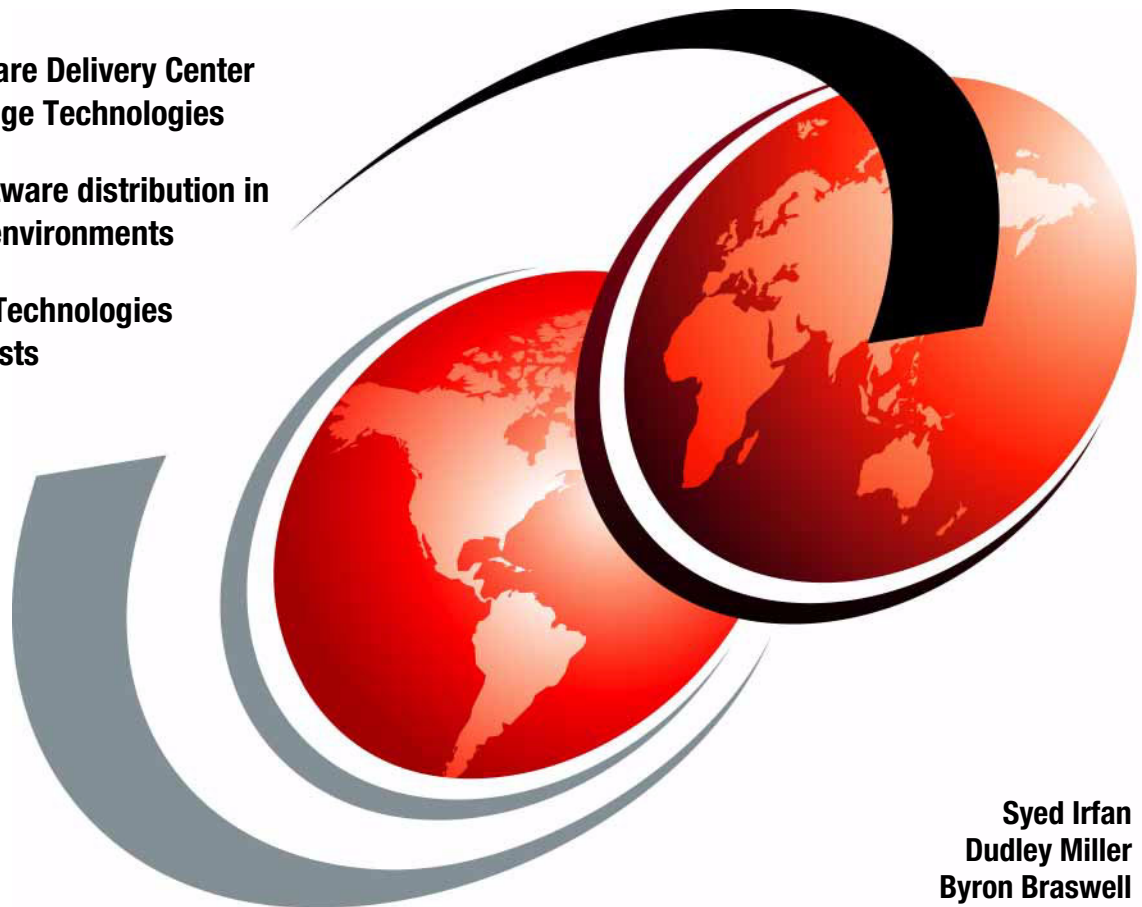


Using ThinkVantage Technologies: Volume 2 Maintaining and Recovering Client Systems

New Software Delivery Center
ThinkVantage Technologies

Simple software distribution in
corporate environments

Use of the Technologies
to lower costs



Syed Irfan
Dudley Miller
Byron Braswell



International Technical Support Organization

**Using ThinkVantage Technologies: Volume 2
Maintaining and Recovering Client Systems**

January 2005

Note: Before using this information and the product it supports, read the information in “Notices” on page xi.

Fourth Edition (January 2005)

This edition applies to Version 2.0 of Rescue and Recovery, Version 1.01 of System Information Center, Version 1.1 of Software Delivery Center, Version 4.5 of Access IBM, Version 5.21 of Client Security Software for ESS, Release 2 of File and Folder Encryption, and Release 1.3 of IBM Client Security Password Manager

© Copyright International Business Machines Corporation 2003, 2004, 2005. All rights reserved.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Noticesxi
Trademarks	xii
Preface	xiii
The team that wrote this redbook	xiii
Become a published author	xvii
Comments welcome	xvii
Summary of changes	xix
January 2005, Fourth Edition	xix
Chapter 1. Introduction	1
1.1 ThinkVantage Technologies	3
1.2 ThinkVantage Technologies process improvements	7
1.3 Implementing a ThinkVantage Technologies solution	8
Chapter 2. Rescue and Recovery	11
2.1 Introducing Rescue and Recovery	12
2.1.1 Rescue and Recovery environment and functions	12
2.1.2 Rescue and Recovery functions	14
2.1.3 Rescue and Recovery components	15
2.1.4 Rescue and Recovery backup methodology	16
2.1.5 Managing backups	18
2.1.6 Rescue and Recovery system requirements	20
2.2 Installing Rescue and Recovery	22
2.2.1 Preparing to install Rescue and Recovery	22
2.2.2 Rescue and Recovery environment configurations	23
2.2.3 Rescue and Recovery installation	29
2.2.4 Silent installation	31
2.2.5 Setting up a Create Base Backup icon on the user's desktop	36
2.2.6 Creating rescue media	37
2.2.7 Uninstall Rescue and Recovery	38
2.3 System backup	38
2.3.1 Backup considerations	39
2.3.2 Setting backup preferences	41
2.3.3 Backing up your system	45
2.3.4 Archiving backups	50
2.3.5 Scheduling backups	52
2.3.6 Disabling scheduled backups	55

2.3.7 Backing up encrypted files	56
2.4 Restoring your system.	56
2.4.1 Using the Rescue and Recovery environment	57
2.4.2 Rescue and Recovery toolbar.	58
2.4.3 Rescue and Recovery menu options	61
2.4.4 Restoring your system from Windows.	70
2.4.5 Restore considerations	79
2.5 Troubleshooting.	79
2.5.1 Installation troubleshooting	79
2.5.2 Backup and Restore troubleshooting information	79
2.5.3 Encryption troubleshooting	81
2.5.4 General troubleshooting and tips	83
2.5.5 Frequently asked questions	88
Chapter 3. IBM System Information Center	91
3.1 Introduction to System Information Center	92
3.1.1 System Information Center features	92
3.1.2 System Information Center components.	94
3.1.3 System Information Center requirements	95
3.1.4 System Information Center overview	95
3.2 System Information Center server installation.	96
3.2.1 Server operating system installation	96
3.2.2 Apache Tomcat Web server installation	97
3.2.3 System Information Center installation	97
3.2.4 Testing the installation	117
3.2.5 Modifying the System Information Center installation.	124
3.3 Logging on to System Information Center.	128
3.3.1 System Information Center user accounts	128
3.3.2 The logon process.	129
3.4 System Information Center main menu.	133
3.5 Assets	133
3.5.1 Upload Asset Scan	135
3.5.2 Register Asset.	140
3.5.3 Manually Add Asset	142
3.5.4 My Assets	143
3.5.5 All Assets	144
3.5.6 Filter	144
3.5.7 Information	144
3.5.8 Users.	145
3.5.9 Change Owner	146
3.5.10 Compare Revisions.	147
3.5.11 Compare Selected	148
3.5.12 Delete	150

3.5.13	Download XML file	150
3.5.14	Edit	151
3.5.15	Reprocess	152
3.5.16	Retire	152
3.5.17	Return	153
3.5.18	Surplus	153
3.5.19	Download Agent Installer	154
3.6	User Management	155
3.6.1	Creating a new user	156
3.6.2	My Details	157
3.6.3	All Users	158
3.6.4	User Details	158
3.6.5	User History	158
3.6.6	Delete	158
3.6.7	Edit	160
3.7	Group management	161
3.7.1	New Group	162
3.7.2	My Groups	163
3.7.3	All Groups	163
3.7.4	Groups	164
3.7.5	Add Users	164
3.7.6	Delete Group	165
3.7.7	Edit Group	165
3.7.8	Remove All Group Members	166
3.8	Reports	167
3.8.1	All Assets	168
3.8.2	Data Maintenance	171
3.8.3	Groups	174
3.8.4	Logs	175
3.8.5	My Assets	176
3.8.6	Software	178
3.8.7	Statistics	180
3.8.8	Tasks	180
3.8.9	ThinkVantage Reports	181
3.8.10	Users	184
3.8.11	Workstation Security	186
3.8.12	All Reports	188
3.8.13	Rearrange report display output	190
3.9	Tasks	192
3.10	Admin	193
3.10.1	View Properties File	194
3.10.2	View Application Log	195
3.10.3	Send Application Log	195

3.10.4	Upload File to Server	195
3.10.5	View Current Server Status	195
3.10.6	Stop and Requeue Background Tasks	196
3.10.7	Interrupt Current Background Tasks	196
3.11	Options	197
3.11.1	Set Current Query as Default	198
3.11.2	Refresh Result	198
3.11.3	Add Query Column	198
3.11.4	Add Query Table	202
3.11.5	Page Options	203
3.12	Output	206
3.13	IBM System Information Gatherer	210
3.13.1	Temporarily installed client agent	210
3.13.2	Permanently installed client agent	211
3.13.3	Installation from product CD	211
3.13.4	Installation from the Web (IBM computers only)	215
3.14	Customization and advanced usage	216
3.14.1	Enterprise environment considerations	216
3.14.2	Deployment scenarios	216
3.14.3	Secure access	218
Chapter 4.	IBM Software Delivery Center	219
4.1	Introduction	220
4.1.1	Software Delivery Center benefits and features	220
4.1.2	Software Delivery Center components	222
4.2	Architecture considerations	224
4.2.1	Architecture considerations	225
4.2.2	Customization considerations	229
4.2.3	Hardware specifications and recommendations	230
4.3	Software Delivery Center server installation details	231
4.3.1	Installing a Windows operating system on the server	231
4.3.2	Installing Software Delivery Center	233
4.3.3	Testing the IBM Software Delivery Center server	244
4.3.4	Providing security for the packages on the file server	249
4.4	Installing the Software Delivery Center client	259
4.4.1	Prerequisite software	259
4.4.2	Supported types of installations	260
4.4.3	Testing the Software Delivery Center client	273
4.5	Building your software library	278
4.5.1	Creating a folder structure for your library	279
4.5.2	Creating a software package	280
4.5.3	Creating a software bundle	285
4.5.4	Creating a portable catalog	285

4.5.5	Using a portable catalog	285
4.5.6	Importing files from another server	286
4.5.7	Command prompt Export/Import interface	286
4.6	Setting up Software Delivery Center infrastructure	287
4.6.1	Setting up a pull infrastructure	288
4.6.2	Setting up a push infrastructure	288
4.6.3	Software Delivery Center package directory replication tips	290
4.7	Using the Software Delivery Center administrator's console	292
4.7.1	Accessing Software Delivery Center administrator's console	293
4.7.2	Managing groups	296
4.7.3	Managing users.	306
4.7.4	Managing software packages and bundles.	312
4.7.5	Creating a digital signature for a secure package.	336
4.7.6	Exporting and importing software packages and bundles.	336
4.7.7	Exporting a portable catalog	351
4.7.8	Managing distributions	354
4.7.9	Managing machines	364
4.7.10	Managing schedules.	367
4.7.11	Using the IBM Software Delivery Center logs	375
4.7.12	Finding help.	381
4.7.13	Logging out of the administrator's console	381
4.8	Using the Software Delivery Center software catalog.	381
4.8.1	Software Delivery Center client applet	382
4.8.2	Accessing the Software Delivery Center server	385
4.8.3	Launching the Software Delivery Center client applet	386
4.8.4	Installing an application.	396
4.8.5	Installing a bundle.	398
4.9	Troubleshooting.	401
4.10	Getting help and support.	403
Chapter 5.	Access IBM	405
5.1	Overview	406
5.2	Access IBM	406
5.2.1	Access IBM user interface	408
5.2.2	Customizing Access IBM and Access Help	409
5.2.3	Customizing Access IBM	410
5.2.4	Access IBM Customization Tool	411
5.3	Access Help	418
5.3.1	Customizing Access Help	419
5.4	Rescue and Recovery.	420
5.5	Access IBM Message Center	421
5.5.1	Local messages versus Web messages.	422
5.5.2	What a message file contains	424

5.5.3	Delivering messages of your own	427
5.6	Update Connector	429
5.6.1	Overview	430
5.6.2	Usage Scenarios	431
5.6.3	The network connection	432
5.6.4	Self-managed Mode	435
5.6.5	SMB LAN Mode	436
Chapter 6.	Embedded Security Subsystem	443
6.1	Overview	444
6.1.1	IBM Embedded Security Chip	444
6.1.2	Features	444
6.1.3	Client Security Password Manager	447
6.1.4	File and Folder Encryption (FFE) Utility	448
6.2	Installation considerations	449
6.2.1	IBM Client Security Software	449
6.2.2	File and Folder Encryption considerations	451
6.2.3	Client Security Password Manager	452
6.3	Prerequisites	452
6.3.1	Before installing the software	453
6.3.2	Setting up a supervisor password on a ThinkPad	454
6.3.3	Setting up an administrator password for a ThinkCentre	455
6.3.4	Clearing the IBM Embedded Security Chip on a ThinkPad	455
6.3.5	Clearing the IBM Embedded Security Chip on a ThinkCentre	456
6.4	Installation instructions	457
6.4.1	Preparation	457
6.4.2	Installing prerequisite device drivers	458
6.4.3	Installing IBM Client Security Software	459
6.4.4	Configuring the IBM Client Security Software for the first time	460
6.4.5	Targus DEFCON Fingerprint Reader	473
6.4.6	Performing an unattended installation	474
6.4.7	Upgrading your version of IBM Client Security Software	480
6.5	Supplemental applications	483
6.5.1	Client Security Password Manager	483
6.5.2	File and Folder Encryption (FFE)	487
6.6	Administrator Utility	491
6.6.1	Starting the Administrator Utility	491
6.6.2	User enrollment	492
6.6.3	Edit user settings	494
6.6.4	Application and policy setup	499
6.6.5	Chip and key settings	508
6.7	Registering fingerprints	515
6.8	Using User Verification Manager protection for Lotus Notes	517

6.9	User Configuration Utility	520
6.9.1	Modify Your Security Settings	520
6.10	Administrator Console	524
6.10.1	UVM passphrase bypass	526
6.10.2	Display/Change fingerprint/smart card override password	527
6.10.3	Create administrator configuration file	528
6.10.4	Encrypt/Decrypt Setup Configuration File	533
6.10.5	Configure Credential Roaming	534
6.11	Roaming profiles	534
6.11.1	Prerequisites	535
6.11.2	Setup	536
6.11.3	Utilization of roaming clients	554
6.11.4	Adding users to a roaming profiles system	554
6.11.5	Unattended install with roaming profiles	556
6.12	Using Adobe Acrobat 6.0 Professional	559
6.12.1	Introduction	559
6.12.2	Prerequisites	560
6.12.3	Installation and configuration	560
6.12.4	Hints and tips	567
6.13	Usage scenarios	568
6.13.1	Windows 2000 and Windows XP clients and Outlook Express	568
6.13.2	Windows 2000 clients using Lotus Notes	569
6.13.3	Windows 2000 clients managed by Tivoli Access Manager	570
6.14	Uninstalling	572
6.15	Troubleshooting	573
6.15.1	Error messages	574
6.15.2	Fail counts on TCPA and non-TCPA systems	574
6.15.3	File and Folder Encryption utility known issues	575
6.15.4	Installation troubleshooting information	577
6.15.5	Administrator Utility troubleshooting information	578
6.15.6	User Configuration Utility troubleshooting information	580
6.15.7	ThinkPad-specific troubleshooting information	581
6.15.8	Microsoft troubleshooting information	581
6.15.9	Netscape application troubleshooting information	585
6.15.10	Digital certificate troubleshooting information	587
6.15.11	Tivoli Access Manager troubleshooting information	587
6.15.12	Lotus Notes troubleshooting information	588
6.15.13	Encryption troubleshooting information	589
6.15.14	UVM-aware device troubleshooting information	589
Appendix A. Rescue and Recovery additional information		591
Values and settings of TVT.TXT		591
Making changes to TVT.txt via cfgmod command		597

RRU command prompt interface RRUcmd	598
Other command prompt tools for IBM Rescue and Recovery	599
Uninstalling Rapid Restore Ultra versions 3.x and Rapid Restore PC 2.x	602
Including and excluding files in backups	603
Appendix B. Alternate SQL database for System Information Center	607
How to use IBM DB2 with System Information Center	608
Testing System Information Center with DB2	616
Remove Cloudscape database	618
Using SQL Server 2000 with System Information Center	618
Test ISIC with Microsoft SQL 2000	625
Remove Cloudscape database	626
Appendix C. Software Delivery Center and System Information Center coexistence	627
Installing both programs on the same machine	628
Appendix D. System Information Gatherer scan uploads	631
Problem description	632
Solution	632
Abbreviations and acronyms	635
Related publications	637
IBM Redbooks	637
Other publications	637
Online resources and education	638
How to get IBM Redbooks	639
Help from IBM	639
Index	641

Notices

This information was developed for products and services offered in the U.S.A.

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

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

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

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

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

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Trademarks

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

@server®
e-server®
Redbooks™
Redbooks) ™
Eserver®
ibm.com®
Cloudscape™
DB2®
DFS™
ETE™

HelpCenter®
ImageUltra™
IBM®
Lotus Notes®
Lotus®
LANClient Control Manager™
NetVista™
Notes®
Rapid Restore™
Redbooks™

Redbooks (logo)™
Rescue and Recovery™
ThinkCentre™
ThinkPad®
ThinkVantage™
Tivoli Enterprise™
Tivoli®
TME®
Update Connector™
WebSphere®

The following terms are trademarks of other companies:

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

Intel, Intel Inside (logos), MMX, and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

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

Preface

IBM ThinkVantage Technologies bring your IBM PCs one step closer to being self-configured, self-optimizing, self-protecting, and self-healing to help save you time and money throughout the life of your systems. In short, ThinkVantage Technologies let you focus your attention on your business, rather than on your computer.

ThinkVantage Technologies are software tools designed to help customers drive down IT support costs (especially those associated with managing and supporting systems after initial roll-out), increase security, and decrease the complexity of today's IT infrastructure.

This IBM Redbook will help you maintain, recover and secure the IBM ThinkVantage Technologies on IBM and third-party desktops and mobiles.

This Redbook is volume two of a two-volume set of ThinkVantage Technologies Redbooks. It describes how to maintain and recover client systems. The first Redbook is *Using ThinkVantage Technologies Volume 1: Creating and Deploying Client Systems*, SG24-7045-01.

This edition adds a chapter on IBM Software Delivery Center (an updated and enhanced replacement for Web-D previously covered in *Using Web-D for Software Distribution*, REDP-3764).

The team that wrote this redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization (ITSO), Raleigh Center.



The team: Dudley Miller, Byron Braswell, Syed Irfan

Syed Irfan is a Senior Systems Management Professional for IBM Global Services. His areas of expertise include the development of electronic software distribution service offerings, transition management, development of electronic software delivery solutions, and project management. He has more than 10 years of experience in the IT industry and is currently the team lead for Software Delivery Center. He is responsible for developing and managing multiple projects related to strategic electronic software distribution initiatives. These include electronic software distribution tools development and support, electronic software distribution technology evaluation, and electronic software distribution services architecture and standards development.

Dudley Miller is a Senior Systems Management Professional for IBM Global Services. He received a Bachelor of Science degree in Engineering Science from the University of Texas at Austin. He has more than 15 years of experience in the IT industry and is currently the lead architect for Software Delivery Center. His areas of expertise include object oriented design and development and enterprise level integration of electronic software distribution tools and services. He is responsible for solution architecture, solution development, and solution deployment of electronic software distribution tools and services.

Byron Braswell is a networking professional at the ITSO, Raleigh Center. He received a Bachelor of Science degree in Physics and a Master of Science

degree in Computer Sciences from Texas A&M University. He writes extensively in the areas of networking and middleware software. Before joining the ITSO four years ago, Byron worked in IBM Learning Services Development in networking education development.

Goran Wibran is a Segment Manager for IBM TCO and ThinkVantage Technologies, based in Research Triangle Park, NC. He helps IBM PCD create solutions for cost-effective and resource-effective IT management, IT process automation and IT system integration. He is one of IBM's leading experts on deploying and managing PC-based products. In his leadership role, he works with the IBM Development teams to create the next generation PC and Server management solutions. He also works as a consultant, helping IBM customers to develop and implement automated IT processes around the world.

Authors who contributed to previous editions of this redbook include:

Haakon Fosshaug is a Technical Advocate and a Technical Support Manager in IBM PCD Norway. He has a Bachelor of Engineering degree in Computer Science. An employee of IBM for five years, he has been extensively involved with helping customers use and implement the ThinkVantage Technologies. His specialties include ThinkVantage tools, especially computer security, networking, and image creation and distribution. He also has in-depth technical support and counseling skills concerning future PC platforms for customers.

Eleanor Howard is a Large Enterprise Field Technical Support Specialist and has worked for IBM France for over six years. She covers France, Belgium, and Luxembourg. Her areas of expertise include providing pre-sales support for ThinkCentre, the IBM Desktop range, and IBM ThinkVantage tools, in particular ImageUltra Builder. She also works with IBM Global Services to develop implementation services for customers around ThinkVantage tools.

David Kohler is a Lead Integration Architect working on the IBM Strategic Consulting team. He has worked for IBM for more than three years and has more than 16 years of experience in the IT industry. He specializes in PC life cycle management, total cost of ownership, information systems management and architecture, application portfolio planning, and global PC rollout project management. He uses ThinkVantage Technologies, wireless connectivity, and security to develop architectural solution designs.

Ive Mattheessens is a Software Engineer with the EMEA IBM Imaging Technology Center, Greenock, UK, who worked on the ImageUltra solution development for international clients in the EMEA region. He has been employed with IBM for 8 years and before joining the IBM Image Technology Center, he worked in IBM Technical Support. He specializes in system and application deployment technologies and has several years of experience with ImageUltra, Software Delivery Assistant, and Rescue and Recovery.

Guy Varendonck is an accredited IT Specialist in EMEA Techline located in Greenock, U.K. In his pre-sales technical support role, he has been extensively involved in supporting IBM Sales and IBM Business Partners with ThinkVantage Technologies. Before joining EMEA Techline, he worked in IBM Technical Support and Fulfillment and was Team Lead in ibm.com. He has been employed with IBM for nine years.

John Zywicki is a Systems Management Professional with IBM Global Services US. He has 13 years of experience in all aspects of PC management, deployment and project leadership for large enterprise accounts. He is a technical project management lead for hardware and software standardization methods, global deployments, and systems management solutions. He has coauthored three ThinkVantage Technology Redbooks. He is also responsible for providing pre-sales and post-sales support and training to IBM internal teams and customers.

Thanks to the following people for their contributions to this project:

Margaret Ticknor
Forsyth Alexander
Tamikia Barrow
Jeanne Tucker
Linda Robinson
ITSO, Raleigh Center

Steven Balog
Frank Benzaquen
Jeff Estroff
Egbert Gracias
Joshua J Jankowsky
John Mayes
Josh Novak
Caroline Patzer
Joe Parker
Ratan Ray
Pritam Pabla
Michaelle Walcutt
David Wall
Jeffrey Witt
Adam Wong
Marilyn J Moore
Dean Suraci
Nathan Bigger
IBM RTP, North Carolina

Gavin Cameron
Craig T Leonard
James MacKenzie
Sohail Syed
IBM UK, Greenock

Ted Bullen
IBM Salt Lake City, Utah

Timothy Brown
Maurice Phillips
IBM Austin, TX

Oscar Aguirre
IBM Chicago, IL

Become a published author

Join us for a two- to six-week residency program! Help write an IBM Redbook dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You'll team with IBM technical professionals, Business Partners and/or customers.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you'll develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our Redbooks to be as helpful as possible. Send us your comments about this or other Redbooks in one of the following ways:

- Use the online **Contact us** review redbook form found at:

ibm.com/redbooks

- Send your comments in an Internet note to:

redbook@us.ibm.com

- Mail your comments to:

IBM Corporation, International Technical Support Organization
Dept. HZ8 Building 662
P.O. Box 12195
Research Triangle Park, NC 27709-2195

Summary of changes

This section describes the technical changes made in this edition of the redbook and in previous editions. This edition may also include minor corrections and editorial changes that are not identified.

January 2005, Fourth Edition

This revision reflects the addition, deletion, or modification of new and changed information described below.

New information

- ▶ In Chapter 1, “Introduction,” the material on IBM Software Delivery Assistant has been updated.
- ▶ Chapter 4, “IBM Software Delivery Center” on page 219 is new.
- ▶ Appendix C, “Software Delivery Center and System Information Center coexistence” on page 627 is new.

Changed information

- ▶ Chapter 5, “Access IBM” on page 405 on page 219 was Chapter 4 in the third edition and Chapter 3 in previous editions.
- ▶ Chapter 6, “Embedded Security Subsystem” on page 443 was Chapter 5 in the third edition and Chapter 4 in previous editions.



Introduction

Over the last decade, controlling complexity has been the goal of every IT manager. Since the introduction of the Internet, new devices and processes have made delivery of service more complex, and it has become critical for IT managers to contain costs. Understanding the total cost of ownership has created the necessity to seek methods to reduce costs while improving service.

Despite reductions in PC hardware costs, many companies have seen costs rise due to increased product complexity, proliferation-related management and support issues. Today, the initial cost of buying a PC is the tip of the iceberg. This emphasis on cost reduction has imposed the requirement for ways to improve the overall PC management process.

What has IBM done to alleviate the stress of these costs? The company has focused research and development efforts around the challenges of reducing total cost of ownership.

Through the evaluation of each phase of the PC life cycle, IBM has developed a number of technologies in hardware and software to reduce IT management costs. Known as ThinkVantage Technologies, they manage the PC LifeCycle from pre-deploy planning through end-of-life disposition.

Figure 1-1 on page 2 is an overview of the functions performed by various ThinkVantage Technologies during the hardware and software life cycles of a typical client PC.

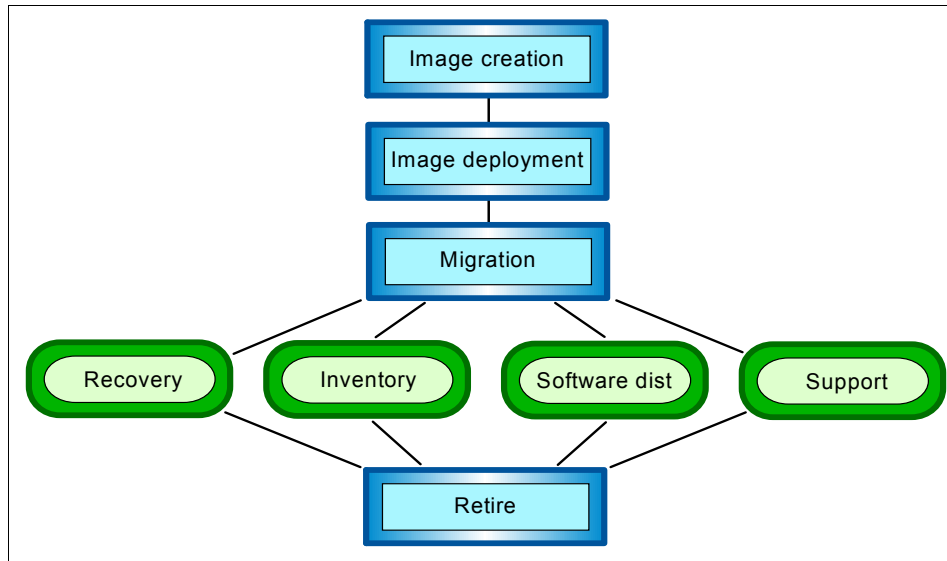


Figure 1-1 High Level ThinkVantage Technologies functions

This chapter provides an overview of the ThinkVantage Technologies:

- ▶ Rescue and Recovery
- ▶ IBM System Information Center
- ▶ IBM Software Delivery Center
- ▶ Software Delivery Assistant (SDA) Version 2.0
- ▶ Access IBM and Access Help
- ▶ Embedded Security Subsystem
- ▶ ImageUltra Builder
- ▶ System Migration Assistant (SMA)
- ▶ Secure Data Disposal (SDD)
- ▶ Access Connections
- ▶ IBM Director
- ▶ Remote Deployment Manager (RDM)

It also discusses ThinkVantage Technologies process improvements and implementation.

1.1 ThinkVantage Technologies

To address key concerns regarding the reduction of costs and to improve return on investment (ROI), the ThinkVantage Tools can be implemented individually or as a complete solution. As a result, organizations can integrate these solutions into their existing environments to complement existing processes or develop new, more cost-efficient processes if those are not already in place.

ThinkVantage Technologies simplify the PC LifeCycle processes in the following ways:

- By improving IT resource utilization
- By improving IT budget usage
- By automating resource intensive tasks
- By minimizing help desk and desk side costs
- By reinforcing best practices
- By delivering low total cost of ownership (TCO)

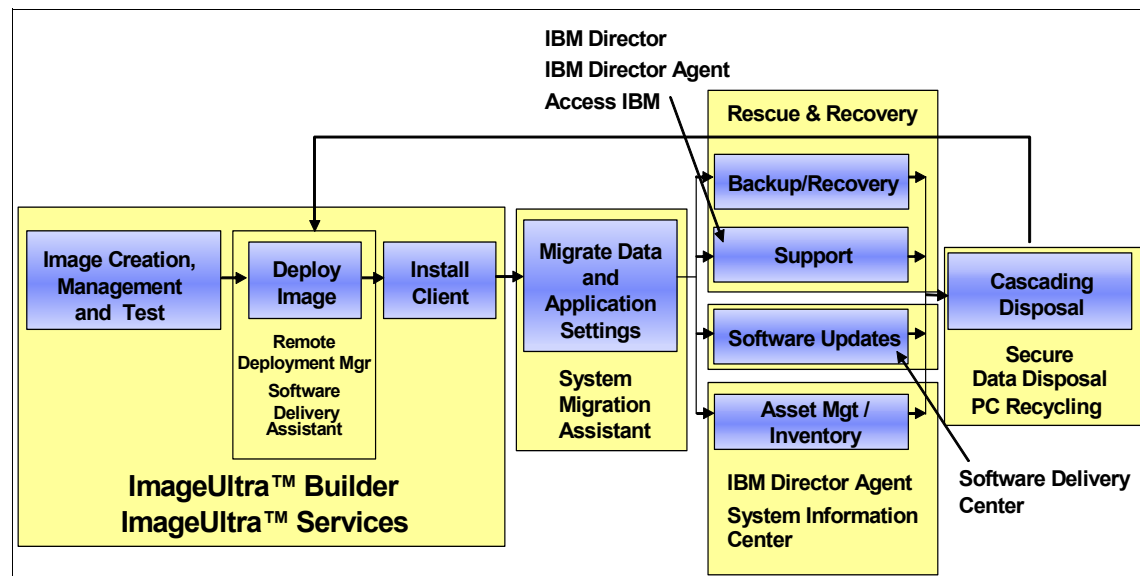


Figure 1-2 Simplifying PC life cycle processes

The two-volume set of ThinkVantage Technology Redbooks cover the products that address each of the functional areas in the PC life cycle. Brief descriptions of these products are provided in the following sections.

Rescue and Recovery

IBM Rescue and Recovery is a one-button solution that includes a set of self recovery tools to help users diagnose, get help and recover from a software

crash, even if the primary operating system will not boot. It helps with everything from complete software failure to occasions when you need only to restore a corrupted or deleted file. And it's easily accessible from the Microsoft® Windows® desktop or by pressing the blue Access IBM button on supported IBM systems (or the F11 key on other personal computers).

Rescue and Recovery is discussed in Chapter 2, “Rescue and Recovery” on page 11.

IBM System Information Center

System Information Center is a cost and resource effective inventory solution that complements and leverages the customer's investment in ThinkVantage Technologies. Features included in System Information Center are easy browser accessibility, minimal resource usage, control of software license management and central management.

System Information Center is discussed in Chapter 3, “IBM System Information Center” on page 91.

IBM Software Delivery Center

IBM Software Delivery Center is a Java™-based Web-enabled software distribution solution that complements and leverages the customer's investment in ThinkVantage Technologies. Software Delivery Center uses industry standard components, is simple to manage, easily integrates into an existing customer network infrastructure, is customizable, and is very cost effective both at the time of implementation and over the long term.

IBM Software Delivery Center is discussed in Chapter 4, “IBM Software Delivery Center” on page 219.

IBM Software Delivery Assistant Version 2.0

IBM Software Delivery Assistant Version 2.0 (SDA 2.0) is a software delivery solution that uses Web-based tools and technology to create software catalogs. These catalogs are used to deliver software components to computers distributed throughout a business on a CD, DVD, or network drive.

If your environment requires network distribution, you should consider IBM Software Delivery Center Version 1.1. Software Delivery Center is a software-distribution product that is simple to manage and easily integrates into an existing customer network infrastructure. It is customizable and cost effective to implement and maintain. Software Delivery Center contains all of the functionality of SDA 2.0.

IBM Software Delivery Center is discussed in Chapter 4, “IBM Software Delivery Center” on page 219.

Access IBM and Access Help

Access IBM and Access Help are comprehensive, on-board help and information centers for your computer. They travel with you, eliminating the need to carry reference manuals or user guides.

Access IBM and Access Help are discussed in Chapter 5, “Access IBM” on page 405.

Embedded Security Subsystem

The IBM Embedded Security Subsystem, available on select IBM computers, consists of the integrated security chip and IBM Client Security Software (download required). Working together, these components provide security not previously available. The integrated security chip provides hardware-based protection of critical security information, including passwords, encryption keys and electronic credentials. The security software provides the interface between security-aware applications and the functionality of the chip. In addition, it provides support for peripheral security devices that control access to the PC itself.

Embedded Security Subsystem is discussed in Chapter 6, “Embedded Security Subsystem” on page 443.

ImageUltra Builder

ImageUltra Builder was designed to help simplify your image creation, deployment, and management. This technology is designed to help enterprises save time and money and to stay productive with a do-it-yourself tool that can allow you to deploy as few as one image across your enterprise. By combining multiple languages, applications and operating systems* into a single hard drive image, you help eliminate or reduce the need for manual application installation, hardware testing and support. This patent-pending technology lets you better control your IT environment for less painful deployments and lower IT costs.

ImageUltra builder allows for the separation of drivers and applications from a traditional image unlike Symantec Ghost and PowerQuest Drive Image. By separating these components, as well as the OS, we greatly reduce the number of images that need to be kept. Since drivers and applications are updated, there is no need to *open* each traditional image to apply the updates. Customers already using Symantec Ghost or PowerQuest Drive Image can incorporate their images into ImageUltra Builder as either semi-portable or system-specific images.

For more information about ImageUltra Builder, refer to *Using ThinkVantage Technologies: Volume 1 Creating and Deploying Client Systems*, SG24-7045.

System Migration Assistant

System Migration Assistant (SMA) enables custom settings, preferences, and data to be migrated from a user's former PC to the new PC accurately, efficiently and effectively. When older computers are refreshed or new computers are introduced, moving user data and system settings to the new system becomes expensive and time-consuming. Removing the problems associated with migration is an important customer satisfaction issue.

For more information about SMA, refer to *Using ThinkVantage Technologies: Volume 1 Creating and Deploying Client Systems*, SG24-7045.

Secure Data Disposal (SDD)

IBM Secure Data Disposal removes all data on a hard disk drive, protecting sensitive information when a drive is re-deployed or retired. After using this process, data will be non-recoverable.

Secure Data Disposal is discussed in *Using ThinkVantage Technologies: Volume 1 Creating and Deploying Client Systems*, SG24-7045.

Access Connections

IBM Access Connections is a connectivity assistant program for your IBM ThinkPad computer that allows you to create and manage location profiles. Each location profile stores all of the network and Internet configuration settings that are needed to connect to a network infrastructure from a specific location such as home or work. By switching between location profiles as you move your computer from place to place, you can quickly and easily connect to a network without having to manually reconfigure your settings and restart your computer each time.

IBM Access Connections is discussed in *Using ThinkVantage Technologies: Volume 1 Creating and Deploying Client Systems*, SG24-7045.

IBM Director

IBM Director V4.1 is the newest release of the industry-leading client/server workgroup manager. IBM Director's tools provide customers with flexible capabilities to realize maximum system availability and lower IT costs. With IBM Director, IT administrators can view and track the hardware configuration of remote systems in detail and monitor the usage and performance of critical components, such as processors, disks, and memory.

IBM Director is discussed in *Implementing Systems Management Solutions using IBM Director*, SG24-6188.

Remote Deployment Manager (RDM)

Remote Deployment Manager provides tools to simplify configuration and deployment of operating systems and applications. Adding a computer to the RDM database allows for remote installation, maintenance, and software updates on client computers.

1.2 ThinkVantage Technologies process improvements

Using the ThinkVantage tools can help optimize the PC life cycle to enhance current processes. The two volumes of *Using ThinkVantage Technologies* cover the creation, deployment, maintenance and recovery elements of the ThinkVantage Technologies.

The tools discussed in these Redbooks are key contributors to deployment optimization. ThinkVantage Technologies allow PCs to be more than just clients.

ThinkVantage Technologies provide optimization and cost avoidance solutions for:

- ▶ Simplified image complexity by delivering a hardware-independent imaging solution
- ▶ Improved application deployment by delivering a detached application deployment solution
- ▶ Rapid transition by delivering a smooth data migration solution
- ▶ *Down the Wire* recovery by delivering a managed system recovery and backup solution
- ▶ Life cycle ends with data removal by delivering a Secure Data Disposal solution
- ▶ Additional solutions for security, deployment, management, support, wireless and more

Many organizations will relate to Figure 1-3 regarding the times for each part of the processes defined. Implementation of the ThinkVantage Technologies will reduce cost and offer opportunities for companies.

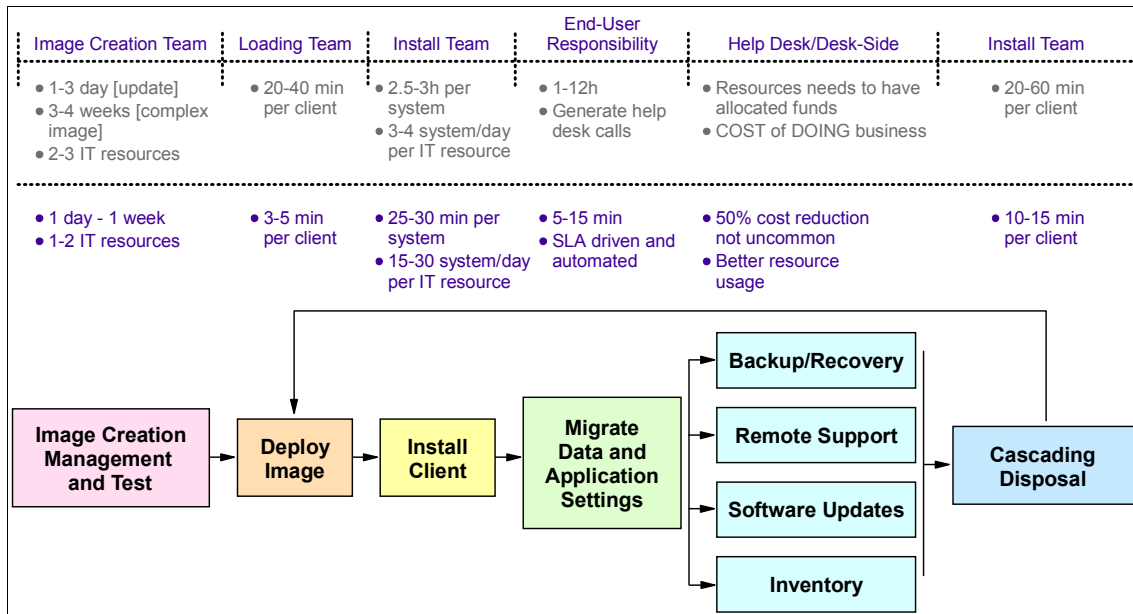


Figure 1-3 ThinkVantage Technologies tools and simplification of PC Life cycle processes

1.3 Implementing a ThinkVantage Technologies solution

Table 1-1 outlines the efforts required to implement the tools to be discussed in both books. It also outlines whether training is recommended or required to ensure a smooth implementation into an organization. You will notice that in a worst case scenario, it will take less than two weeks to get staff trained on all of the tools mentioned in the chart below. Many of the tools have optional training and can be learned through the use of this Redbook or existing product documentation.

Table 1-1 Implementing ThinkVantage Technologies

	IBM PCD Tool	People needed to implement	Process change required	Training needed
Imaging	ImageUltra Builder	2-5 Skilled Administrator for Large Enterprise Company 1 skilled Administrator for Small Medium Business Company	Yes, to build image, but the deployment of image remains similar	Yes, Required 2 day training
	Software Delivery Center	1-3 Skilled Administrator for LE 1 Skilled Administrator for SMB	Yes, to regroup applications by line of business or dept.	Optional 1 day training
Network Deployment	Rapid Deployment Manager (RDM)	1-3 Skilled Administrator for LE 1 Skilled Administrator for SMB	No existing process with image deployment best practice	Yes, recommended 1 day training
Migration	System Migration Assistant (SMA)	1 Skilled Administrator for LE and SMB	No existing process with automated migration best practice	Optional 2 day training
Recovery	Rescue and Recovery	1 Skilled Administrator for LE and SMB	Yes, to create hidden recovery partition on local hard drive	Optional 2 day training

	IBM PCD Tool	People needed to implement	Process change required	Training needed
Management	IBM Director Agent	1-3 Skilled Administrator for LE 1 Skilled Administrator for SMB	No, existing process with system management best practice	Included in IBM Director training
	IBM Director	1-3 Skilled Administrator for LE 1 Skilled Administrator for SMB	No, existing process with system management best practice	Yes, recommended 2 day training
	System Information Center	1-3 Skilled Administrator for LE 1 Skilled Administrator for SMB	No, existing process with asset management practice	Included in IBM Director training
Disposal	Secure Data Disposal	1 IT staff for LE and SMB	No, existing process with Hard Drive Data Disposal best practice	Optional 1 day training

Low	Med	High
-----	-----	------

Note: The scale is relative to the uptime of other ThinkVantage Technologies and migration tools. It is not a measure of good, average and poor.



Rescue and Recovery

IBM Rescue and Recovery is a robust data backup, data restore, and support environment that greatly reduces overall business costs. This chapter outlines the function and features of the tool along with advanced features and troubleshooting.

New improvements not in Rapid Restore Ultra Version 3.0 include:

- ▶ Faster and smaller backups
 - Backup hard disk partition is no longer required
 - No defragmentation operation
- ▶ Improved installation and deployment
 - Fast user installation and simplified interface
 - No new partitions created or resizing
- ▶ More support for devices: USB, CD, DVD, network, hard disks
- ▶ Customizable backups
 - Five incremental backups is the default
 - Up to 32 customizable backups
- ▶ Broad customization options for IT

2.1 Introducing Rescue and Recovery

Rescue and Recovery is an enhanced support environment for one-button disaster recovery. Users can recover damaged files and software crashes to stay productive. In addition, Rescue and Recovery lowers support costs by avoiding support calls or reducing the time to solve problems. When you encounter a software problem, you can use Rescue and Recovery to:

- ▶ Get connected through direct access to the Web or local content
- ▶ Retrieve files that were not backed up prior to a system problem
- ▶ Get extensive system information about BIOS, hardware, and software without the need for a reboot
- ▶ Recover files and systems by restoring from a backup or using rescue media to recover from the most serious software problems such as a master boot record (MBR) corruption

There are two major components of Rescue and Recovery:

- ▶ The Rescue and Recovery environment, which starts even if the Windows operating system (OS) will not open
- ▶ Rescue and Recovery functions, which are available in both the Rescue and Recovery environment and Windows environments

There are some features of Rescue and Recovery that run under the Windows OS. In some instances, system information used in the Rescue and Recovery environment is gathered while Windows is running. If the Windows operating system malfunctions, that malfunction alone will not prevent the Rescue and Recovery environment from operating normally.

2.1.1 Rescue and Recovery environment and functions

The Rescue and Recovery environment provides an emergency workspace for situations when Windows will not start. Rescue and Recovery runs under the Windows Pre-installation Environment (Windows PE).

Windows PE is a small Windows release of Windows XP. It provides a 32-bit boot environment that replaces the functionality of DOS. The Windows PE environment offers the look, feel, and function that are familiar to Windows users and helps them solve some problems without consuming IT staff time.

