten.
SORT.EXE	Sortieren von Eingabedaten.
SUBST.EXE	Zuordnen eines Pfads zu einem Laufwerkbuchstaben.
XCOPY.EXE	Kopieren von Dateien und Verzeichnisstrukturen.

Vorbereitung und Installation

Vorbereitung

Wenn ein Signierschlüssel verwendet wird, muss der Administrator das Tool zur Paketerstellung mit dem Parameter /NEWKEY ausführen, um einen neuen Signierschlüssel zu generieren.

Konfiguration

Es sind mehrere Konfigurationselemente erforderlich. Diese Elemente sind in der Datei TVT.TXT enthalten.

Repository

Auf jedem Client muss eine Liste von Repositorys vorhanden sein. Diese muss Diskettenlaufwerke sowie das Laufwerk C:\ und mindestens ein Netzlaufwerk umfassen, das mit einer allgemeinen Namenskonvention angegeben ist: `mailbox =` gibt das Laufwerk und den Pfad für die Positionen von Mailboxen an, wobei diese Angaben durch Kommata getrennt und in der Reihenfolge ihrer Wichtigkeit aufgeführt sind. Beispiel:

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

Planungsinformationen

Der Planungsmodus gibt die Häufigkeit von Überprüfungen an.

Tabelle 61. Planungsmodi

Planungsmodus	
SCHED_NONE	0x000
SCHED_MINUTELY	0x001

Tabelle 61. Planungsmodi (Forts.)

Planungsmodus	
SCHED_DAILY	0x002
SCHED_WEEKLY	0x004
SCHED_MONTHLY	0x008
SCHED_STARTUP	0x010
SCHED_WAKEUP	0x020
SCHED_USB_ATTACH	0x040
SCHED_NETWORK_ATTACH	0x080

```
[Scheduler]
Task1=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
```

Signierschlüssel

Wenn Signierschlüssel verwendet werden, müssen diese an den Client verteilt werden. Die mit dem Befehl APKGMES erstellte Datei "keyfile.pub" enthält den Schlüssel. Jeder autorisierte öffentliche Signierschlüssel ist in der Datei TVT.TXT wie folgt aufgeführt: `pubkey X = ...`. Dabei steht *X* für eine ganze Zahl, und es können bis zu neun öffentliche Schlüssel gespeichert werden. Sie können diesen Wert mit der Funktion APUBKEY festlegen. Wenn `nosig =` den Wert 1 aufweist, dürfen nicht signierte (mit dem Parameter /NOSIG erstellte) Pakete ausgeführt werden.

Anmerkung: Wenn dieser Wert nicht 1 beträgt oder wenn in der Datei TVT.TXT öffentliche Schlüssel vorhanden sind, werden keine nicht signierten Pakete ausgeführt.

Netzlaufwerke

Die folgenden Werte werden mit der AUNCPW-Funktion `RscDrvY` festgelegt. Jeder Abschnitt von `RscDrv` enthält Informationen zu einem freigegebenen Netzverzeichnis. Für Antidote Delivery Manager können bis zu zehn freigegebene Netzverzeichnisse definiert werden.

- UNC = Die allgemeine Namenskonvention des Laufwerks, mit dem Sie Antidote Delivery Manager verbinden müssen
- User = Verschlüsselter Benutzername
- Pwd = Verschlüsseltes Kennwort
- Ref = Der Referenzname, der dieser Verbindung zugeordnet werden soll

Installation auf Clients

Rescue and Recovery 2.0 muss auf allen Clients installiert werden. Die oben vorbereitete Konfiguration kann entweder bei der Installation oder später erfolgen.

Serverinfrastruktur

Der Administrator muss freigegebene Netzverzeichnisse für das Repository einrichten oder eine FTP- oder HTTP-Site bereitstellen. Für Programmkorrekturen kann ein zusätzliches Repository erforderlich sein.

Einfacher Systemtest – Benachrichtigung in der Anzeige

Script vorbereiten und packen

Schreiben Sie auf einem beliebigen System, auf dem Antidote Delivery Manager installiert ist, ein Script mit dem Namen GO.RRS. Fügen Sie darin die folgende Zeile ein: `MSGBOX /MSG "Hello World" /OK`. Führen Sie den Befehl direkt über die Eingabeaufforderung aus, um sicherzustellen, dass er wie gewünscht funktioniert. Führen Sie anschließend in dem Verzeichnis, in dem sich die Datei GO.RRS befindet, den Befehl APKGMSG aus, um eine Nachricht zu erstellen. Stellen Sie die Nachrichtendatei in eines der Repositoryverzeichnisse auf Ihrem Computer, und überprüfen Sie die ordnungsgemäße Ausführung.

Implementierung

Bevor Sie den Antidote Delivery Manager implementieren, sollten Sie folgende Schritte ausführen:

1. Die Positionen für die Mailboxen bestimmen.
   - *Mailboxen* sind als Verzeichnisse in freigegebenen Netzverzeichnissen, in lokalen Systemen auf einem Festplattenlaufwerk oder auf einem austauschbaren Datenträger oder auf einer FTP- oder HTTP-Site definiert.
   - Es kann von Nutzen sein, über mehrere Mailboxen zu verfügen, für den Fall, dass auf eine Mailbox nicht zugegriffen werden kann. Sie können bis zu zehn Mailboxpositionen definieren.
   - Clients sollten für Mailboxen im Netz nur über schreibgeschützten Zugriff verfügen; der Schreibzugriff sollte beschränkt werden.
2. Mailboxen in der TXT.TXT-Datei definieren:
   - Bearbeiten Sie in einem Donatorsystem, auf dem Rescue and Recovery installiert ist, die Datei TVT.TXT im Verzeichnis *C:\Program Files\IBM\ThinkVantage*.
   - Erstellen Sie in der Datei TVT.TXT einen neuen Abschnitt `rescue`.
   - Fügen Sie im Abschnitt ″rescue″ folgenden Eintrag hinzu:

     ```
     mailbox=
     ```

     und fügen Sie Ihre Mailboxverzeichnisinformationen hinzu. Mailboxen auf dem lokalen Laufwerk weisen beispielsweise folgende Form auf:

     ```
     [rescue]
     mailbox=C:\ADM\Mailbox,
      \\Network\Share
     ```

     Mailboxen auf einer FTP-Site weisen folgende Form auf:

     ```
     ftp://ftp.Ihremailbox.com
     ```

     Mailboxen auf einem freigegebenen Netzlaufwerk weisen folgende Form auf:

     ```
     \\Network\Share
     ```

     Anmerkungen:

     a. HTTPS wird für Mailbox-Funktionen nicht unterstützt.

b. Der HTTP-Webserver muss so konfiguriert sein, dass die Indexerstellungsfunktion und die Funktion zum Auflisten von Dateien aktiviert sind.

Die Laufwerkbuchstaben können sich unter Windows Professional Edition im Vergleich zu Ihrer normalen Betriebssystemumgebung ändern. Laufwerk C: wird seinen Namen höchstwahrscheinlich ändern. Um dies zu umgehen, verwenden Sie die Umgebungsvariable *CUSTOS*, die immer auf das Laufwerk verweist, auf dem sich das typische Betriebssystem des Kunden befindet. Das oben angegebene Beispiel würde sich dadurch ändern in:

```
mailbox=%CUSTOS%\ADM\Mailbox,ftp://ftp.Ihremailbox.com, \\Network\Share
```

Die Länge der Zeichenfolge ist beliebig, sofern die Standards für die verwendete Einheit und das verwendete Protokoll eingehalten werden. Wenn Sie zum Beispiel eine lokale Datei verwenden, darf die Länge des Pfades 256 Zeichen nicht überschreiten.

- Mehrere Mailboxeinträge müssen durch Kommata oder Semikolons voneinander getrennt sein.
- Antidote Delivery Manager durchsucht die angegebenen Mailboxpositionen nacheinander nach Paketen.