The IBM Rescue and Recovery environment comprises a number of functions grouped into four major categories (see also 2.4.1, “Using the Rescue and Recovery environment” on page 57):

- ▶ Rescue and Restore
 - Recovery overview: this function links users to help topics about the various recovery options that IBM provides.
 - Rescue files: this function enables users to copy files created in Windows applications to removable media or to a network. Users can continue to work even though their workstation is down.
 - Restore from backup: this function helps users restore files that have been backed up Rescue and Recovery.
 - Restore factory contents: this function provides a method to erase the hard disk and reinstall the software that IBM preinstalled on the computer.
- ▶ Configure
 - Configuration overview: this function links to Rescue and Recovery environment help topics that cover configuration.
 - Set recovery password: with this function, a user or administrator can protect the Rescue and Recovery environment with a password.
 - Access BIOS: this opens the IBM BIOS Setup Utility program.
- ▶ Communicate
 - Communication overview: this function links to related help topics in the Rescue and Recovery environment.
 - Open browser: this starts the Opera Web browser. (Web or intranet access requires a wired Ethernet connection.)
 - Download files: this provides the capability to download files.
 - Map network drive; this helps users access network drives for network restores, software downloads or file transfer.
- ▶ Troubleshoot
 - Diagnostic overview: this links to Rescue and Recovery diagnostics help topics.
 - Diagnose hardware: this function opens the PC Doctor application that can perform hardware tests and report results.
 - Create diagnostic disks: this creates disks for diagnostic purposes.
- ▶ System information: this function provides details regarding the computer and its hardware components.
- ▶ Activity and asset log viewer: this feature details recent user activity and computer hardware to aid in problem determination and resolution. The log viewer provides a readable way to view activity and asset log entries.

2.1.2 Rescue and Recovery functions

Rescue and Recovery is a managed-recovery utility that protects computers from software-related systems failures. In the event of a system failure, you can use Rescue and Recovery to restore the contents of the primary hard disk to a previously saved state.

Rescue and Recovery enables you to perform the following functions:

- ▶ Schedule daily, weekly, or monthly backups:
Rescue and Recovery enables you to schedule backup operations so that your valuable data is automatically protected. See 2.3.5, “Scheduling backups” on page 52.
- ▶ Save backup files to a hidden, protected folder:
Rescue and Recovery stores the backup files in a hidden, protected folder on the local hard disk, thereby minimizing the use of network bandwidth during a backup and restore operation.
- ▶ Restore files to any number of back-up states:
Rescue and Recovery can save a number of backup images in the protected folder. Users can decide how many backups to store on the local drive. Five incremental backups will be stored on the local drive by default, if size permits. For information about how to perform this function, see 2.3.3, “Backing up your system” on page 45.
- ▶ Restore files after an operating-system failure:
Under normal circumstances you can use Rescue and Recovery from the Windows interface. However, if an operating-system failure prevents you from accessing the Windows interface, you can use Rescue and Recovery from the IBM Rescue and Recovery environment to perform a full system-recovery operation.
- ▶ Protect the entire software image, including user data:
Rescue and Recovery protects the entire contents of the hard disk, including the Windows OS, software applications, registry settings, network settings, fix packs, desktop settings, and unique data files. See 2.3.3, “Backing up your system” on page 45.
- ▶ Copy backups to network or removable media:
If your computer has access to a network drive, USB hard disk drive, or a recordable DVD or CD drive, you can use Rescue and Recovery to copy backup files to these devices. This provides an additional level of protection. These devices can then be used to restore the contents of the hard disk in the event of a hard disk drive failure. See 2.3.4, “Archiving backups” on page 50.

- ▶ Backup directly to network drives or removable media:

If your computer has access to a network drive, a USB hard disk drive, or a recordable DVD or CD drive, Rescue and Recovery enables you to backup files to these devices, thus providing an additional level of protection. These devices can then be used to restore the contents of the hard disk in the event of a hard disk drive failure. See 2.3.3, “Backing up your system” on page 45.
- ▶ Support Enterprise-wide recovery and backup policies:

Rescue and Recovery supports a command-prompt interface, which can be used with systems management tools to integrate enterprise-wide recovery and backup policies. For detailed information consult the *IBM Rescue and Recovery Customization and Deployment Guide*, which you can download from this Web site:

<http://www.ibm.com/pc/support/site.wss/document.do?lnocid=MIGR-54502>
- ▶ Restore single files or folders:

You can use Rescue and Recovery to view, select, and recover one or more individual files or folders from a backup image. See “Restoring individual files and folders” on page 73.
- ▶ Exclude specific files or folders from backup:

Rescue and Recovery allows you to exclude specific files or folders from a backup operation. Excluding files and folders reduces the size of the backup and increases the speed of the backup operation. See 2.3.2, “Setting backup preferences” on page 41 and “Including and excluding files in backups” on page 603.

2.1.3 Rescue and Recovery components

Rescue and Recovery provides functionality in both the Rescue and Recovery environment (Windows PE) and the Windows environment. Rescue and Recovery includes the following main components:

- ▶ Scheduler

This component invokes the backup process on a periodic basis. The periods supported are daily (at a specified time) and weekly (on a particular day of the month at a specified time). The Scheduler runs as a Windows service so that it functions even when no one is logged onto the computer.
- ▶ Windows interface

With this component, a user can customize Rescue and Recovery behavior. From this interface, you can define a backup schedule, initiate a backup immediately, copy backups onto removable media, restore the system from a backup, and select individual files to restore. Large enterprise administrators

can restrict this interface to enforce a company-wide policy. The policy settings are defined in a text file as part of the installation operation.

- ▶ IBM Rescue and Recovery Engine

This component performs backup and restore operations.

- ▶ command-prompt interface

This component provides an interface for automated scripting that enables custom image deployment and enterprise management functionality. See 2.2.4, “Silent installation” on page 31 and “RRU command prompt interface RRUcmd” on page 598

- ▶ Online help

This component provides guidance for using the features and capabilities of the Rescue and Recovery.

2.1.4 Rescue and Recovery backup methodology

How Rescue and Recovery handles incremental backups of your system is described in this section. The Rescue and Recovery program stores multiple backup images on your hard drive. Each backup image reflects the state of your hard disk at the time of its creation.

There are two types of backup images:

- ▶ Base backup image

This compressed, complete file-based backup file is created when you perform your initial backup following installation of Rescue and Recovery. This file reflects the state of your hard disk at the time that Rescue and Recovery is installed. All files on your hard disk at that time are saved in the base backup image. This backup image cannot be updated.

- ▶ Incremental backup images

The incremental backup files archive the files that have changed since the last incremental backup was taken. New backups should be initiated whenever your system software is updated or a database or application is added. Only new files and those that do not match those in the base backup image are saved in an incremental backup file.

Up to 32 incremental backup images are supported. The *MaxNumberOfIncrementalBackups* parameter is used to specify the number of incremental backups to maintain. The following figures illustrate a Rescue and Recovery operation using a file named sample.txt and *MaxNumberOfIncrementalBackups=5*.

Figure 2-1 shows the different versions of sample.txt after the base backup and five incremental backups were taken. Notice that when backups three and five were taken, sample.txt had not changed, so it was not backed up.

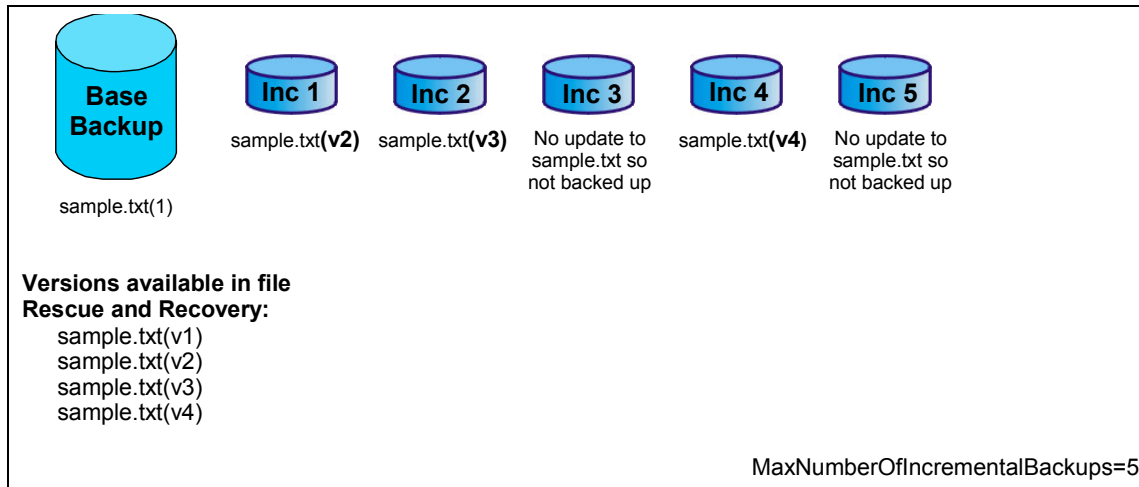


Figure 2-1 Default five incremental backups outline

When the sixth incremental backup is taken, Rescue and Recovery combines the two oldest incremental backups (Inc1 and Inc 2 in this example). When making the sixth incremental backup, sample.txt (v2) (Inc 1) will be deleted and only the newer sample.txt(v3) will be on the combined incremental backup Inc 2a as shown in Figure 2-2. The number of incremental backups remains at five.

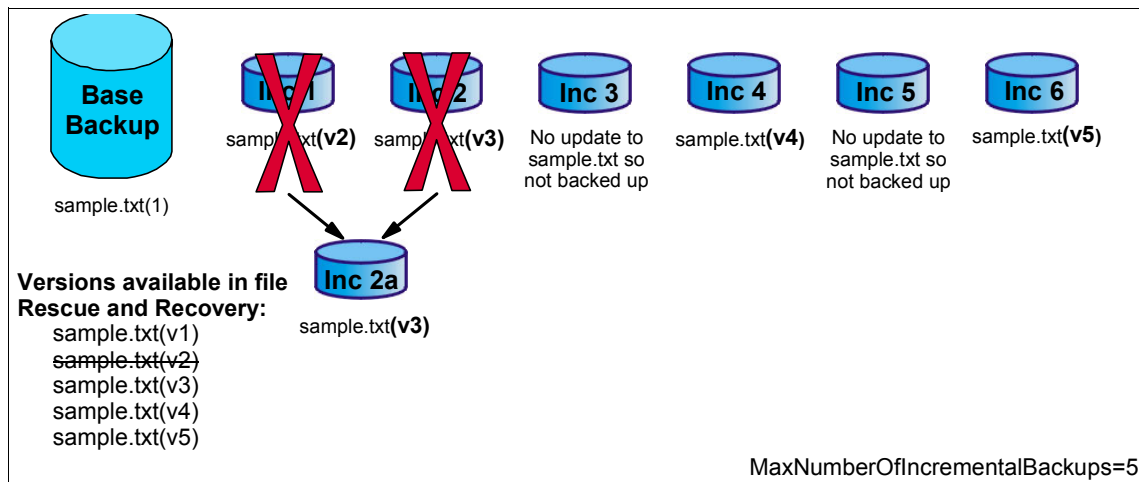


Figure 2-2 Incremental backup number six

Making an additional backup gives the results depicted in Figure 2-3. Since no changes were made to sample.txt (v3) after incremental backup Inc 2 and before backup Inc 3, sample.txt (v3) will be part of the combined incremental backup Inc 3a while the total incremental backups remains at five with sample.txt (v1,v3,v4,v5,v6) available to restore from.

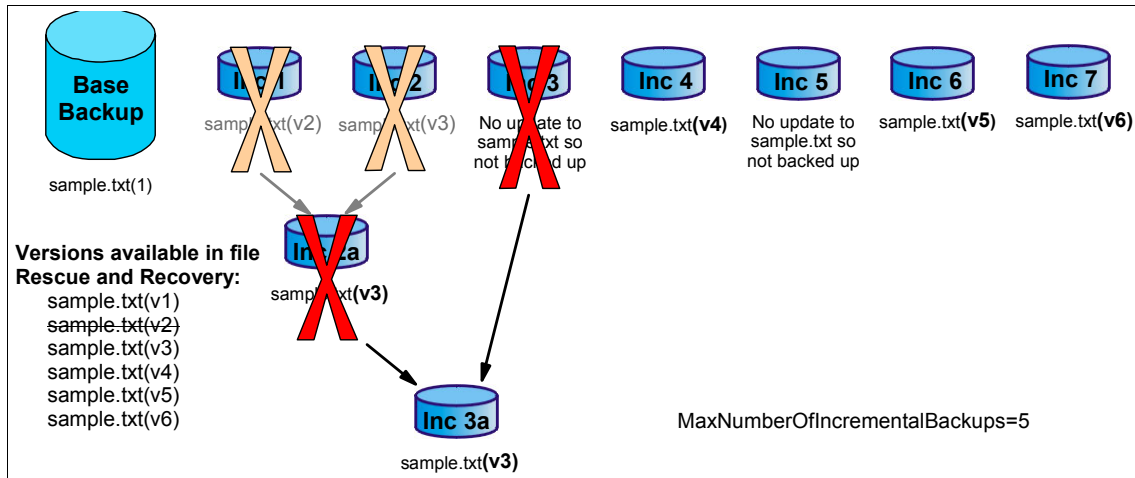


Figure 2-3 Additional backups

Note: `MaxNumberOfIncrementalBackups` can be set in the file TVT.txt. The value can be any value from 2 to 32 with default = 5. TVT.txt will be discussed in more detail later in this chapter. For all possible settings and values in TVT.txt file, please consult “Values and settings of TVT.TXT” on page 591.

2.1.5 Managing backups

You can use Rescue and Recovery to schedule backups at a specified time and frequency, thereby managing how often the hard disk is backed up. If you prefer to perform backup operations manually, or you need to perform a backup operation between scheduled backups, you can use the backup function to perform an on-demand backup operation.

IBM Rescue and Recovery saves the incremental backups in a hidden, protected folder. Five incremental backups will be stored on the local drive by default, if size permits.

Managing backup and recovery for the enterprise

The IBM Rescue and Recovery program includes the following system management features:

► command-prompt interface

The command-prompt interface provides an interface for automated scripting, which enables custom image deployment and enterprise management functionality. The Rescue and Recovery command-prompt interface can be used in a Windows environment and can be automated with systems management tools, including:

- IBM Director
- IBM LANClient Control Manager
- Tivoli TME
- Microsoft SMS.

Note: For more information, see “Performing a base backup from the command prompt” on page 35.

► Customizable installation options

IT administrators can personalize Rescue and Recovery by setting policy. See also “Customizing Rescue and Recovery for silent installation” on page 34. The following options are available:

- Hide the Windows interface
- Set the backup schedule
- Modify the amount of storage space allocated for Rescue and Recovery

By default, Rescue and Recovery backs up the primary partition and any extended partitions on the primary hard disk and stores the backups in a hidden, protected folder on the hard drive. During the installation process, you have the option of initiating a complete system backup. Ideally, this base backup should not be taken until your computer has all the necessary software installed and configured. Additional incremental backups are automatically created by subsequent backup operations.

With Rescue and Recover, IT administrators can create, store, and manage multiple backup images in an enterprise because of the feature that allows the storage of multiple images. Users can also manage additional levels of backups while the operating system is running. Their data are protected because they are stored separately from the backup images.

2.1.6 Rescue and Recovery system requirements

IBM systems

The IBM systems shown in Table 2-1 are supported by Rescue and Recovery.

Table 2-1 Supported IBM systems

Marketing Name	Machine Type
Thinkpad X Series	2884, 2885, 2890, 2891, 2661, 2662
ThinkPad T Series	2373, 2734, 2374, 2376, 2378, 2379, 2366, 2367, 2647, 2648
ThinkPad R Series	2656, 2657, 2658, 2659, 2681, 2682, 2683, 2684, 2685, 2722, 2723, 2724, 1829, 1830, 1831, 1832, 1833, 1836, 2892, 2893, 2898, 2899
ThinkPad A Series	2652, 2653, 2654
ThinkPad G Series	2388, 2389, 2384, 2387
ThinkCentre A50p, M50, S50	8183, 8184, 8416, 8417, 8418, 8429, 8419, 8320, 8185, 8413, 8186, 8187, 8414, 8188, 8189, 8415, 8190, 8430, 8431, 8192, 8193, 8194, 8432, 8195, 8433, 8196, 8197
ThinkCentre A30	8191, 8198, 8199, 8316, 8434, 2296
NetVista M42	8181, 8182, 8301, 8303, 8304, 8305, 8306, 8307, 8308
Netvista A30p	8309, 8310, 8311, 8312, 8313, 8314, 8315
Netvista S42	8317, 8318, 8319, 6826
Netvista M41	6790, 6791, 6792, 6793, 6794, 6795, 6796, 6797, 6825, 6823
Netvista A22p	6343, 6349, 6350, 2292
Netvista A21	6336, 6337, 6339, 6341, 6342, 2256, 2257, 6346, 6347, 6348

OEM systems

System requirements differ for systems produced by other equipment manufacturers (OEMs). These requirements are listed in Table 2-2.

Table 2-2 OEM System requirement

Hardware	Specification
Processor	Speed and type recommended by Microsoft Windows (compatible with Windows 2000 Professional and Windows XP Pro and Home).
System Memory	128MB
Hard Drive	1.5GB of free hard disk space. (The base install uses 930MB and does not include Rescue and Recovery backups.)
Video	VGA-compatible video that supports a resolution of 800 x 600 and 24-bit colors. For non-shared video memory systems, a minimum of 4MB of video RAM is required. For shared video memory systems, a minimum of 4MB must be allocated.
Network	Only wired PCI-based Network adapters are supported. Network device drivers included in the Rescue and Recovery environment are the same drivers that are pre-populated in Microsoft Windows XP Professional operating system and are independent of the Windows operating system.
Software	Windows 2000 Professional SP3 or higher, Windows XP Home or Windows XP Professional.

Note: Installation of Rescue and Recovery on an OEM system requires the purchase of a license.

Additional Information

Rescue and Recover supports booting from non-IBM external devices such as a USB hard disk drive, CD-R/RW, DVD-R/RW/RAM, or DVD+R/RW. However, the non-IBM external device must fully support one or more of the following specifications:

- ▶ BIOS Enhanced Disk Drive Services-2
- ▶ USB Mass Storage Specification for Bootability
- ▶ El Torito Bootable CD-ROM Format Specification
- ▶ Compaq Phoenix Intel® BIOS Boot Specification
- ▶ ATAPI Removable Media Device BIOS Specification
- ▶ USB Mass Storage Class Specification Overview

2.2 Installing Rescue and Recovery

This section outlines the installation of IBM Rescue and Recovery. The following topics are covered:

- ▶ 2.2.1, “Preparing to install Rescue and Recovery” on page 22.
- ▶ 2.2.2, “Rescue and Recovery environment configurations” on page 23.
- ▶ 2.1.6, “Rescue and Recovery system requirements” on page 20.
- ▶ 2.2.3, “Rescue and Recovery installation” on page 29.
- ▶ 2.2.4, “Silent installation” on page 31.
- ▶ 2.2.5, “Setting up a Create Base Backup icon on the user’s desktop” on page 36.
- ▶ 2.2.6, “Creating rescue media” on page 37.

2.2.1 Preparing to install Rescue and Recovery

IBM Rescue and Recovery setup includes two phases:

- ▶ Installation
- ▶ Base backup

The installation phase illustrated in Figure 2-4 on page 23 consists of the following steps:

1. Qualifying and determining the system configuration
2. Installing the components of the application, services, and drivers that operate under the Windows OS
3. Installing the Rescue and Recovery Master Boot Record (MBR)
4. Installing the IBM Rescue and Recovery environment (sometimes called the pre-desktop environment)
5. Rebooting

For an enterprise rollout, the required reboot at the end of installation may be undesirable for various reasons. Among these is the interruption of a scripted process or batch installation of multiple applications.

Rescue and Recovery can be configured not to reboot at the end of the installation phase. For additional options, see the *IBM Rescue and Recovery Customization and Deployment Guide*, which comes with the product.

The base backup phase follows the reboot. A base backup must be taken before incremental backups can be performed.

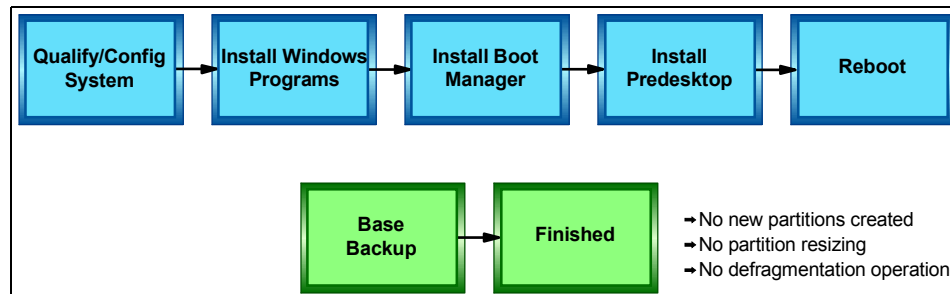


Figure 2-4 Installation process

2.2.2 Rescue and Recovery environment configurations

Rescue and Recovery supports several hard disk drive configuration scenarios. Therefore, Rescue and Recovery must install a custom Master Boot Record (MBR). This MBR receives notifications from Windows or from the keyboard at boot time. Based on the input, the appropriate partition will boot either Windows or the Rescue and Recovery environment.

Default installation

If you are installing Rescue and Recovery on a hard disk that does not have an IBM_SERVICE partition or a PARTIES (Protected Area Runtime Interface Extension Services area, Rescue and Recovery will be installed according to the software defaults.

The Rescue and Recovery environment by default is located in a virtual partition that must be installed on the C: drive (the primary partition of the master hard disk drive) of the computer. It consists of two directories, \minint and \preboot. This is illustrated in Figure 2-5.

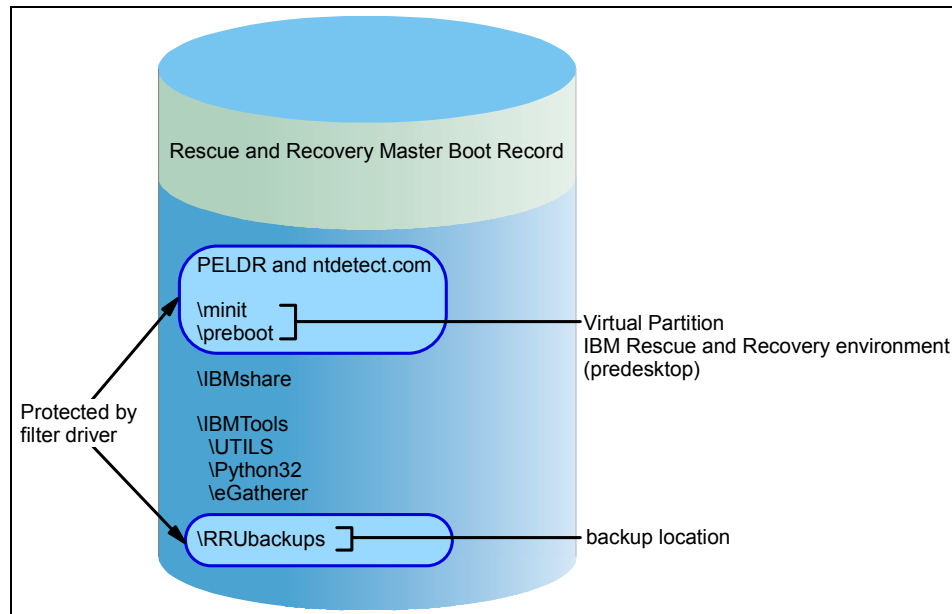


Figure 2-5 Default installation

Both of these directories are protected by the same filter driver that protects the \RRUbackups backup location.

Note: The location \RRUbackups is only protected by the filter driver on the primary drive. If you backup to a USB drive or secondary hard drive, the \RRUbackups location is hidden and not protected by the filter driver.

IBM computers with a type 1C IBM_SERVICE partition

IBM computers with a type 1C IBM_SERVICE partitioned are IBM computers that were announced prior to January 2003, or computers that have an ImageUltra™ Builder disk image. The Rescue and Recovery installation in this scenario is similar to the default installation.

As with the default installation, the Rescue and Recovery environment is installed into a virtual partition. However, the Rescue and Recovery environment will link to the IBM_SERVICE partition to restore the factory contents or the ImageUltra Builder disk image. This is illustrated in Figure 2-6.

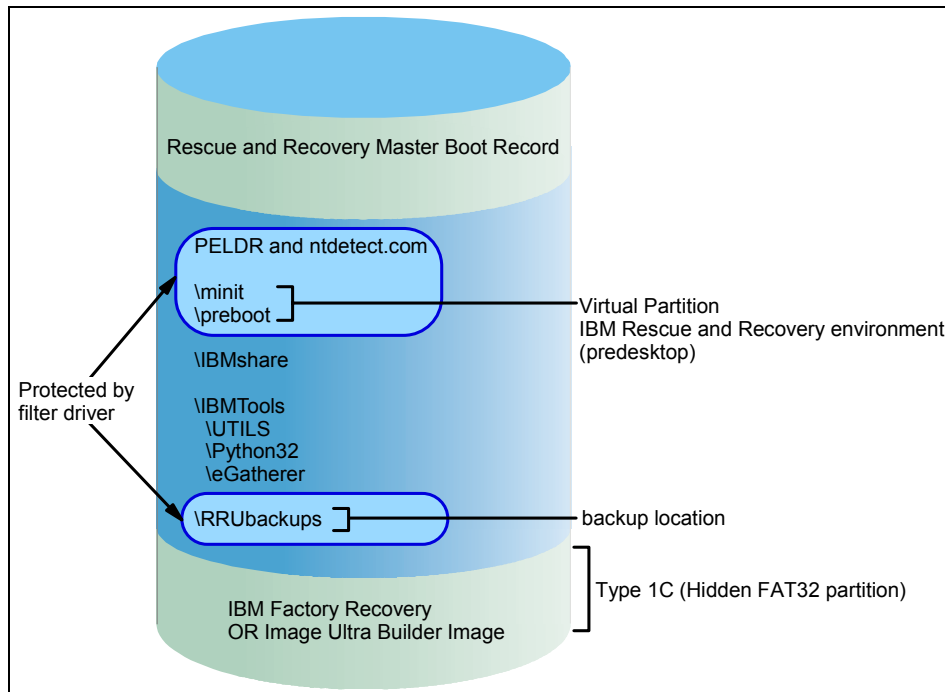


Figure 2-6 Installation on a system with a type1C IBM_Service partition

IBM computers with a PARTIES area

IBM computers that have a PARTIES (Protected Area Runtime Interface Extension Services) area were announced during 2003. The installation in this scenario is similar to a default installation. The Rescue and Recovery environment is installed into a virtual partition as though it were a default installation. However, the Rescue and Recovery environment will link to the PARTIES area to initiate a restore of factory contents or diagnostics. This is illustrated in Figure 2-7.

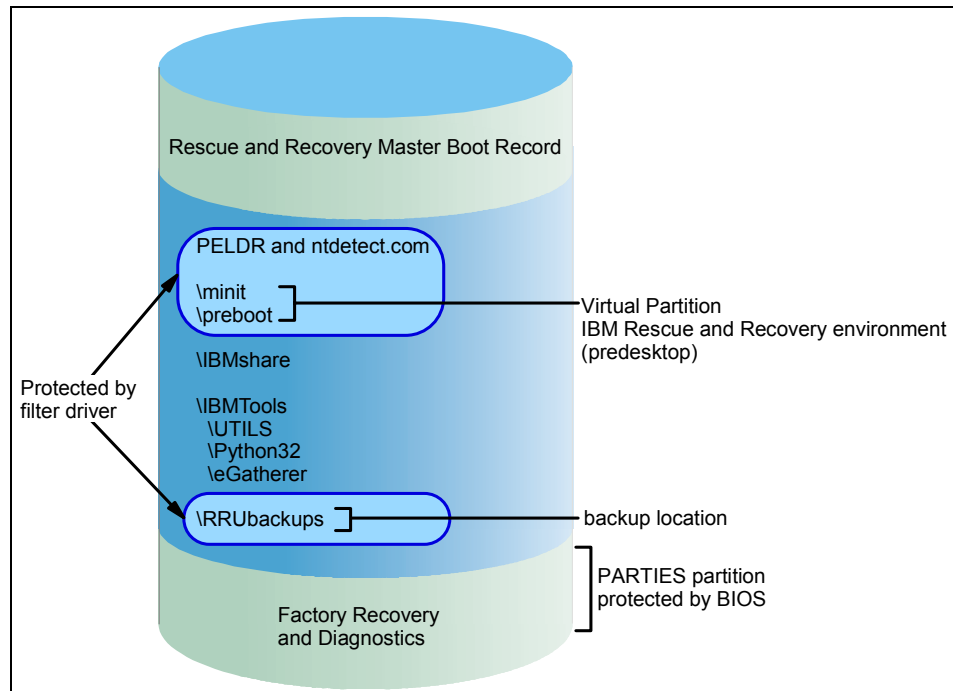


Figure 2-7 Installation on system with a PARTIES area

IBM computers with a PARTIES area and a type 1C IBM_SERVICE partition

IBM computers with this configuration were announced during 2003 and also have an ImageUltra disk image in the IBM_SERVICE partition. The IBM Rescue and Recovery installation for these computers is similar to a default installation. The Rescue and Recovery environment is installed into a virtual partition. However, the Rescue and Recovery environment will link to the PARTIES area to initiate a restore of factory contents or diagnostics as shown in Figure 2-8.

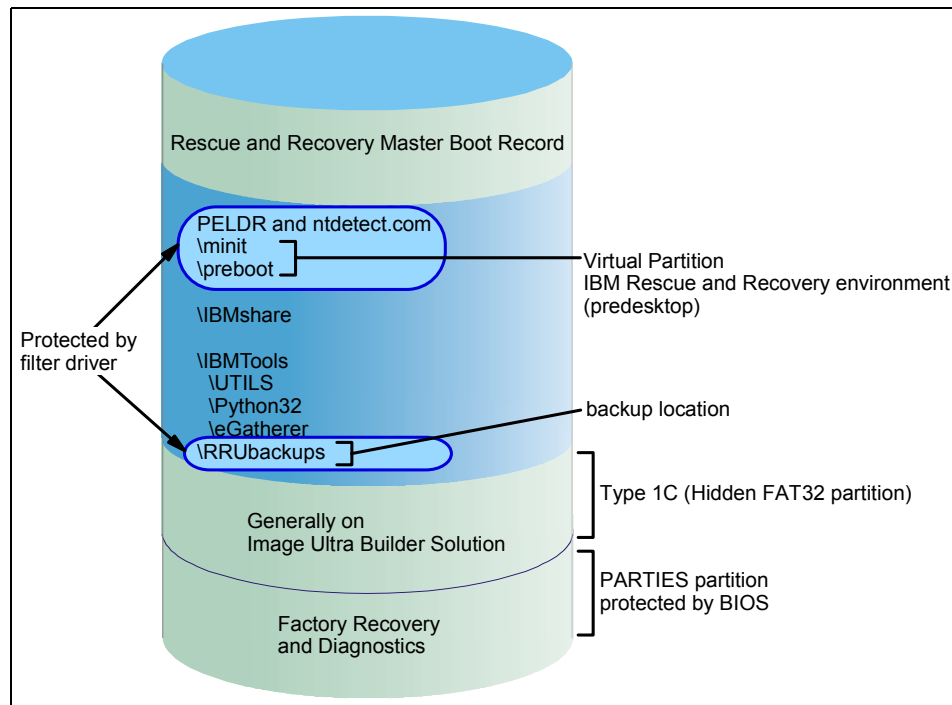


Figure 2-8 Installation on a system with a PARTIES area and type 1C service partition

IBM computers with Rescue and Recovery preinstalled in a type 12 partition

IBM computers announced in the first quarter of 2004 and that come with the IBM Rescue and Recovery environment preinstalled will have this configuration. The Rescue and Recovery environment resides entirely in a type 12 partition, not in the virtual partition as with the previous scenarios. In addition to the Rescue and Recovery environment, the factory recovery and system diagnostics will also reside in the type 12 partition. However, the Rescue and Recovery backups will not reside in the type 12 partition. See Figure 2-9.

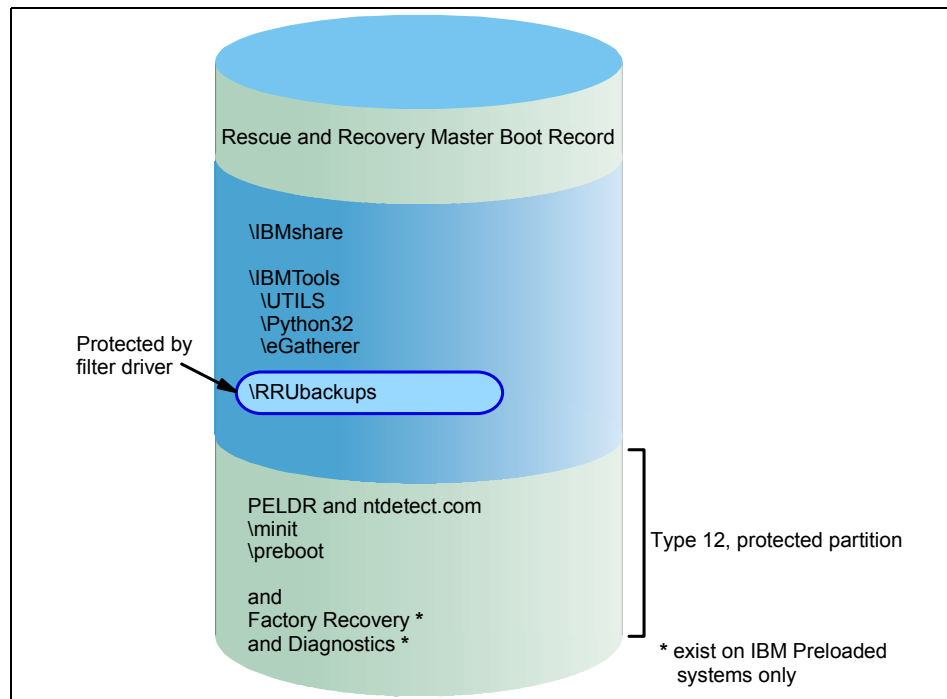


Figure 2-9 Systems with Rescue and Recovery preinstalled in a type 12 partition

The key advantage to placing the Rescue and Recovery environment in a type 12 partition is the excellent protection it affords the files required to open the Rescue and Recovery environment. By contrast, when the Rescue and Recovery environment is placed in a virtual partition, several files are placed in the root of the C drive. The filter driver does not protect these files, because they are shared with Windows boot files (for example, NTDETECT.COM). When placed on the root of the C drive, it is possible that an end user could delete these. If these files are deleted or otherwise become unusable, the end user would be unable to boot to the Rescue and Recovery environment.

When the Rescue and Recovery environment is placed in a type 12 partition, however, Windows will prevent all users from accessing that partition. The files required to open the Rescue and Recovery environment are highly protected. With the Rescue and Recovery environment secured in the type 12 partition, only corruption of the MBR would prevent access to the Rescue and Recovery.

If the MBR becomes corrupted, an external version of the IBM Rescue and Recovery environment must be used. Currently, IBM supports CD and USB hard disk drive-based versions of the Rescue and Recovery environment that are created with the Create Rescue Media applet in the Access IBM folder of the Start Menu.

2.2.3 Rescue and Recovery installation

There are three basic methods of installing Rescue and Recovery:

- ▶ Single-computer standard installation
- ▶ Multiple-computer image deployment from a donor computer
- ▶ Remote installation with application and installation customization

This section describes the installation of Rescue and Recovery on an IBM system with Windows XP Professional. It is a basic single-user, single-system manual installation. Multiple-computer image deployment and remote installation and customizations are described in the *IBM Rescue and Recovery Customization and Deployment Guide*, which is provided with the product. You can download this document from the following Web site:

<http://www.ibm.com/pc/support/site.wss/document.do?ln docid=MIGR-54502>

For a silent installation and simple deployment scenario, see 2.2.4, “Silent installation” on page 31 and 2.2.5, “Setting up a Create Base Backup icon on the user’s desktop” on page 36.

Note: Before installing IBM Rescue and Recovery, you must first uninstall earlier versions of the software. If an earlier version of Rapid Restore is detected, you will be prompted to uninstall the older application. For instructions about how to uninstall the previous version see “Uninstalling Rapid Restore Ultra versions 3.x and Rapid Restore PC 2.x” on page 602.

To begin the installation process:

1. Download the installable program named setup_ibmrrXXXX.exe (where XXXX is the version number, which was 1033 at the time this book was written) from the Web site:

http://www.ibm.com/pc/support/site.wss/license.do?filename=thinkvantage_en/setup_ibmrr1033.exe

2. Execute the installation program.
3. The first window that opens is the IBM Rescue and Recovery Setup. It prepares the InstallShield Wizard.
4. When the Welcome window of the Install Wizard opens, read the information and click **Next**.
5. When the License Agreement window opens, choose **Accept** and click **Next**.
6. The next window indicates the destination folder. The default folder is c:\Program Files\IBM\IBM Rapid Restore Ultra\. Click **Next**.
7. Click **Install** to begin the program installation.
8. The next window (Figure 2-10) allows you to choose to launch IBM Rescue and Recovery after restart. Click **Finish** to complete the installation.

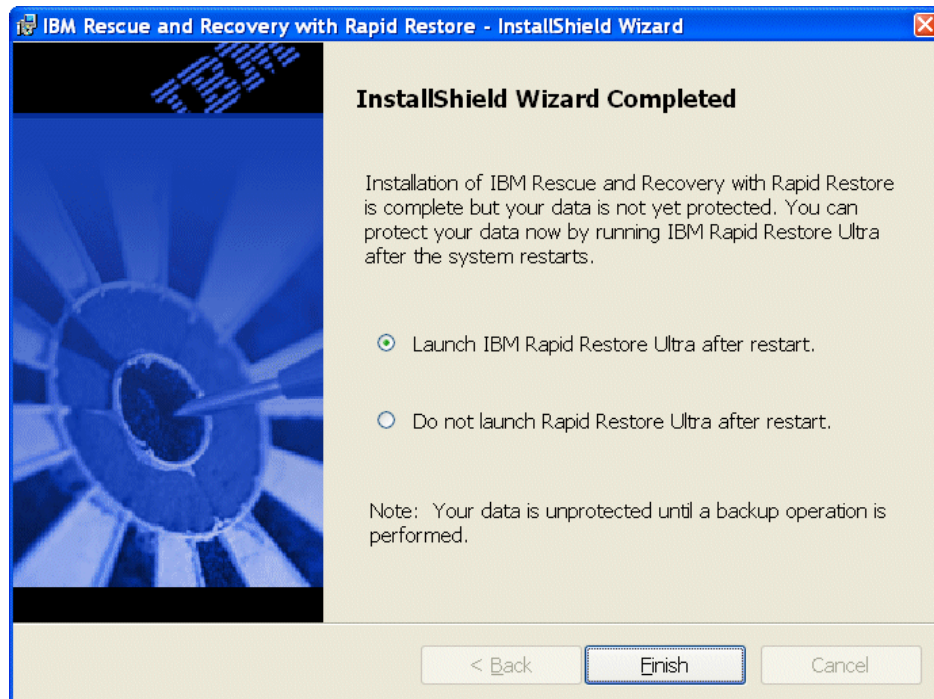


Figure 2-10 Final installation window

9. If you choose the Launch IBM Rescue and Recovery after restart option, you will be presented with the IBM Rapid Restore graphical user interface (GUI) as shown in Figure 2-11 on page 31.

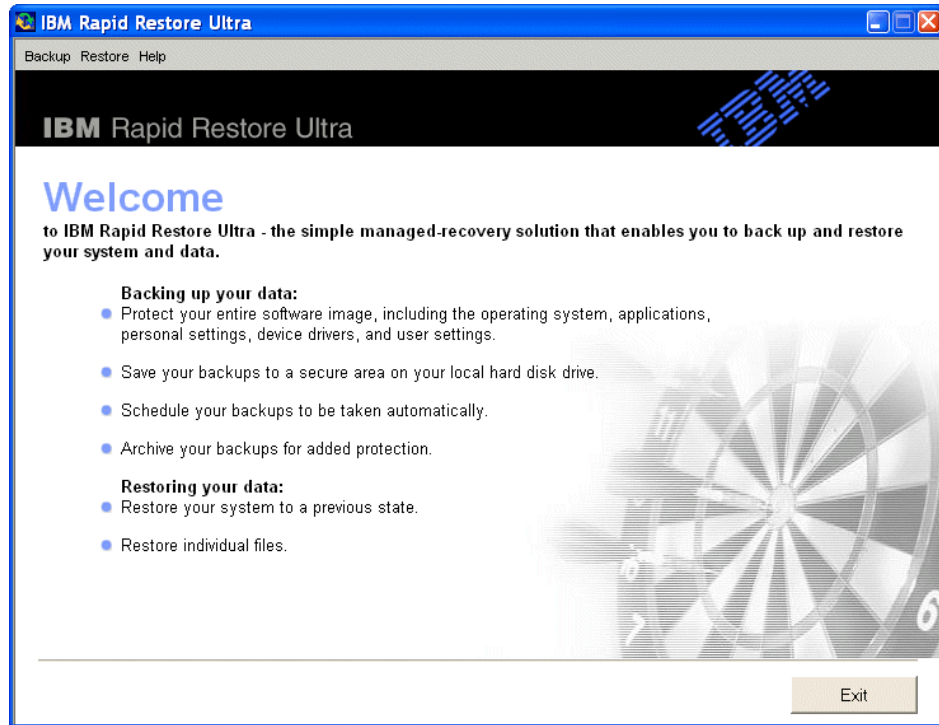


Figure 2-11 IBM Rapid Restore GUI

2.2.4 Silent installation

This section describes a possible silent installation described in *IBM Rescue and Recovery Customization and Deployment Guide*. This may be used when creating an application module in ImageUltra Builder. A silent install involves pre-defining installation and customization parameters so that the actual install process does not require input from the user.

In this scenario, we describe a four-step approach:

1. Performing an administrative install (unpacking installation source files)
2. Customizing Rescue and Recovery
3. Manually installing Rescue and Recovery using MSIEXE
4. Performing a base backup from the command prompt

Performing an administrative install

The Windows Installer can perform an administrative installation of an application or product to a network for use by a workgroup or for customization purposes.

For the Rescue and Recovery installation package, an administrative installation unpacks the installation source files to a specified location.

Launching an administrative installation opens a series of windows that prompt you to specify the location for unpacking the setup files. The default extract location is C:\IBMRNR as shown in Figure 2-12. If you need to place the files that are extracted during an administrative install on a network resource, extract the files locally first. Then copy the extracted files to the network location.

Note: An administrative install is very useful for deploying IBM Rescue and Recovery to multiple systems. It saves a significant amount of installation time once the install file setup_ibmrrXXXX is unpacked.

To perform the administrative install, follow the following steps:]

1. Open a command prompt in the directory containing setup_ibmrrXXXX.exe and type the following:

```
setup_ibmrrXXXX.exe /a
```

A window such as the one shown in Figure 2-12 will open.

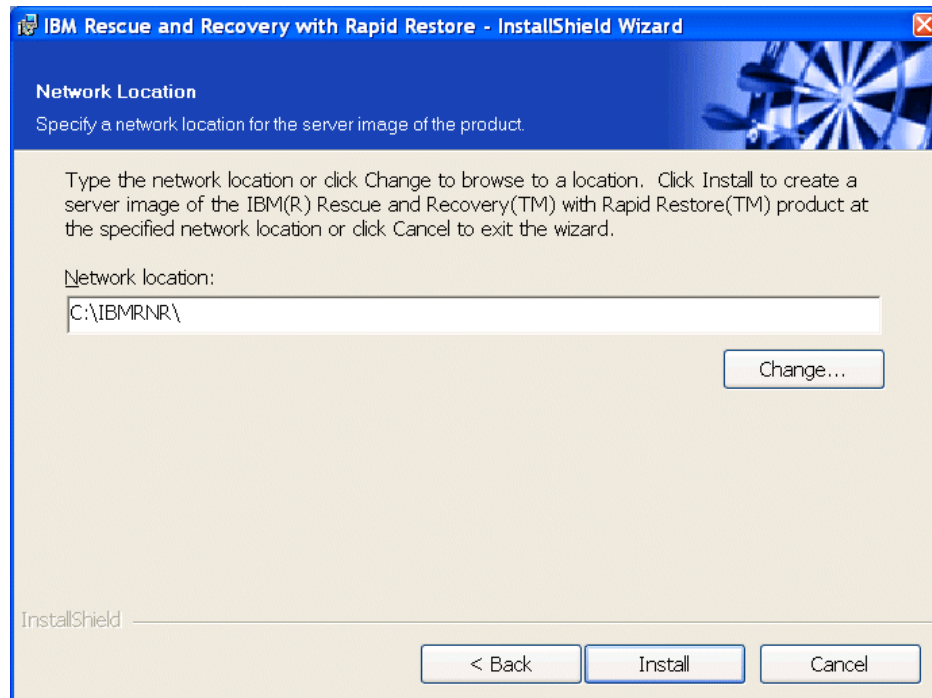


Figure 2-12 Administrative installation

2. Select **Change** to alter the destination location of the IBM Rescue and Recovery Installation files.
3. Select **Install** to start the administrative installation. The window shown in Figure 2-13 opens.