3. Wenn ein Benutzername und ein Kennwort für eine FTP- oder HTTP-Verbindung erforderlich sind, verwenden Sie folgendes Format:

   ```
   ftp//Benutzername:Kennwort@ftp.Ihremailbox.com
   ```

4. Für Benutzernamen und Kennwörter für Mailboxen in freigegebenen Netzverzeichnissen gilt:

   Die Einträge für Benutzernamen und Kennwörter werden verschlüsselt in der Datei TVT.TXT gespeichert. Um im Donatorsystem einen Eintrag hinzuzufügen, gehen Sie wie folgt vor:

   a. Öffnen Sie ein DOS-Fenster.
   b. Wechseln Sie in das Verzeichnis `C:\Program Files\IBM ThinkVantage\Rescue and Recovery\ADM`.
   c. Führen Sie folgenden Befehl aus:

      ```
      auncpw /add \\Network\Share /user Benutzername /pwd Kennwort /ref refID
      ```

      Dadurch wird folgender Eintrag in der Datei TVT.TXT erstellt:

      ```
      [RscDrv0]
      UNC=\\Network\Share
      User=01E23397A54D949427D5AF69BF407D5C
      Pwd=04E22197B34D95943ED5A169A0407C5C
      Ref=refID
      ```

   Anmerkungen:

   a. Dieser Eintrag kann auf jedem System verwendet werden, das Antidote Delivery Manager zum Zugreifen auf dasselbe freigegebene Verzeichnis verwenden soll.
   b. Antidote Delivery Manager kann bis zu zehn freigegebene Netzverzeichnisse verwenden.
   c. Zusätzlich zu den zehn freigegebenen Netzverzeichnissen können weitere Mailboxeinträge hinzugefügt werden, etwa über FTP oder lokal.
   d. Die Datei AUNCPW.EXE verfügt über weitere Funktionen zum Kennwortmanagement. Geben Sie AUNCPW /? in die Befehlszeile ein, oder schlagen Sie in Tabelle 59 auf Seite 191 nach.

5. Erstellen Sie ein Schlüsselpaar mit einem öffentlichen und einem privaten Antidote Delivery Manager-Schlüssel. Es wird empfohlen, dazu die Funktionalität zum Erstellen eines Schlüsselpaars mit einem öffentlichen und einem privaten Schlüssel von Antidote Delivery Manager zu verwenden. Antidote Delivery Manager verwendet ein Schlüsselpaar mit einem öffentlichen und einem privaten Schlüssel, um die Authentizität von Paketen zu überprüfen. Der private Schlüssel sollte sorgfältig geschützt und nicht weitergegeben werden. Der zugehörige öffentliche Schlüssel sollte sich auf jedem Client befinden, der von Antidote Delivery Manager verwaltet wird. Um ein Schlüsselpaar mit einem öffentlichen und einem privaten Schlüssel auf einem Nicht-Donatorsystem zu erstellen, auf dem Rescue and Recovery installiert ist, gehen Sie wie folgt vor:
   a. Öffnen Sie ein DOS-Fenster.
   b. Wechseln Sie in das Verzeichnis C:\Program Files\IBM ThinkVantage\Rescue and Recovery\ADM.
   c. Führen Sie folgenden Befehl aus:
      ```
      apkgmes.exe /newkey mykey
      ```
      Dadurch werden zwei Dateien erstellt, "mykey.pub" und "mykey.prv", für den öffentlichen und für den privaten Schlüssel.
   d. Kopieren Sie den öffentlichen Schlüssel in das Verzeichnis C:\Program Files\IBM ThinkVantage\Rescue and Recovery\ADM des Donatorsystems.
   e. Öffnen Sie die Datei mit einem Textverarbeitungsprogramm, wie zum Beispiel "notepad.exe".
   f. Kopieren Sie den Inhalt der Datei in die Zwischenablage.
   g. Geben Sie Folgendes in die Befehlszeile ein:
      ```
      apubkey.exe /add x
      ```
      x steht dabei für den Inhalt der Zwischenablage.
   h. Dadurch wird folgender Eintrag im Abschnitt "rescue" der Datei TVT.TXT vorgenommen: `pubkey0=906253...`
   - In der Datei TVT.TXT können bis zu zehn öffentliche Schlüssel gespeichert werden.
   - Die Datei APUBKEY.EXE verfügt über weitere Funktionen zum Management von öffentlichen Schlüsseln. Geben Sie in die Befehlszeile `APUBKEY /?` ein, oder schlagen Sie in Tabelle 59 auf Seite 191 nach.
6. Erstellen Sie die Überprüfung "Schedule Antidote Delivery Manager" (mehrere Planungen sind erlaubt). Antidote Delivery Manager muss dazu regelmäßig auf dem System ausgeführt werden. Um einen Zeitplan festzulegen, der alle 20 Minuten ausgeführt wird, sollte der folgende Text in die Datei TVT.TXT des Donatorsystems hinzugefügt werden:
   ```
   [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
   ```