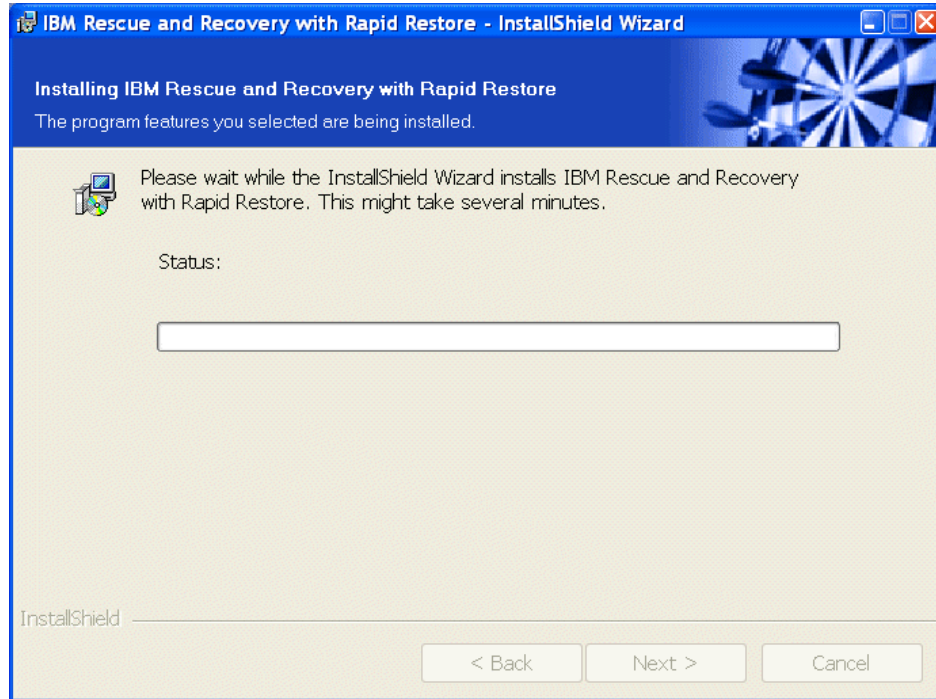


Figure 2-13 Administrative installation progress

4. Select **Finish** on the window shown in Figure 2-14 on page 34 to complete the administrative installation.

The unpacked installation files will be located in the C:\IBMRNR directory. As an alternative, you may extract the setup files from setup_ibmrrXXX to the C:\IBMRNR directory using the following command:

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

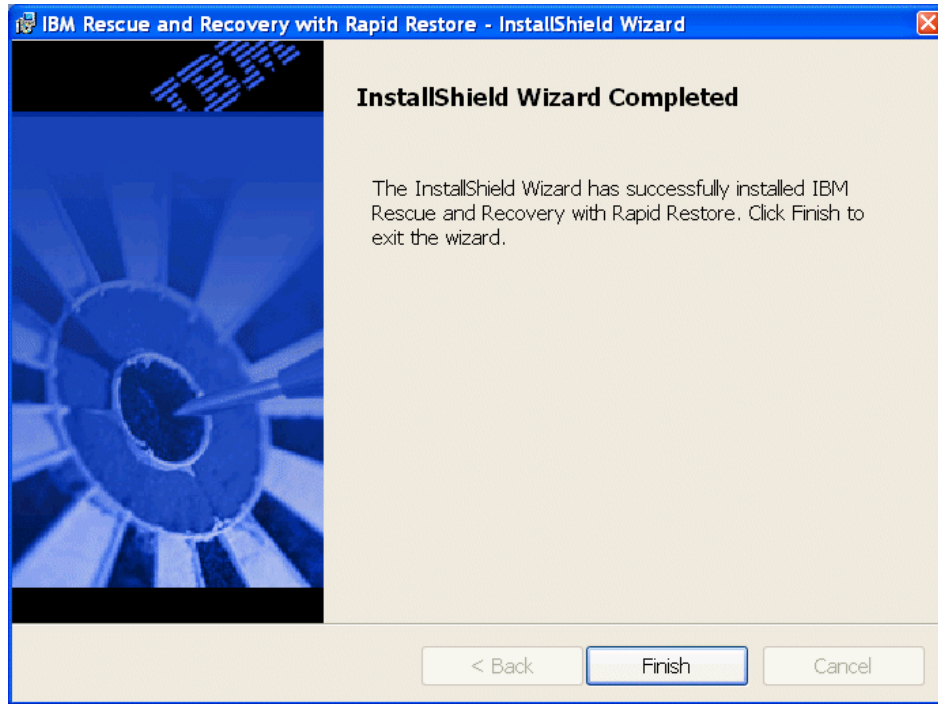


Figure 2-14 Administrative installation finish

Customizing Rescue and Recovery for silent installation

Before proceeding with the product installation, it is possible to customize Rescue and Recovery with the TVT.txt control file. For example, if you want to install IBM Rescue and Recovery and have the GUI hidden from all users except Administrators, proceed as follows:

1. Open the file TVT.txt in C:\IBM\NR\program files\IBM\IBM Rapid Restore Ultra.
2. Add the line:
`HideGUI=0`
3. Add:
`GUIGroup=Administrators`
4. Save and close.

After the installation of IBM Rescue and Recovery, access to the GUI will only be granted to Administrators. For all possible settings and values of TVT.txt, consult “Values and settings of TVT.TXT” on page 591 and the *IBM Rescue and Recovery Customization and Deployment Guide*.

Note: Please note that the TVT.txt file can be altered at any time, either before or after the product installation, depending on the user's permissions. In this example, if you do not want Administrators to have access to the GUI, remove `GUIGroup=Administrators` in `TVT.txt` in `C:\program files\IBM\IBM Rapid Restore Ultra`. For more information about making scripted changes to `TVT.txt`, consult "Making changes to `TVT.txt` via `cfgmod` command" on page 597.

Silent installation of Rescue and Recovery using MSIEXEC

To perform a silent install of the setup files (including a reboot at the end) using MSIEXEC, enter the following command at the command prompt:

```
start /WAIT msixec /i "C:\IBMRR\IBM Rescue and Recovery with Rapid Restore.msi" /qn
```

To perform a silent install of the setup files (without a reboot at the end) using MSIEXEC, enter the following command:

```
start /WAIT msixec /i "C:\IBMRR\IBM Rescue and Recovery with Rapid Restore.msi" /qn REBOOT="R"
```

As part of a deployment, the above command can be put into batch files and incorporated with ImageUltra Builder to create an install module.

If there is no requirement to perform a silent install, you can use the following command:

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

To uninstall Rescue and Recovery using MSIEXEC, type:

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

Note: Only the MSIEXEC install can be used after an administrative install.

Performing a base backup from the command prompt

The following command, which can be easily put into a batch file as part of your deployment procedures, allows you to make a base backup from the command prompt. From the command prompt, enter:

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

Note: `%RRU%` is the system variable that points to where the program files of IBM Rescue and Recovery are installed.

This will create a base backup on the local hard drive. For more information about using the Rescue and Recovery command prompt interface, consult “RRU command prompt interface RRUcmd” on page 598 and the *IBM Rescue and Recovery Customization and Deployment Guide*.

Summary

What we have shown in this section is how to unpack the installation files, perform a silent install of the application, and do a base backup. In the next section, these elements are combined to create a base backup icon to provide the user with a convenient base backup tool.

2.2.5 Setting up a Create Base Backup icon on the user’s desktop

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

1. Perform an administrative install as described in “Performing an administrative install” on page 31.
2. Customize the TVT.txt file as shown in “Customizing Rescue and Recovery for silent installation” on page 34.
3. Initiate the MSI install deferring the reboot with:

```
start /WAIT msixec /i "C:\IBMR\IBM Rescue and Recovery with Rapid  
Restore.msi" /qn REBOOT="R"
```

4. Delete the temporary files in c:\IBMRNR.
5. Create an icon in Documents and Settings\All Users\Desktop called Create Base Backup.
6. Create a batch file (.BAT) with the following command, and link to the created icon from a location you choose:

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

7. Run Sysprep on the system.
8. Create the image for deployment.

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

2.2.6 Creating rescue media

After installation, it is advisable to create rescue media, such as CDs, DVDs, or a USB hard disk drive. These media provide a source from which to recover system files if a system failure prevents you from gaining access to the Windows environment or the Rescue and Recovery workspace. To make the rescue media, proceed as follows:

1. Select **Start** → **All Programs** → **Access IBM** → **Create rescue media**.
2. Select the radio button CD or USB and click **OK** as shown in Figure 2-15.



Figure 2-15 Creating rescue media

- a. If you select **CD**, you will be presented with a prompt like the one in Figure 2-16. Click **OK** and the CD will be created.



Figure 2-16 Creating Rescue Media on CD

- b. If you select **USB**, you will be presented with a prompt similar to the one shown in Figure 2-17 on page 38. Click **OK**. Your system will reboot, and the rescue media will be created on the USB drive.

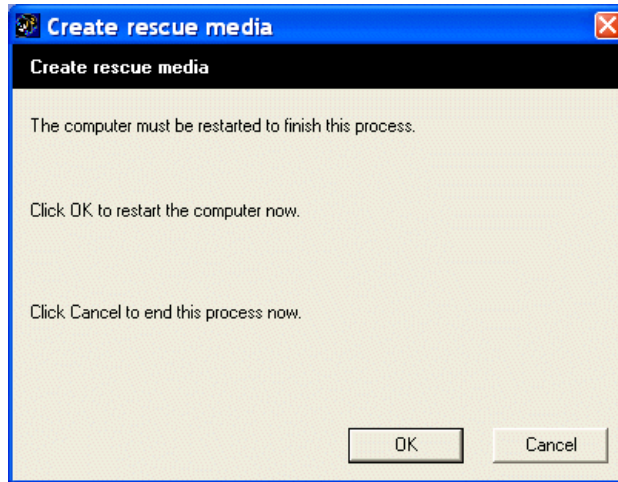


Figure 2-17 Creating rescue media on USB

Note: This process is correct at the time this document was published; however, creating rescue media may be incorporated into future releases of the application.

2.2.7 Uninstall Rescue and Recovery

If you need to uninstall Rescue and Recovery, follow the steps below:

1. Open the Add/Remove programs wizard from Control Panel.
2. Select **IBM Rescue and Recovery with Rapid Restore Ultra** and click the **Remove** button.
3. You will be asked to reboot the system to complete the uninstall process.
4. Click **OK**.

IBM Rescue and Recovery will be removed from your system. To perform a silent uninstall, consult “Silent installation of Rescue and Recovery using MSIEXEC” on page 35.

2.3 System backup

This section covers the procedures you can use to back up your system using Rescue and Recovery features.

2.3.1 Backup considerations

Rescue and Recovery lets you create and manage numerous backups on multiple devices. By default, with Rescue and Recovery, you can store a base backup and five incremental backups locally on your hard disk drive, over a network, on removable media (such as a USB hard disk drive, DVD drive, or CD drive), or on any combination of these drives. It is important to think through your backup strategy before changing your backup storage selections.

With Rescue and Recovery, you can restore your system to a number of backup states, thereby supporting multiple levels of protection. Rescue and Recovery default settings establish a basic level of protection; however, your specific backup strategy and schedule should be customized to meet your specific needs.

When you initiate a manual backup operation using Rescue and Recovery, or when a scheduled backup operation occurs, you can choose where you want to save your backup files. These selections are saved and become the default settings for any ensuing backup operations. However, it is important to understand how IBM Rescue and Recovery will respond when these selections are changed. Therefore, when you perform or schedule a backup operation, you must think through the following considerations:

- Where you want to save your backup files. You can select from the available devices installed on your computer from the window illustrated in Figure 2-18. Select each device.

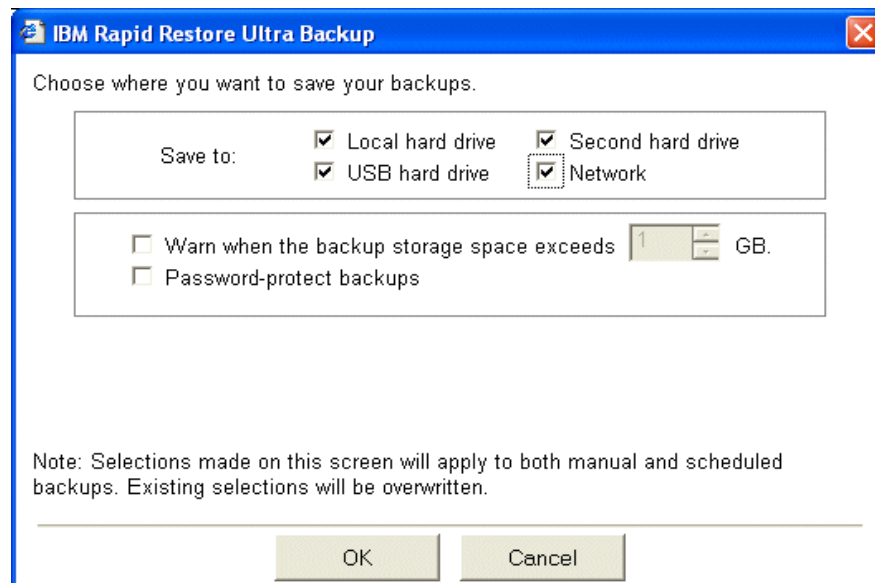


Figure 2-18 Selecting devices

When a new device is selected, Rescue and Recovery creates a *duplicate backup* on each device that is selected. By default, copies of the base backup and five incremental backups can be stored on each device.

- ▶ Deleting old backup files. This same window allows you to clear previously selected devices. When you clear the check box for a device, Rescue and Recovery will no longer save backups to that device, and a dialog box will display asking if you want to delete the backups that are stored on that device. See Figure 2-19.

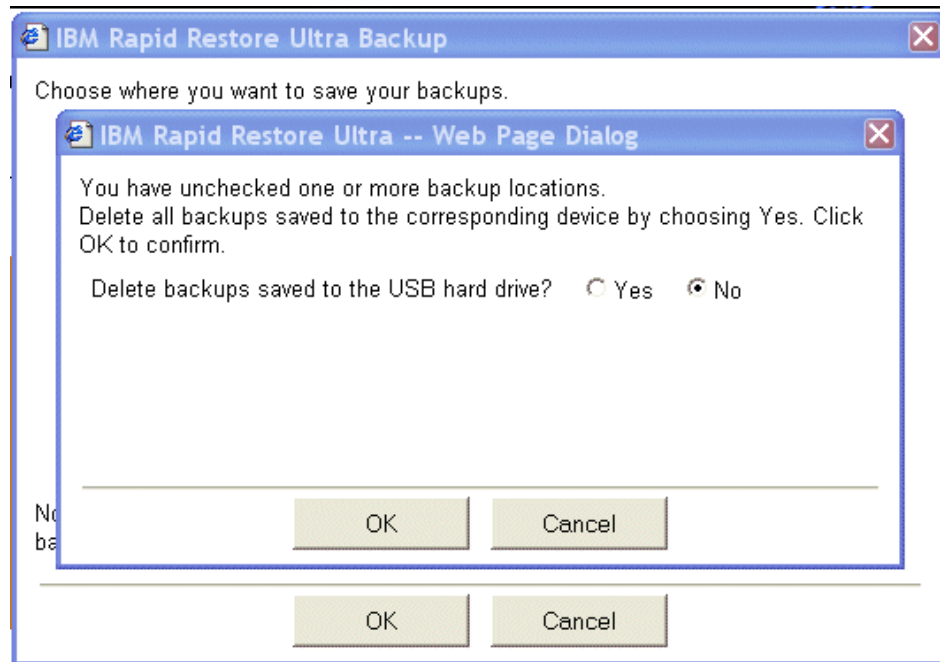


Figure 2-19 Selecting to save backups

- ▶ Delete or archive old backup files. If you do not delete the stored backups, and if the device is later selected again, any previous backups contained on the device will be overwritten by any new backup operation.

If you want to archive previous backups from devices that you later deselect, it is best to archive them to removable media, such as a CD or DVD. If these devices are reselected at a later time, the new backup operation will delete all previous backups.
- ▶ Delete all backup files. You can delete all backup files from all attached devices simply by clearing all of the check boxes when selecting where to save backups. After that, a dialog box informs you that this selection will result in all backups being deleted when the next backup operation is performed. To

reset the base backup and delete all previous backups, simply clear all devices listed on the window shown in Figure 2-18 on page 39 and initiate a new backup operation. All backups will be deleted. Backups can also be deleted from the command prompt interface with the RRUcmd command. See “RRU command prompt interface RRUcmd” on page 598.

2.3.2 Setting backup preferences

How you should set your Rescue and Recovery preferences depends on a number of variables. Use the following information to determine what settings best suit your needs. Most users fall into one of the following categories:

- ▶ Large enterprise users

Some large enterprise users have system administrators who prefer to manage the settings of IBM Rescue and Recovery. These settings are set for the entire enterprise and can be used or changed remotely.

- ▶ Small business users

Small business users that do not have system administrator support should set their preferences mindful of their business needs and the limitations of their workstation. Depending upon the available space available on their hard drive, network considerations, and their sensitivity to data loss, small business users should establish a strategy that includes scheduled backups and systematic copying of saved backup files. Backup features such as backup encryption and password protection should also be considered.

- ▶ Storage-sensitive users

Computer users that must conserve space on their hard drives should set their backup preferences to preserve hard disk space. Storage-sensitive users can reduce the default number of backups stored on the local hard disk, or they can store their backups directly to a remote device, such as a USB hard disk drive or a network location. If this is not possible, remote users can systematically copy their backup files to a removable medium, such as a CD drive or DVD drive.

- ▶ Mobile computer users

Mobile computer users must be sensitive to the possibility of data theft and data loss. Consequently, mobile computer users should use the backup encryption and password protection features, and should copy their backups for safe keeping. Mobile computer users might consider keeping a set of backup CDs or DVDs with their computer.

The Rescue and Recovery program has other features that are useful and convenient for many users. The following functions can help reduce backup size,

save user time, and provide additional protection from data loss. Additional Rescue and Recovery features include:

- ▶ **Exclude function**

Excluding files or folders can help backup operations complete more quickly and reduce the overall backup size. Common folders to be excluded might include a folder containing temporary files or a folder containing copies of server mail files. When excluding files from a backup, make sure that the excluded files are not necessary for the continued operation of the computer. Otherwise, if this backup is used in a restore procedure, the computer will not function properly.

- ▶ **Wake from suspend function**

Use this function to set the computer to awake from a suspended state. This enables backup operations to be scheduled while users are away, even if the computer is in suspend mode. This function might not be appropriate for some mobile computer users. See “Procedure for scheduling backups” on page 53.

Setting preferences

The *Set your preferences* window lets you customize IBM Rescue and Recovery backup functionality by enabling users to select which partitions, files, and folders to include or exclude.

Important: Configuration settings made in the *Set your preferences* window will apply to both manual and scheduled backups. All existing configuration settings will be overwritten.

To set your preferences, complete the following procedure:

1. Open Rescue and Recovery.
2. Click **Backup**.
3. Select **Set Preferences**.

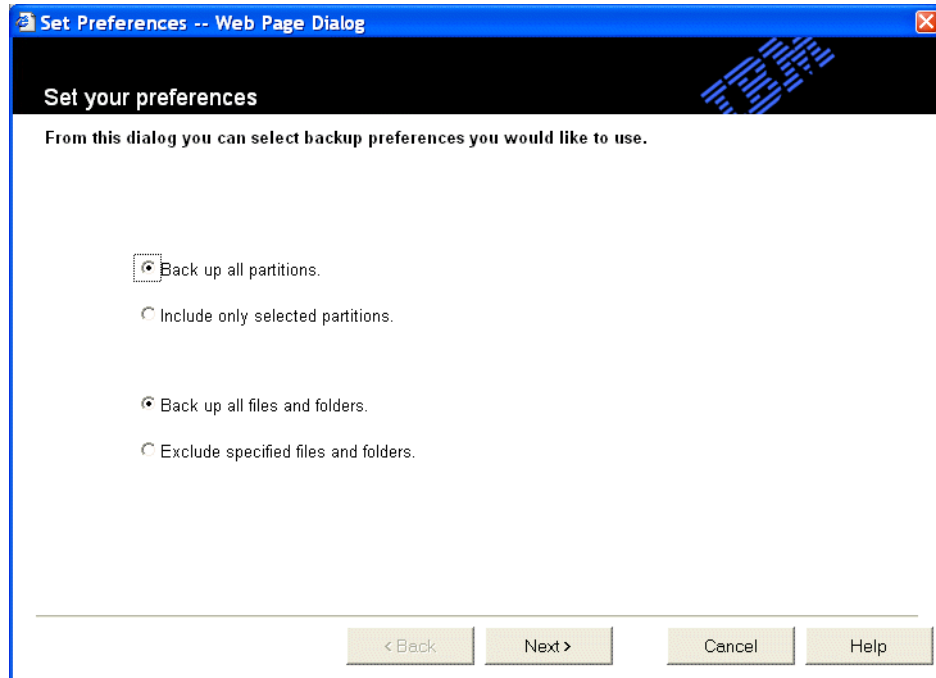


Figure 2-20 Set Preferences window

4. From the Set Preferences window (Figure 2-20), choose one of the following partition backup options:

- a. Back up all partitions

This option is the default setting. It backs up all partitions on the local hard drive. It provides the most backup protection and ensures that you have every file backed up.

- b. Include only selected partitions

When you select the **Include only selected partitions** radio button and click **Next**, a window opens that displays all of the partitions on your local hard drive. Only the partitions you select will be backed up. This option is useful when you do not want to back up all the partitions on your hard drive.

5. Choose one of the following file and folder backup options:

- a. Back up all files and folders

This option is the default setting. It backs up all files and folders on the selected partitions of the local hard drive. It provides complete backup protection for the selected partitions.

- b. Exclude specified files and folders.

When you select the **Exclude specified files and folders** radio button and click **Next**, a window opens. Click the + next to the folder to expand its contents as shown in Figure 2-21. Select the files or folders you wish to exclude from the backup.

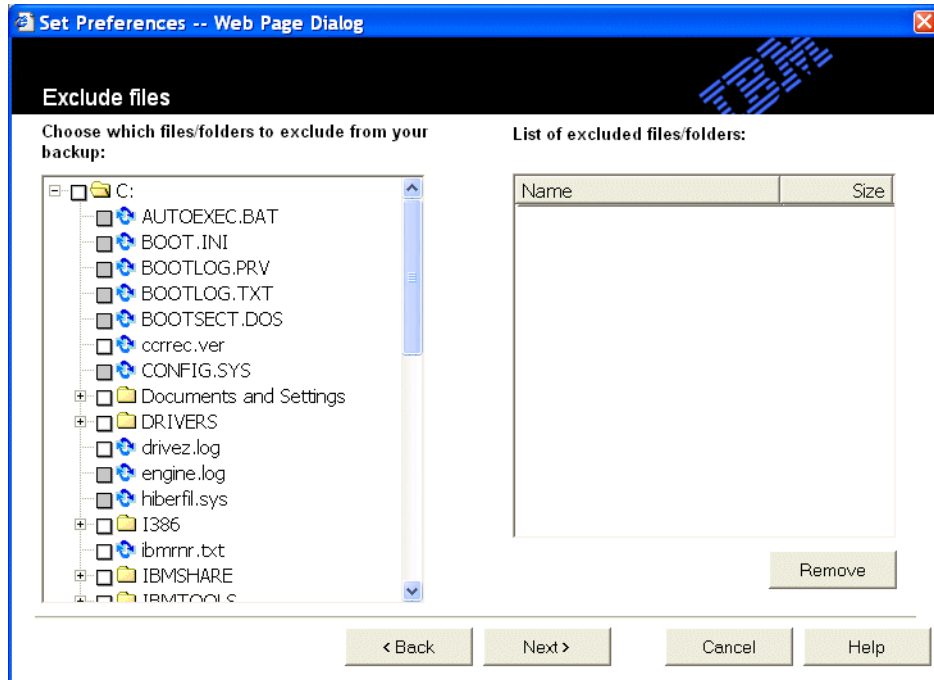


Figure 2-21 Exclude window

Restriction: Some files and folders on the selected partitions might not be available for exclusion. The Exclude files option does not enable users to exclude files or folders that are essential to the operating system or the system-restore process.

6. Click **Next**.
7. The summary window displays the choices that you have made. Use this window to review your choices before continuing with any further backup operations. Click the **Back** button if you need to make any selection changes.

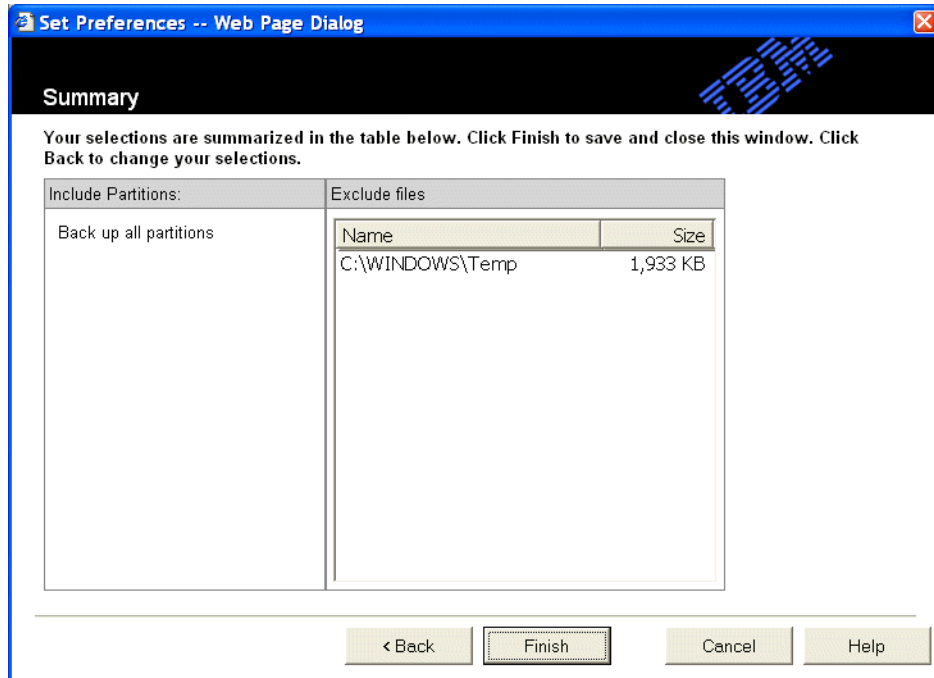


Figure 2-22 Preferences Summary window

8. Click **Finish** to accept the preference settings you selected.

2.3.3 Backing up your system

Rescue and Recovery uses a hidden, protected folder (\RRUbackups) on the local hard disk to save your compressed backup files. It also backs up and protects the entire contents of the hard disk, including the Microsoft Windows OS, software applications, registry settings, network settings, fix packs, desktop settings, and unique data files. To initiate a backup procedure, use the *Back up now* window (shown in Figure 2-24 on page 47). A backup of the entire image (base backup) is required before any incremental backups can be done.

Before you begin your initial backup operation, it is best to complete the following tasks:

- ▶ Load all applications.
- ▶ Configure and set up all user specific printers.
- ▶ Configure and set up all user specific network connections.
- ▶ Run a virus scan.

- If you are backing up to network drive location, create a shared directory for the backup files.

Manual Backup Procedure

To initiate a manual backup operation, complete the following steps:

1. From the Rescue and Recovery main window, click **Backup** and select **Back up now** from the menu.

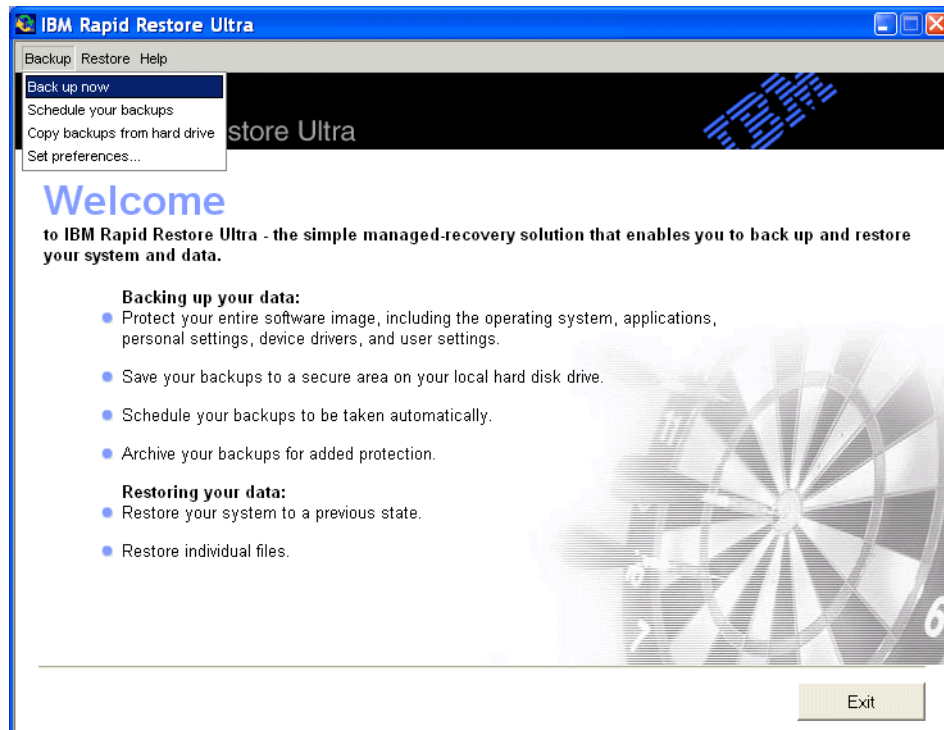


Figure 2-23 Main Backup window

2. Name the backup files by typing a name in the Save as field. This step is optional, but is very useful when differentiating between user specific saved backup files. All backup files will automatically be stamped with the date and time of their creation. See Figure 2-24 on page 47

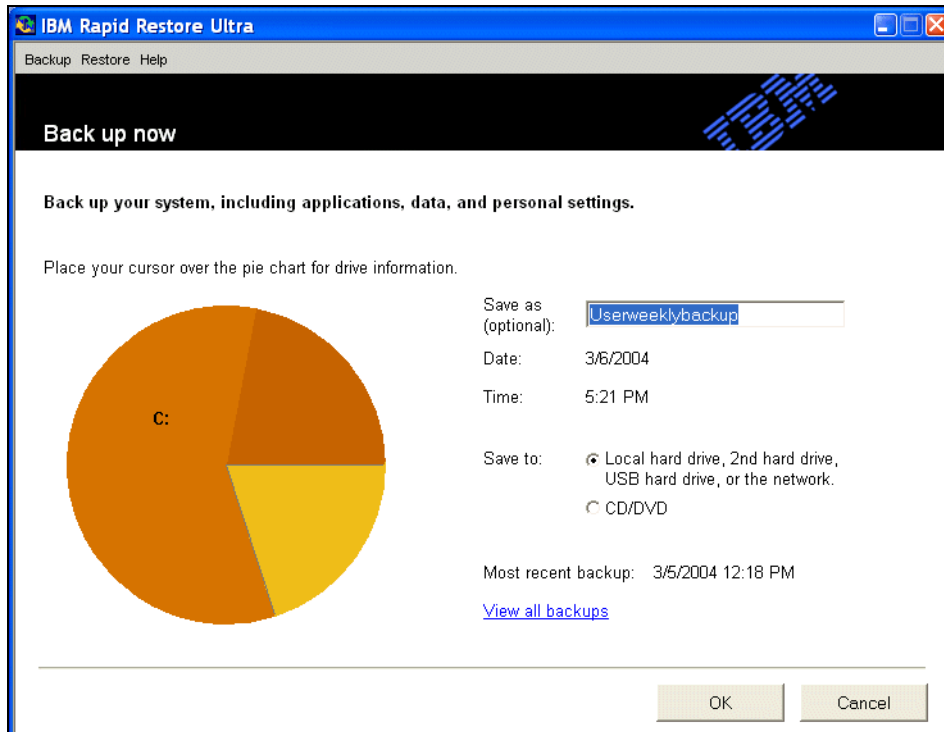


Figure 2-24 Backup location and name in Back up now window

Note that the **Back up now** window also displays a pie chart that illustrates the amount of free space available on your hard drive. You can view the partition current free space by moving your cursor over the partitions on the pie chart.

3. Select the device or devices to which you want to save the backup files by choosing the appropriate **Save to** radio button and clicking **OK**. Radio button selections include:
 - Local hard drive, 2nd hard drive, USB hard drive, or the network
 - CD or DVD
4. If you choose a local hard drive, 2nd hard drive, USB drive, or the network, the Backup to location window will open. See Figure 2-25 on page 48.

In this window, choose a location or multiple locations for your backup files using the appropriate check box or check boxes.

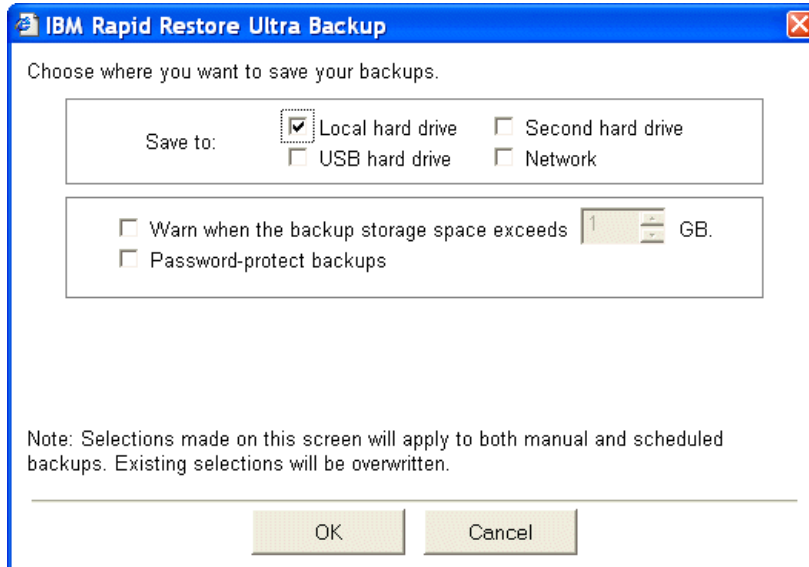


Figure 2-25 Backup to location window

5. If you select **Network** in the *IBM Rapid Restore Ultra Backup* window (Figure 2-25), a *Map Network Drive* window will open and ask for the Path, Username, and Password. Enter the path to the shared backup location (for example, \\server\share). See Figure 2-26.

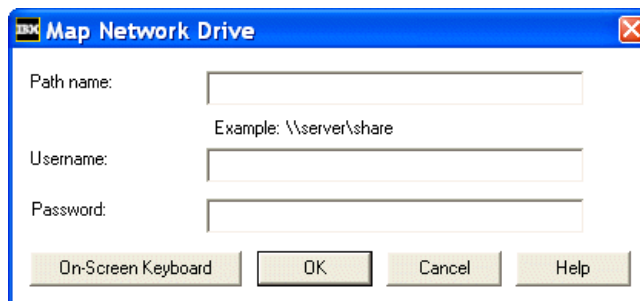


Figure 2-26 Map Network Drive window

Important: If you back up multiple machines to a shared network resource, you must make sure that each machine has its own unique backup location on the shared drive, otherwise one machine will overwrite the backup files of another one if they use the same location.

6. If desired, use the **Warn when the backup storage space exceeds xx MB** check box to establish a storage threshold for Rescue and Recovery to monitor the storage capacity of your backup media as shown in Figure 2-25 on page 48. This option enables you to specify the amount of storage space in the hidden, protected folder. Valid options range from 1 GB to the maximum available space on your hard drive. This option does not reserve any space on the hard drive, rather it sets a trigger that will notify you if the selected storage threshold is reached.

Note: Selecting this feature will prompt the user to continue if backup storage space exceeds xx MB in a manual backup mode only. A scheduled backup will proceed with no prompt using the available space on the hard drive.

7. If desired, add a password to your backup files by selecting **Password-protect backups** (see Figure 2-25 on page 48). This option enables you to protect your backup with a password. Users will be required to provide the password before a restore procedure can be initiated. Rescue and Recovery and the Rescue and Recovery environment use the same password. When a backup is password protected through the Rescue and Recovery interface, it is also necessary to provide this password to access the Rescue and Recovery environment. Likewise, if a password is set for the Rescue and Recovery environment, this same password is required to restore a backup with Rescue and Recovery. Password protection is disabled by default.
8. Click **OK** after making the selections shown in Figure 2-25 on page 48.
9. If you selected to backup to a CD or DVD, the prompt depicted in Figure 2-27 will display. Choose your recording device and click **OK** to proceed.



Figure 2-27 Choose CD or DVD prompt

10. A message to make sure blank media is entered in your CD or DVD drive will be displayed. Click **OK** for the backup process to begin. If you want to know how many disks the direct backup to CD or DVD media will require, proceed as follows:

- a. From your desktop, open **My Computer** and right click the **C:\ drive**. Then choose **Properties**.
- b. Select the **General** tab. It will identify the used space on your hard drive.
- c. Divide the used space by the capacity of your backup media (e.g. CDs are typically 650MB, DVDs are typically 4.7GB) and then round the result up to the next integer. Used space includes files that won't be backed up (existing backups, hibernation file, etc.).

Important: Make sure that your system is connected to an AC power supply before initiating a backup, restore, or archive procedure. Failure to do so can result in data loss, or an irretrievable system failure.

2.3.4 Archiving backups

Rescue and Recovery enables you to use removable media (USB hard disk drive, DVD drive, or CD drive) to restore the contents of the hard disk in the event of a hard disk drive failure.

Copying your backup files to removable media enhances backup protection and enables you to restore your system from any of your archived backup files.

To archive your backups, complete the following procedure:

1. From the Rescue and Recovery main window, click **Backup** and select **Copy backups from hard drive** from the menu as shown in Figure 2-28 on page 51.

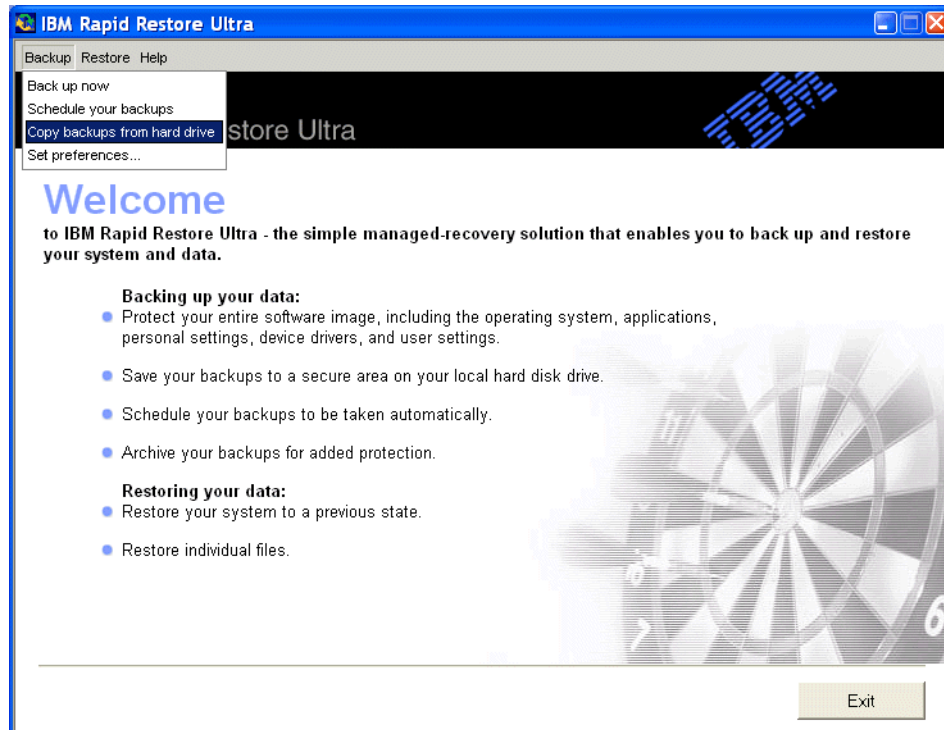


Figure 2-28 Choose Copy Backups from hard drive

2. Select the medium you want to save your backup files to by clicking the appropriate radio button. The backup files that will be copied are listed on the user interface. See Figure 2-29.

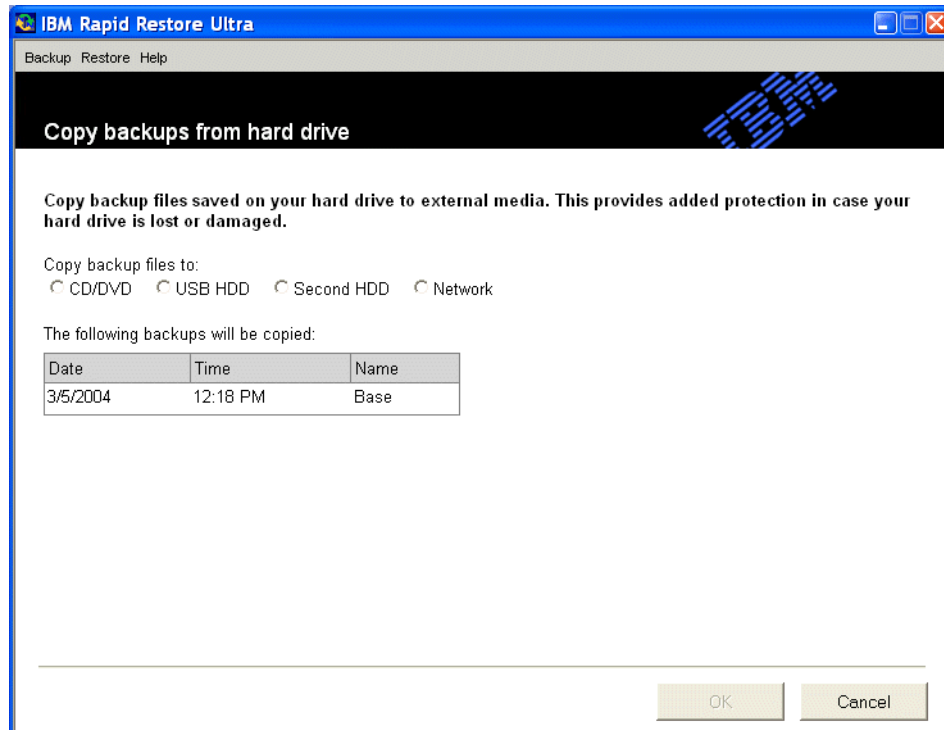


Figure 2-29 Copy backups from hard drive selection window

3. Click **OK** to continue.

Note: For the program to display the number of CDs or DVDs that are required when using this media, you must be logged on as the administrator.

2.3.5 Scheduling backups

Establishing a schedule for your backup operations ensures that your files will be systematically protected without user intervention. Use the Schedule your backups feature to schedule automatic backup operations to take place on a daily, weekly, or monthly basis on a day and at a time of your choosing. This function is disabled in the default Rescue and Recovery settings. It can be enabled as required. If you prefer not to have backup operations take place

automatically, you can use the Schedule your backups feature to disable scheduled backup operations if this was enabled previously.

If the computer has been shut down or is in standby mode when a backup operation is scheduled to take place, the backup operation will not take place at the scheduled time unless the Launch backup when in suspend mode function has been enabled. If this feature is not enabled, when the computer is started or awakened from the sleep mode, Rescue and Recovery displays a message asking if you want to perform a backup operation at that time.

Procedure for scheduling backups

To schedule backups, take the following steps:

1. From the IBM Rescue and Recovery main window, click **Backup** and select **Schedule your backups** from the drop-down list. See Figure 2-30.

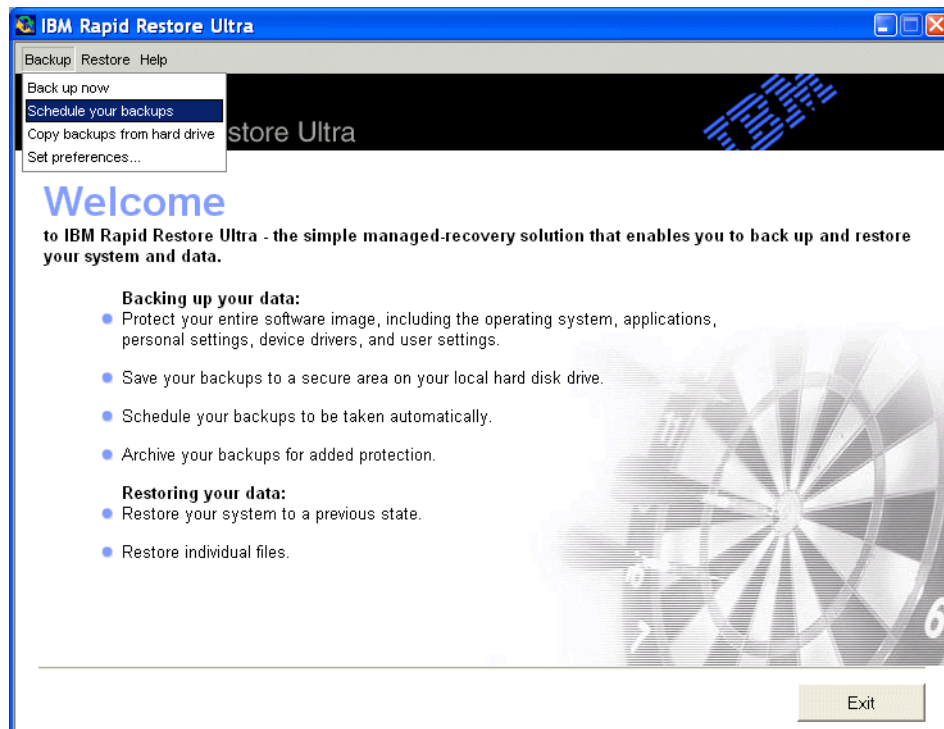


Figure 2-30 Select Schedule your backups from the dropdown list

2. Select the **Schedule: On** radio button to display the Frequency and Time settings as shown in Figure 2-31.

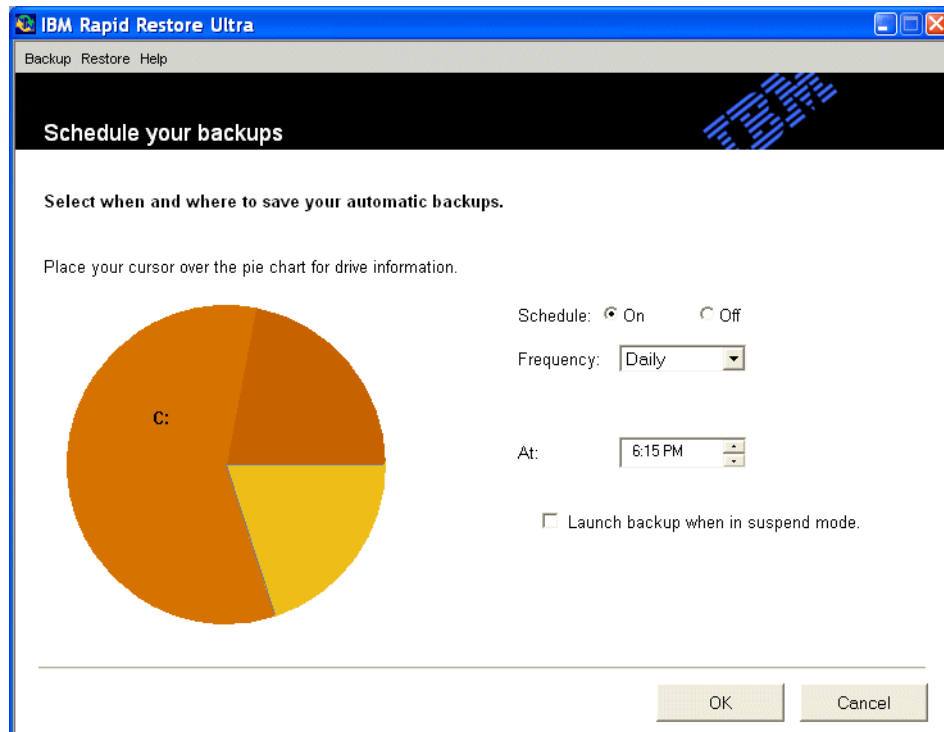


Figure 2-31 Frequency and Time window

3. Select the **frequency**, **time**, and **day** of your scheduled backups.

Restriction: Rescue and Recovery does not allow you to specify a scheduled monthly backup operation to take place on the 29th, 30th, or 31st day of the month. However, you can schedule the backup operation to take place at the end of the month.

4. Select the **Launch backup when in suspend mode** check box, if required.
5. Click **OK**.
6. Select the device or devices to which you want to save the scheduled backups. Options include the local hard drive, a second hard drive, a USB hard drive, or a network. You can select more than one device. See Figure 2-25 on page 48.

Note: If you are backing up to more than one device in a scheduled backup, make sure that all the devices are available. If one of the devices is not available, then the backup will not proceed.

7. Establish a storage threshold for Rescue and Recovery to monitor, if desired. Select **Warn when the backup storage space exceeds X MB**. This option enables you to specify the amount of storage space available to the hidden, protected folder (\RRUbackups). Valid options range from 1 GB to the maximum available space on your hard drive. This option does not reserve any space on the hard drive. It sets a trigger that will notify you when the selected storage threshold is reached. As mentioned before, this selection will not prevent a scheduled backup from proceeding if the threshold has been exceeded.
8. Add a password to your backup files, if desired, by selecting **Password-protect backups**. This option enables you to protect your backup with a password. Users will be required to provide the password before a restore procedure can be initiated. IBM Rescue and Recovery and the IBM Rescue and Recovery environment use the same password. When a backup is password protected through the IBM Rescue and Recovery interface, it is also necessary to provide this password to access the IBM Rescue and Recovery environment. Likewise, if a password is set for the IBM Rescue and Recovery environment, this same password is required to restore a backup using IBM Rescue and Recovery. Password protection is disabled by default.
9. Click **OK** to initiate the backup operation.

Selections made on this window will apply to both manual and scheduled backups. Existing selections will be overwritten.

2.3.6 Disabling scheduled backups

To disable scheduled backup operations, complete the following procedure:

1. From the Rescue and Recovery main window, click **Backup**.
2. Click **Schedule your backups**.
3. Select the **Schedule: Off** radio button. See Figure 2-31 on page 54.
4. Click **OK**.

No further automatic backup operations will occur unless you enable the scheduling function again. You can perform backup operations manually by selecting Backup now under the Backup menu on the Rescue and Recovery main window.

2.3.7 Backing up encrypted files

When backing up encrypted files, Rescue and Recovery provides support for the following encryption methods:

- ▶ Windows Encrypting File System (EFS)
- ▶ IBM File and Folder Encryption (FFE)

Restriction: Previous versions of Rapid Restore Ultra or Rapid Restore PC are not compatible with these encryption techniques.

During a backup operation, Rescue and Recovery ensures that both Windows EFS and IBM FFE files are backed up in their encrypted format. During a *full-restore* operation only, Rescue and Recovery ensures that both Windows EFS and IBM FFE files are restored to their original location in their encrypted format. Rescue and Recovery also enables users to restore individual encrypted files and folders from an *incremental* backup with the following limitations:

- ▶ Windows EFS files

Individual files encrypted by Windows EFS can only be restored using Rescue and Recovery from the Windows operating system and for the current logged in user. These files cannot be restored using the IBM Rescue and Recovery preboot environment.

- ▶ IBM FFE-encrypted files

Individual files encrypted by IBM FFE can only be restored using the IBM Rescue and Recovery preboot environment. Furthermore, these files must be restored to their original location to be successfully restored.

Important: If you use FFE, you should ensure that the database that FFE uses to track which folders are protected by FFE also has an .NSF extension. To ensure the files are always backed up, include the entry c:\Program Files\IBM\Security*flt.nsf in the ibmincl file.

2.4 Restoring your system

In this section, we describe the different ways Rescue and Recovery allows you to restore your system both from the Windows environment (see 2.4.4, “Restoring your system from Windows” on page 70) and from the Rescue and Recovery environment (See 2.4.1, “Using the Rescue and Recovery environment” on page 57 through 2.4.3, “Rescue and Recovery menu options” on page 61). We also describe the process of using the additional features in the Rescue environment.

2.4.1 Using the Rescue and Recovery environment

Rescue and Recovery provides an environment that runs independently of and is hidden from the Windows operating system. Because the Rescue and Recovery workspace is hidden, it is immune from most types of virus attacks and provides a safe place from which to perform rescue and recovery operations that might not be possible in the Windows environment.

Restrictions and limitations

The Rescue and Recovery workspace is designed for emergency use only, not day-to-day operations. To help ensure that the Rescue and Recovery workspace is ready if you need it and prevent data in the Rescue and Recovery workspace from being accidentally modified or infected by a virus, the following restrictions have been implemented:

- ▶ You cannot store data in the Rescue and Recovery workspace. All data must be stored in the Windows environment or on other media, such as diskettes, a USB hard disk or a network drive.
- ▶ You cannot install application programs in the Rescue and Recovery workspace.

There are also the following functional limitations:

- ▶ You cannot print from the Rescue and Recovery workspace.
- ▶ Network, Internet and intranet communications require a wired Ethernet connection. Dial-up and wireless connections are not supported.
- ▶ Although USB devices are supported, you must attach them to the USB connector before you open the Rescue and Recovery workspace. Otherwise, they will not be recognized.
- ▶ Support for USB diskette drives is currently limited to the following:
 - IBM USB Portable Diskette Drive (05K9276)
 - IBM ThinkPad USB Diskette Drive (22P7056)

Accessing the Rescue and Recovery workspace

To access the Rescue and Recovery workspace, press the blue Access IBM button on a ThinkPad or the F11 key on a ThinkCentre to interrupt the boot.

Note: For ThinkPad systems that did not come with IBM Rescue and Recovery installed, make sure the BIOS is at the latest available level to use the Access IBM key. Otherwise, you must use the F11 key.

When the Rescue and Recovery workspace is launched you will be presented with a Welcome dialog with a brief description of the features that are available. This is illustrated in Figure 2-32.

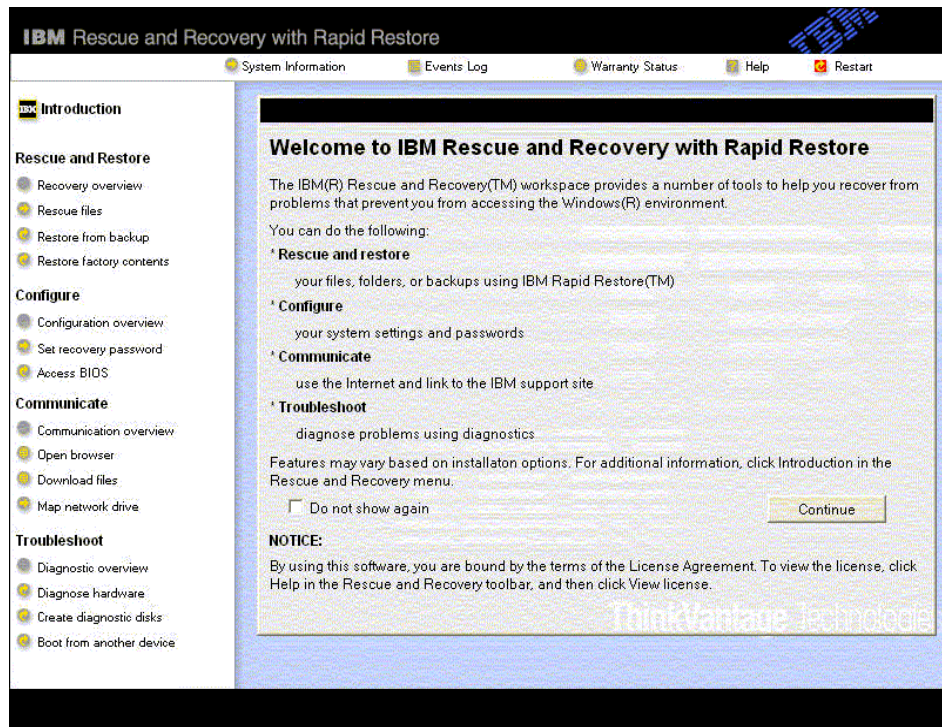


Figure 2-32 Rescue and Recovery welcome window

Click **Continue** to access the toolbar and menu options in the Rescue and Recovery environment.

2.4.2 Rescue and Recovery toolbar

The Rescue and Recovery toolbar allows you to access the following types of information that might assist in diagnosing a problem.

System information

When you click **System Information** on the Rescue and Recovery toolbar, you will be presented with the System Information Viewer as shown in Figure 2-33 on page 59. The information presented in the System Information Viewer enables you to see key hardware and software information about your computer.

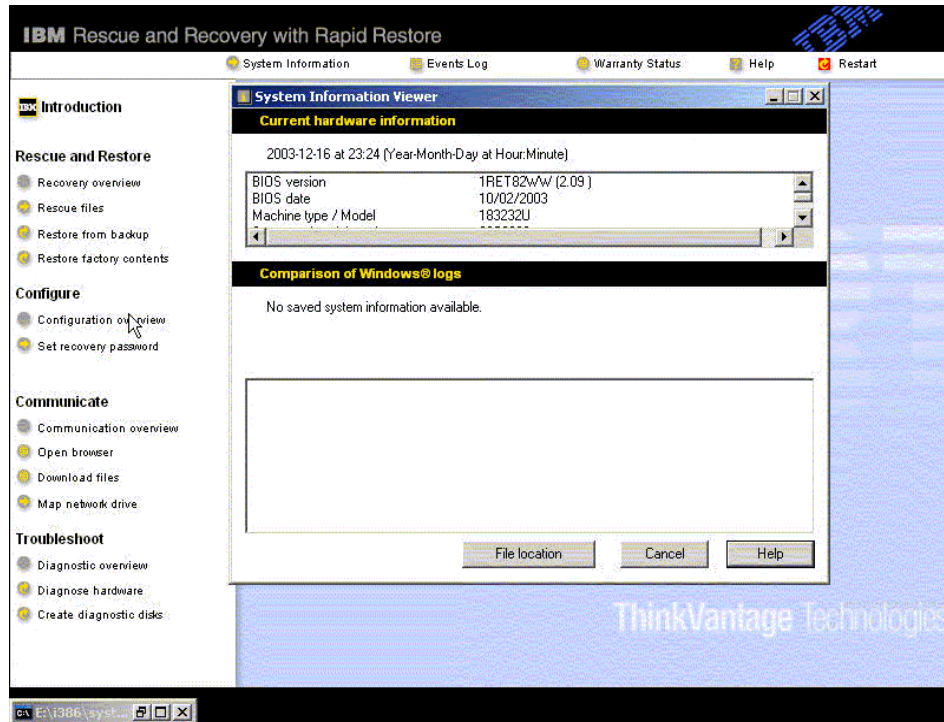


Figure 2-33 Rescue and Recovery System Information Viewer

This information is valuable when trying to diagnose a problem. For example, it can help you identify if and when a change occurred on your computer that might have coincided with a failure. The information is shown in two different formats:

1. Current hardware information:

Provides limited information about your computer in its current state as detected by the Rescue and Recovery workspace.

2. Comparison of Windows logs:

Provides detailed information about your computer hardware and software as detected in the Windows environment and recorded in the two most recent system-information logs. Any changes between the logs are identified by an asterisk.

Note: By default, snapshots of your computer system information are scheduled to be recorded in the system-information log on a weekly basis.

Events log

When you click **Events Log** in the Rescue and Recovery toolbar, the Events Log Viewer, shown in Figure 2-34, opens. Events are recorded in the events log after certain events or tasks associated with Rescue and Recovery operations are performed. For example, when a Rescue and Recovery backup operation takes place, the date, time, completion status, and other associated information are recorded in the events log.

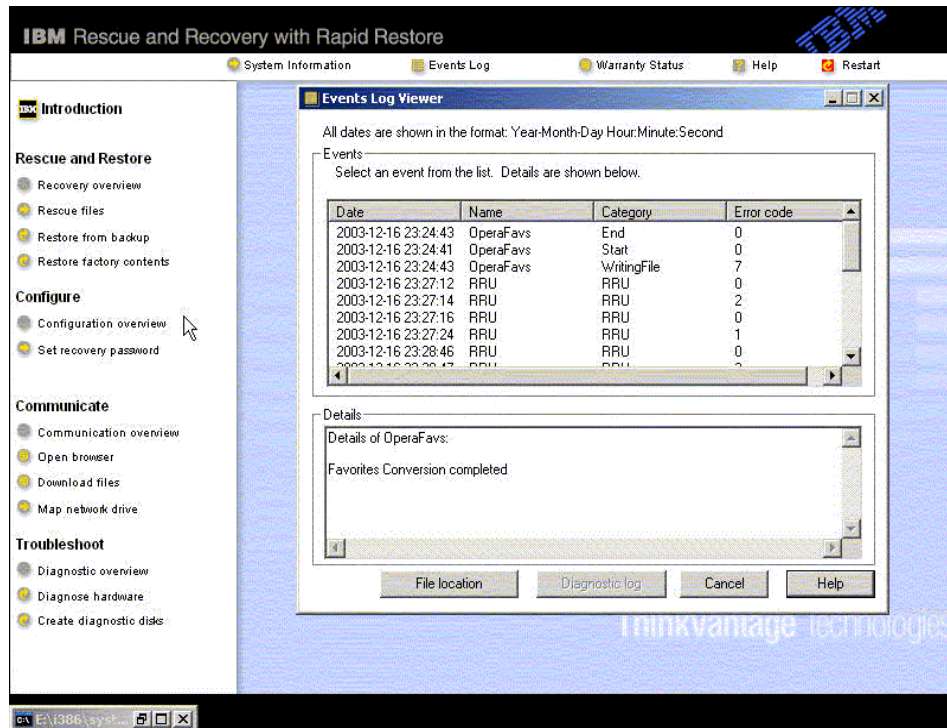


Figure 2-34 Rescue and Recovery Event Log view

The Events Log Viewer provides two levels of information:

1. Events

This provides a summary of the events, including when each event took place and any errors that might have occurred.

2. Details

This provides details about a selected event.

Warranty status

When you click **Warranty Status** from the Rescue and Recovery toolbar, an IBM Web page that lists all the applicable warranties and their expiration statuses for your computer as illustrated in Figure 2-35 appears.

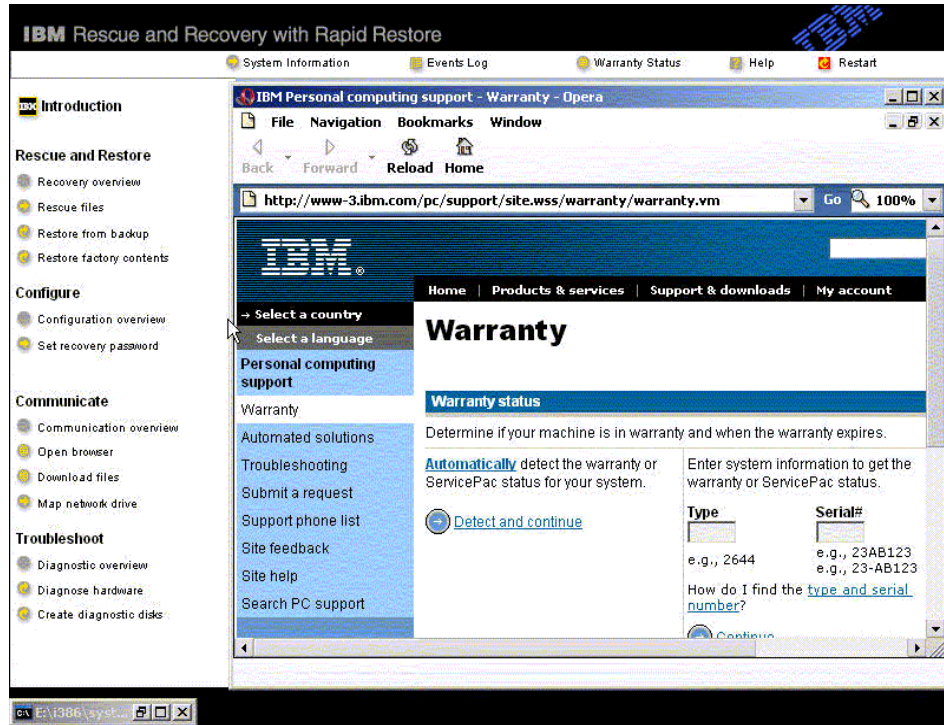


Figure 2-35 Rescue and Recovery Warranty status view

Note: This function requires access to the Internet through a wired Ethernet connection.

Restart

If you select **Restart** from the Rescue and Recovery Toolbar, you will restart your system.

2.4.3 Rescue and Recovery menu options

The menu options in the Rescue and Recovery Environment are grouped into four major categories as shown in Figure 2-35 on the left side panel. We discuss each of these in this section.

Rescue and Restore

This group of menu items provides three primary recovery options that address almost any situation:

- ▶ Rescue files from your hard disk or from a backup
- ▶ Restore your hard disk from a backup
- ▶ Restore your hard disk to its original factory content

Recovery Overview

Recovery Overview links users to help topics about the various recovery options that IBM provides. To access this function, click **Recovery Overview** and follow the steps in the easy-to-navigate windows that will open.

Rescue files

The Rescue files function enables you to locate files that were created or stored in the Windows environment and transfer those files to a network drive or other media (such as diskette or USB hard disk drive). You can use any of the following as the source for your files:

- ▶ Local hard disk drive
- ▶ Network drive
- ▶ Backup created by Rescue and Recovery (this backup can be stored on a local disk, network drive, or USB hard disk)

If you click **Rescue Files**, the Restore Files and Folders window illustrated in Figure 2-36 on page 63 opens.

To restore individual files and folders, you can follow the same procedure as described in “Restoring individual files and folders” on page 73 from step 2.

This method is extremely useful if:

- ▶ You are unable to start Windows and need to continue working with rescued files on another computer.
- ▶ You need to make copies of one or more files before restoring the hard disk from a backup.
- ▶ You need to restore the hard disk to its factory content.

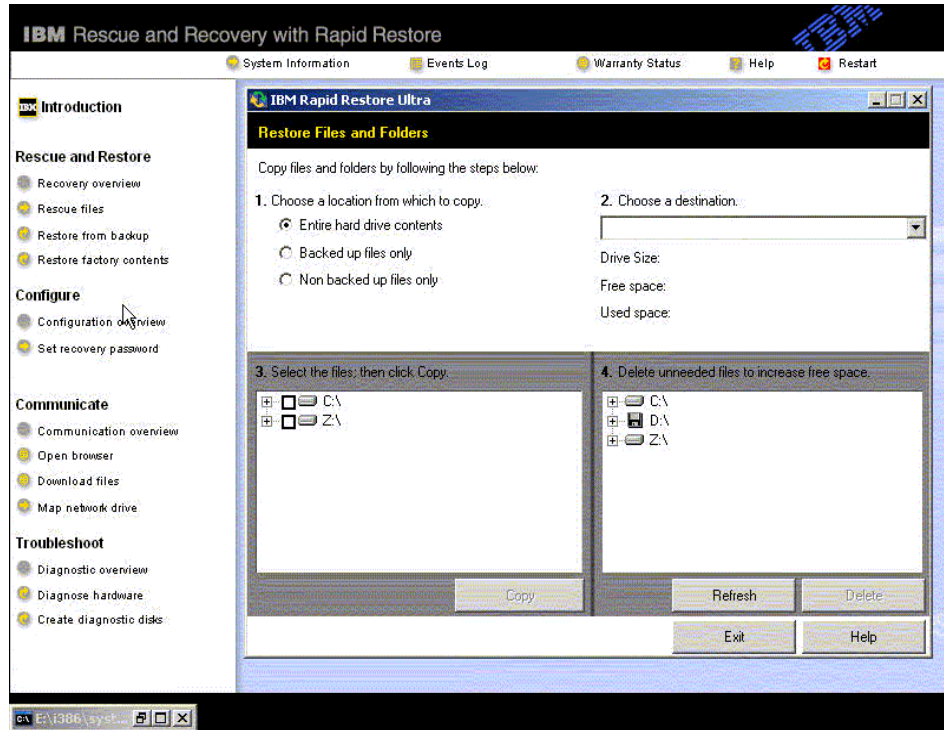


Figure 2-36 Restore Files and Folders window

Restore from backup

This option restores the hard disk to a previously stored state that you created through a Rescue and Recovery backup operation. Rescue and Recovery backup operations are performed in the Windows environment only. See 2.3.3, “Backing up your system” on page 45.

To Restore from backup:

1. Click **Restore from Backup**. You will be presented with the Restore from Backup dialog box such as the one pictured in Figure 2-37 on page 64.

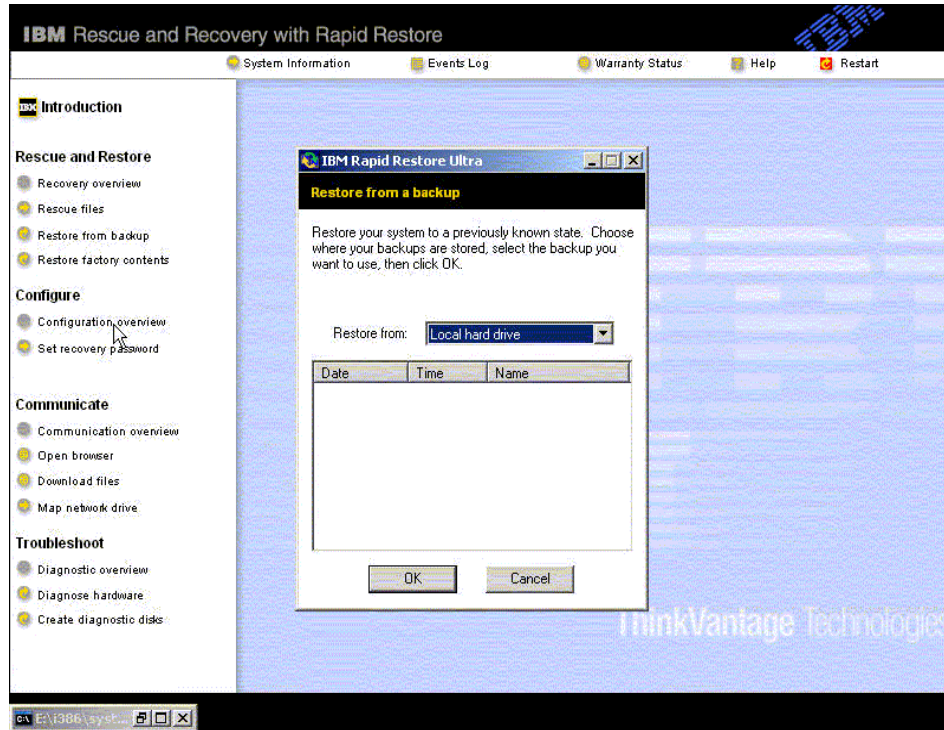


Figure 2-37 Rescue and Recovery Restore from a backup window

2. Select the source device you want to use to restore your files. If you want to restore from a network resource, map a network drive first. See “Map network drive” on page 68.

Note: Detachable devices (such as USB hard disks) must be connected before you start the Rescue and Recovery workspace.

The available backups with date stamp on the chosen device will display as shown in Figure 2-37.

3. Choose the backup you want to restore to and click **OK**.

A window similar to the one shown in Figure 2-38 on page 65 will open.

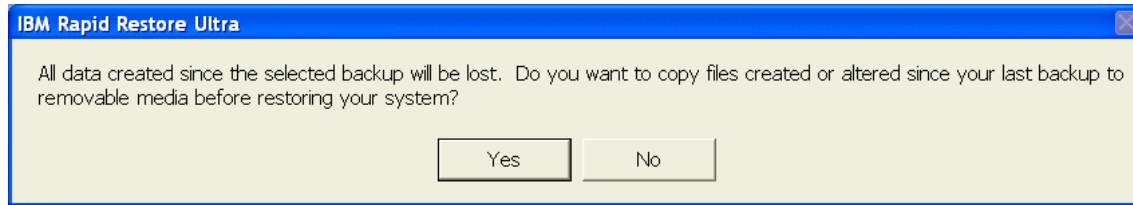


Figure 2-38 Files not backed up

- a. Choose **Yes** and the window shown in Figure 2-36 on page 63 will open. Follow the procedure for restoring single files and folders as described in “Restoring individual files and folders” on page 73.
- b. Choose **No** and you will start the restore process immediately.

Restore factory contents

If you select **Restore factory contents** from the toolbar, a window prompting you to remove all diskettes and CD media opens. Click **OK** to reboot your system. The system will reboot in the IBM Recovery program.

Note: This feature is only available if you have an IBM system with a factory preload or a system with a service partition that includes all the system data.

Restoring factory contents will reformat the primary partition of your hard disk and then reinstall your operating system, device drivers, and factory installed software. The hard disk is restored to the same state as it was when the computer was originally manufactured.

Configure

The Configure category on the Rescue and Recovery toolbar has the following selections:

- ▶ Configuration overview

When you click **Configuration Overview**, you access the Recovery environment help topics that pertain to configuration.

- ▶ Set recovery password

The Set recovery password function sets up a password for accessing the Rescue and Recovery environment.

Note: Rescue and Recovery and the Rescue and Recovery environment use the same password. When a backup is password protected through the IBM Rescue and Recovery interface, it becomes necessary to provide this password to access the Rescue and Recovery environment. Likewise, if a password is set for the IBM Rescue and Recovery environment, that same password is required to restore a backup using Rescue and Recovery. Password protection is disabled by default.

To set the recovery password, follow the procedure below:

- a. Click **Set recovery password**. The Rescue and Recovery set password window will open.
- b. Type your new password in the New password field. Passwords are case sensitive. You can use letters, numbers, and the following symbols:
- c. ‘~!@#\$%&*()_+={ } [] \ : “; ’ ./
- d. Type your new password again in the Confirm new password field.
- e. In the Hint field, type a phrase associated with the password in case you forgot the password and need something to remind you. You can leave this field blank.
- f. Click **OK**. A confirmation message is displayed.

► **Access BIOS**

This menu option enables you to enter the BIOS setup utility so you can set up several types of passwords, enable and disable hardware features, and modify settings associated with certain hardware features.

To access the BIOS setup utility, select **Access BIOS** from the toolbar. Click **OK** in the next window. The system will reboot into the BIOS setup utility.

Note: For legacy systems that did not come with Rescue and Recovery preinstalled, make sure the system is at the latest BIOS level. Otherwise, this option might not be available.

Communicate

The Rescue and Recovery workspace gives you the ability to communicate over the network, even if a software or driver problem prevents you from doing so in the Windows environment.

Note: Communicating over the network requires a wired Ethernet connection. Wireless and dial-up connections are not supported.

The following selections are available from the Communications menu:

- Communication overview

If you select **Communication overview**, you will be presented with the related help topics in the Rescue and Recovery environment.

- Open browser

You can use the browser to set up and use a Web-based e-mail account or access information about the Internet or intranet that might be critical to your business. You can also access Web pages that are bookmarked as favorites in the Windows environment from here.

To use the browser, click **Open Browser** in the Rescue and Recovery menu to access an IBM Web page like the one illustrated in Figure 2-39.

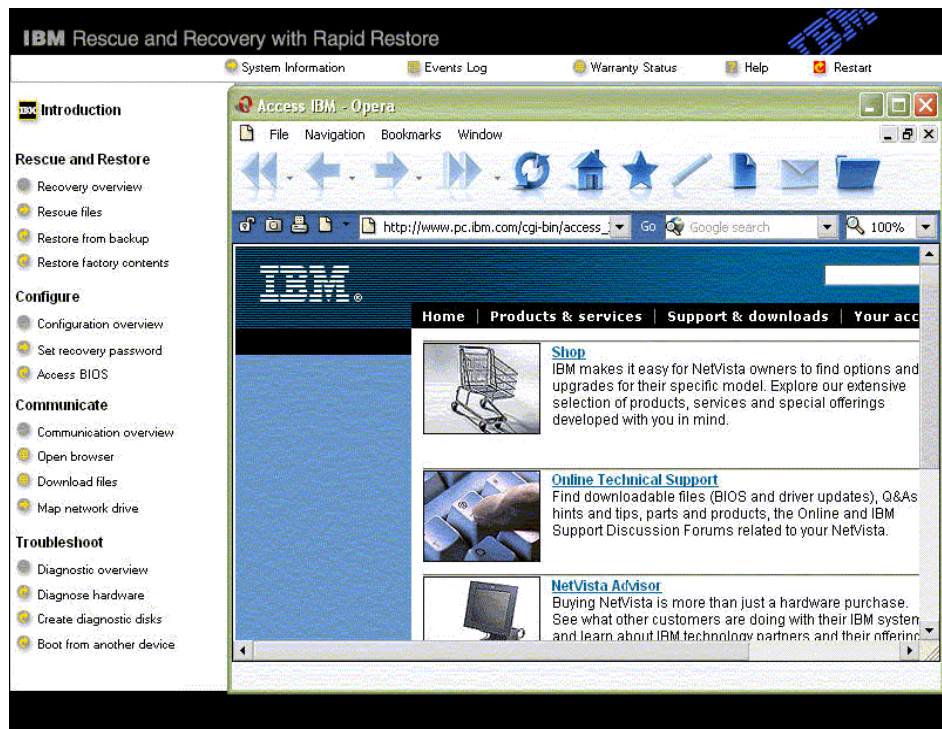


Figure 2-39 Open browser window

- Download Files

If you need an updated or replacement file (such as a device driver) to correct a problem, the Rescue and Recovery workspace provides a direct link to an IBM Web page designed specifically for your computer.

To access this Webpage, click **Download files** in the Rescue and Recovery menu. You will be directed to the multiple file download site of IBM in the Opera browser as shown in Figure 2-40.

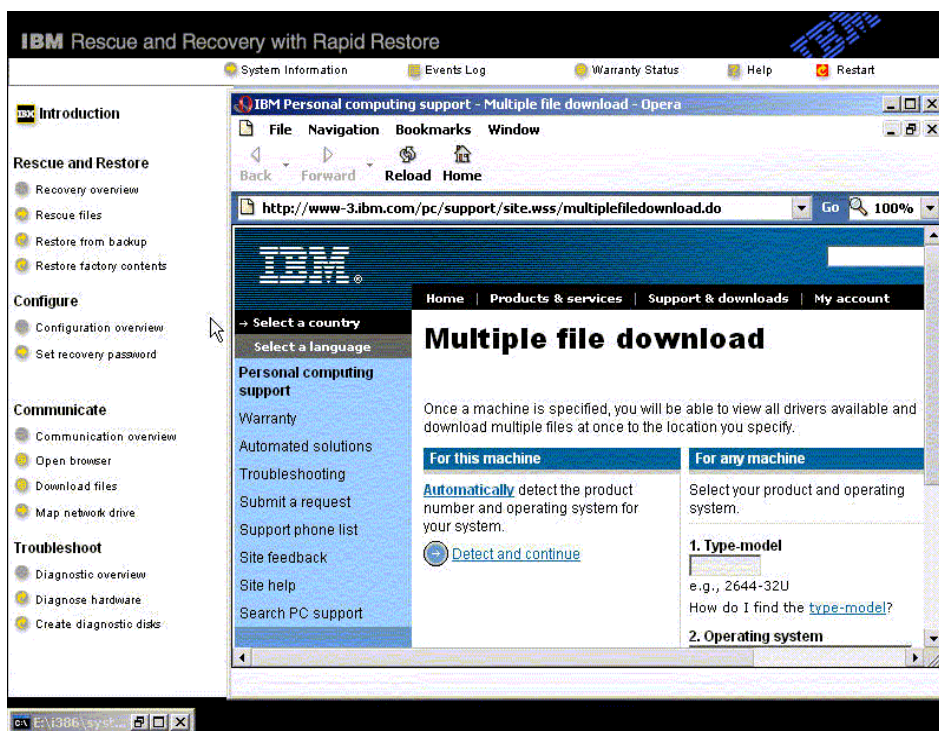


Figure 2-40 Rescue and Recovery download file window

Note: Files are automatically downloaded to the C:\IBMSHARE folder.

► Map network drive

This function enables you to map network drives to use for accessing or saving files. To map a network drive proceed as follows:

- a. Click **Map net work drive** in the Rescue and Recovery menu. You will be presented with a prompt like the one shown in Figure 2-41 on page 69.

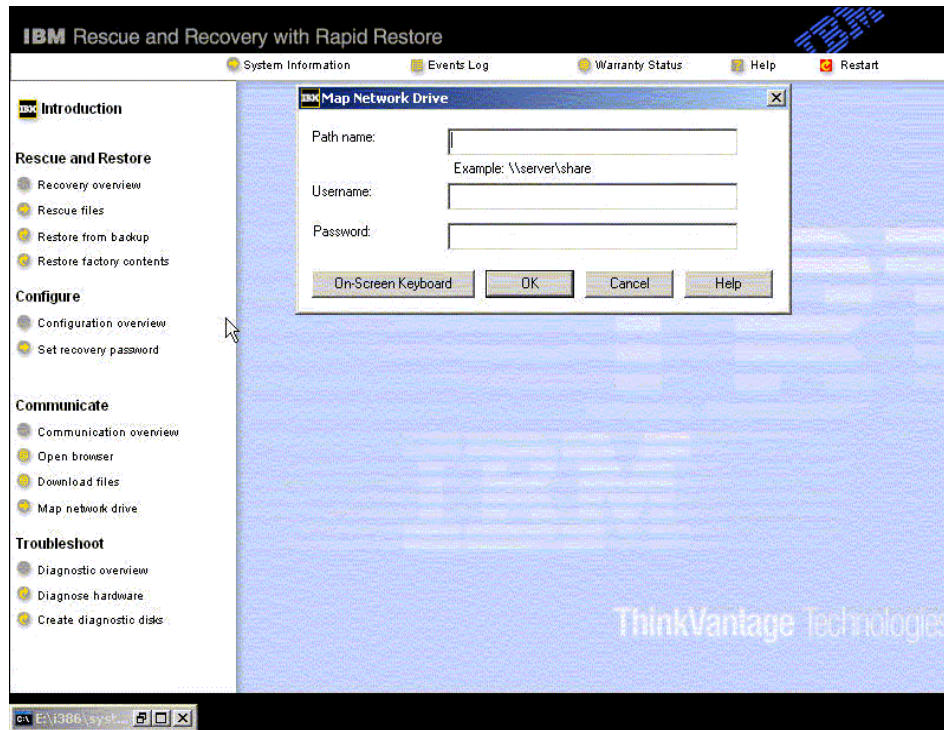


Figure 2-41 Rescue and Recovery map network drive window

- b. Enter the server name and share (for example, \\server\share).
- c. Enter your user name and password, and click **OK**.
- d. You will see a dialog box that states that \\server\share is mapped to drive :x (or whatever the drive letter is).

Note: You can only access the mapped network drive through the Rescue Files menu option. See “Rescue files” on page 62. Files copied onto the network resource, cannot be pulled back unless a backup on the mapped network drive is available.

Troubleshoot

The following selections are available from the Troubleshoot menu:

► Diagnostic overview

If you select **Diagnostic overview**, you will access the Rescue and Recovery diagnostics help topics.

► Diagnose hardware

The Diagnose hardware enables you to run diagnostic routines against a single device, multiple devices or the complete computer. These diagnostic routines test the hardware only; they do not check the software configuration settings associated with the Windows operating system or application programs installed in the Windows environment.

To diagnose hardware:

- a. Click **Diagnose hardware** in the Rescue and Recovery menu. You will be prompted to restart your system.
- b. Click **OK**.
- c. Click **Restart** on the Rescue and Recovery toolbar.

Your system will reboot and start PC-Doctor, an application that allows you to perform system diagnostics. Consult the PC-Doctor Help files for more information.

Note: If you suspect a software problem, and you are able to access the Windows environment, you should run a diagnostic program designed to be run in the Windows environment such as PC-Doctor for Windows. This program is preinstalled on many IBM computers.

Create diagnostic disks

This function lets you create a set of diagnostic diskettes containing the PC-Doctor for DOS program. The first diskette of the set will be bootable. You can then boot your computer with these diskettes to start the diagnostics program.

To create diagnostic disks:

1. Select **Create Diagnostic disks** from the Rescue and Recovery menu. You will be prompted to restart your system.
2. Click **OK**.
3. Click **Restart** on the Rescue and Recovery toolbar.
4. Use the instruction that follow to create the diskettes.

2.4.4 Restoring your system from Windows

You can use Rescue and Recovery to restore your system or to restore individual files or folders. Performing a system-restore operation restores the contents of your hard disk to a previously saved state. This includes the operating system, software applications, registry settings, network settings, fix packs, desktop settings, and data files.

Rescue and Recovery program enables you to restore files to any number of backup states. Each backup is differentiated by its creation time and date, also by a unique backup name that you create. IBM Rescue and Recovery can restore your system from a complete backup or individual files stored in any of the following locations: the local hard drive, CD-R drive, DVD drive, USB hard drive, or a network drive.

Restoring from a full system backup

Before beginning the restore process, make sure that the backup media containing your backup is attached or the network drive is mapped. Then, take the following steps:

1. From the IBM Rescue and Recovery interface, select **Restore your system** from the menu as shown in Figure 2-42.

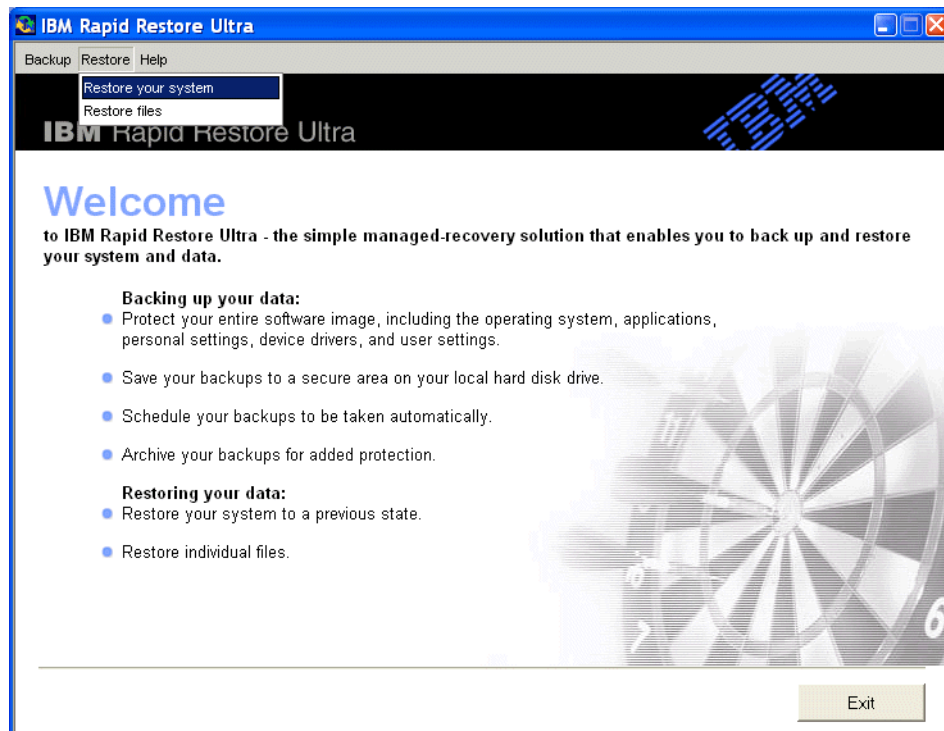


Figure 2-42 Choose *Restore your system* from the main window

2. Click the radio button for the source location of the backup you wish to restore. The backups stored on the selected drive will be displayed as shown in Figure 2-43.

If the system is not able to find a backup in the specified location, a prompt asks you to select a new location. If this occurs, you should select the connection to the specified device.

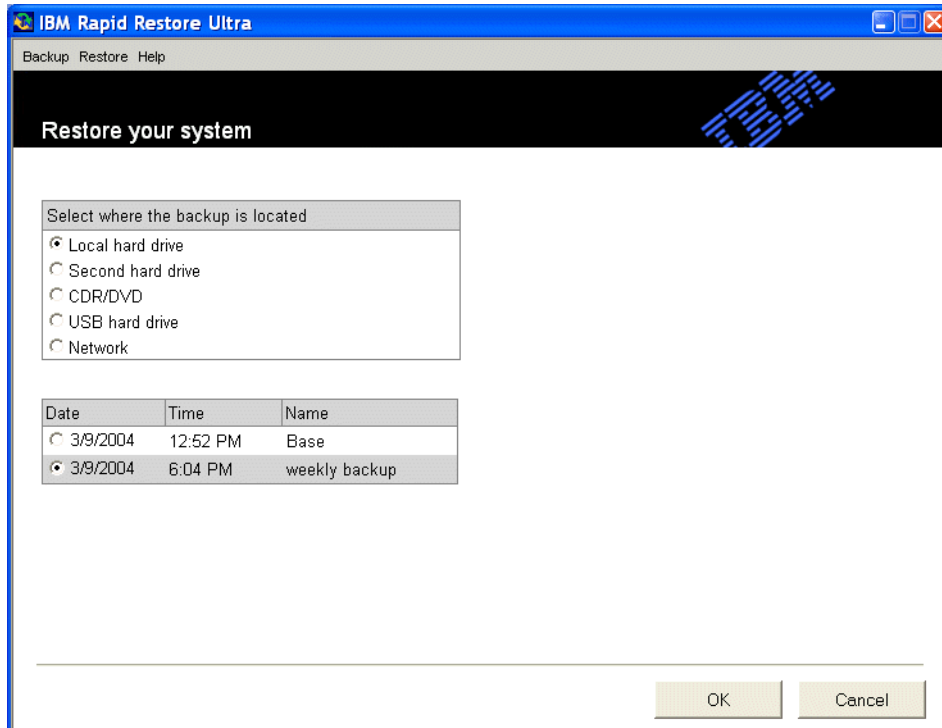


Figure 2-43 Restore source location selections

3. Click the radio button for the specific backup you want to use.

Tip: Selecting your latest stored backup for system recovery is the best choice because the newest incremental backup will install the base image and all previous backups.

4. Click **OK** to continue.

5. The window shown in Figure 2-44 opens. You now have the option of backing up files created since the last iterative backup. Selecting **Yes** will display the Restore Files and Folder window shown in Figure 2-47 on page 75. Proceed as described in “Restoring individual files and folders” on page 73. Otherwise click **No** to restore your system.

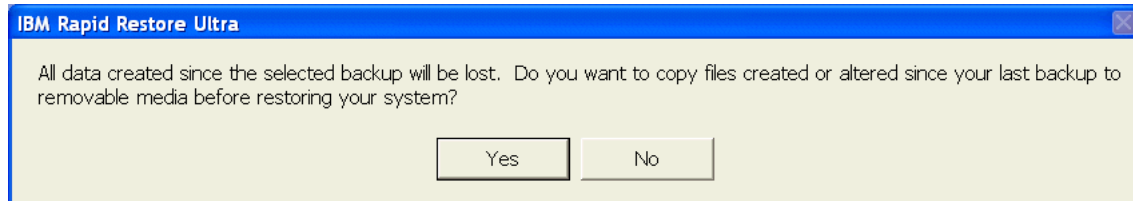


Figure 2-44 Saving files that have not been backed up

The message shown in Figure 2-45 displays, advising you that all data created since the selected backup will be lost.