ScheduleMode ist dabei das Ereignis, das die Übermittlung des Antidote Delivery Manager-Pakets auslöst. Die Parameter lauten:

Tabelle 62. Parameter für Antidote Delivery Manager

Parameter	Wert
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

Anmerkungen:

a. Die Planungsfunktion kann in der Predesktop Area nicht ausgeführt werden.

b. Weitere Information hierzu finden Sie im Abschnitt „Sicherungen und zugehörige Aufgaben planen" auf Seite 167.

7. Erstellen Sie ein Antidote Delivery Manager-Paket.

   Nachdem Sie die vorigen Schritte ausgeführt haben, erstellen und verteilen Sie nun Ihr erstes Paket. Führen Sie auf dem Administratorsystem (einem Nicht-Donatorsystem) folgende Schritte aus:

   a. Erstellen Sie ein Verzeichnis, wie zum Beispiel *C:\ADM\Build*.

   b. Erstellen Sie in diesem Verzeichnis eine Datei mit dem Namen GO.RRS, und fügen Sie folgenden Text hinzu:

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

   c. Speichern und schließen Sie die Datei.

   d. Wechseln Sie in das Verzeichnis C:\Program Files\IBM ThinkVantage\Rescue and Recovery\ADM.

   e. Führen Sie folgenden Befehl aus:

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

   f. Dadurch wird ein Paket mit dem Namen HELLOPKG*JJMMTTSSmm*.ZAP erstellt, in dem *JJMMTTSSmm* durch das aktuelle Datum und die aktuelle Uhrzeit ersetzt werden.

8. Kopieren Sie HELLOPKG*JJMMTTSSmm*.ZAP in die Mailboxposition, die Sie in Schritt 2 angegeben haben.

9. Rufen Sie Antidote Delivery Manager auf.

   a. Wenn der Zeitgeber auf dem Donatorsystem abgelaufen ist, wird das Paket ausgeführt, und die Nachricht "Hello World" wird angezeigt.

   b. Wenn Sie nicht bis dahin warten möchten, können Sie im Donatorsystem "C:\Program Files\IBM ThinkVantage\Rescue and Recovery\ADM\mailman.exe" eingeben.

Beispiele

Es folgen einige Beispiel für die Verwendung von Antidote Delivery Manager:

Beispiel 1

In diesem Beispiel geht es um ein Paket zum Reparieren eines Computers, der durch Virenbefall oder bedingt durch einen falschen Eintrag in der Registrierungsdatenbank dauerhaft eine Systemabsturzanzeige anzeigt.

1. Angenommen, der Clientcomputer zeigt die Systemabsturzanzeige aufgrund eines Virus an, der über den Schlüssel "Run" (Ausführen) in der Registrierungsdatenbank ausgeführt wird. Um dies zu beheben, muss eine Datei mit dem Namen "go.rrs" erstellt werden, die den Befehl *reg* ausführt. Eine Liste der Microsoft-Befehle finden Sie im Abschnitt „Unterstützte Microsoft-Befehle" auf Seite 195. Der Befehl "reg" entfernt den Wert aus der Registrierungsdatenbank und löscht die ausführbare Datei wenn möglich vom System. Der Inhalt weist in etwa folgende Form auf:

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

2. Legen Sie Ihre Datei "go.rrs" in Ihrem Verzeichnis *c:\adm\build* ab, und führen Sie folgenden Befehl aus:

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

3. Kopieren Sie REMOVEVIRUS*JJTTSSmm*.ZAP in Ihre Mailbox.
4. Booten Sie alle Clients, und drücken Sie die Taste Access IBM/F11 oder die Eingabetaste, um die Predesktop Area aufzurufen, in der die Datei "mailman.exe" beim Systemstart ausgeführt wird. Führen Sie anschließend das Paket REMOVEVIRUS aus.