6. Click **OK** to restore your system.

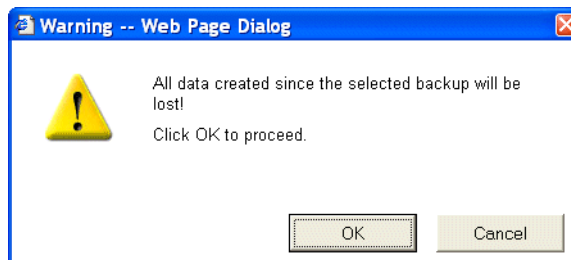


Figure 2-45 Data overwrite warning window

Restoring individual files and folders

The Restore Files and Folders window enables you to copy files and folders from your stored Rescue and Recovery backup to your local hard drive and to the following types of external media:

- ▶ Diskette (through an integrated diskette drive or USB diskette drive)
- ▶ USB hard disk drive
- ▶ USB key
- ▶ A network drive

To restore one or more individual files, complete the following procedure:

1. From the IBM Rescue and Recovery interface, click **Restore** and select **Restore files**. See Figure 2-46.

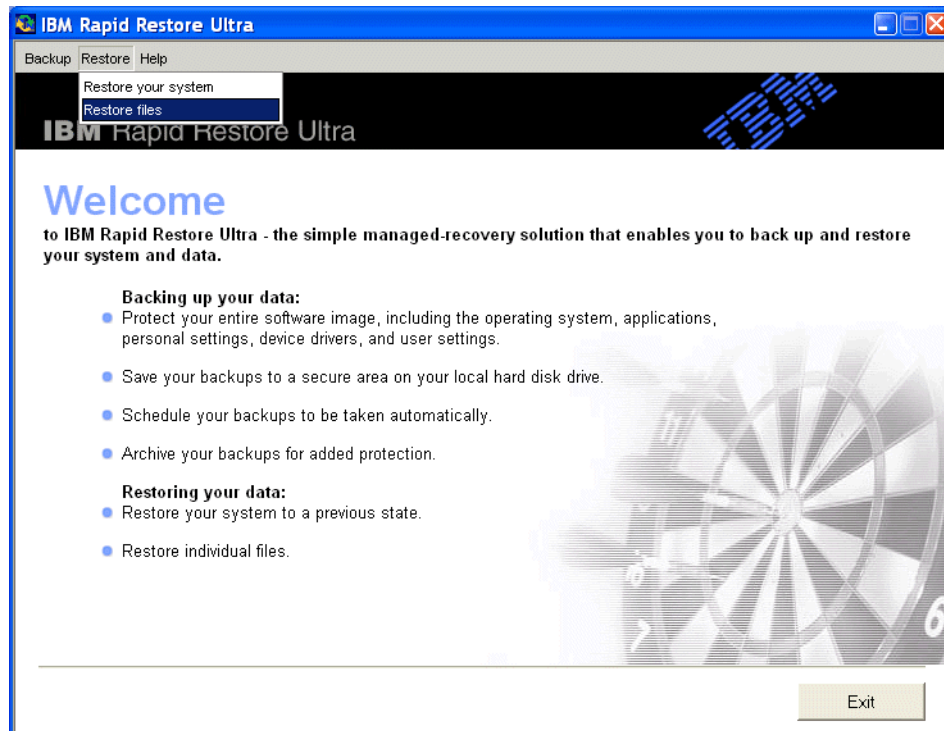


Figure 2-46 Restore files window

2. Choose the location for the files to be copied (see Figure 2-47 on page 75):
 - Entire hard drive contents
This selection enables you to browse the hard disk drive to find the file, or files, that you want to rescue.
 - Backed up files only
With this selection, you can browse and rescue only files that were backed up using the IBM Rescue and Recovery program.
 - Non-backed up files only
This selection allows you to browse and rescue only those files on your hard disk that were created or changed since the last time a backup operation was performed by Rescue and Recovery.

– My Recent Documents only

This selection is available only if you choose to view non-backed up files. It enables you to limit your non-backed-up files view to show only recent documents saved in your Windows environment. Use the drop-down menu to select the appropriate user account that contains the recent documents you want to rescue.

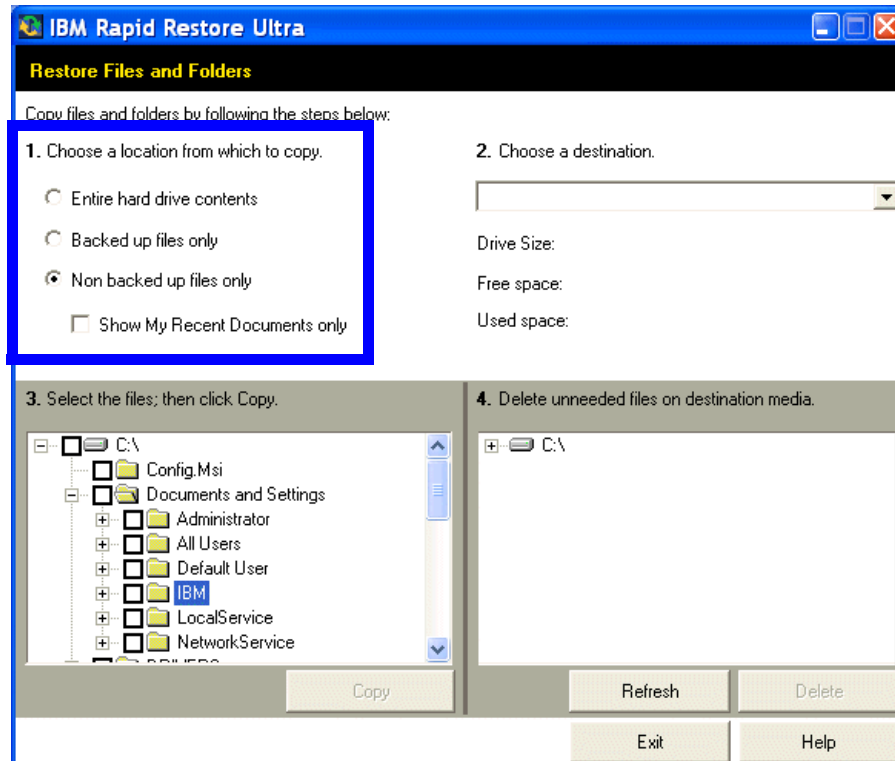


Figure 2-47 Restore files and folders window

- From the drop-down menu, choose the drive destination that you wish the files to be restored to (see Figure 2-48). This can be your C drive, original location, or any attached device or network location. The amount of free and used space for the selected medium is displayed.

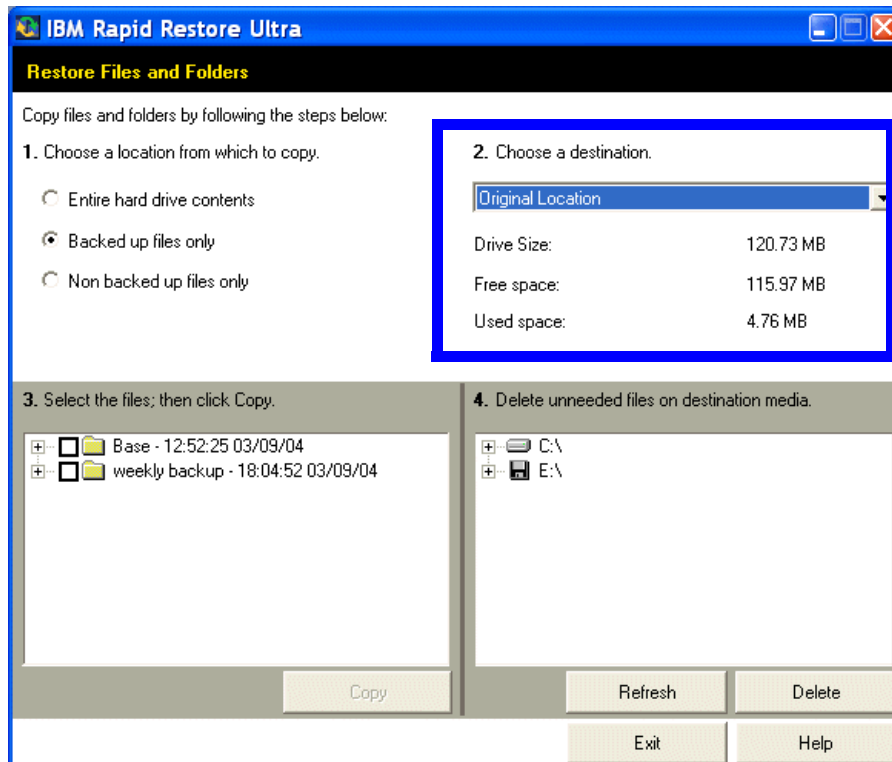


Figure 2-48 Destination window

Important: Only mapped network drives are displayed in the provided interface. If you want to use a network drive, you must map the drive before continuing with the procedure. After mapping a network drive, you might need to click the **Refresh** button before the drive is displayed in the interface.

4. Select the files you want to restore in box 3. Select files by expanding the file menu (by clicking the + sign) and selecting each file or folder you wish to rescue. See Figure 2-49.

Marking a folder or drive letter will result in restoring all files and folders contained within that directory structure. As each is marked, the amount of free and used space shown for the destination medium is updated.

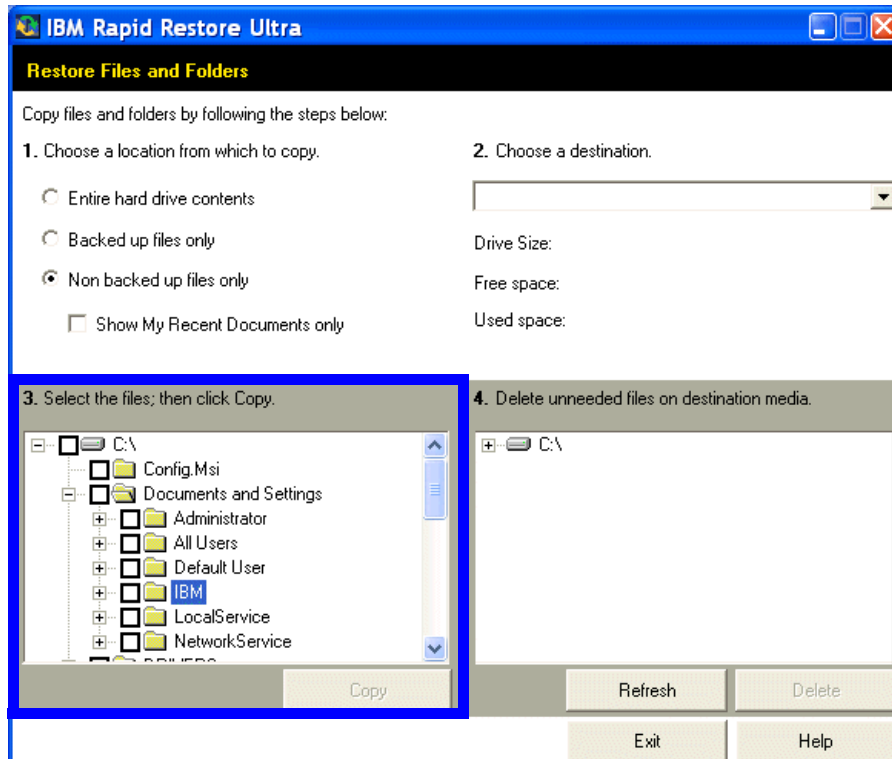


Figure 2-49 Select files window

5. Click **Copy** and then **OK**. The file transfer begins.

A message may display that the file or directory already exists on the destination.

6. Click **Yes** if you wish to overwrite the existing file or **No** if you do not.

7. If Rescue and Recovery determines that there is not enough space on your destination medium to copy the files you want to restore, a message is displayed indicating that there is insufficient space on the destination drive. To delete unneeded files from the destination medium, expand the file menu under Delete unneeded files to increase the free space and mark the check box next to each item you want to delete. Then, click **Delete**.
8. When you have cleared sufficient space, click **Copy** to start the file transfer process again.

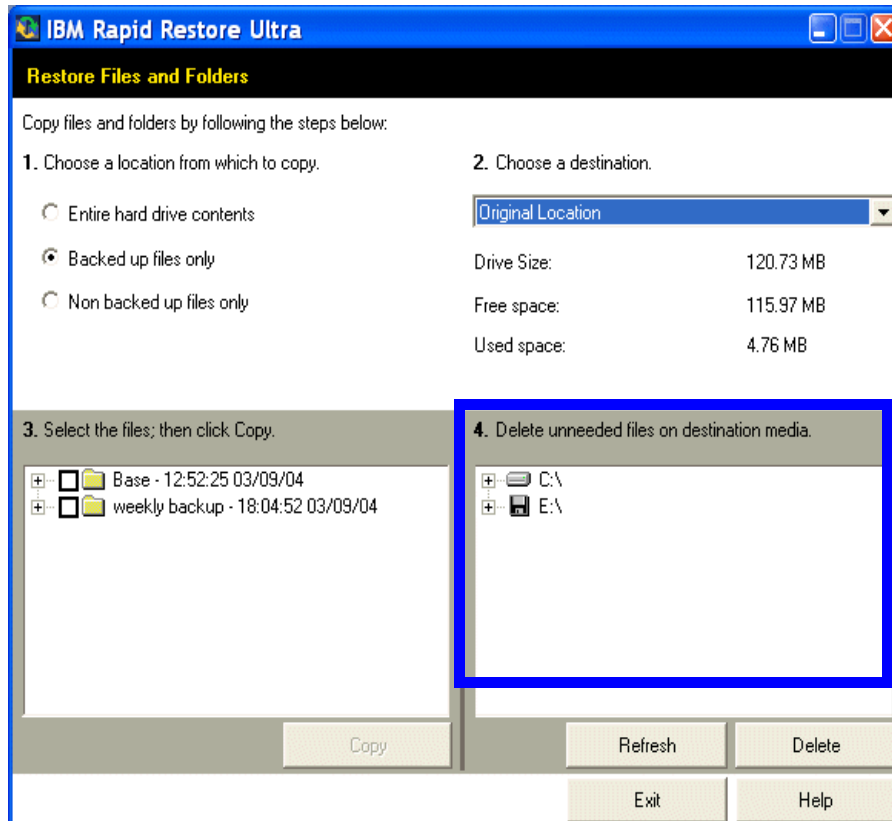


Figure 2-50 Delete unneeded files window

9. When the file transfer process is complete, click **OK**. Then, click **Exit** to close the window.

2.4.5 Restore considerations

When you are performing a restore operation, take the following considerations into account:

- ▶ All data created since the selected backup will be erased from your computer.
- ▶ If your system is not connected to an AC power supply when you initiate a backup, restore, or archive procedure, you may experience data loss or an irretrievable system failure.

2.5 Troubleshooting

This section focuses on the Rescue and Recovery troubleshooting features.

2.5.1 Installation troubleshooting

The following information might be helpful if you encounter trouble while attempting to install or uninstall the IBM Rescue and Recovery software.

Unable to install Rescue and Recovery

Rescue and Recovery cannot be reinstalled over certain previous versions. The earlier version must be uninstalled prior to installing the newer version. Rescue and Recovery must be installed on the C drive.

Uninstalling the software

To uninstall Rescue and Recovery from a computer with Windows 2000 Professional or Windows XP, you must have administrator rights. For more information about user accounts, see the help system provided with the operating system. When a non-administrator tries to uninstall Rescue and Recovery, an error message will appear indicating that Rescue and Recovery files are corrupt, although no files are actually corrupt. If an administrator uninstalls Rescue and Recovery, this message will not be displayed and Rescue and Recovery will uninstall correctly.

2.5.2 Backup and Restore troubleshooting information

The following information is helpful if you encounter trouble while attempting a backup operation using Rescue and Recovery software.

- ▶ You can only backup files to mapped network drives. If you want to use a network drive, you can map the drive during the backup procedure. After mapping a network drive, you might need to click the **Refresh** button before the drive is displayed in the provided interface.

- ▶ User accounts are included in backup and restore operations. Therefore, if you restore your system to a time when a user did not exist or had a different password, that user will not be able to log in.
- ▶ If the Rescue and Recovery interface is closed while performing a Windows incremental backup, Rescue and Recovery will continue to back up files in the background.

Backup operation is slow

Backup performance depends upon the size and type of operation being performed. Backup operation performance can be optimized by performing frequent backups. Running another program, such as an anti-virus program, while creating a backup image will adversely affect backup performance. Do not run any programs while creating a backup image. Run anti-virus programs before or after performing a backup operation.

Scheduling dates on the 29th, 30th, or 31st

Rescue and Recovery does not allow you to specify a scheduled backup on the 29th, 30th, or 31st day of the month. However, you can schedule a backup for the end of the month.

Unable to select the Copy backups from hard drive function

If the Copy backups from hard drive option is not available, the user does not have an external device attached to the computer. Attach a CD, DVD, or USB hard drive to the computer and try again. To restore a backup set from a CD, DVD or USB drive, the appropriate drive must be a supported boot option for the computer you are restoring. In order to perform a CD-R archive, the hard drive must have at least 700MB of free space.

User cannot log on after a restore operation

This problem will occur on multiuser systems when a new user is added and a backup operation takes place before the new user logs on for the first time. To remedy this problem, the IT administrator must add the new user again and either restart the computer, or have the new user log on before the next backup operation. To prevent this problem, restart the computer after adding a new user or ensure that the new user logs on before the next incremental backup is taken.

Power management

The following actions might occur when restoring Rescue and Recovery under various power management conditions such as standby, hibernate, and power loss. They are not cause for alarm.

- ▶ When a Microsoft Windows backup or CD-R Archive is in progress and the system requests to enter standby or hibernate, Rescue and Recovery stops

the backup in progress and allows the power request to proceed. When Windows resumes, it will record the backup as failed and query the user to run it again.

- ▶ When a Microsoft Windows restore is in progress, the power request could be rejected, but the restore could continue.
- ▶ When a Rescue and Recovery environment backup is in progress, the power request could occur, and the user would have to reinitiate the backup.
- ▶ When a Rescue and Recovery environment restore is in progress, the power request could occur, and the user would have to initiate a new IBM Rescue and Recovery environment restore to return the machine to a stable configuration.

2.5.3 Encryption troubleshooting

Rescue and Recovery will back up both Windows EFS and IBM Client Security Software FFE files in their encrypted form. If you use FFE, you should ensure that the database that FFE uses to keep track of what folders are protected by FFE also has an .NSF extension.

To ensure that these files are always backed up, you should include the entry `c:\Program Files\IBM\Security*flt.nsf` in the `ibmincl` file. This ensures that the database file for FFE is backed up. Loss of this file will prevent access to the FFE-protected files and folders.

Restoring from a backup that contains encrypted files

If you restore operations from a base or incremental backup, both EFS-encrypted and FFE-encrypted files will successfully be restored. The encrypted files introduce no limitations to a full restore operation.

Restoring individual encrypted files and folders from a backup

Single file restores of encrypted files (FFE and EFS) do have some limitations in the Rescue and Recovery environment.

Table 2-3 summarizes which encrypted files can best be restored using Single File Restore in each environment.

Table 2-3 Single file restore support

	Rescue and Recovery in a Windows environment	Rescue and Recovery in a Rescue and Recovery Environment
Restore FFE?	No	Yes
Restore EFS?	Yes (logged on user only)	No

Rescue and Recovery enables users to restore individual, encrypted files and folders from a backup with the following limitations:

- ▶ Windows EFS files

Individual files encrypted by Windows EFS can only be restored using Rescue and Recovery from the Windows operating system. These files cannot be restored using Rescue and Recovery from the Rescue and Recovery preboot environment.

- ▶ IBM FFE-encrypted files

Individual files encrypted by IBM FFE can only be restored using Rescue and Recovery from the IBM Rescue and Recovery preboot environment. Furthermore, these files must be restored to their original location to be successfully restored.

Rescuing encrypted files that are not in a backup

Support for rescuing or copying encrypted files that are not in a backup is as follows:

- ▶ From within the Windows operating system, users can copy encrypted files that are not in a backup from within the Windows operating system as follows:

- Windows EFS-encrypted files

Individual files encrypted by Windows EFS can only be rescued using the Windows Explorer utility. Use Windows Explorer to copy the encrypted files to removable media before initiating the restore process.

- IBM FFE-encrypted files

IBM FFE-encrypted files that are not in a backup cannot be rescued or copied from within the Windows operating system.

- ▶ From within the IBM Rescue and Recovery environment, individual encrypted files cannot be rescued or copied from within the IBM Rescue and Recovery preboot environment.

Note: Full hard disk encryption programs generally do not work with Rescue and Recovery because they require a master boot record program in order to operate.

2.5.4 General troubleshooting and tips

Table 2-4 provides solutions for general troubleshooting problems and tips to help with troubleshooting.

Table 2-4 General troubleshooting and tips

Symptoms	Solution
MBR corruption system cannot boot into rescue environment.	A the time of this publication, the following procedure was correct: Create bootable rescue media according to the steps explained on the following Web site: http://www-306.ibm.com/pc/support/site.wss/document.do?lnocid=MIGR-54498 Or recover from backups to CD-R, CD-RW or DVD media.
Failed motherboard requires a replace (and you are using UUID protection).	As soon as you complete the motherboard replacement, perform a backup. This will capture the new UUID and propagate it to the original backup.
Cannot run IBM Rescue and Recovery using wireless and dial-up connectivity.	There is no wireless or dial-up capability from the IBM Rescue and Recovery workspace. Only wired Ethernet is supported.
Pointing device functions	All pointing devices will operate as two-button devices within the IBM Rescue and Recovery workspace.
Attempting to recover a system using DVD-RAM disks, without success	The IBM Rescue and Recovery workspace does not support booting from a DVD-RAM disk as an external device. As a result, do not create rescue media, product recovery CDs, backups, or archive backups using DVD-RAM media if you intend to boot from an external device. Other DVD formats are supported.

Symptoms	Solution
Error messages display during file restoration while the IBM Rescue and Recovery help system is open	If you have both the IBM Rescue and Recovery program and its help system open while attempting to perform a Backup Now, the program will close and you will receive an error message. Despite this message, the backup operation is underway. Simply close the error message. To check on the progress of your backup, reopen the Rescue and Recovery program and the progress will be indicated.
Error message Not Responding displays when backing up large files	Ignore the message. The file transfer operation is still underway and can be verified by the progress bar indicated on the window where the file transfer operation was started.
Drives and drive letters are not the same as in the Windows environment.	When you are transferring files, the drive letters used for the location and destination directories might not represent drive letters typically used in your Windows environment. One way of locating the drive that is known as your C drive is to expand each directory and look for folders commonly associated with the C drive such as the My Programs folder or a the Documents and Settings folder.
Computer with Windows 2000 operating system will not boot while attempting to access IBM Rescue and Recovery workspace.	If you install Windows 2000, and there is a USB memory key attached to the computer at the time of installation, then a TXTSETUP.SIF is inserted in the C drive root directory. If you attempt to enter the IBM Rescue and Recovery workspace with the TXTSETUP.SIF in the C drive root directory, your computer will not boot into the Rescue and Recovery workspace successfully. To prevent this problem, either detach the USB memory key before installing Windows 2000 or delete or rename the TXTSETUP.SIF file in the C root directory before entering the Rescue and Recovery environment.

Symptoms	Solution
Screen flashes when IBM Rescue and Recovery opens.	Depending on the video card installed on your computer, there might be a series of flashes when the IBM Rescue and Recovery workspace is opened
Low video resolution affects access to and performance of the IBM Rescue and Recovery environment.	The video RAM that came with your computer is typically set to store a default capacity of 8MB. Having a video RAM lower than 8MB might adversely affect performance of the IBM Rescue and Recovery program. If video RAM is set to less than 2MB the Rescue and Recovery pre-desktop area will not be displayed correctly. Change video settings in BIOS.
Startup-interrupt prompt does not display.	If you do not see the startup-interrupt prompt during startup, it might be that the prompt displayed too quickly. If this occurs and you want to interrupt the startup process and access the Rescue and Recovery environment, press and hold the Enter key and then turn on the computer. Release the Enter key when the Rescue and Recovery environment opens.
Norton Antivirus 2002 and 2003 cannot complete a virus scan on a system with IBM Rescue and Recovery installed.	Symantec is providing IBM customers with a free upgrade to Norton Antivirus 2004 due to a defect that was found in Norton Antivirus 2002 and 2003 after customers downloaded and installed Rescue and Recovery.
During creation of the recovery media and manually restarting the system, the IBM Service partition shows in Windows Explorer after restart. This can occur after aborting, or rebooting during the creation of the recovery media. Do not attempt to remove this hard disk drive letter.	Recreate the recovery media and allow the process to complete.
The Windows start menu key will not perform a function under the IBM Rescue and Recovery environment.	The IBM Rescue and Recovery environment does not support all on-screen keyboard functions. Rescue and Recovery is working as designed.

Symptoms	Solution
A non-alphanumeric character such as an empty space or hyphen does not work in the IBM Rescue and Recovery environment.	Some non-alphanumeric characters are not recommended in IBM Rescue and Recovery. Rescue and Recovery is working as designed.
Another computer backup was overwritten when using Rescue and Recovery to backup to a network drive.	<p>The Rescue and Recovery network backup feature uses a Microsoft network share to store its backups. If another computer uses the same network share, it will overwrite the existing backup. Therefore, a network share must be established prior to a backup operation. This can be managed several ways:</p> <ol style="list-style-type: none"> 1. Use a single network share, and create multiple folders, where each user uses the same User ID with a unique folder as the backup destination. 2. Create multiple network shares, with a unique User ID per share (so folders are unique.)
The Rescue and Recovery Windows user interface shows backups that have been manually deleted.	This can occur when backups stored on a USB hard disk drive or network are deleted with Windows Explorer and a subsequent backup (or copy backups) recreates the deleted files. Also, it is possible that there are backups on other media that are not displayed, but are actually valid. Booting to the Rescue and Recovery environment will display these. Rescue and Recovery is working as designed.
The system's restore points are not saved in Rescue and Recovery's backup.	When restoring using Rescue and Recovery, System Restore will log an error message in the Windows Event Viewer. If you start System Restore, any prior System Restore Points will not be available. If you must restore to an earlier point in time, use Rescue and Recovery to restore to that time, and then use Rescue Files and Folders for any additional data.

Symptoms	Solution
During a restore to a hard disk drive greater than 32 GB, a FAT32 partition is converted to NTFS.	<p>This may be caused by a limited user that has not been configured correctly. To reset the NTFS attributes to those specified please follow these steps:</p> <ol style="list-style-type: none"> 1. Logon as Administrator and click Start. Select Run. 2. Type <code>cac!s c:*.* /T /E /C /G Everyone:F</code> and press the Enter key. <p>Another cause for this could be that Microsoft Installer deleted the install package too soon, and the product was removed. To resolve this, Run Rescue and Recovery and use Rescue Files and Folders to restore the c:\Windows\installer folder. Then run uninstall again.</p>
The IBM Rescue and Recovery Environment has limited multitasking capabilities.	<p>IBM Rescue and Recovery is not intended to be a productivity environment, but a rescue environment. For example, if you run Restore System and Rescue Files and Folders concurrently, your system may hang up. Reboot to the IBM Rescue and Recovery environment and run only the desired application.</p>
Rescue and Recovery fails to restore your computer.	<p>This may be caused by one of the following reasons:</p> <ul style="list-style-type: none"> ► You have replaced your hard disk drive with a smaller hard disk drive and all the data cannot be restored. In this case, you should either obtain a larger hard disk drive or use the Rescue Files and Folders to restore selected data from the backup. ► If you are restoring from CD or DVD, the media may be damaged. Use a different backup (if available) to restore your computer or recover the ThinkPad system from the factory image. ► You may have exceeded the available memory capacity. In this case, reboot. Do not open other applications and restart the restore process.

Symptoms	Solution
In some Rescue and Recovery environments, the dialog box may not appear after processing a request.	Press the Alt and Tab keys at the same time to bring any dialog boxes to the foreground.
Some Rescue and Recovery features will not function.	Rescue and Recovery checks to see if prior versions are installed. However, if Rescue and Recovery is installed, it will not prevent installation of prior versions of Rapid Restore. If a prior version of Rapid Restore is installed, some functions may not function properly. In this case, uninstall prior versions of Rapid Restore and Rescue and Recovery. Then reinstall IBM Rescue and Recovery

2.5.5 Frequently asked questions

Table 2-5 provides frequently asked questions (FAQs) about Rescue and Recovery and their answers.

Table 2-5 FAQ

Question	Answer
Why should I upgrade to Rescue and Recovery?	Rescue and Recovery offers not only many improved features and performance, but it is also easier to deploy and install. It offers more customization options, works on non-IBM machines, and enables large enterprise IT departments to extend its recovery and support environment to avoid help desk calls and desk-side visits.
Will I be able to install over RRU 3.01?	No, an uninstall of RRU will be required. This takes approximately 20 minutes for most users.
Will I be able to preserve my backups from RRU 3.01?	No. The backups will be lost in the uninstall. However, if you run a backup immediately after install, you should have full protection and can do file and folder restore from the new base backup. Concerned users should create a set of Rescue and Recovery archive CDs.

Question	Answer
Will my existing command-prompt scripts work with Rescue and Recovery?	No. New scripts and customizations are required due to an entirely new core system install.
If I have the Access IBM pre-desktop (also known as PARTIES, the current pre-OS), will Rescue and Recovery work?	Yes, the existing tools such as BIOS setup will be available, and the Access IBM pre-desktop will be replaced by IBM Rescue and Recovery.
Will RRU 3.01 still be available?	Yes, it is available on the Web for legacy and new systems. Ongoing future support for new systems is still to be determined.
If I have purchased Rapid Restore for non-IBM systems previously, will I be entitled to the new version?	No, a new license for the software must be purchased. This can be handled via the standard bid process.
Are legacy IBM systems entitled to IBM Rescue and Recovery?	Yes. See the IBM Web site for supported systems: http://www.ibm.com/pc/support/site.wss/MIGR-4Q2QAK.html%20



IBM System Information Center

IBM System Information Center is a Java server application designed to meet the asset inventory and management needs of the small and medium-sized business (SMB). Inventory collection and management are two of the basic areas for lowering PC life cycle costs. System Information Center is a new IBM ThinkVantage Technology that provides a cost and resource-effective inventory management solution. The ThinkVantage Technology products have proven to help businesses lower Total Cost of Ownership (TCO). System Information Center complements and leverages an investment in ThinkVantage Technologies.

In this chapter, we describe the purpose of System Information Center and explain how to install and use it. The following topics are covered:

- ▶ Introduction to System Information Center
- ▶ System Information Center server installation considerations and details
- ▶ How to use System Information Center
- ▶ Scenarios and best practices
- ▶ Customization and advanced usage

3.1 Introduction to System Information Center

System Information Center is a small and flexible inventory management tool that gathers inventory information from a client system. It sends this information to the System Information Center database, where it is stored. The information in the database can then be accessed with a Web browser.

System Information Center is designed for Small and Medium Business customers, who do not require a large enterprise inventory management solution (for example, IBM Tivoli, which typically supports 20,000-seat and greater environments). System Information Center provides a cost-effective and resource-effective inventory management solution.

System Information Center can benefit SMBs as follows:

- ▶ SMBs can use System Information Center to leverage existing server assets. For example, System Information Center can be installed on an existing Web server.
- ▶ The process of collecting asset data can be automated and scheduled. A small client application that is required to gather the information will be installed during the registration of each client on the System Information Center server.

To learn more about System Information Center in an enterprise environment, see 3.14.1, “Enterprise environment considerations” on page 216.

3.1.1 System Information Center features

System Information Center offers the following features:

- ▶ Easy browser accessibility

The System Information Center server is Web-based and can be accessed with Microsoft Internet Explorer version 6.0 or higher. This offers a familiar interface.

Administrators have a single interface for direct access of asset information. Predefined reports can be run using the Web browser on the System Information Center server. These reports can be exported as files or e-mailed.

- ▶ Minimal resource usage on client systems

The IBM System Information Gatherer program (client) is a small, non-resident, 710 KB single file executable application. It is active only when needed. When an agent is running the System Information Gatherer program, it consumes less than 4.5 MB of RAM. The agent can store the results of the

inventory scan on the client system if it is not connected to the network. The results can be delivered later to the System Information Center server.

- ▶ Control software license usage

System Information Center can be used to identify software licenses that are not used. Administrators can then uninstall the software (manually or with a corresponding tool), thereby freeing up the expensive license. License control ensures compliance with quantity licensing agreements for individual applications.

- ▶ Central management

With System Information Center, mobile computers, desktops, servers, and non-PC assets such as monitors, printers, PDAs, and so on can be centrally managed via the administrator web console (non-PC assets must be manually added to the System Information Center server).

- ▶ Single point solution

System Information Center is a single point solution for central inventory management. The System Information Center server can have its database, Web server and System Information Center application on the same physical server.

- ▶ Secure access

System Information Center can be customized to connect to a company's Lightweight Directory Access Protocol (LDAP) service. If no LDAP service exists, System Information Center Web services include user access control. There are three types of System Information users:

- Users
- Superusers
- System Information Center Administrators

- ▶ Database integration

System Information Center installs IBM Cloudscape, a 100% Java SQL database. This database provides a quick installation and integration solution for System Information Center. System Information Center can also use other SQL databases that support Java Database Connectivity (JDBC) connections, if an enterprise database is required or an existing SQL database is already available. System Information Center can utilize other SQL databases with minimal changes to the installation. See Appendix B, "Alternate SQL database for System Information Center" on page 607 for additional information and examples.

When Cloudscape is used, an SMB can migrate to an enterprise SQL database such as IBM DB2 as required in the future. System Information Center is designed to work with any standards-based SQL server that provides connectivity through JDBC.

Other SQL databases that may meet the enterprise need are:

- IBM DB2
- Oracle
- Microsoft SQL Server
- PostgreSQL

3.1.2 System Information Center components

A complete System Information Center solution has the following components:

- ▶ Microsoft Windows 2000 or 2003 Server
- ▶ SQL database with JDBC support
- ▶ Java Web server
- ▶ System Information Center
- ▶ IBM System Information Gatherer program agent

The IBM System Information Gatherer program agent supports IBM and non-IBM systems. The agent is free when used on IBM systems. For non-IBM systems, a small fee is charged. The agent reads information from the Windows Registry, Windows Management Instrumentation (WMI) and the SMBIOS of a client computer.

After collecting the data from the computer, the IBM System Information Gatherer program creates a file with all the information in it. This file can include:

- ▶ Processor type and speed
- ▶ Memory size
- ▶ PCI devices
- ▶ Logical disk information
- ▶ Operating system information
- ▶ Device drivers
- ▶ Installed software
- ▶ Regional settings

IBM System Information Gatherer is also accommodates portable computers. The collected inventory information can be stored locally. When network connectivity is restored, the inventory information will be sent to the System Information Center database.

The following client operating systems are supported by IBM System Information Gatherer agent:

- ▶ Windows 2000
- ▶ Microsoft Windows XP

Other operating systems may be supported through the customization of System Information Center provided by an IBM Global Services IT Specialist during

onsite visits. The following additional customization services are also available through IBM Global Services:

- ▶ Creation of new reports
- ▶ Customization of Web pages
- ▶ Integration with other solutions

Contact Gavin Cameron at gcameron@uk.ibm.com or Goran Wibran at wibran@us.ibm.com.

3.1.3 System Information Center requirements

System Information Center is supported on Windows 2000 Server or Windows 2003 Server. The Web browser used to access the System Information Center server must be Internet Explorer 6.0 or higher. The minimum hardware for a System Information Center server is: 120 MB of hard drive space and 1.0 GB of RAM. This is in addition to any requirements needed for Tomcat and alternative enterprise databases.

3.1.4 System Information Center overview

The System Information Center server receives the client data from the IBM System Information Gatherer agent. It then stores the information in an SQL database. System Information Center provides a user friendly Web interface for modifying and deleting data and generating reports based on the information stored in the database. These reports can be displayed in a Web browser, stored as an output file, or e-mailed.

Figure 3-1 on page 96 provides an overview of the System Information Center components.

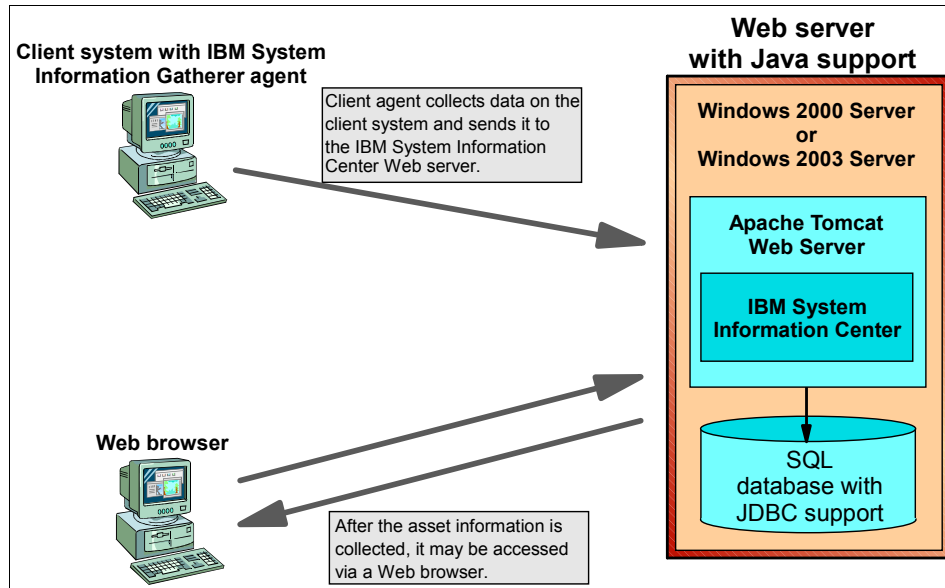


Figure 3-1 System Information Center components

3.2 System Information Center server installation

In this section, we describe how to install System Information Center and its prerequisite software.

3.2.1 Server operating system installation

The procedure for server operating system installation consists of these steps:

1. Install Microsoft Server 2000 or 2003.
2. Install Service Pack 4 for Microsoft Server 2000.
3. Ensure that the server has a static IP address.
4. Ensure that no other service or applications are using TCP/IP port 80 (for example, Microsoft Internet Information Services (IIS) should not be running).

3.2.2 Apache Tomcat Web server installation

To install Apache Tomcat Java Web server version 4.1.30:

1. Download the Web server from the following Web site:
<http://archive.apache.org/dist/jakarta/tomcat-4/v4.1.30/bin/jakarta-tomcat-4.1.30.zip>
2. Create a directory named tomcat4 in the root of the C drive.
3. Copy the jakarta-tomcat-4.1.30.zip to the tomcat4 directory.

Important: System Information Center expects the directory name to be C:\tomcat4, so do not change it.

The folder structure should look like that shown in Figure 3-2.

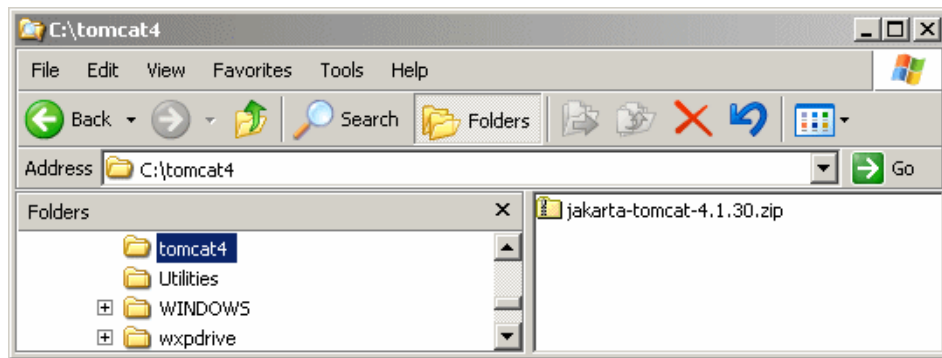


Figure 3-2 Tomcat zip file location

Note: During the System Information Center installation, the Tomcat zipped file will be extracted to the \isic\tomcat\ directory.

3.2.3 System Information Center installation

The following installation process for System Information Center also installs the default Cloudscape SQL database and the required Java Development Kit (JDK).

1. Unzip the System Information Center compressed file to a temporary location.
2. Execute the setup.exe file.

3. The window shown in Figure 3-3 opens.

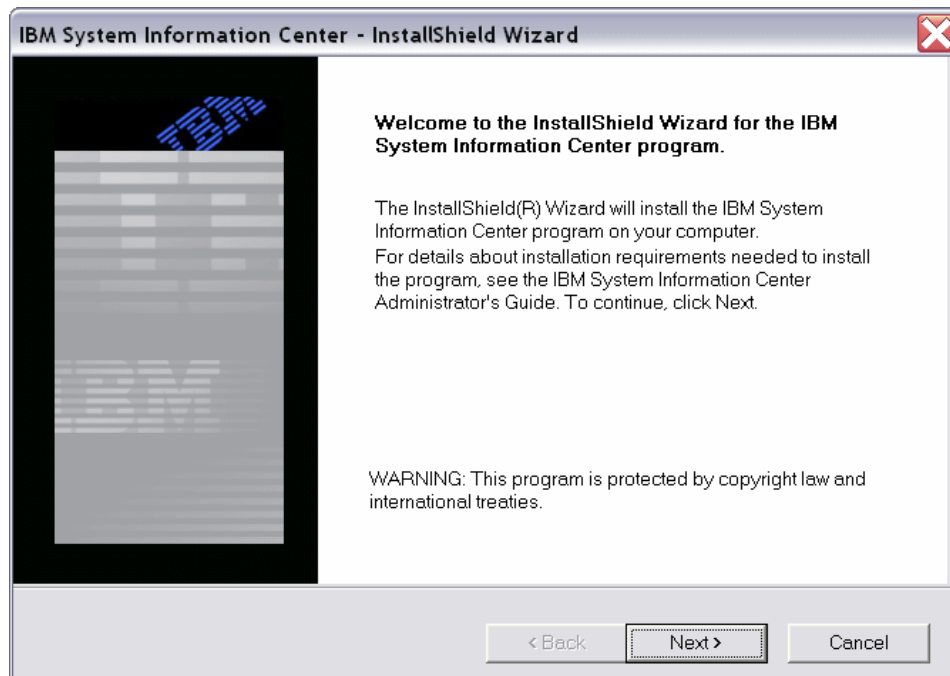


Figure 3-3 System Information Center setup welcome window

4. Select **Next** to continue.

5. The window shown in Figure 3-4 opens. This window reminds the installer of the Tomcat version and file location requirement for proper System Information Center installation. The correct version of the Tomcat zip file must be in the location shown in this window (a directory named C:\tomcat4) before proceeding with the installation of System Information Center.

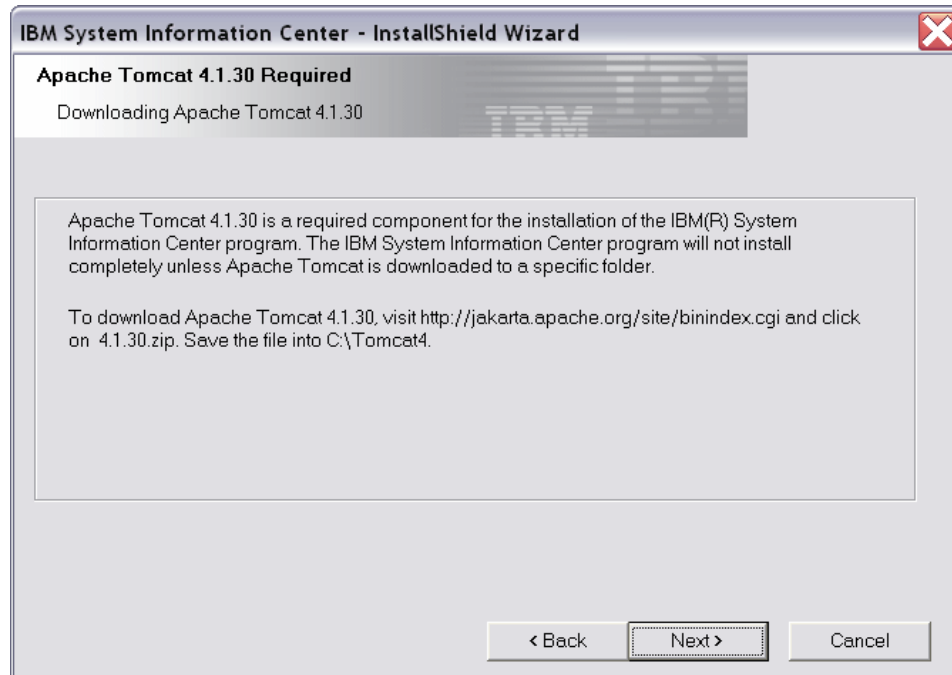


Figure 3-4 Apache Tomcat 4.1.30 warning window

6. Select **Next**.
7. If all System Information Center prerequisites and conditions are satisfied, the license agreement shown in Figure 3-8 on page 103 opens.
If the install process detects invalid software or an incorrect hardware configuration, some or all of the following windows open.