Beispiel 2

In diesem Beispiel wird eine Quick Fix Engineering-Aktualisierung oder eine Programmkorrektur an Clientmaschinen versandt.

1. Erstellen Sie ein Verzeichnis, in dem die Scriptdatei und die Dateien mit der Programmkorrektur gespeichert werden, wie zum Beispiel *C:\adm\patchbuild*.
2. Legen Sie die ausführbare Datei mit der Erweiterung "gfe" oder die Datei mit der Programmkorrektur im Verzeichnis c:\adm\patchbuild ab.
3. Erstellen Sie eine Datei mit dem Namen "go.rrs", und fügen Sie darin folgende Zeilen hinzu. Passen Sie jedoch die Zeile an, die die Microsoft Quick Fix Engineering-Aktualisierung oder die Programmkorrektur ausführt und installiert. Da diese Programmkorrektur nur unter einem normalen Windows-Betriebssystem installiert werden kann, verhindert dieses Script, dass die Programmkorrektur unter Windows Professional Edition installiert wird.

   ```
   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. Stellen Sie die Datei ″go.rrs″ in das Verzeichnis c:\adm\patchbuild, und führen Sie folgenden Befehl aus:

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

5. Kopieren Sie PATCHBUILD*JJTTSSMM*.ZAP in Ihre Mailbox.
6. Die Programmkorrektur wird entweder bei der nächsten geplanten Ausführung der Datei ″mailman.exe″ oder bei einem Neustart der Clientmaschine ausgeführt.

Möglichkeiten, zu überprüfen, ob ein Paket ausgeführt wurde oder nicht

- **Fail log (Fehlerprotokoll)**

  Diese Datei ist normalerweise im Verzeichnis *c:\ibmtools\utils\rescue* gespeichert. Wenn eine Datei mit der Erweiterung ″zap″ mit einem anderen Wert als Null beendet wird, wird sie in diese Datei eingetragen.

- **Rescue log (Wiederherstellungsprotokoll)**

  Diese Datei befindet sich normalerweise im Verzeichnis *c:\ibmshare*. Sie enthält ausführlichere Informationen, um zu bestimmen, warum ein Paket fehlgeschlagen ist, oder um sich zu vergewissern, dass ein Paket funktioniert hat. Diese Datei enthält Zeile für Zeile den Inhalt einer Datei mit der Erweiterung ″zap″.

- **Success Log (Erfolgsprotokoll)**

  Diese Datei ist normalerweise im Verzeichnis *c:\ibmtools\utils\rescue* gespeichert. Wenn eine Datei mit der Erweiterung ″zap″ mit dem Wert Null beendet wird, wird sie in diese Datei eingetragen.

Beispiel 3

In diesem Beispiel wird eine FTP- oder eine HTTP-Site in der Predesktop Area verwendet:

1. Definieren Sie eine externe Website für Pakete:

   ```
   ftp.Ihremailbox.com
   ```

2. Erstellen Sie öffentliche/private Schlüssel. Siehe dazu Schritt 5.
3. Fügen Sie die Mailbox wie folgt in der Datei TVT.TXT hinzu:

   ```
   mailbox=ftp://Benutzername:Kennwort@ftp.Ihremailbox.com
   ```

4. Wenn der Benutzer die Taste ″Access IBM″/F11 oder die Eingabetaste drückt, um auf die Predesktop Area zuzugreifen, wird das Antidote Delivery Manager-Paket beim Booten in der Predesktop Area ausgeführt.

Beispiel 4

In diesem Beispiel wird die Datei ″xmltool.exe″ verwendet, um bestimmte Clients auszuwählen:

1. Verteilen Sie die xml-Datei mit den Informationen, anhand derer Sie Ihre Clientmaschinen vergleichen möchten, über Active Directory, Systems Management Server oder ein anderes Management-Tool.

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

2. Fügen Sie in der ersten Zeile der Datei ″go.rrs″ eine Zeile ein, die das xml-Tool verwendet. Diese Zeile ist ein Beispiel für ein Paket, das NUR Zielmaschinen aus der Marketingabteilung auswählen würde.

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

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

Angriff eines gefährlichen Virus

Im folgenden Beispiel wird das mögliche Vorgehen bei der Bekämpfung eines gefährlichen Virus veranschaulicht. Das Vorgehen besteht im Wesentlichen darin, den Netzbetrieb auszuschalten, in Rescue and Recovery zu booten, dann die Registrierungsdatenbank zu reparieren, eine Ersatzdatei in die entsprechende Position zu kopieren, anschließend wieder in Windows XP zu booten und den Netzbetrieb wiederherzustellen. Zu Demonstrationszwecken muss die folgende Anwendung syntaktisch aktualisiert werden.

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.
```

Anhang G. Bemerkungen

Möglicherweise bietet Lenovo die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim Lenovo Ansprechpartner erhältlich. Hinweise auf Lenovo Lizenzprogramme oder andere Lenovo Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von Lenovo verwendet werden können. Anstelle der Lenovo Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von Lenovo verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremdservices liegt beim Kunden.

Für in dieser Dokumentation beschriebene Erzeugnisse und Verfahren kann es Lenovo Patente oder Patentanmeldungen geben. Mit der Auslieferung dieser Dokumentation ist keine Lizenzierung dieser Patente verbunden. Lizenzanfragen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

Lenovo (United States), Inc
500 Park Offices Drive, Hwy 54
Research Triangle Park, NC 27709
USA
Lenovo Director of Licensing

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Lenovo kann jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Die in diesem Dokument beschriebenen Produkte sind nicht zur Verwendung bei Implantationen oder anderen lebenserhaltenden Anwendungen, bei denen ein Nichtfunktionieren zu Verletzungen oder zum Tode führen könnte, vorgesehen. Die Informationen in diesem Dokument beeinflussen oder ändern nicht die Lenovo Produktspezifikationen oder Gewährleistungen. Keine Passagen in dieser Dokumentation stellen eine ausdrückliche oder stillschweigende Lizenz oder Anspruchsgrundlage bezüglich der gewerblichen Schutzrechte von Lenovo oder von anderen Firmen dar. Alle Informationen in dieser Dokumentation beziehen sich auf eine bestimmte Betriebsumgebung und dienen zur Veranschaulichung. In anderen Betriebsumgebungen werden möglicherweise andere Ergebnisse erzielt.

Werden an Lenovo Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Verweise in diesen Informationen auf Websites anderer Anbieter dienen lediglich als Benutzerinformationen und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses Lenovo Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer gesteuerten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Marken

Die folgenden Namen sind in gewissen Ländern Marken der Lenovo Group Limited:

- Lenovo
- Rescue and Recovery
- ThinkPad
- ThinkCentre
- ThinkVantage
- Rapid Restore

Intel ist in gewissen Ländern eine Marke oder eine eingetragene Marke der Intel Corporation oder einer ihrer Tochtergesellschaften.

Folgende Namen sind in gewissen Ländern Marken der International Business Machines Corporation: IBM, Lotus und Lotus Notes.

Microsoft, Windows und Windows NT sind in gewissen Ländern Marken der Microsoft Corporation.

Andere Namen von Unternehmen, Produkten oder Services können Marken oder Servicemarken anderer Unternehmen sein.

Glossar

AES (Advanced Encryption Standard). Bei *AES* handelt es sich um eine Verschlüsselungstechnik mit *symmetrischem Schlüssel*. Seit Oktober 2000 verwendet die US-Regierung diesen Algorithmus als Verschlüsselungstechnik, wobei AES die DES-Verschlüsselung ersetzt hat. AES bietet höhere Sicherheit gegen Brute-Force-Attacken als 56-Bit-DES-Schlüssel. AES kann ggf. 128-, 192- und 256-Bit-Schlüssel verwenden.

BIOS-Administratorkennwort (ThinkCentre) / BIOS-Supervisorkennwort (ThinkPad). Mit dem Administratorkennwort/Supervisorkennwort wird die Möglichkeit zum Ändern der BIOS-Einstellungen gesteuert. Dies umfasst das Aktivieren/Inaktivieren des integrierten Sicherheitschips und das Löschen des SRK (Storage Root Key), der im TPM (Trusted Platform Module) gespeichert ist.