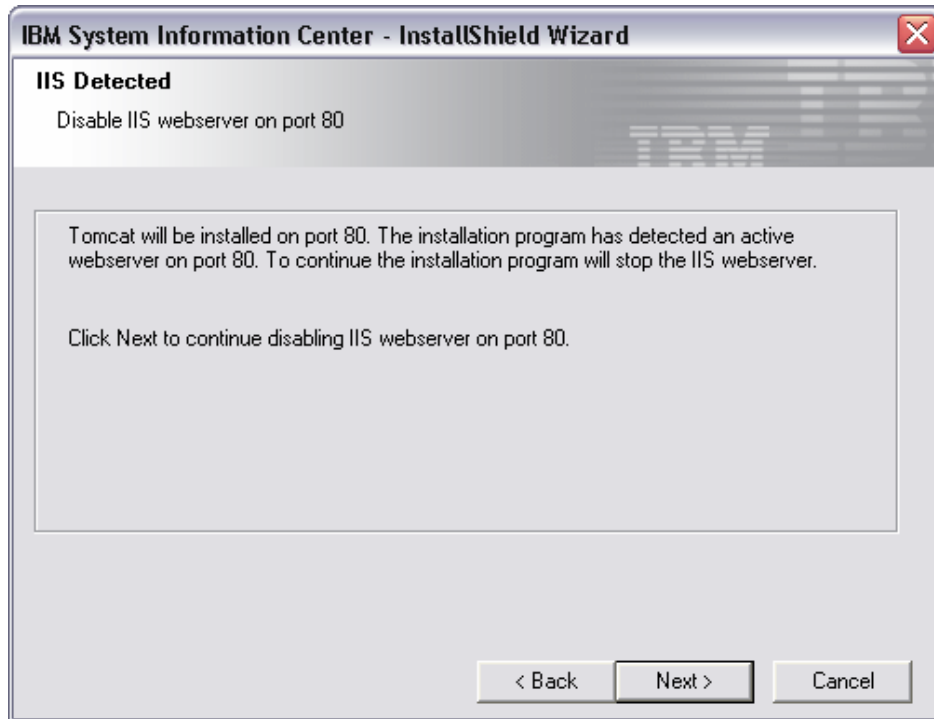


Figure 3-5 IIS running on system error window

8. The window shown in Figure 3-5 opens if Microsoft Internet Information Server (IIS) is running on this system. Since IIS and Tomcat both use port 80, the System Information Center installation will not continue until the IIS service has been set to manual and stopped.

9. If any of the prerequisites have not been met for System Information Center, the window shown in Figure 3-6 opens.

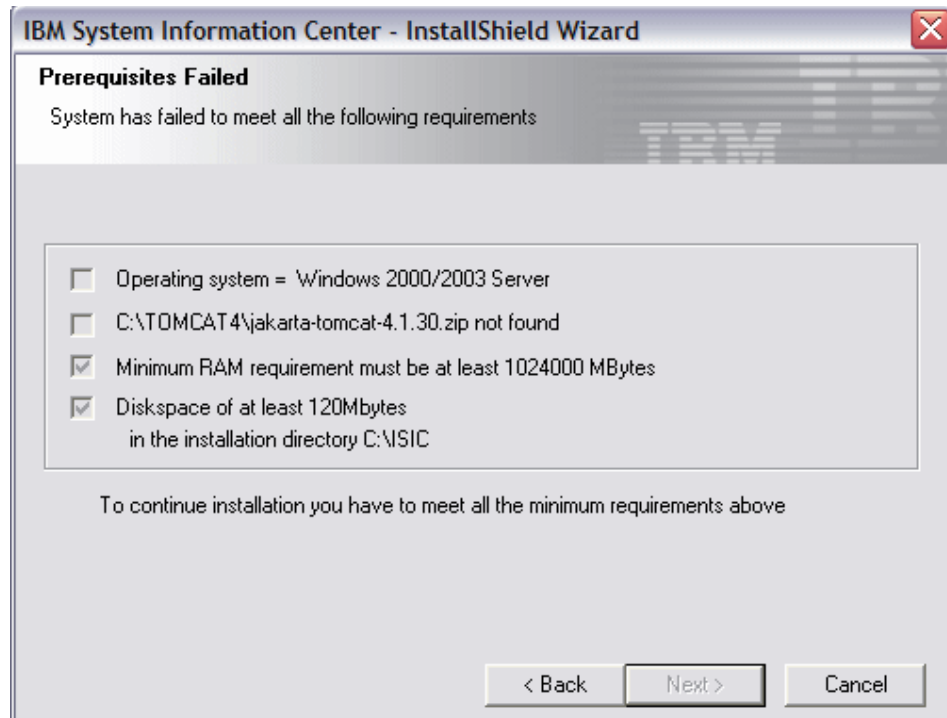


Figure 3-6 Prerequisites failure window

Note that the top two boxes shown in Figure 3-6 are not selected. This means that these System Information Center prerequisite checks failed.

- a. The first check box indicates if System Information Center is being installed on a supported operating system. Microsoft Windows Server 2000 and 2003 are the only supported platforms. In this example, we tried to install IBM System Information Center on a Windows XP system (unsupported).
- b. The second check box indicates if System Information Center found the Tomcat 4.1.30 zip file in the correct location. The zip file must be located in C:\tomcat4\jakarta-tomcat-4.1.30.zip. In this example, we did not copy the Tomcat 4 installation .zip file to the directory required by System Information Center.
- c. The third check box indicates if the installation server has enough RAM. System Information Center requires 1.0 GB of RAM.

- d. The final check box indicates if the installation server has the required 120 MB of free hard drive space.

You must select **Cancel** to exit the installation process and correct the errors.

- 10. If the System Information Center installation process detects a problem with the Tomcat 4 installation file, the window shown in Figure 3-7 opens.

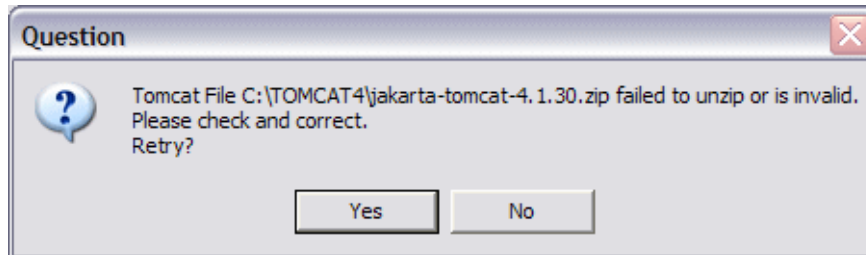


Figure 3-7 Tomcat installation file problem

Correct the problem and select **Yes** to continue

- 11. The window shown in Figure 3-8 opens if all prerequisites have been met and port 80 is not in use by another service. Read the license agreement and accept the terms in the license agreement shown in Figure 3-8.

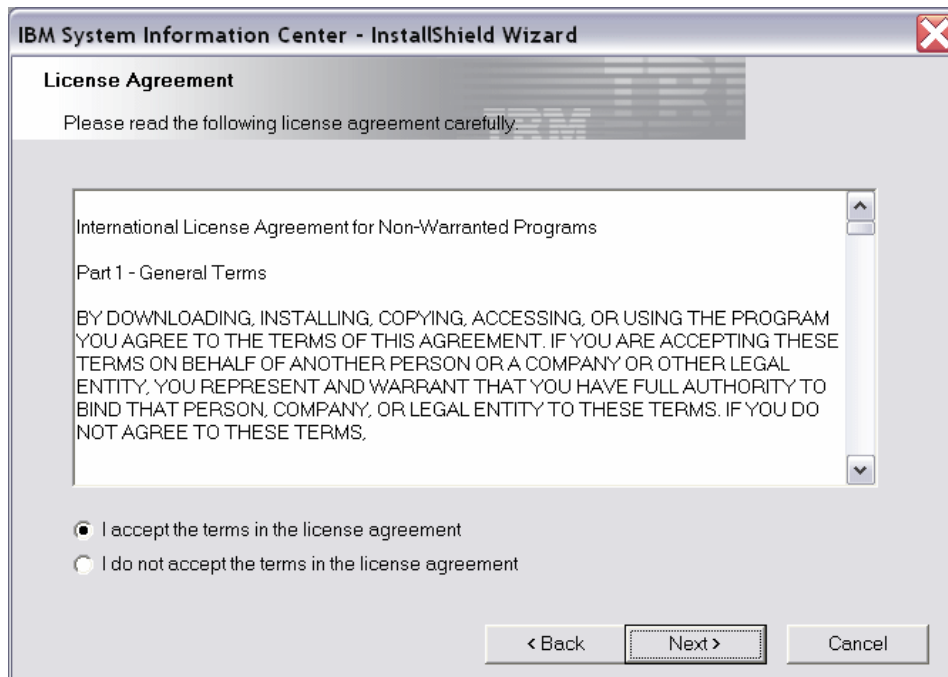


Figure 3-8 System Information Center License Agreement

12. Select **Next** to continue. The window shown in Figure 3-9 opens.

13. In Figure 3-9, a decision must be made on the type of installation to perform.

Quick performs an install using defaults for many of the System Information Center installation parameters, while **Custom** allows full control over all the installation options.



Figure 3-9 Setup Type - Quick

The installation process can be run again to modify any settings that are made during the initial installation. The modify procedure is described in 3.2.5, “Modifying the System Information Center installation” on page 124.

For details on a Quick install, continue with the following steps. If a Custom install is desired, proceed to “Custom install” on page 107.

Quick Install

1. Select **Quick** in the window shown in Figure 3-9.
2. Select **Next**. The window shown in Figure 3-10 opens.

The screenshot shows a Windows-style dialog box titled "IBM System Information Center - InstallShield Wizard". The dialog has a standard Windows title bar with a close button (red X) in the top right corner. The main content area is titled "Web site Settings" and has a subtitle "Defining specific URLs and e-mail addresses". Below this, there is a paragraph of text: "The IBM(R) System Information Center program provides a way for you to define information that automatically populates e-mails:". There are three input fields: "Server name for asset scans" with the value "intranet.yourcompany.com", "URL for uploading asset scans:" with the value "http://intranet.yourcompany.com/isic", and "Administrator's e-mail address for reporting problems:" with the value "ISICadmin@yourcompany.com". At the bottom right, there are three buttons: "< Back", "Next >" (which is highlighted with a dashed border), and "Cancel".

Figure 3-10 Web site settings

3. In Figure 3-10, the box labeled **Server name for asset scans** is the fully qualified domain name of the System Information Center server where you wish the inventory data to be uploaded to. By default, the name of the server that System Information Center is being installed on opens. The value you enter for server name can be changed at a later time using the modify procedure described in 3.2.5, "Modifying the System Information Center installation" on page 124.

Note: Below the **Server name for asset scans** input box shown in Figure 3-10, the fully qualified domain name of the system you are installing System Information Center on will be displayed dynamically in the **URL for uploaded asset scans** field. This field will be auto filled with the server name by default.

In Figure 3-10, insert the email address of the System Information Center administrator in the box labeled **Administrator's email address to report problems**.

4. Select **Next**. The windows shown in Figure 3-11 opens.

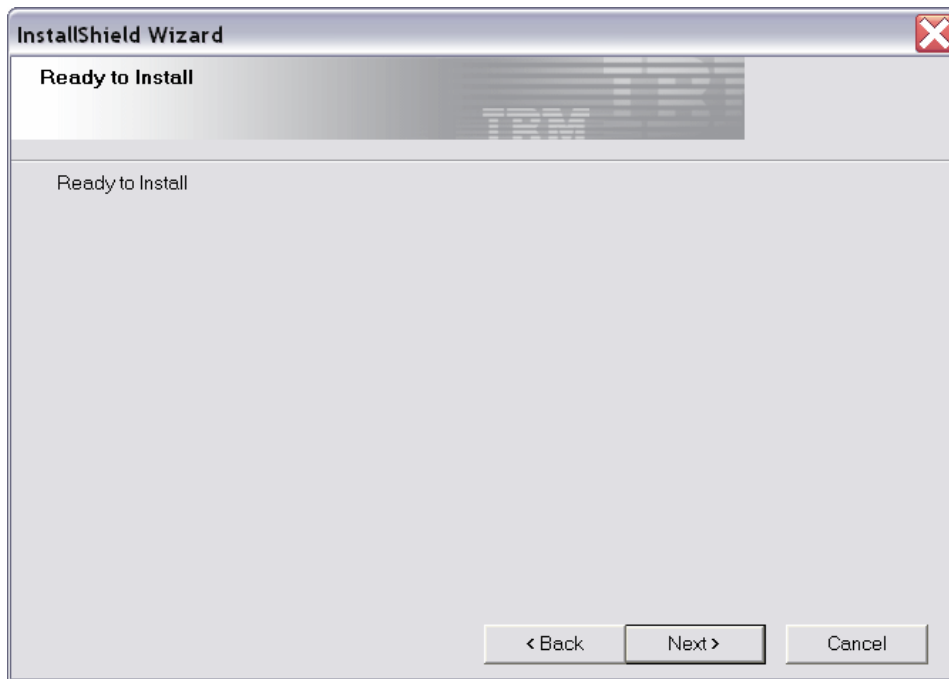


Figure 3-11 Ready to Install

5. Select **Next** to begin the install. The window shown in Figure 3-12 opens when the installation has completed.

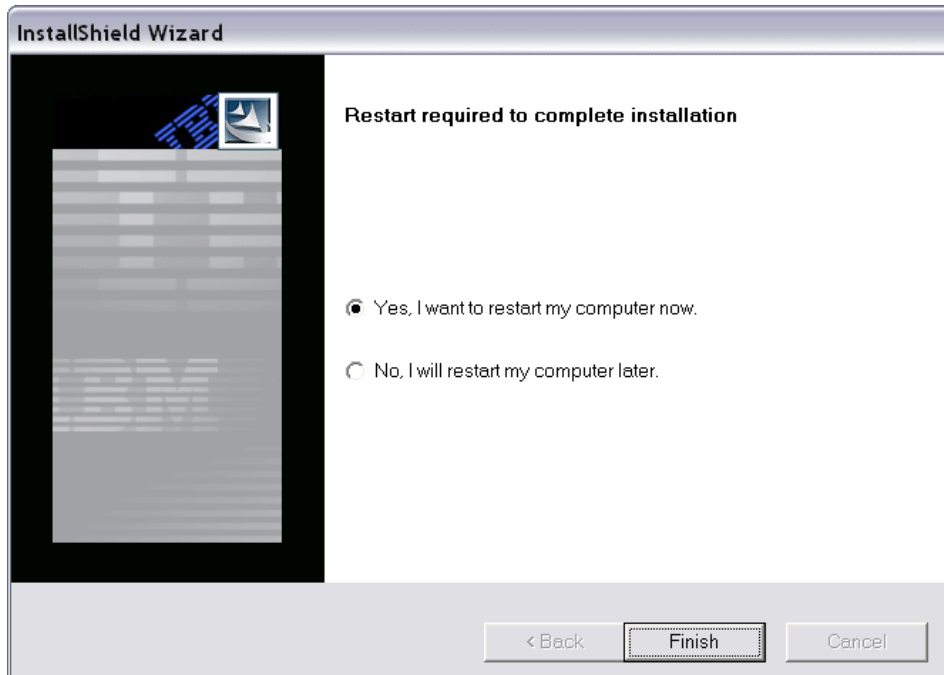


Figure 3-12 Restart computer

6. Select **Yes, I want to restart my computer now.**
7. Select **Finish** to complete the installation of System Information Center and restart the computer.

See 3.2.5, “Modifying the System Information Center installation” on page 124 for how to modify the IBM System Information Center installation parameters after it has been successfully installed.

Skip to “Testing the installation” on page 117 to continue the installation process.

Custom install

A custom installation of System Information Center allows you to configure more of the settings that assume default values when using the quick installation process discussed previously.

1. To perform a custom install of System Information Center, select **Custom** from the window shown in Figure 3-13.

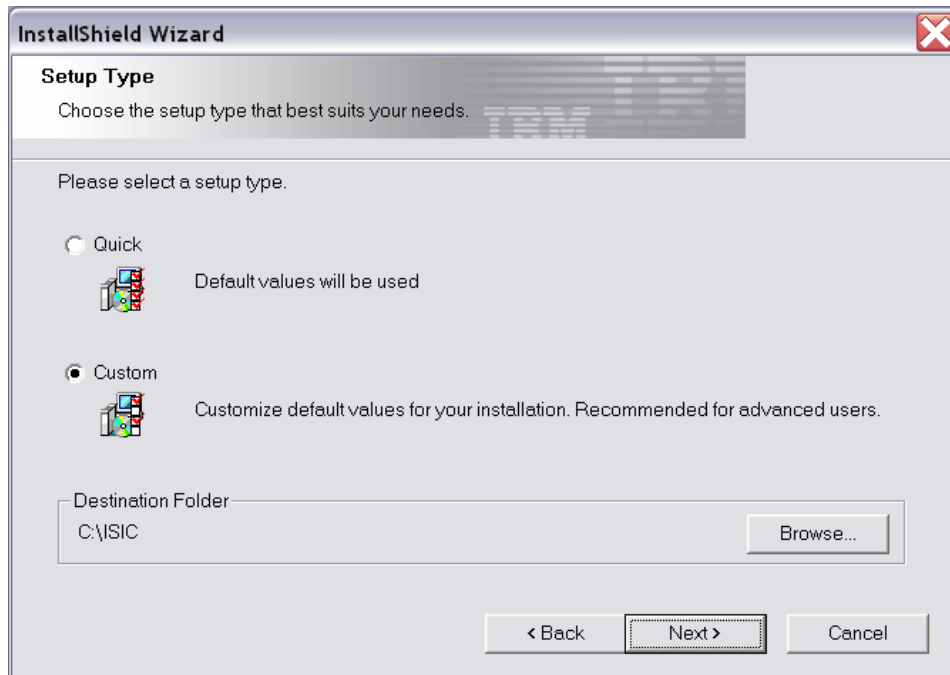


Figure 3-13 Setup Type - Custom

2. After the Custom option has been selected, select **Next** to proceed to the window shown in Figure 3-14.

IBM System Information Center - InstallShield Wizard

E-mail Settings

Defining optional e-mail settings for your environment

The IBM(R) System Information Center program provides various functions for sending information using e-mail. E-mail functionality provides user accounts with scheduled task results, asset requests, and additional asset information.

☒ Enable e-mail functions

E-mail settings

SMTP server name/IP address:

Return e-mail address:

☒ Enable SMTP authentication

SMTP userid:

SMTP password:

< Back Next > Cancel

Figure 3-14 E-mail Settings - example

3. If you choose to enable the e-mail support in System Information Center, select the **Enable e-mail functions** box in Figure 3-14, and input the email settings.

The **Return e-mail address** field should contain the e-mail address of the System Information Center administrator.

4. Select **Next**. The window shown in Figure 3-15 opens.

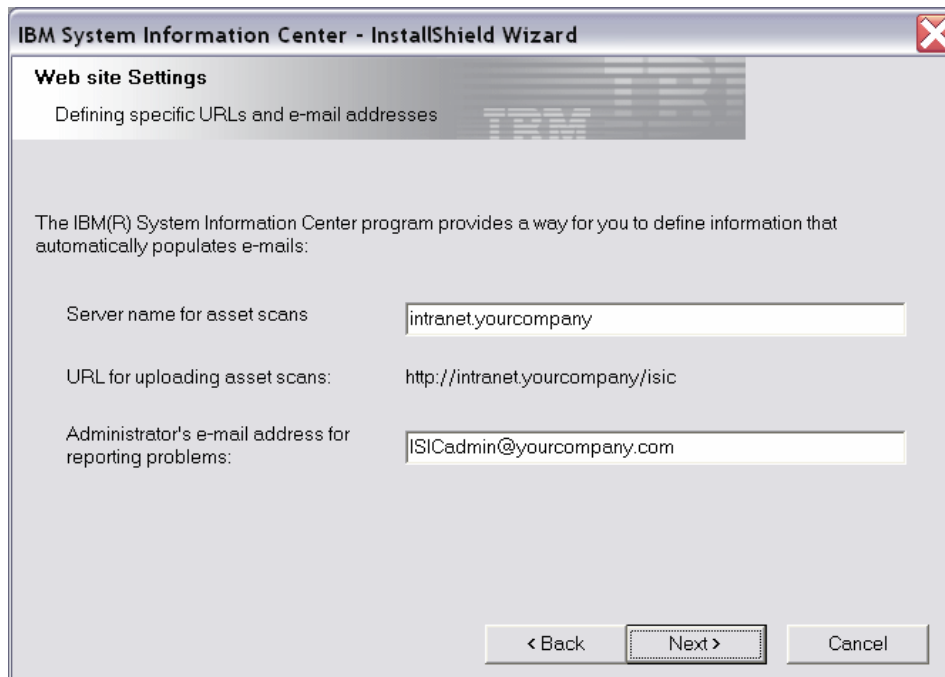


Figure 3-15 Web site Settings - example

5. In Figure 3-15, the box labeled **Server name for asset scans** is the fully qualified domain name of the System Information Center server where you wish the inventory data to be uploaded to. By default the name of the server that System Information Center is being installed on opens. The value you enter for server name can be changed at a later time using the modify procedure described in 3.2.5, "Modifying the System Information Center installation" on page 124.

Note: Below the **Server name for asset scans** input box shown in Figure 3-10, the fully qualified domain name of the system you are installing System Information Center on will be displayed dynamically in the **URL for uploaded asset scans** field. This field will be auto filled with the server name by default.

In Figure 3-15, insert the email address of the System Information Center administrator in the box labeled **Administrator's email address to report problems**.

6. Select **Next**. The windows shown in Figure 3-16 opens.



Figure 3-16 Action Authority Settings

7. The window shown in Figure 3-16 allows you to select what command and control privileges will be allowed for each System Information Center user type:

- User
- Superuser
- Administrator

Select the desired user types that will be authorized to perform each action.

For more information about IBM System Information Center user types, see 3.6, “User Management” on page 155.

8. Select **Next**. The window shown in Figure 3-17 opens.

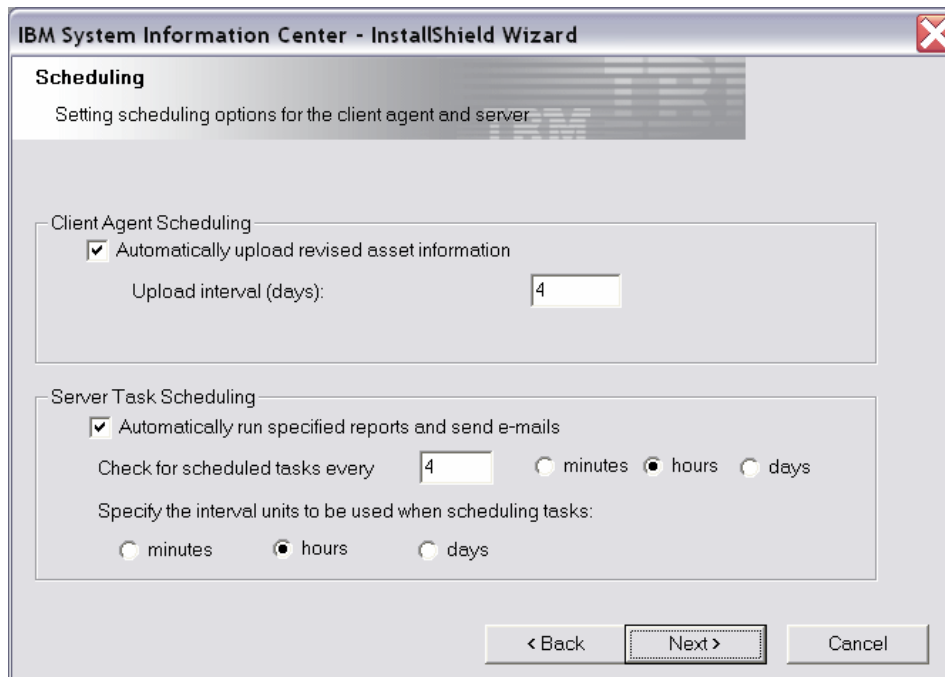


Figure 3-17 Scheduling

9. The window shown in Figure 3-17 allows you to configure automatic client and server scheduling of tasks. The client agent can be configured to automatically upload revised asset information on a fixed schedule, while the System Information Center server can be configured to automatically generate reports and send e-mails.

Note: The selection of **minutes**, **hours**, or **days** under **Specify the interval units to be used when scheduling tasks** is used for all task scheduling (except for Client-Agent Scheduling and Server Task Scheduling shown on this window). This value is the unit of time that all tasks in System Information Center will use for scheduling. This value cannot be changed for different tasks. For example, if hours was selected as the unit of time during the install, and a task is scheduled for 3 days, then 36 hours would have to be used.

10. When all settings are configured, select **Next**. The window shown in Figure 3-18 opens.



Figure 3-18 Setting password options

11. In Figure 3-18, the password requirements for System Information Center users are set.

Note: Note that any changes you may make to the password settings shown in Figure 3-18 do not apply to the ADMIN user ID created automatically during IBM System Information Center installation.

The ADMIN account uses the default rules displayed in Figure 3-18 when System Information Center is first installed. The initial password for the ADMIN account is “password”. Passwords are not case sensitive.

12. After making all of the desired changes, select **Next**. The window shown in Figure 3-19 opens.

IBM System Information Center - InstallShield Wizard

Form Settings
Defining required fields used during asset registration

Choose one or more fields that are required in order for an asset or user to be successfully added to the database. The following displays marked fields that are required by default.

Asset Demographics Form

<input type="checkbox"/> Asset Tag	<input type="checkbox"/> Department	<input checked="" type="checkbox"/> Floor	<input type="checkbox"/> Owner
<input checked="" type="checkbox"/> Asset Type	<input checked="" type="checkbox"/> Description	<input type="checkbox"/> Location	<input checked="" type="checkbox"/> Status

User Demographics Form

<input type="checkbox"/> Address	<input checked="" type="checkbox"/> Employee ID	<input type="checkbox"/> Nickname	<input type="checkbox"/> Title
<input type="checkbox"/> Country	<input checked="" type="checkbox"/> Location	<input type="checkbox"/> Office phone number	<input type="checkbox"/> Town
<input checked="" type="checkbox"/> Department	<input type="checkbox"/> Mobile phone number	<input type="checkbox"/> Postal code	<input checked="" type="checkbox"/> User ID
<input checked="" type="checkbox"/> E-mail	<input checked="" type="checkbox"/> Name	<input checked="" type="checkbox"/> Password	

Defaults < Back Next > Cancel

Figure 3-19 Form Settings

13. Use the window shown in Figure 3-19 to denote which fields will be required fields when a client enters data into an asset or user form. All of the fields listed in Figure 3-19 will be available for the client to populate, but only the ones selected on this window will be required.

Required fields are indicated with an “*” on the asset or user form. The required fields can be changed after System Information Center installation by following the procedures documented in 3.2.5, “Modifying the System Information Center installation” on page 124.

14. After making all of the desired changes, select **Next** to continue to the window shown in Figure 3-20.

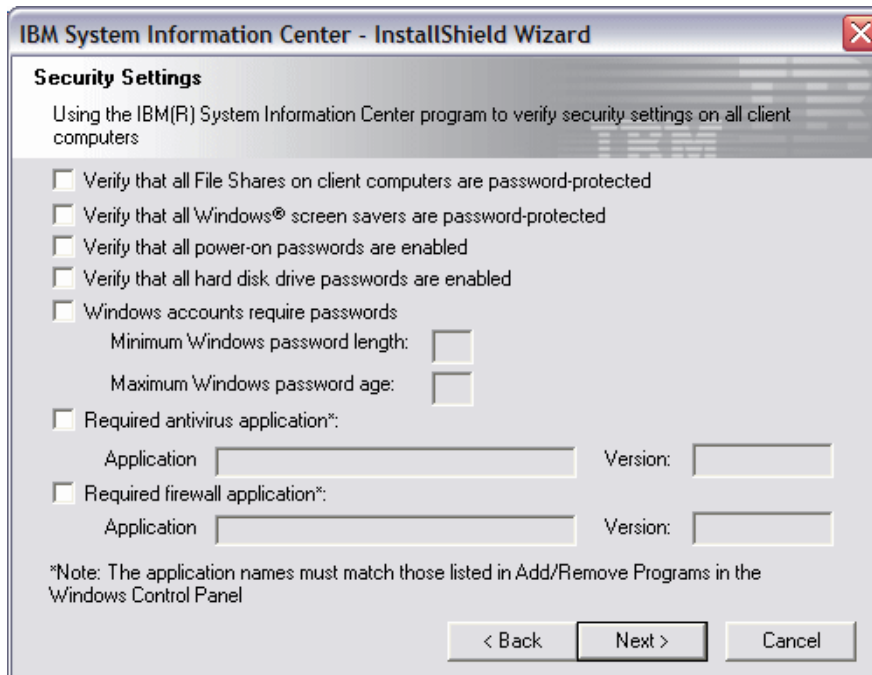


Figure 3-20 Security Settings

15. IBM System Information Center can be configured to verify client compliance with certain security settings that may be required by company security policies.

The window shown in Figure 3-20 is used to configure this feature. This window displays the settings to be used to set up a query that will run on client systems. This query checks for security settings that have been selected.

16. After all changes are made, select **Next** to proceed to the window shown in Figure 3-21.

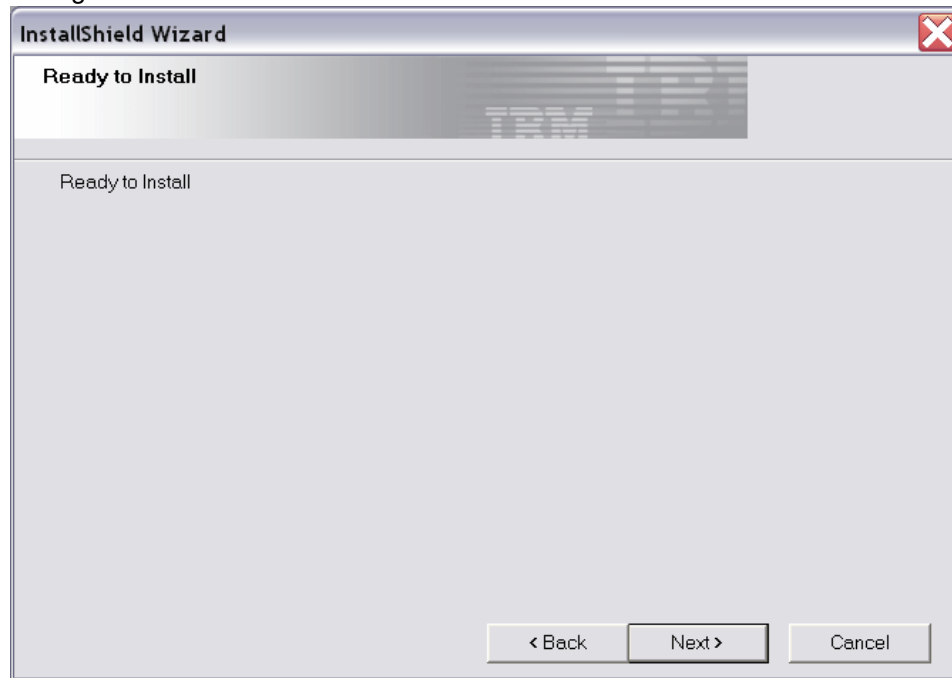


Figure 3-21 Restart computer - custom

17. Select **Next** to begin the install. The window shown in Figure 3-22 opens when the installation has completed.

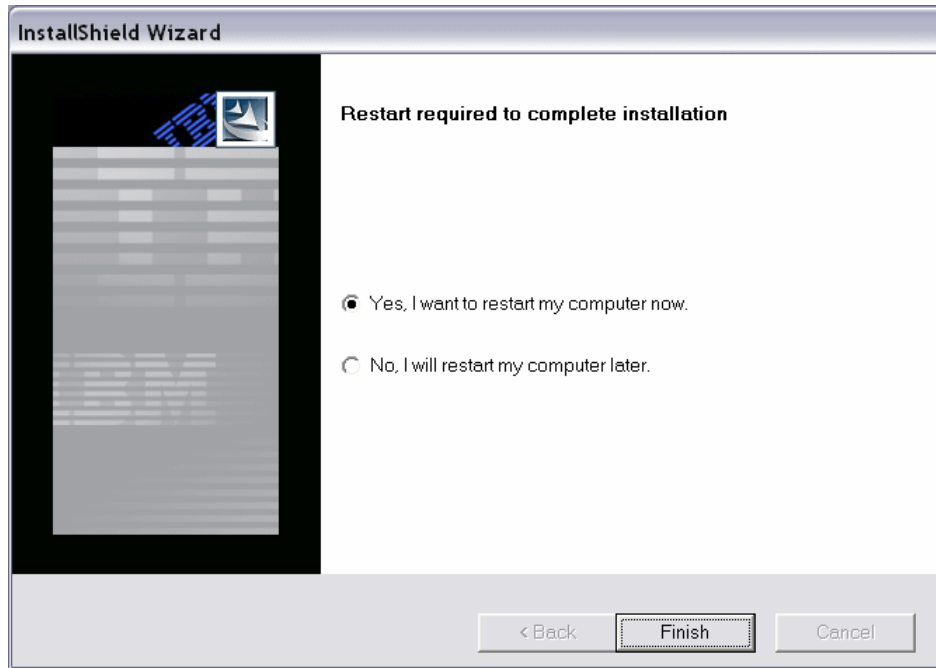


Figure 3-22 Restart computer - custom

18. Select **Yes, I want to restart my computer now.**

19. Select **Finish** to complete the installation of System Information Center and restart the computer.

20. The `c:\tomcat4\` directory can now be deleted. See the note following Figure 3-2 on page 97 for more information.

See 3.2.5, “Modifying the System Information Center installation” on page 124 for how to modify the IBM System Information Center installation parameters after it has been successfully installed.

The following section discusses how to verify and test the IBM System Information Center after initial installation.

3.2.4 Testing the installation

After you have installed System Information Center, you may wish verify and test the installation.

Verifying that the installation was successful

To verify that the System Information Center installation was successful, perform the following steps:

1. Open the Windows Services applet.
2. Ensure that the Tomcat service is running. Select **Administrative Tools** → **Services** and locate the service as shown in Figure 3-23.

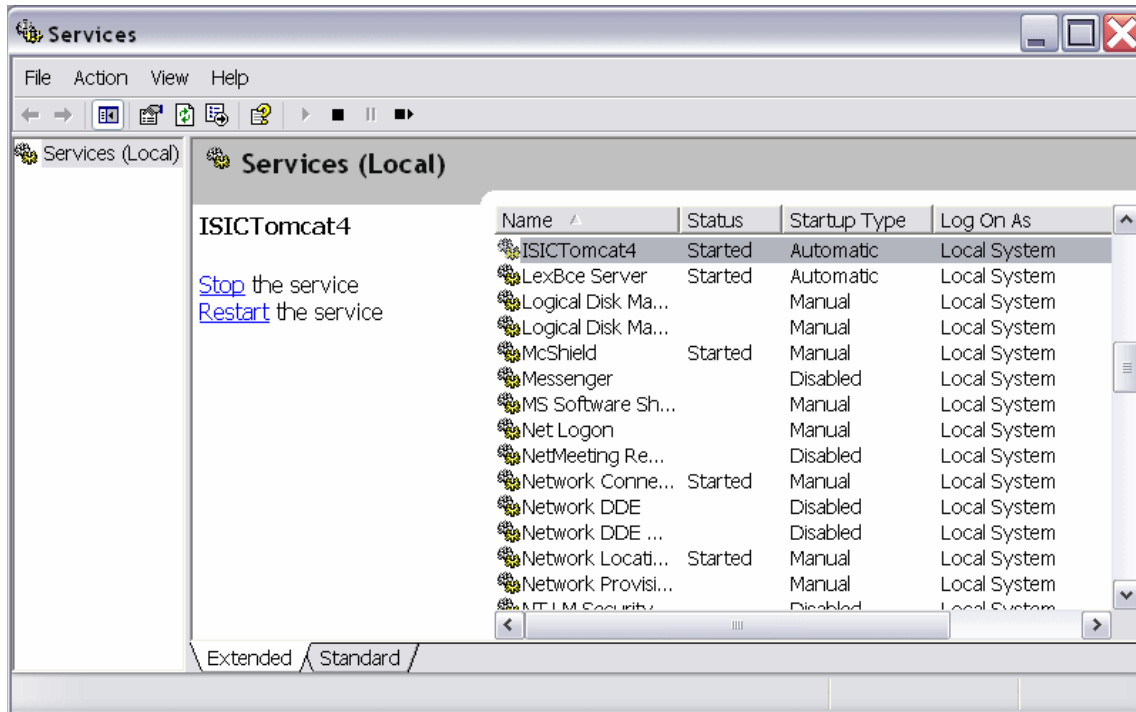


Figure 3-23 System Information Center Tomcat Service page

3. Ensure that the ISICTomcat4 service is set to **Automatic** and that it is started.
4. Close the services utility.
5. Open Internet Explorer 6 to the following URL:
`http://localhost`
6. The window shown in Figure 3-24 should be displayed.

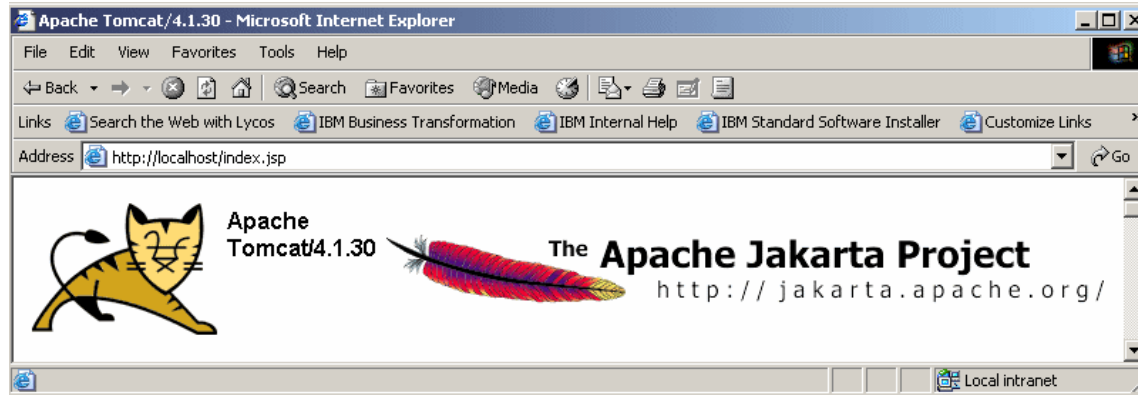


Figure 3-24 Tomcat 4.1.30 default home page

7. The window shown in Figure 3-24 will appear if the Tomcat installation was successful.
8. If the installation was *not* successful, open Windows Explorer and point to:
`C:\ISIC\tomcat\jakarta-tomcat-4.1.30\webapps\tomcat-docs\index.html`
 You'll find the necessary information for troubleshooting the Apache Tomcat Web server.

Security settings for Apache Tomcat Web server

It is a best practice not to use the default server administrator account for running applications on the server. It is assumed that a Windows local account has already been created with local administrative privileges. The name of this local user account is not important as long as it is unique to the server.

To ensure that the Apache Tomcat service is not running under the local system account (which can be a security issue), change the logon credentials of this service using this procedure:

1. Go to **Control Panel** → **Administrative Tools** → **Services** to open the window shown in Figure 3-25 on page 120.

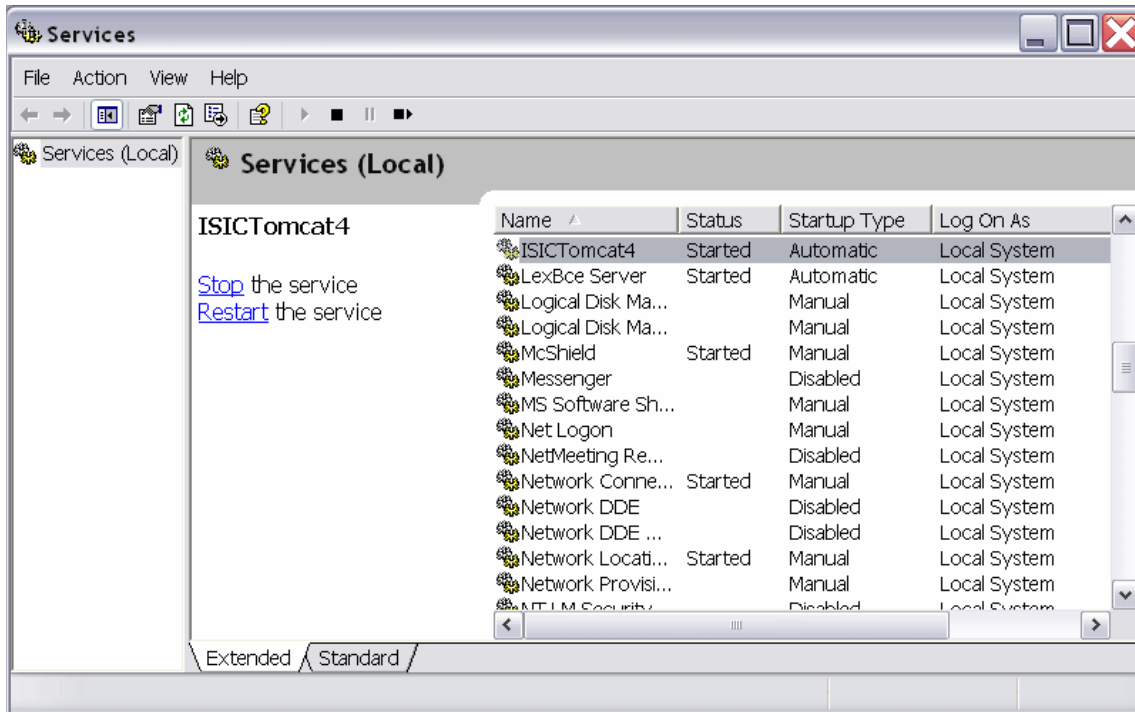


Figure 3-25 System Information Center Tomcat Services page

2. Stop the Apache Tomcat (ISICTomcat4) service.
3. Right-click the service and select **Properties**. This opens the window shown in Figure 3-26.

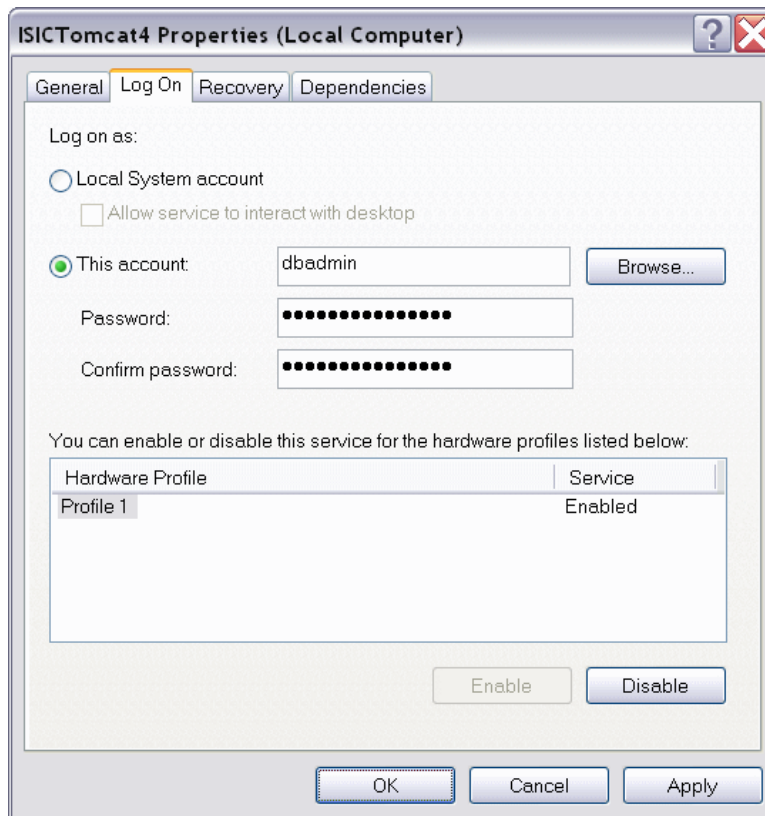


Figure 3-26 Changing account credentials of the Tomcat service

4. As shown in Figure 3-26, insure that the **Log On** tab is selected. Select the **This account** button and enter a Windows user name (one with administrator authority) and password. If you are running System Information Center with an SQL database other than the Cloudscape database supplied with System Information Center (refer to Appendix B, “Alternate SQL database for System Information Center” on page 607), use the same account and password as used for the database administrator. Click **OK**.
5. Start the Apache Tomcat service.

Start Tomcat and System Information Center

To start Tomcat and System Information Center:

1. Open Internet Explorer and type `http://localhost` in the Address field. The Tomcat default Web page opens (see Figure 3-24 on page 119).

2. Type `http://localhost/isic` in the Address field. This opens the System Information Center logon window shown in Figure 3-27, an indication that the installation was successful.

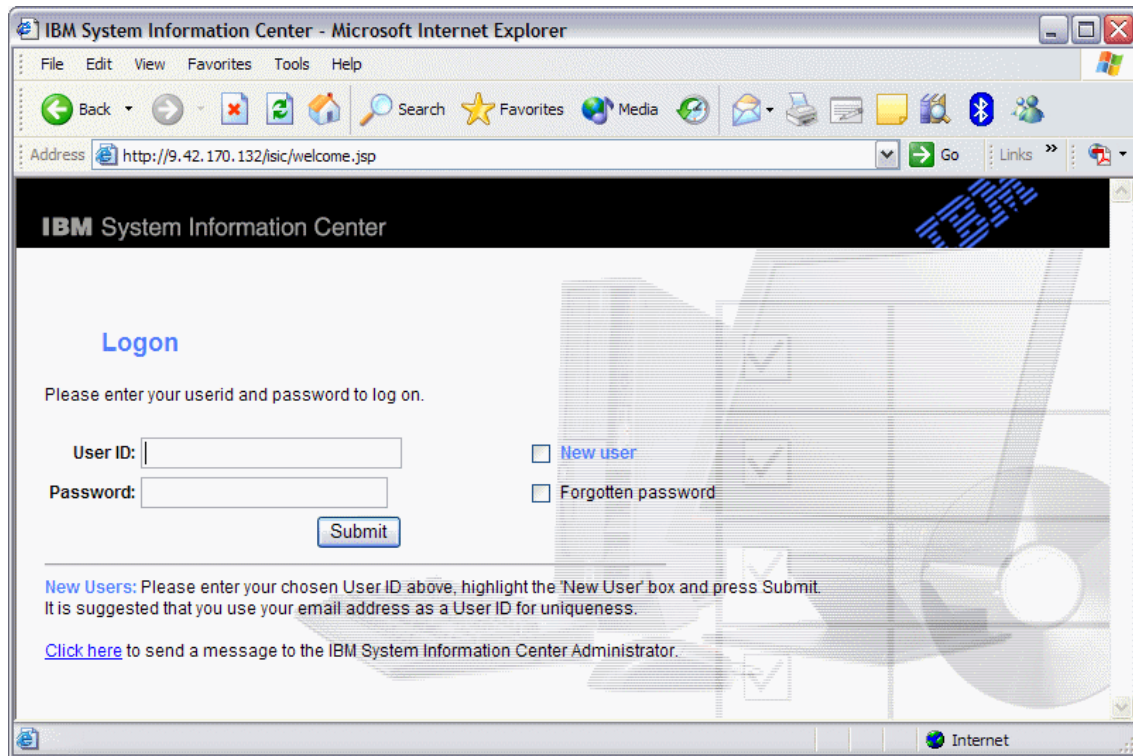


Figure 3-27 Logon page of System Information Center

Important: The only user account that is created during the System Information Center installation is a default administrator with a user ID of *admin* and password of *password*. To log on to System Information Center the first time, you must use this user ID and password.