Integrierter Sicherheitschip. ″Integrierter Sicherheitschip″ ist ein anderer Name für das TPM (Trusted Platform Module).

Speicher-Rootschlüssel (SRK, Storage Root Key). Beim Speicher-Rootschlüssel (SRK) handelt es sich um ein öffentliches Schlüsselpaar mit mindestens 2.048 Bit. Er ist ursprünglich leer und wird bei der Zuordnung des TPM-Eigners erstellt. Dieses Schlüsselpaar verbleibt immer im integrierten Sicherheitschip. Es dient zum Verschlüsseln (Verpacken) von privaten Schlüsseln für das Speichern außerhalb des TPM (Trusted Platform Module) und zum Entschlüsseln der Schlüssel, wenn diese wieder in das TPM geladen werden. Der SRK kann von jedem Benutzer mit Zugriff auf das BIOS gelöscht werden.

TPM (Trusted Platform Module). TPMs (Trusted Platform Modules) sind integrierte Schaltkreise für besondere Zwecke, die zum Ermöglichen einer strengen Benutzerauthentifizierung und Maschinenprüfung in Systeme integriert werden. Der Hauptzweck von TPMs ist es, den unberechtigten Zugriff auf vertrauliche und sensible Informationen zu verhindern. Das TPM ist eine auf Hardware aufbauende Sicherheitsbasis, die eine Vielzahl von Verschlüsselungsservices auf einem System zur Verfügung stellen kann. Ein anderer Name für das TPM ist ″integrierter Sicherheitschip″.

Verschlüsselungssysteme. Verschlüsselungssysteme können allgemein als Verschlüsselung mit symmetrischem Schlüssel, bei der ein einzelner Schlüssel für die Verschlüsselung und Entschlüsselung von Daten genutzt wird, und als Verschlüsselung mit öffentlichem Schlüssel, bei der zwei Schlüssel (ein öffentlicher Schlüssel, der allen bekannt ist, und ein privater Schlüssel, auf den nur der Besitzer des Schlüsselpaars Zugriff hat) verwendet werden, klassifiziert werden.

Verschlüsselung mit öffentlichem Schlüssel/asymmetrischem Schlüssel. Algorithmen mit öffentlichem Schlüssel verwenden gewöhnlich ein Paar zusammengehöriger Schlüssel. Dabei handelt es sich um einen geheimen privaten Schlüssel und einen öffentlichen Schlüssel, der verbreitet werden kann. Die beiden Schlüssel eines Paares sollten nicht voneinander abgeleitet werden können. Der Begriff ″Verschlüsselung mit öffentlichem Schlüssel″ wird von der Idee, die Informationen zum öffentlichen Schlüssel allgemein zugänglich zu machen, abgeleitet. Daneben wird auch der Begriff ″Verschlüsselung mit asymmetrischem Schlüssel″ verwendet, da nicht alle Parteien über dieselben Informationen verfügen. Auf gewisse Weise ″verschließt″ ein Schlüssel ein Schloss (Verschlüsselung) und ein anderer Schlüssel ist für das ″Aufschließen″ des Schlosses (Entschlüsselung) erforderlich.

Verschlüsselung mit symmetrischem Schlüssel. Bei Verschlüsselung mit symmetrischem Schlüssel wird für die Verschlüsselung und für die Entschlüsselung von Daten derselbe Schlüssel verwendet. Verschlüsselungen mit symmetrischem Schlüssel sind einfacher und schneller. Ihr größter Nachteil besteht darin, dass die beiden Parteien einen sicheren Weg finden müssen, den Schlüssel austauschen. Bei Verschlüsselung mit öffentlichem Schlüssel besteht dieses Problem nicht, da der öffentliche Schlüssel auf einem nicht gesicherten Weg verbreitet werden kann und der private Schlüssel nie übertragen wird. AES (Advanced Encryption Standard) ist ein Beispiel für einen symmetrischen Schlüssel.

ThinkVantage

Teilenummer: 41R9854

(1P) P/N: 41R9854