3. Enter *admin* in the User ID field, *password* in the Password field, and click **Submit** to access the Change Details page for the administrator user account. At this time, you must change the Administrator password.

Attention: The settings for the required user fields (see Figure 3-19 on page 114) and password rules (see Figure 3-18 on page 113) that were set during System Information Center installation do not apply to the ADMIN account created during System Information Center installation. The required fields and password rules for the administrator account are the System Information Center defaults.

Verifying the version of System Information Center

The installed version of System Information Center can be verified from the System Information Center main menu. From the Help menu, select **About System Information Center** as shown in Figure 3-28.

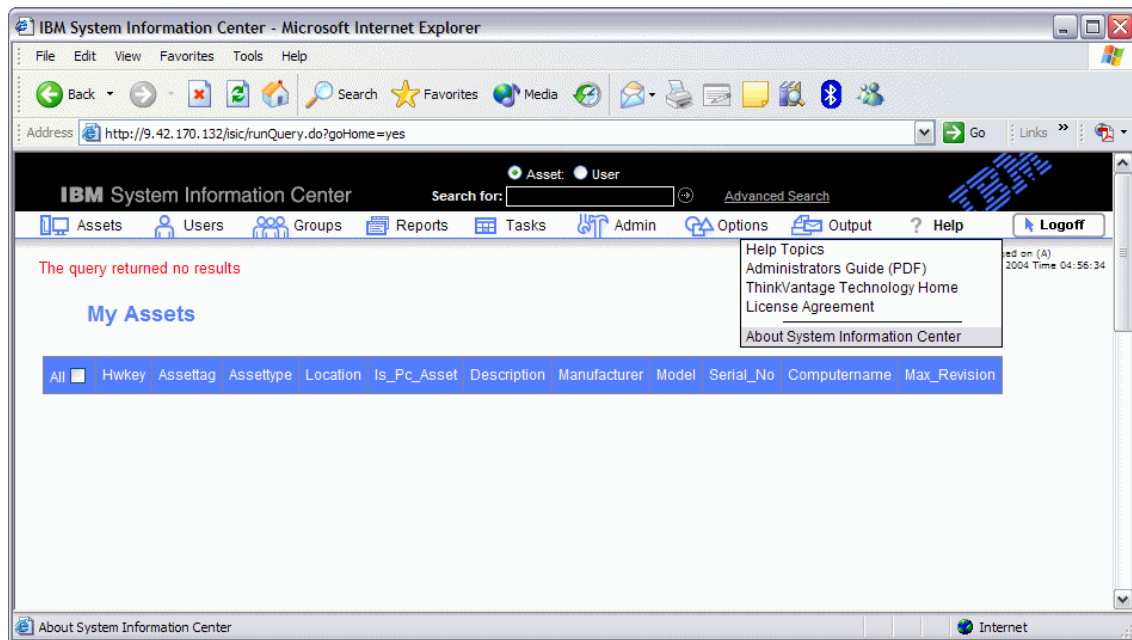


Figure 3-28 System Information Center Help menu

This opens a window (see Figure 3-29 on page 124) with the System Information Center version level.

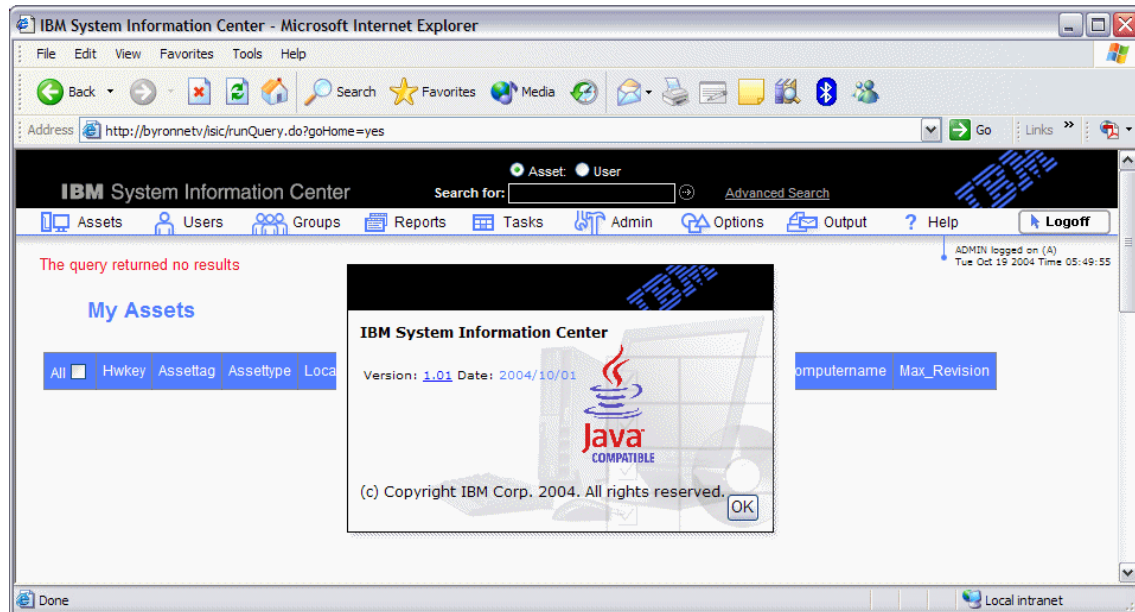


Figure 3-29 System Information Center version information

3.2.5 Modifying the System Information Center installation

You can change the options and settings that were selected during the initial installation of System Information Center quickly and easily. This section discusses how to modify System Information Center installation parameters after the initial installation.

This modification is performed using the Add/Remove Programs applet in the Windows Control Panel as follows.

1. Select the **Change/Remove** button associated with System Information Center as illustrated in Figure 3-30.

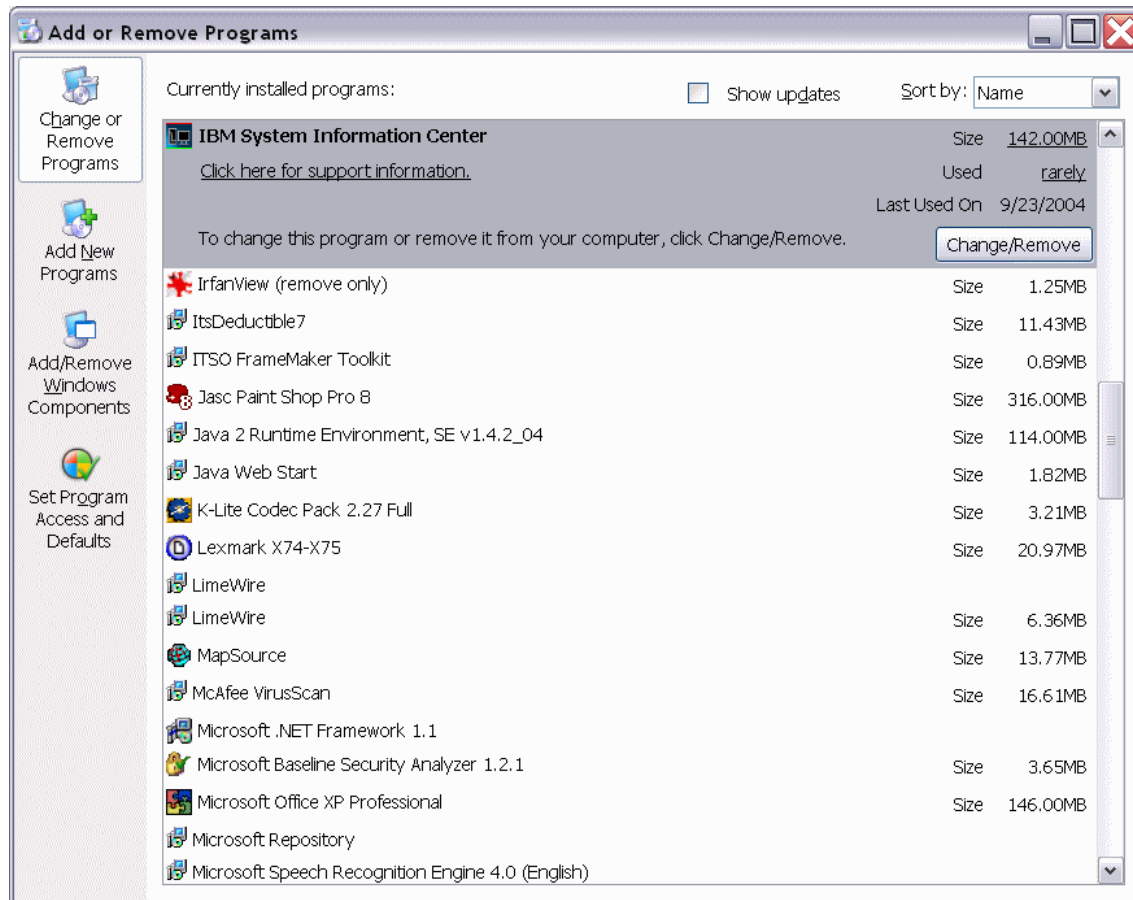


Figure 3-30 Change/Remove System Information Center in the Windows Add/Remove Programs applet

2. The window shown in Figure 3-31 opens. Select **Modify**.



Figure 3-31 Welcome window

3. Select **Next**. The window shown in Figure 3-32 opens.

4. The installation option window shown in Figure 3-32 is the same window as shown in Figure 3-9 on page 104 and in Figure 3-13 on page 108.

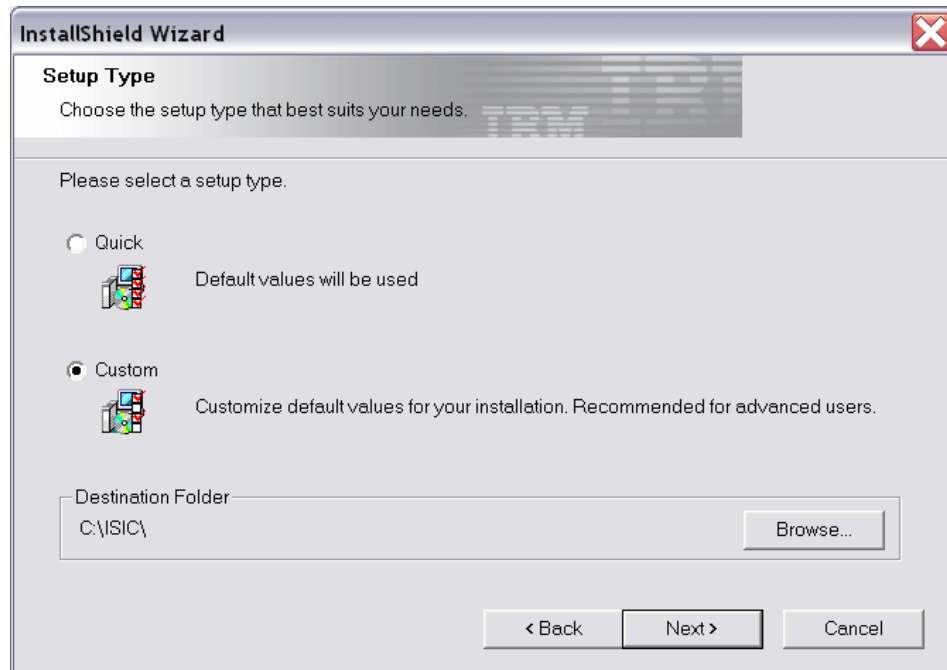


Figure 3-32 Selecting a setup type

From the window shown in Figure 3-32, a quick install as described in “Quick Install” on page 104 can be performed, or a custom install as described in “Custom install” on page 107. All of the settings that are available during the install can be modified from this modify routine.

5. Select the setup type you wish to perform, and click **Next** to continue with the System Information Center modifications.

6. When the modify install process is complete, the window shown in Figure 3-33 opens. A restart of the system is not required after modifying System Information Center settings, but the Tomcat service must be restarted before any modifications to System Information Center can function.

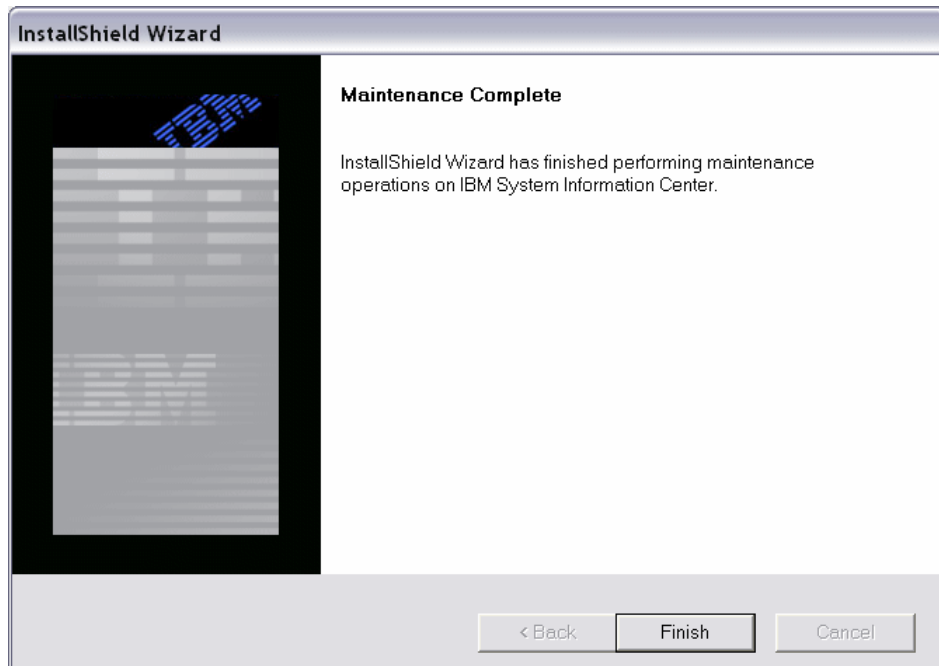


Figure 3-33 Maintenance Complete page

7. Click **Finish** to close the modify page.

3.3 Logging on to System Information Center

In this section, we describe how to log on to System Information Center for the first time and user accounts.

3.3.1 System Information Center user accounts

System Information Center supports three types of user accounts:

- User

This is the most limited account type. Most System Information Center accounts will be User.

- Superuser

A superuser can perform all User tasks, as well as certain advanced functions such as creating reports.

- Administrator

An administrator can perform all tasks.

Note: For more information about System Information Center user types, see the *System Information Center Administrator's Guide* installed with System Information Center in \ISIC\web\help\ISICADM.pdf.

The installation of System Information Center automatically creates a System Information Center Administrator user type named *admin* with a password of *password* (passwords are not case sensitive). The first time an administrator user logs in, the System Information Center **Change details** opens. The administrator must enter a new password for the administrator user ID at this time.

3.3.2 The logon process

System Information Center user accounts can be created by a user with Administrator authority. Also, any user can create an account by logging in to System Information Center the first time and registering.

To start the logon process, open Microsoft Internet Explorer 6.0 and type `http://localhost/isic` in the Address field.

Attention: The System Information Center administration Web interface is fully supported only with Microsoft Internet Explorer 6.0 or higher.

The System Information Center logon window opens. No matter what type of user logs on the System Information Center server, or what machine the user is accessing System Information Center from, the logon window will be the same. See Figure 3-34 on page 130.

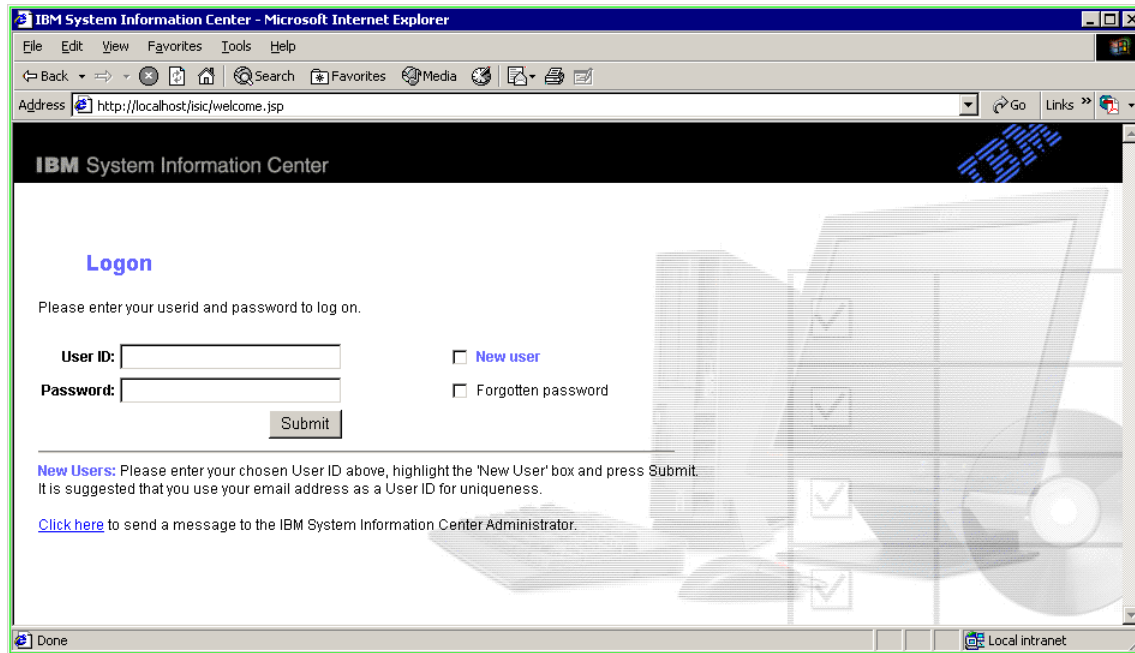


Figure 3-34 Logon page

There are two possible paths that can be taken at this point. Which path is taken depends on whether:

- ▶ The user is a new user and does not have a System Information Center user name.
- ▶ The user already has a user name from a previous login or one that was created by the System Information Center Administrator.

If the user does not have a user name

Users can create their own user names from the initial page. If a user does not have a user name and password, they can simply enter their desired user ID, select **New user** and then click **Submit**. This opens a new page like that illustrated in Figure 3-35 on page 131.

IBM System Information Center

Add User

User ID: * Number/Street:

Email address: Building:

Title: Town:

Forename: * Country:

Surname: * Postcode:

Preferred name: Office Number:

Employee ID: Mobile Number:

Department: Password: *

Location: Please retype password: *

Do you wish to register an asset? ☒

* indicates a required field

Figure 3-35 Adding a user

On this page, the user can enter demographic and location information. The fields marked with an asterisk (*) are required.

Important: Fields marked with an “*” are required fields. The System Information Center Administrator can change the required fields at any time by modifying the installation (see 3.2.5, “Modifying the System Information Center installation” on page 124 and Figure 3-19 on page 114. These properties are stored in the isic.properties file located in:

C:\ISIC\web\WEB-INF\classes\

This file can be manually edited after System Information Center installation. The changes will not take effect until the System Information Center Tomcat 4 service has been restarted.

Tip: It is important to define a policy for creating user names so that they are consistent. We recommend using e-mail addresses. This makes it easier for an administrator to locate users.

In the bottom left corner of the window, there is a check box labeled *Do you wish to register an asset?* that is selected by default. If you click **Submit** when this is selected, the page where users can register their computers in the System Information Center database opens. (For more information, see 3.5, “Assets” on page 133.)

If you clear this check box and click **Submit**, you create a new user in System Information Center and open the system page shown in Figure 3-36. The new user only has user rights unless an administrator changes the user type. For more information about changing user rights, see 3.6.7, “Edit” on page 160.

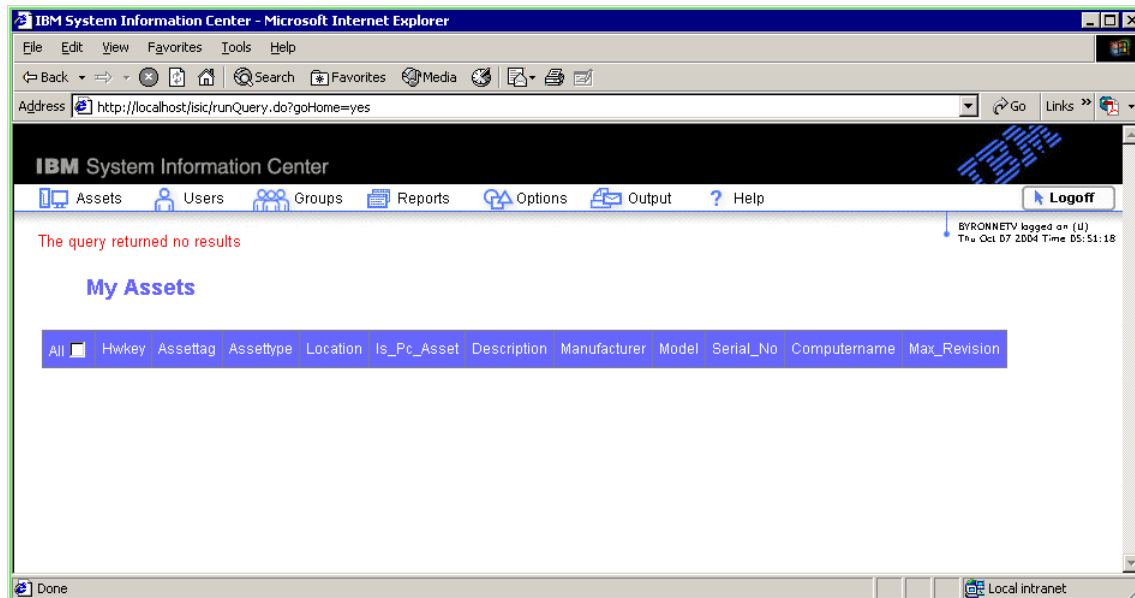


Figure 3-36 Main page

If the user already has a user name and password

On the logon page (Figure 3-34 on page 130), the user can type in the user name and password they already have in the system. When you enter your user ID and password and click **Submit**, the user will be taken to the main page shown in Figure 3-36.

3.4 System Information Center main menu

The System Information Center main menu is illustrated in Figure 3-37.

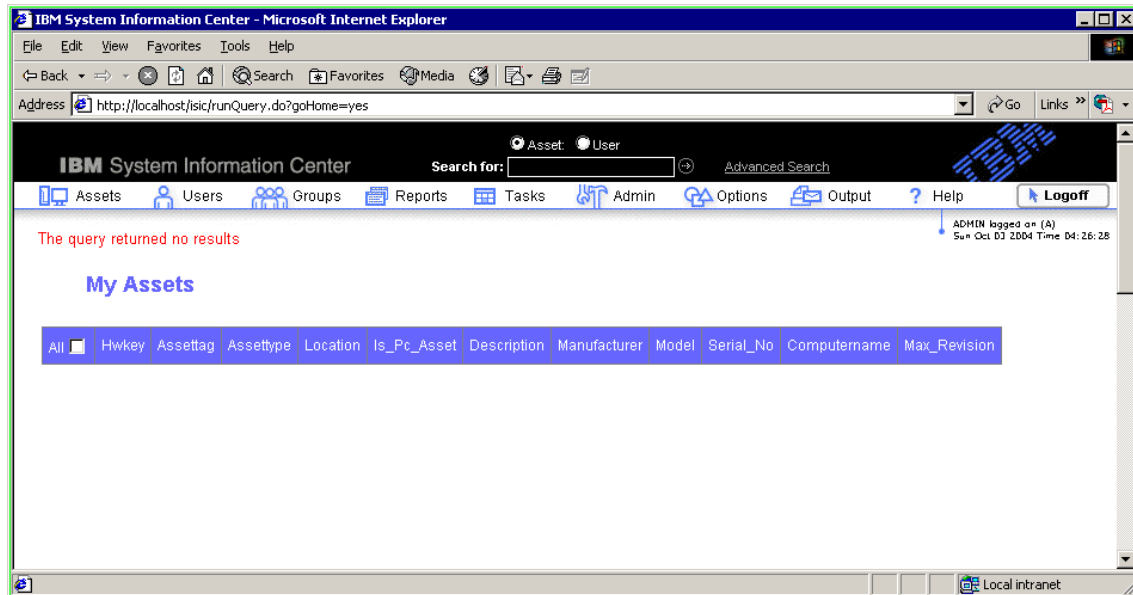


Figure 3-37 System Information Center main menu

These sections discuss the System Information Center main menu selections:

- ▶ 3.5, "Assets" on page 133
- ▶ 3.6, "User Management" on page 155
- ▶ 3.7, "Group management" on page 161
- ▶ 3.8, "Reports" on page 167
- ▶ 3.9, "Tasks" on page 192
- ▶ 3.10, "Admin" on page 193
- ▶ 3.11, "Options" on page 197
- ▶ 3.12, "Output" on page 206

3.5 Assets

On the main page in System Information Center, there is a menu item called *Assets* (see Figure 3-38 on page 134). This is where you can view, add, and edit asset information. In this section, we explain the features of this part of System Information Center.

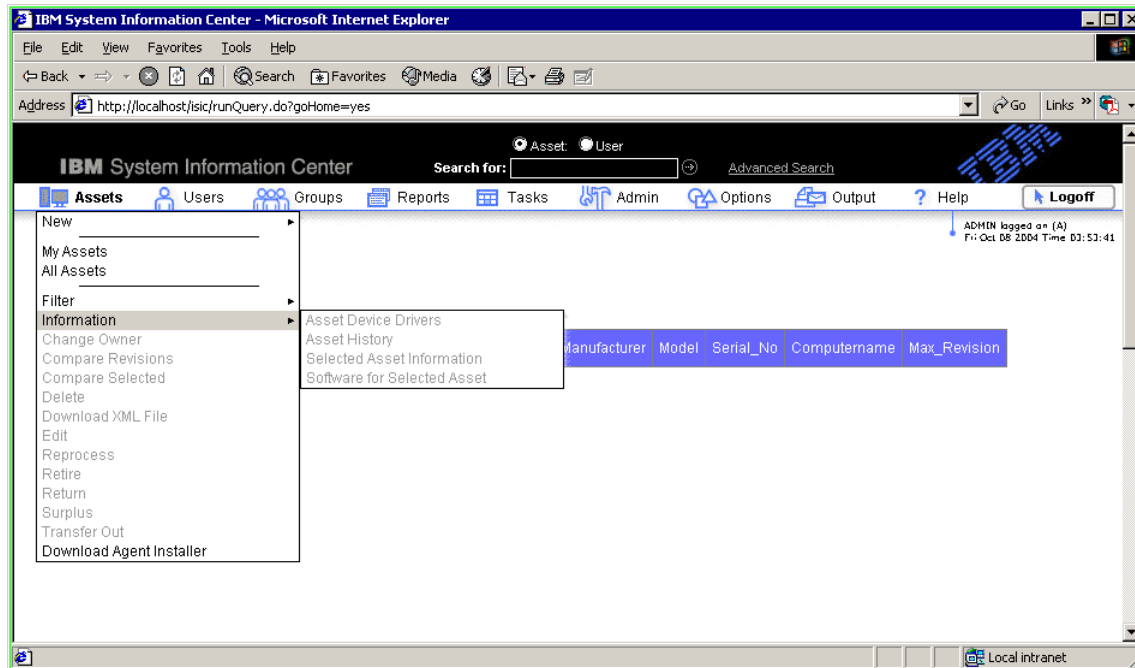


Figure 3-38 Asset menu on main page

With asset management you can perform the following tasks:

- ▶ Add assets to the system
- ▶ View the assets for the user currently logged on
- ▶ View all assets in the system
- ▶ Define filters for reports based on asset selection
- ▶ View asset information
- ▶ Change the owner of an asset
- ▶ Compare revisions
- ▶ Compare assets
- ▶ Delete assets
- ▶ Download an XML file with asset information
- ▶ Edit an asset
- ▶ Reprocess an asset
- ▶ Retire an asset
- ▶ Return an asset
- ▶ Surplus an asset
- ▶ Transfer an asset
- ▶ Download an agent to run on the client computer

The number of menu items available depends on the user's rights (user type).

3.5.1 Upload Asset Scan

From the Upload Asset Scan page, you can easily upload the information about the asset you are currently managing or upload an eGatherer information file collected from another computer. When you use this feature, you do not have to type in any information about location or a description of the computer.

This page is best suited for uploading existing information or for a simple upload of the information about the client for storage in the database. For more accurate information, we recommend that you use the Register Asset feature instead of the Update Asset Scan. See 3.5.2, “Register Asset” on page 140 for more information.

The functions described in this section will be the same for all users.

Note: The illustrations used in this section were created by a user with administrator rights. The menu names are the same.

The instructions for accessing Upload Asset Scan are:

1. Log on to the system as described in 3.3, “Logging on to System Information Center” on page 128. The main page (Figure 3-39) appears.

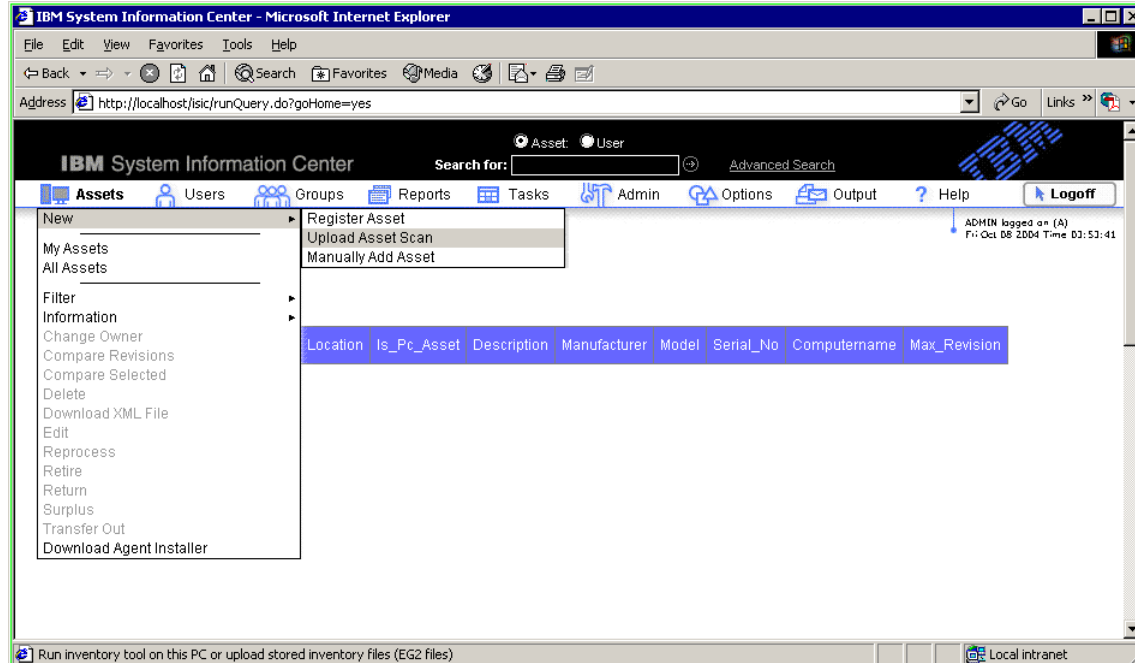


Figure 3-39 Main page

- From the main page, select **Assets** → **New** → **Upload Asset Scan** to open the Upload Asset Scan page (Figure 3-40).

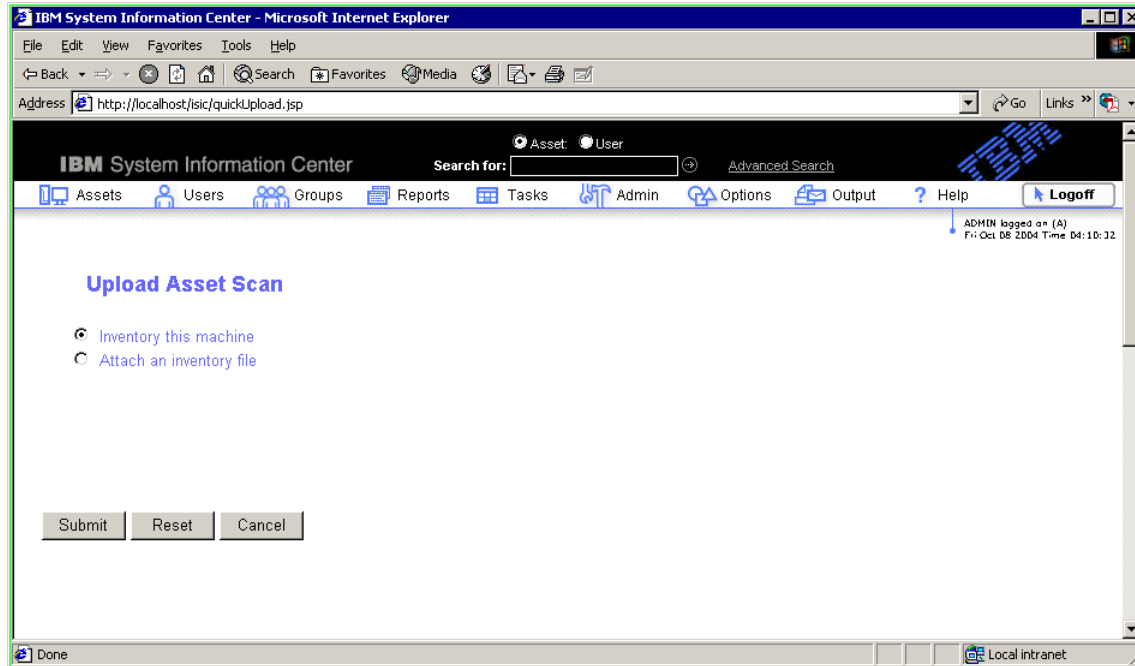


Figure 3-40 Upload Asset Scan page

Note: If you are using the asset upload function on the client for the first time, a security message may open and ask if you would like to install and run IBM System Information Gatherer. To use System Information Center automatic features, click **Yes**.

On the Upload Asset Scan page, there are two alternatives:

- ▶ Inventory this machine
- ▶ Attach an inventory file

Inventory this machine

This feature allows users to inventory the machine they are currently using, and upload current information. If the asset has been previously registered by an Upload Asset Scan, it will refresh the information currently stored for that asset. If not, it will generate a new record for the asset without the location information.

To inventory the machine, perform the following steps:

1. From the Upload Asset Scan page, select **Inventory this machine**.
2. Click **Submit**. The machine will start the eGatherer client and submit the information it gathers to the server. This procedure will take approximately 10 to 20 seconds, depending on the speed of the computer and network.
3. When the computer has uploaded the information to the System Information Center server, the machine you are using will return to the System Information Center main page. It will take 20 to 30 seconds to update the information in the database, so you may not see the updated information immediately. We recommend waiting 30 seconds. Then, to see the updated information, refresh the page.

Attach an inventory file

This feature allows users to import a file from another machine and upload it to the System Information Center database. This feature is used if you would like to import a system information file gathered from a computer that is not connected to the same network as the System Information Center server, or if you cannot connect to it. To take advantage of this feature, you must run the eGatherer client on the computer you would like to gather the information from. Then, you must migrate the output file from this application to machine that can communicate with the System Information Center server.

To use the inventory file function, perform the following steps:

1. From the Upload Asset Scan page (Figure 3-40 on page 136) select **Attach an inventory file**. Click **Submit** to open the window illustrated in Figure 3-41 on page 138.

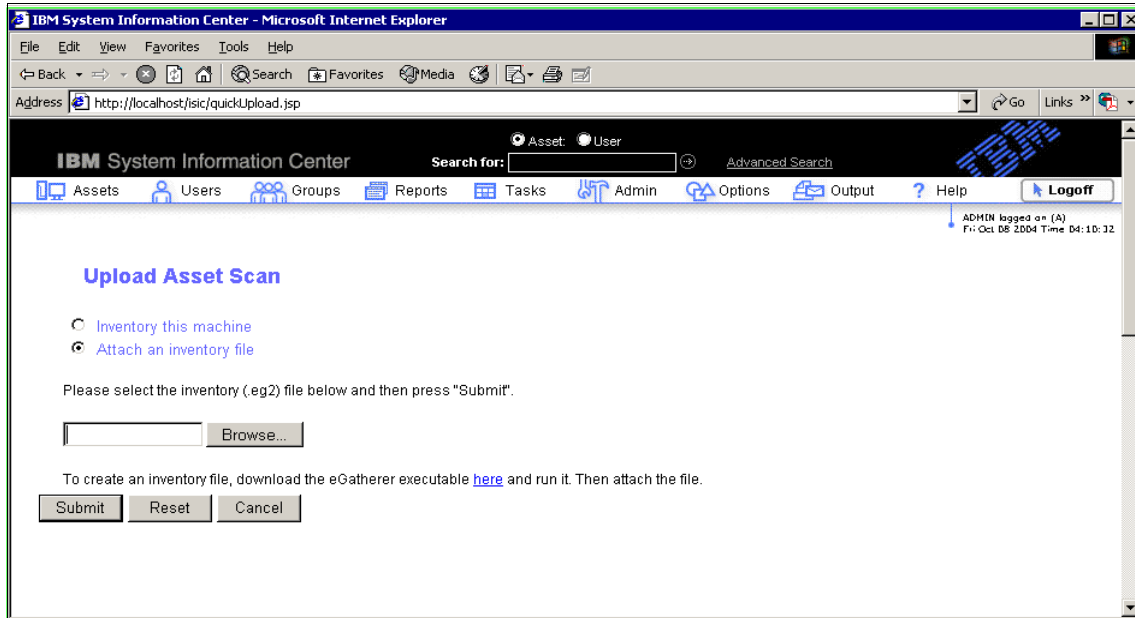


Figure 3-41 Attach an inventory file

2. If you do not have the eGatherer client, click the link at the bottom of the page to download it locally.
3. Copy the egather2.exe file to the machine you would like to gather information from.
4. Start the egather2.exe utility on the client. This opens a new window (Figure 3-42 on page 139).

```

Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

c:\>cd egatherer

c:\egatherer>egather2

IBM Technical Support Information Gatherer
(c) Copyright 2000-2004 IBM Corporation
Version 2.37 Lynx OEM

Install Driver ..... OK
Create XML Output File ..... OK
Create Gatherer File ..... OK
SYSTEM SUMMARY ..... OK
TIME ZONE ..... OK
SCSI Devices ..... OK
IDE DEVICE INFORMATION ..... OK
SMBIOS INFORMATION ..... OK
LOGICAL DISK INFORMATION ..... OK
DISPLAY INFORMATION ..... OK
Windows Startup Information ..... OK
DEVICE DRIVERS AND SERVICES ..... OK
REGIONAL SETTINGS ..... OK
LIST OF RUNNING PROCESSES ..... OK
MEMORY INFORMATION ..... OK
PCI DEVICES ..... OK
PCI ADAPTER INFORMATION ..... OK
WORKSTATION SECURITY ..... OK
DEVICE MANAGER ..... OK
Installed Software ..... OK
NETWORK ..... OK
ASSETID ..... Failed
LOTUS NOTES ..... Not Found
SYSTEM EVENTS LOG ..... Not Found
IBM TUI Usage ..... Not Found
NT Application Event Log ..... OK
NT System Event Log ..... OK
Close XML Output File ..... OK
Close Gatherer File ..... OK
Remove Driver ..... OK
Run complete, rc = 0

c:\egatherer>

```

Figure 3-42 egather2.exe utility

5. After the utility has finished collecting information, a file is created. This file must be transferred to a machine with connectivity to the System Information Center server. The location of the file will vary depending on how you started the utility. If you used the command prompt mode, the file will be in the same directory as you started it from. If you used the utility in Windows Explorer mode, the file will be located on the desktop. If you cannot find the file, search for a file with an .eg2 extension.

The name of the file is created from several variables but it will always end with .eg2. As illustrated in Figure 3-42, the file name created for our test was IBM-2647T1U-78RCM98.EG2, and it is based on the machine type, model number, and serial number of the machine on which we ran the egather2 command. When you locate the file, copy it to a machine that has access to the System Information Center server.

6. After you have copied the file, return to the menu shown in Figure 3-41 on page 138. Click **Browse** and navigate to the correct file.

7. Select the file and click **Submit**. Your file containing the system information will be uploaded and processed on the System Information Center server.

3.5.2 Register Asset

To add location information along with the asset information uploaded to the System Information Center database, you should use this System Information Center feature. It can add more detailed information than the Upload Asset Scan.

The functions described in this section will be the same for all users.

Note: The illustrations used in this section were created by a user with regular user rights. The menu names are the same.

Note: If it is the first time the asset upload function has been used on the client, you may receive a security message. This message asks you if you would like to install and run IBM System Information Gatherer. You must click **Yes** to use the automatic features of System Information Center.

Use the Register Asset feature as follows:

1. Log on to System Information Center as described in 3.3, “Logging on to System Information Center” on page 128.
2. From the main page (see Figure 3-38 on page 134), select **Assets** → **New** → **Register Asset**. A new page (Figure 3-43 on page 141) opens.

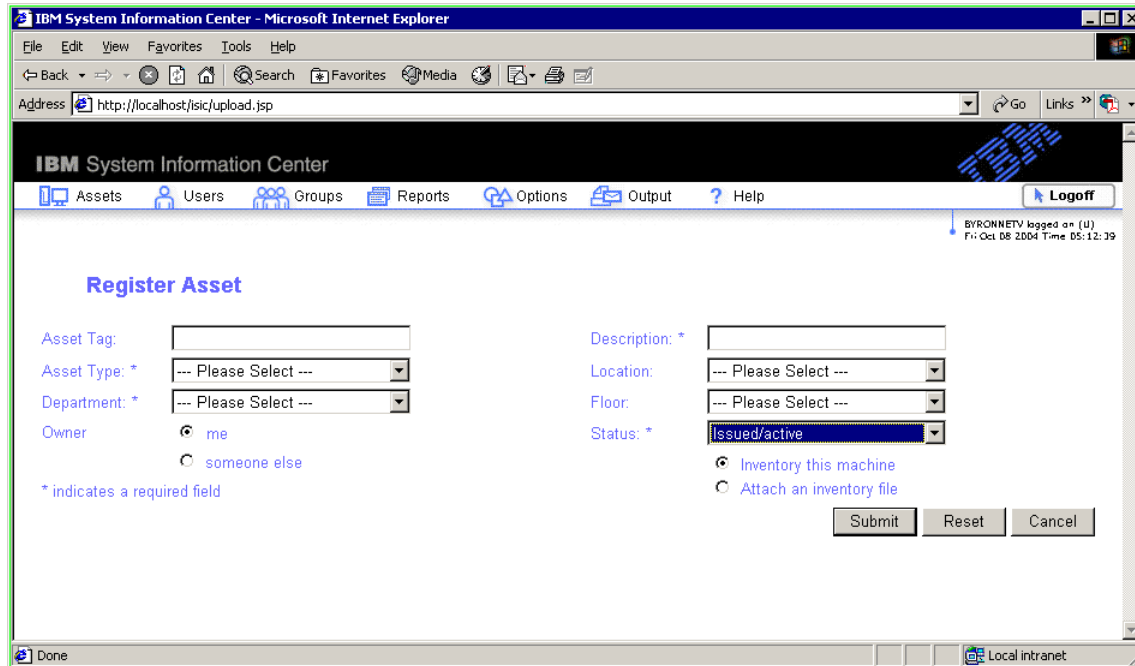


Figure 3-43 Register Asset page

3. Enter information in the available fields. The fields marked with an asterisk (*) are required. You must make a selection from the menus in these fields to continue. If the menus are empty or do not contain the information you want, select **Other**. A new field will appear below the menu that allows you to enter information you would like to add. The information you enter in that field will be available for other users through the menu as soon as you submit the asset.

Figure 3-44 on page 142 is an example of the Register Asset page looks like when you select **Other** because the menus do not contain information that is specific to your location or demographics.

Compare Figure 3-43 with Figure 3-44 on page 142 to get an understanding of the fields that are added with **Other** is selected in a required field.

Note: The System Information Center Administrator should determine and specify the selections available in these menus to ensure consistent demographic and location information throughout an enterprise.

IBM System Information Center - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print

Address http://localhost/isic/upload.jsp Go Links

IBM System Information Center

Assets Users Groups Reports Options Output ? Help Logoff

BYRONNETV logged on (U)
Fri Oct 08 2004 Time 05:12:39

Please enter a description

Register Asset

Asset Tag:

Asset Type: *

Please specify:

Department: *

Please specify:

Owner
☒ me
☐ someone else

* indicates a required field

Description: *

Location:

Please specify:

Floor:

Status: *

☒ Inventory this machine
☐ Attach an inventory file

Submit Reset Cancel

Done Local intranet

Figure 3-44 Other fields permitting location-specific input

4. You can add the asset to another existing user in the system. To do this, select **someone else**. (If **me** is selected, the asset is added to you.) You can then select which user will receive the asset from the menu that appears.
5. You can use an eGatherer file instead of uploading information about the machine you are logged in on. If you would like to add information from a file, select **Attach an inventory file** and select your inventory file. This is the same method you use with Upload Asset Scan.
6. After you made your selections, click **Submit**. The asset will be processed.

3.5.3 Manually Add Asset

You can manually add an asset to System Information Center on the Manually Add an Asset page. This page does not contain any form of automation. Therefore, any type of unit can be added. Examples of such devices are printers, PDA equipment, monitors, or computers.

If you would like to manually add an asset, perform the following steps:

1. Log on to the system as described in 3.3, "Logging on to System Information Center" on page 128.

- From the main page (Figure 3-38 on page 134), select **Assets** → **New** → **Manually Add Asset**. A new page that looks like Figure 3-45 opens.

IBM System Information Center - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print

Address http://localhost/lsic/addOtherAsset.jsp Go Links

IBM System Information Center

Assets Users Groups Reports Options Output Help Logoff

BYRONNETV logged on (U)
Fri Oct 08 2004 Time 05:45:43

Manually Add an Asset

Asset Tag:

Asset Type: *

Department: *

Manufacturer: *

Model: *

Owner

☒ me

☐ someone else

* indicates a required field

Description: *

Location: *

Floor: *

Status: *

Serial: *

☒ PC asset

☐ Non-PC Asset

Submit Reset Cancel

Done Local intranet

Figure 3-45 Manually Add an Asset page

- Enter the information. The fields marked with an asterisk (*) are required. These fields must have values or you cannot continue.
- If you would like to add the asset to another user, select **someone else** and select the desired user.
- When you are finished adding all the information, click **Submit**. The information will be added to the System Information Center database.

3.5.4 My Assets

This menu item allows you to view the assets currently linked to the logged on user. Follow the instructions below to use it:

- From the main page (see Figure 3-38 on page 134), select **Assets** → **My Assets**. This opens a new page that shows the assets currently allocated to your user profile.

3.5.5 All Assets

This menu provides you with a list of all the assets in System Information Center. To use this feature, take the following steps

1. From the main page (Figure 3-38 on page 134), select **Assets** → **All Assets**.
2. A new page will appear that shows all assets in the system.

3.5.6 Filter

Use this feature to filter other tasks you perform in System Information Center as follows:

1. From the main page (Figure 3-38 on page 134), select **Assets** → **Filter**. You may see as many as four possible filter types:
 - Asset Info By Selected Asset Type
 - Asset Info By Selected Location
 - Asset Info By Selected Location And Asset Type
 - Asset User
2. Select the appropriate choice.
3. A new list of assets based on the selection you did will appear in a new page.

3.5.7 Information

You can use the Information selection to view more advanced details about an asset. You can do this as follows:

1. From the main page (Figure 3-38 on page 134), select **Assets** → **All Assets**.
2. Select the asset you would like more information about.
3. From the main page, select **Assets** → **Information**. You will be able to select from one of the following information types:
 - Asset Device Drivers
 - Asset History
 - Selected Asset Information
 - Software for Selected Asset
4. Select the appropriate choice.

The following sections provide more information about the different selections.

Asset Device Drivers

Selecting **Asset Device Drivers** opens a list of drivers for the selected asset. You only obtain driver information for the assets that are uploaded to the server through automation; information for assets that you have entered manually are not provided.

Asset History

Selecting **Asset History** opens a history log of the selected asset. This is used mainly for verifying whether updates were processed successfully.

Selected Asset Information

Selecting **Asset Information** opens a page showing all the information stored about an asset including location information.

Software for Selected Asset

Selecting this menu item opens a page that shows all the software installed on the selected computer.

When a specific software item is selected from the list of software installed on a machine, the Filter menu (described in 3.5.6, “Filter” on page 144) features two new items:

1. Models With Selected Software
2. Models Without Selected Software

When you select one of the applications and use this filter function, you obtain a list of all machines with a specific application installed. This feature is very useful for locating prohibited software in your network. If, for example, a peer-to-peer program is prohibited, you can find a machine with that software on it and then request a list of all other machines with this software.

3.5.8 Users

This menu item is used to see which assets are assigned to a user. To take advantage of this feature, take the following steps:

1. Follow the procedure to show all users. From the main page (Figure 3-38 on page 134), select **Users** → **All Users**.
2. Indicate the user by selecting the check box labeled with the user name.
3. Select **Assets** → **Users** → **Users Assets**. This opens a new page that shows the assets assigned to the selected user.

3.5.9 Change Owner

This menu item is used to change the owner (in System Information Center) of an asset. If detailed reporting is required, it is important that the asset is bound to the correct user.

1. From the main page (Figure 3-38 on page 134), select **Assets** → **All Assets**.
2. Select the asset for which you would like to change the owner. You can select the asset by various means. However, you must select an asset.
3. Select **Assets** → **Change Owner**. This opens a new page (Figure 3-46).

IBM System Information Center - Microsoft Internet Explorer

Address: http://localhost/jsic/processTransfer.do?action=ChangeOwner&row=2

IBM System Information Center

Search for: [] Advanced Search

Assets Users Groups Reports Tasks Admin Options Output Help Logoff

ADMIN logged on (A)
Sun Oct 10 2004 Time 03:52:40

Action is to change the owner of the selected asset(s)

HWKEY	USERKEY	FORENAME	SURNAME	ASSETTAG	ASSETTYPE	MANUFACTURER	MODEL	SERIAL_NO	COMPUTERNAME	MAX_REVISION
2	2	Byron	Braswell		NetVista	IBM	831048U	KADW039	BYRONNETV	1

User search [] Select User [Braswell, Byron (ROAMINGT41)]

Enter a reason if appropriate [] Select Yes to approve transaction [No]

Submit Reset Cancel

Figure 3-46 Changing the owner of an asset

4. Select the user to whom you wish to transfer the asset from the menu provided or perform a search for that user.
5. Enter a reason for the transfer if appropriate in the field provided.
6. Select **Yes** in the second dropdown menu to approve the transaction.
7. Click **Submit**. The asset transfers to the new user and the System Information Center main page opens again.

3.5.10 Compare Revisions

The Compare Revisions feature is used to compare different revisions of the system information stored about an asset. For example, if you make a change on a machine, and then perform a new asset upload, it will create a new revision of the computer in the System Information Center database. If you have the IBM System Information Gatherer client installed on the asset, it will automatically update the asset when you make a change.

To use this feature, follow these instructions:

1. From the main page (Figure 3-38 on page 134), select **Assets** → **All Assets**.
2. Select the asset you for which you wish to compare revisions. You can select the asset by various means. However, you must select an asset.
3. Select **Assets** → **Compare Revisions** to open the System Information page (Figure 3-47).

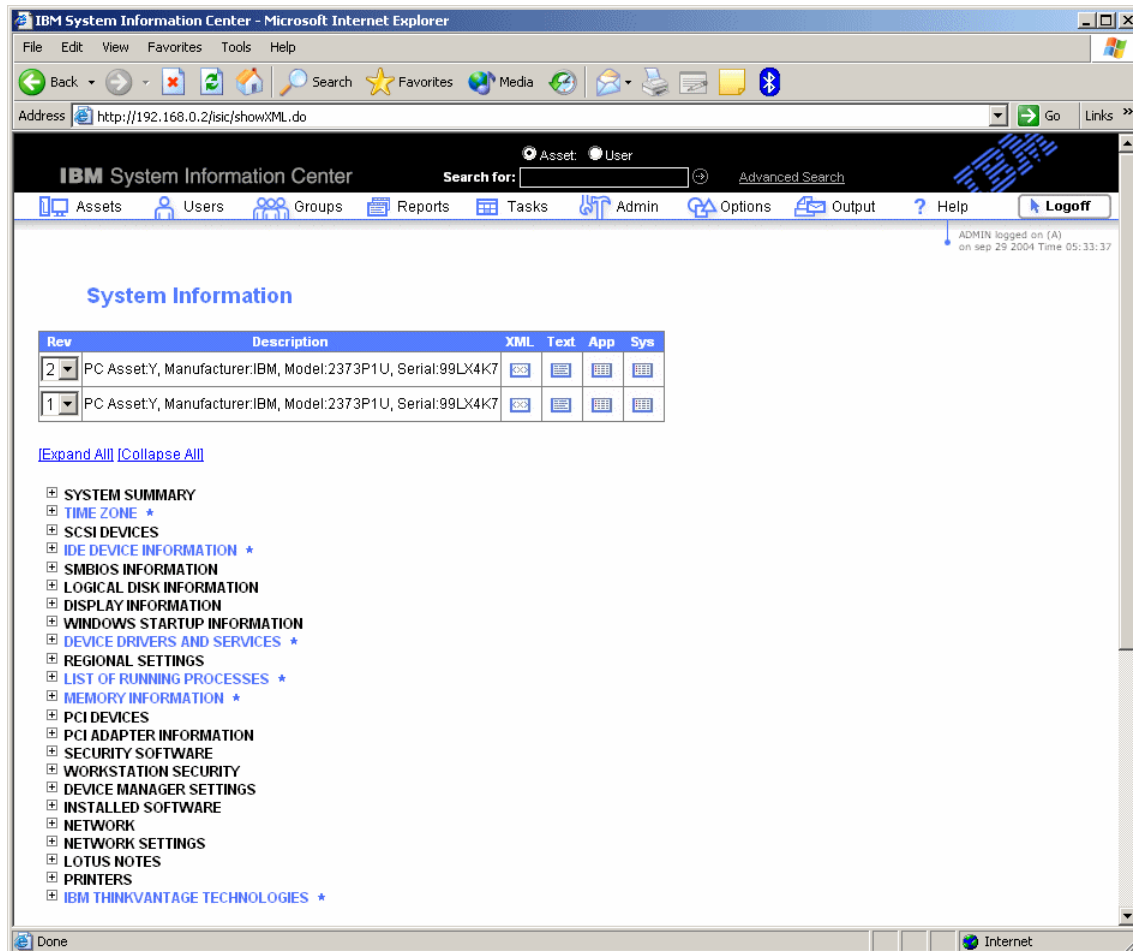


Figure 3-47 Comparing revisions

4. Select the different versions of system information you would like to compare from the menus on this page. The items that are marked in blue indicate that there is a difference between the selected revisions for that specific item.

3.5.11 Compare Selected

This System Information Center feature can compare two different machines and show the user the differences between them.

To use this feature, take the following steps:

1. From the main page (Figure 3-38 on page 134), select **Assets** → **All Assets**.
2. Select the assets you would like to compare.
3. Select **Assets** → **Compare Selected** to open the page shown in Figure 3-48.

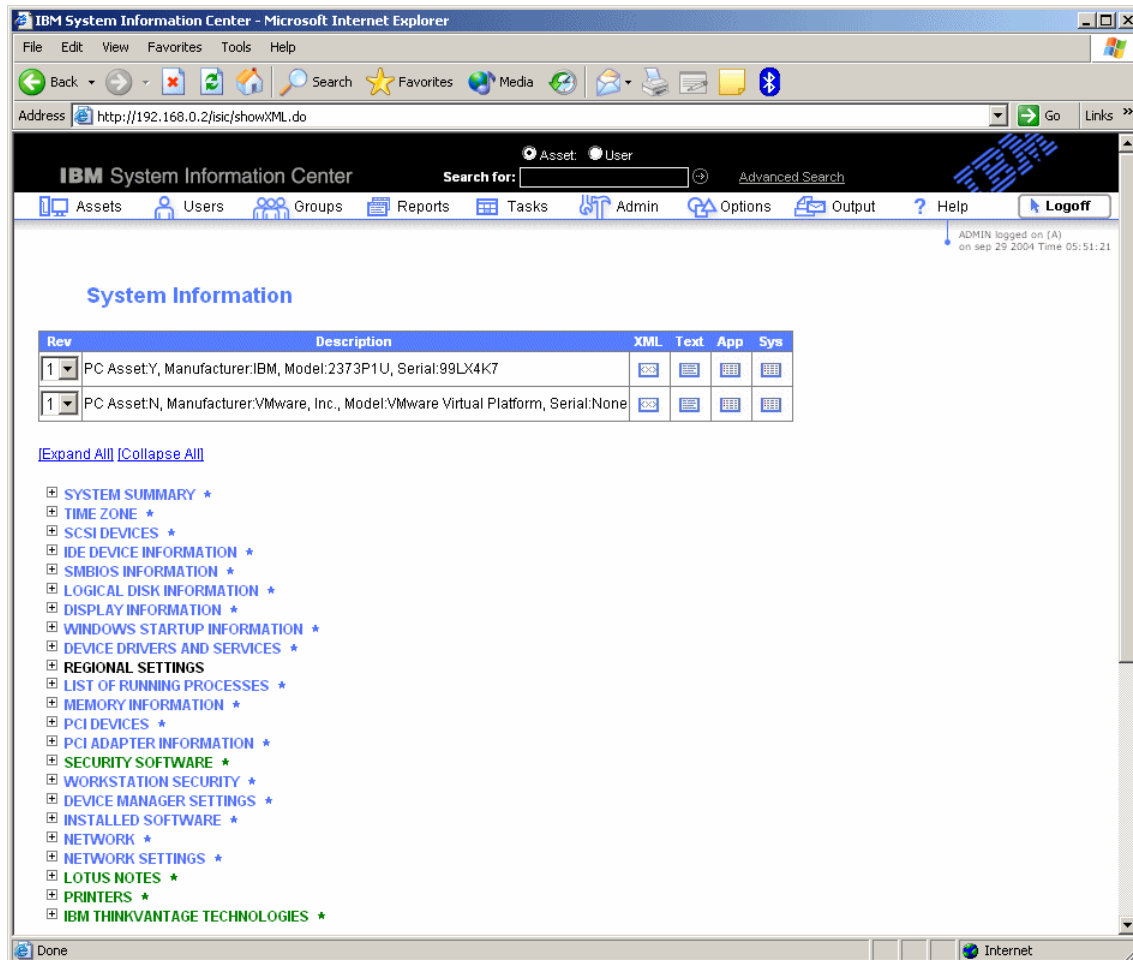


Figure 3-48 Comparing selected assets

4. You can now compare the different assets by looking at the fields marked in another color.

3.5.12 Delete

System Information Center has a feature that allows you to delete an asset from the System Information Center database. Once the deletion is made, no tracking information will remain.

To delete an asset, follow these instructions:

1. From the main page (Figure 3-38 on page 134), select **Assets** → **All Assets**.
2. Select the asset you would like to delete.
3. Select **Assets** → **Delete**. This opens the page shown in Figure 3-49.

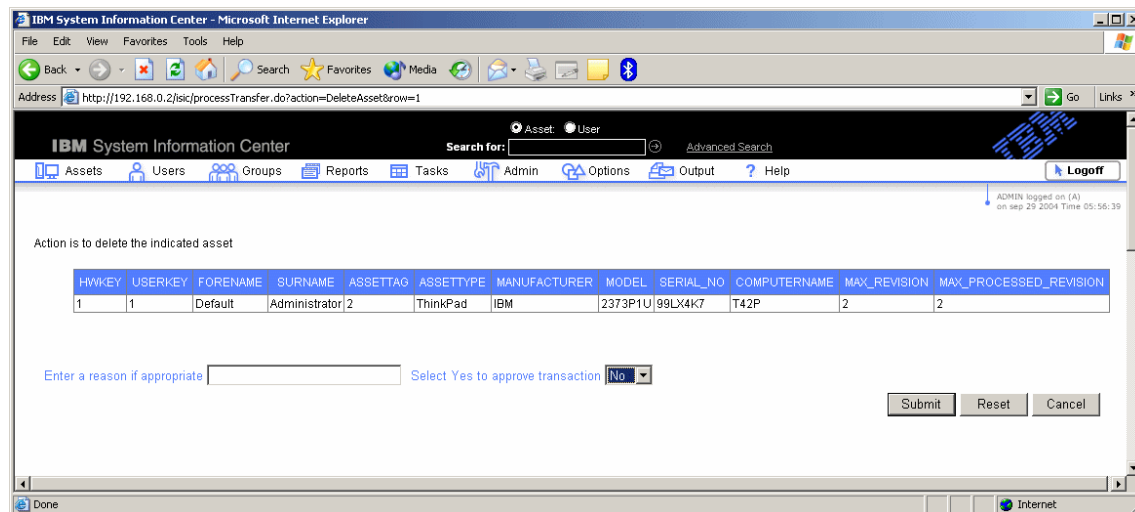


Figure 3-49 Delete asset from the System Information Center database

4. Enter a reason if appropriate.
5. Select **Yes** in the menu to approve the transaction.
6. Click **Submit**.
7. The selected asset is deleted. You will be returned to the main page.

3.5.13 Download XML file

Use this feature when you would like to download the asset information as an XML file, which can be used in other compliant software.

1. From the main page (Figure 3-38 on page 134), select **Assets** → **All Assets**.
2. Select the asset for which you would like to download an XML file.

3. Select **Assets** → **Download XML file**.
4. A prompt asks you if you would like to save or run the file.
5. Click **Save** to save the file at the desired location.

3.5.14 Edit

Use this feature to edit either a manually added or an automatically added asset as follows:

1. From the main page (Figure 3-38 on page 134), select **Assets** → **All Assets**.
2. Select the asset you would like to edit.
3. Select **Assets** → **Edit** to open a page like that shown in Figure 3-50.

The screenshot shows the 'Update Asset Details' page in the IBM System Information Center. The page title is 'Update Asset Details' and the instruction is 'Update asset details and press submit to continue'. The form contains the following fields:

- Manufacturer: IBM
- Model: 23739HU
- Description: ThinkPad T41
- Asset Type: --- Please Select ---
- Department: --- Please Select ---
- PC asset: false
- Serial: KP9Z511
- Asset Tag:
- Location: --- Please Select ---
- Floor: --- Please Select ---
- Status: Issued/active

At the bottom right, there are three buttons: Submit, Reset, and Cancel. The browser window title is 'IBM System Information Center - Microsoft Internet Explorer' and the address bar shows 'http://localhost/isic/updateAssetInfo.do?row=3'.

Figure 3-50 Edit asset details

4. Edit the desired fields.
5. Click **Submit**. The changes will be saved and you will return to the main page.

3.5.15 Reprocess

This feature reprocesses the data for an asset. You may use it to override corrupted data in the System Information Center database as follows:

1. From the main page (Figure 3-38 on page 134) click **Assets** → **All Assets**.
2. Select the asset you would like to reprocess.
3. From the main page (Figure 3-38 on page 134) click **Assets** → **Reprocess**.
4. The selected asset will be reprocessed and you will be returned to the main page.

3.5.16 Retire

Retiring stores information about an asset in the database for later use. Use this feature as follows:

1. From the main page (Figure 3-38 on page 134), select **Assets** → **All Assets**.
2. Select the asset you would like to retire.
3. Select **Assets** → **Retire** to open a page like that shown in Figure 3-51.

IBM System Information Center - Microsoft Internet Explorer

Address: http://192.168.0.2/isic/processTransfer.do?action=Retire&row=2

IBM System Information Center

Search for: [] Asset: [] User: [] Advanced Search

Assets Users Groups Reports Tasks Admin Options Output Help Logoff

ADMIN logged on (A) on Sep 29 2004 Time 06:27:42

Action is to retire the indicated asset

HWKEY	USERKEY	FORENAME	SURNAME	ASSETTAG	ASSETTYPE	MANUFACTURER	MODEL	SERIAL_NO	COMPUTERNAME	MAX_REVISION	MAX_PROCESSED_REVISION
3	1	Default	Administrator	1	ThinkPad	IBM	2373P1U	99LX4K7	T42P	1	1

Enter a reason if appropriate [] Select Yes to approve transaction [No]

Submit Reset Cancel

Figure 3-51 Retire an asset

4. Enter a reason if required.
5. Select **Yes** to approve the retirement.
6. The selected asset is reprocessed and you return to the main page.

3.5.17 Return

Use this feature to submit a request to return an asset that is registered in System Information Center to the leasing company as follows:

1. From the main page (Figure 3-38 on page 134) click **Assets** → **All Assets**.
2. Select the asset you would like to return to the leasing company.
3. Select **Assets** → **Return** to open the page illustrated in Figure 3-52.

The screenshot shows the IBM System Information Center interface in a Microsoft Internet Explorer browser window. The address bar shows the URL: `http://192.168.0.2/isic/processTransfer.do?action=Return&row=2`. The page header includes the IBM logo and navigation tabs: Assets, Users, Groups, Reports, Tasks, Admin, Options, Output, and Help. A search bar is present with a 'Search for:' field and a 'Logoff' button. A message indicates 'ADMIN logged on (A) on sep 29 2004 Time 06:32:33'. The main content area features a table with the following data:

HWKEY	USERKEY	FORENAME	SURNAME	ASSETTAG	ASSETTYPE	MANUFACTURER	MODEL	SERIAL_NO	COMPUTERNAME	MAX_REVISION	MAX_PROCESSED_REVISION
3	1	Default	Administrator	1	ThinkPad	IBM	2373P1U	99LX4k7	T42P	1	1

Below the table, there is a form with the following elements:

- A text input field labeled 'Enter a reason if appropriate'.
- A dropdown menu labeled 'Select Yes to approve transaction' with 'No' selected.
- Three buttons: 'Submit', 'Reset', and 'Cancel'.

Figure 3-52 Return asset

4. Enter a reason if required.
5. Select **Yes** to approve the return request.
6. A transfer request for the asset is sent to the Administrator.

3.5.18 Surplus

To designate an asset as surplus in the System Information Center database, take the following steps:

1. From the main page (Figure 3-38 on page 134), select **Assets** → **All Assets**.
2. Select the asset you would like to designate as surplus.
3. Select **Assets** → **Surplus**. This opens the page shown in Figure 3-53 on page 154.

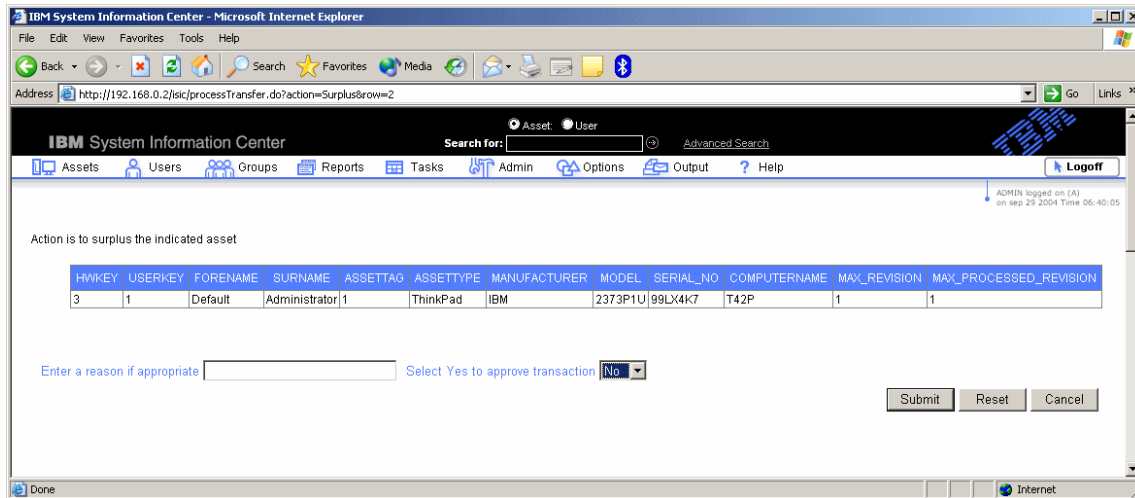


Figure 3-53 Surplus an asset

4. Enter a reason if for surplus if required.
5. Select **Yes** in the menu to approve the surplus request.
6. The selected asset will be marked as surplus in the database and you will be returned to the main page

3.5.19 Download Agent Installer

Use Download Agent Installer to download the IBM System Information Gatherer agent installer (isig_oem.exe) to the machine you are currently using. This is an alternative to installing the agent from the System Information Center CD. (For more information about this agent, see 3.13, “IBM System Information Gatherer” on page 210.) To take advantage of this feature, follow this procedure:

1. From the main page (Figure 3-38 on page 134), select **Assets** → **Download Agent Installer**. A prompt asks you if you would like to save or run the file.
2. Click **Save** to save the file at the desired location or **Run** to install the application immediately.
3. If you clicked **Save**, execute the downloaded file to install the IBM System Information Gatherer agent on your client system. (See 3.13.2, “Permanently installed client agent” on page 211 for additional information.)

3.6 User Management

To be able to use the System Information Center, you must have at least one user defined in the system. System Information Center supports three different user account types:

- ▶ User account

User account functions work with asset information specifically belonging to that user. Examples include adding assets, viewing asset history, comparing asset information, and processing an asset transfer request. Most accounts within a business are User accounts.

- ▶ Superuser account

Superusers can perform the same tasks that users can, as well as more advanced functions such as developing specialized asset reports and viewing asset information across an enterprise.

- ▶ Administrator account

Administrators can perform the same tasks that users can and can also modify asset information across an enterprise, e-mail asset information, schedule asset scans, and approve asset requests.

Note: An administrator user account called *admin* is created automatically when System Information Center is installed. The password is *password*.

The number of System Information Center users defined on the system depends on the needs and requirements of your company's business policy. If you wish to add, change or delete users, your System Information Center user ID must have system administrator rights. User account type is an attribute that can be edited with the user management functions provided by System Information Center.

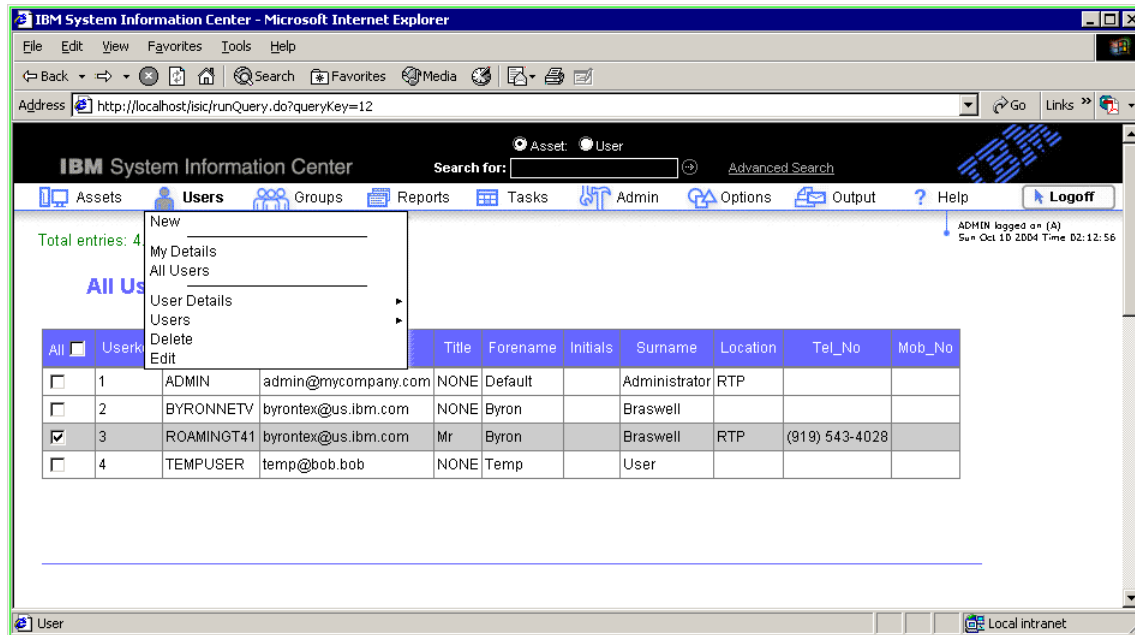


Figure 3-54 Users menu

From the Users menu (Figure 3-54), you can perform the following tasks:

- ▶ Create a new user
- ▶ Check the details of a user currently logged on to System Information Center
- ▶ View all users
- ▶ View selected user details
- ▶ View selected user information
- ▶ View selected user history
- ▶ Delete selected user
- ▶ Edit selected user

The only menu item non-administrators have is the **My details** function that shows the user information. All the other menu items are available only while logged on to an Administrator account.

3.6.1 Creating a new user

To create a new user in System Information Center, complete the following procedure:

1. From the main page (Figure 3-54), select **Users** → **New** to open the page shown in Figure 3-55 on page 157.

IBM System Information Center - Microsoft Internet Explorer

Address: http://localhost/Isic/register.jsp

IBM System Information Center

Search for: [] Advanced Search

Assets Users Groups Reports Tasks Admin Options Output ? Help Logoff

ADMIN logged on (4)
Sun Oct 10 2004 Time 12:27:23

Add User

User ID: * [hfenblatt@mycompany.com] Number/Street: [21 Baker]

Email address: [hfenblatt@mycompany.com] Building: [O-2]

Title: [----- Please Select -----] Town: [London]

Forename: * [Heinrick] Country: [UK]

Surname: * [Fienblatt] Postcode: [W-4567]

Preferred name: [Rick] Office Number: [44 207 666666]

Employee ID: [1040] Mobile Number: []

Department: [P-EYE] Password: * []

Location: [HQ] Please retype password: * []

Do you wish to register an asset? ☒

* indicates a required field

Submit Reset Cancel

Figure 3-55 Add User page

2. Enter the information requested. The fields marked with an asterisk (*) are required fields. These mandatory fields were designated during the installation of System Information Center.

If you would like to register an asset after adding the user, select **Do you wish to register an asset?** When all the requested information is filled in, click **Submit**.

3. If you indicated that you wished to register assets, the asset registration page opens. If you did not, you will return to the main menu.

3.6.2 My Details

This menu item is used if you want to check the details of the current logged on user. While logged on as an Administrator, you also have the possibility to change the settings of any user. To use My Details, select **Users** → **My Details** from the main menu (Figure 3-54 on page 156). This opens a new page that shows your information.

3.6.3 All Users

If an administrator wants to see a list of all the users defined in the System Information Center system, he or she can use the All Users feature. This is also the feature an administrator must select to edit other users defined to System Information Center.

From the main page (Figure 3-54 on page 156), select **Users** → **All Users** to open a new page that shows a list of all users defined to System Information Center.

3.6.4 User Details

To retrieve basic location information about a selected user, an administrator can use the User Details feature by following these steps:

1. From the main page (Figure 3-54 on page 156), select **Users** → **All Users**.
2. From the list of available users, select the specific user.
3. Select **Users** → **User Details** → **Selected User Details** to open a new page that shows all the details of the selected user.

System Information Center users with an account type of *User account* cannot use this feature. They can, however, see details for their account using the My Details feature. For more information, see 3.6.2, “My Details” on page 157.

3.6.5 User History

Use this feature to display the operations that have taken place on a selected user's computer. To obtain the display, take the following steps:

1. From the main page (Figure 3-54 on page 156), select **Users** → **All Users**.
2. From the list of available users, select the specific user.
3. Select **Users** → **Users** → **User History** to open a page that shows the user's history.

3.6.6 Delete

Administrators can use this feature to delete a user from the System Information Center database as follows:

1. From the main page (Figure 3-54 on page 156), select **Users** → **All Users**.
2. From the list of available users, select the specific user to delete.
3. Select **Users** → **Delete** as shown in Figure 3-56 on page 159.

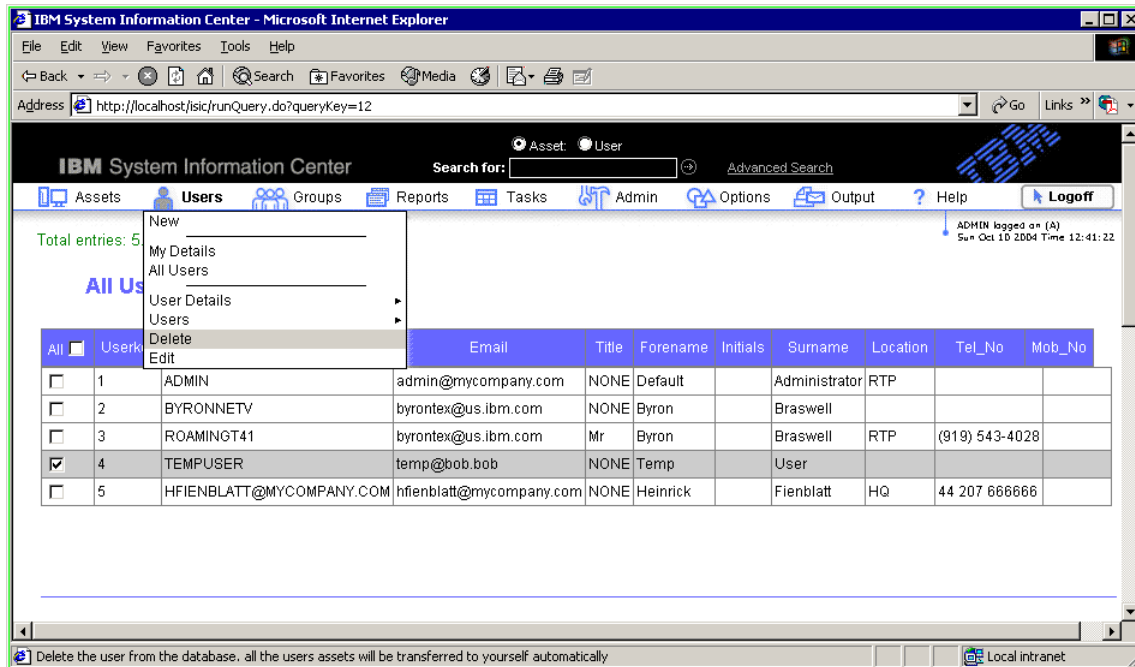


Figure 3-56 Select user to delete

4. A new page opens that looks like Figure 3-57.

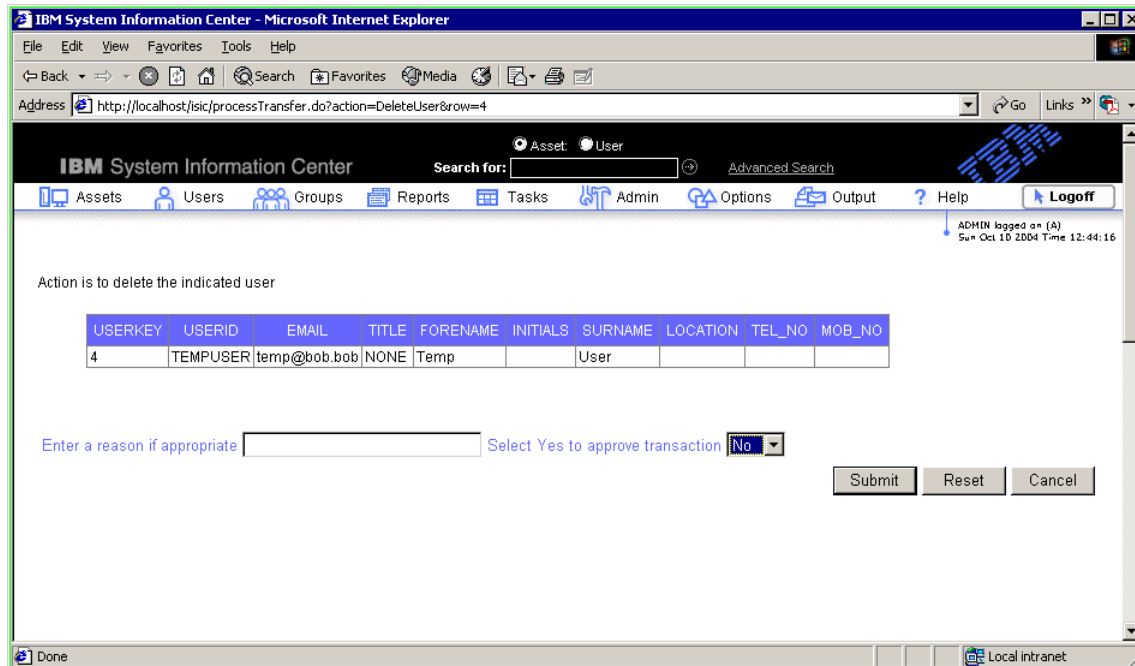


Figure 3-57 Delete user

5. Enter a reason if appropriate in the field provided and select **Yes** to approve the transaction.
6. Click **Submit**. The selected user will be deleted from the system. All assets belonging to that user will be automatically transferred to your administrator account.

3.6.7 Edit

This menu item is used to edit the details of a user. This menu item is also used by and Administrator to change the rights a user has to the system.

1. From the main page (Figure 3-54 on page 156), select **Users** → **All Users**.
2. From the list of available users, select the specific user to edit.
3. Select **Users** → **Edit** to open the Change details page (Figure 3-58 on page 161).

IBM System Information Center - Microsoft Internet Explorer

Address: http://localhost/isic/changeDetails.do?row=2

IBM System Information Center

Search for: [] Advanced Search

Assets Users Groups Reports Tasks Admin Options Output Help Logoff

ADMIN logged on (A)
Sun Oct 10 2004 Time 12:45:41

Change details

Update user details and press submit to continue

User ID: *	<input type="text" value="BYRONNETV"/>	Number/Street:	<input type="text" value="711 Maple St"/>
Email address:	<input type="text" value="byrontex@us.ibm.com"/>	Building:	<input type="text" value="B-72"/>
Title:	<input type="text" value="----- Please Select -----"/>	Town:	<input type="text" value="Bellview"/>
Forename: *	<input type="text" value="Jasper"/>	Country:	<input type="text" value="USA"/>
Surname: *	<input type="text" value="Weems"/>	Postcode:	<input type="text" value="68005"/>
Preferred name:	<input type="text" value="Jazz"/>	Office Number:	<input type="text" value="(402) 555 1212"/>
Employee ID:	<input type="text" value="172136"/>	Mobile Number:	<input type="text" value=""/>
Department:	<input type="text" value="Accounting"/>	Password:	<input type="password" value="*****"/>
Location:	<input type="text" value="West campus"/>	Please retype password:	<input type="password" value="*****"/>
Created:	<input type="text" value="2004-10-07 17:50:33.562"/>	Last Update:	<input type="text" value="null"/>
Password Expired: N		Authority:	<input type="text" value="User"/>

* indicates a required field

Submit Reset Cancel

Figure 3-58 Edit user

- Edit the fields. You can also change the selected user's type by selecting a different type in the Authority menu. When you have finished editing, click **Submit**. The changes you made are saved and you return to the main page.

3.7 Group management

With System Information Center, you can combine users into different groups. This allows you to maintain better control of your users by user type, location, or both. Group management is not a required function in System Information Center. However, the group function reduces the complexity of controlling and monitoring access to your system.

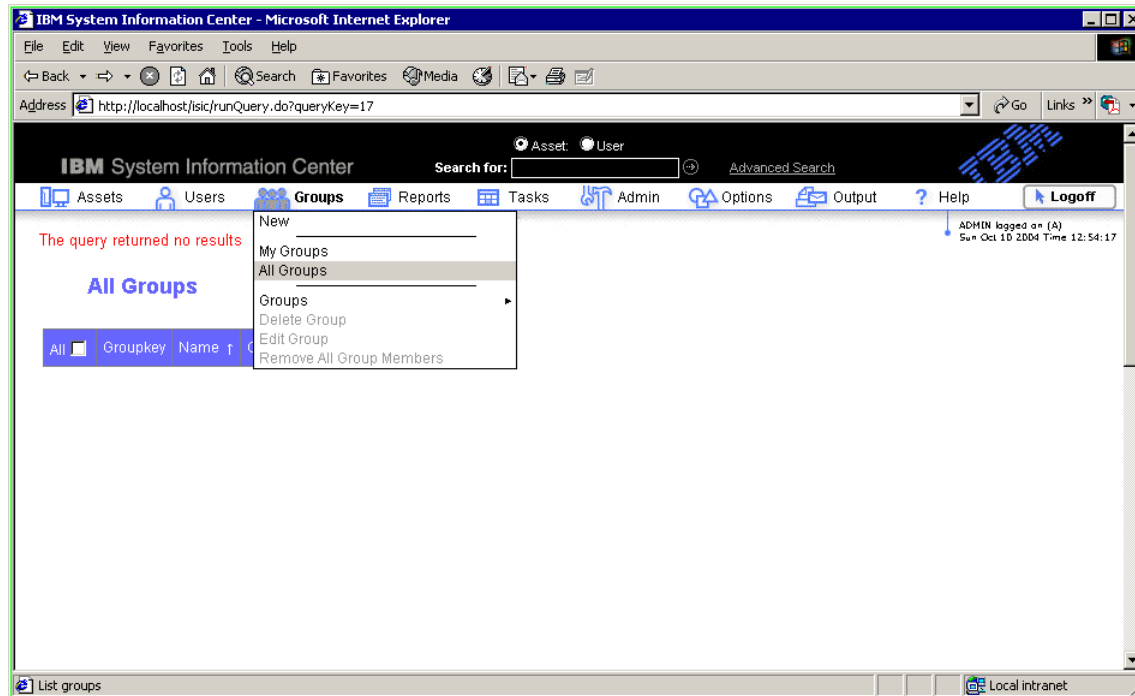


Figure 3-59 Group menu on main page

With group management and an administrator account, you can perform the following tasks from the Group menu illustrated in Figure 3-59:

- ▶ Create a new group
- ▶ View the group of a someone currently using System Information Center
- ▶ Look at all groups in the system
- ▶ Look at the members in a group
- ▶ Delete a group
- ▶ Edit a group
- ▶ Remove all group members

The only available function for those with an account type of *User account* is the **My Group** menu item.

3.7.1 New Group

New Group is used to create a new group in System Information Center as follows:

1. From the main page (Figure 3-59), select **Groups** → **New** to open the page shown in Figure 3-60 on page 163.

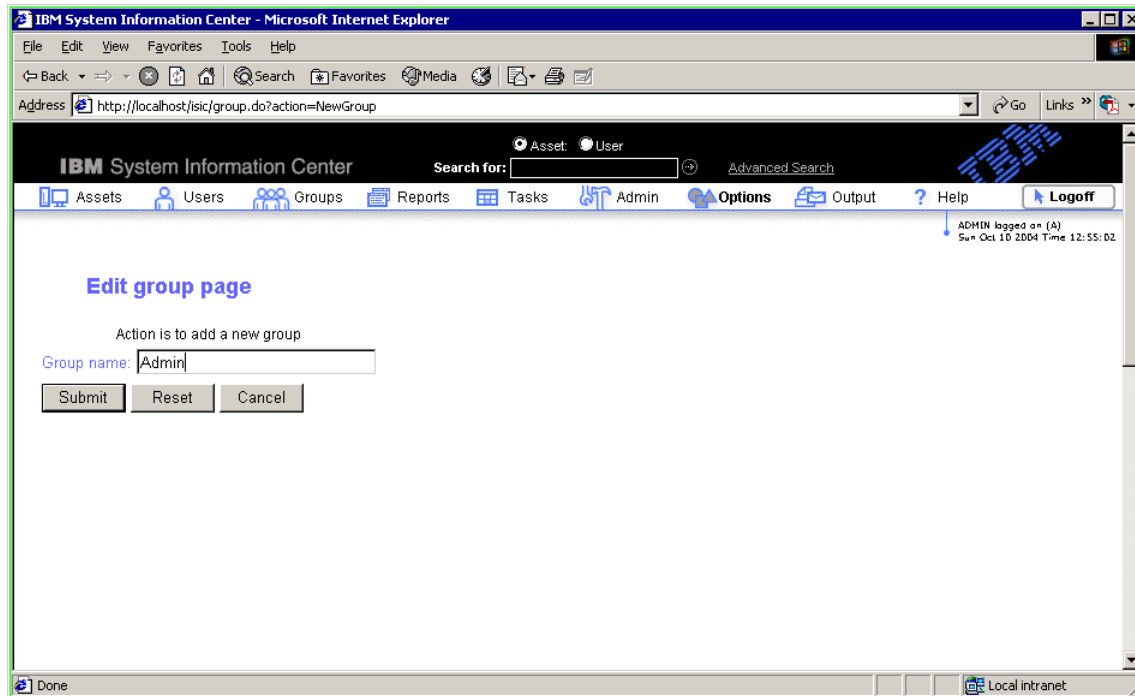


Figure 3-60 Edit group page

2. In the field marked **Group name**, enter the name of the group.
3. Click **Submit**. The group will be saved in System Information Center.

3.7.2 My Groups

A user logged on to System Information Center can use My Groups to view the groups to which he or she belongs. From the main page (Figure 3-59 on page 162), select **Groups** → **My Groups** to obtain a list of your groups.

3.7.3 All Groups

All Groups provides a list of all the groups that are defined for the System Information Center server. To use this feature, select **Groups** → **All Groups** from the main page (Figure 3-59 on page 162).

3.7.4 Groups

Use Groups to view the members of a specific group as follows:

1. From the main page, select **Groups** → **All Groups**.
2. In the All Groups list, select the group.
3. Select **Groups** → **Groups** → **Group Members**. This opens a new page that lists the members.

3.7.5 Add Users

Use this feature to add users to a group. The group must be created (see 3.7.1, “New Group” on page 162) before you are able to add users to a group as follows:

1. List all System Information Center users using the procedure described in 3.6.3, “All Users” on page 158.
2. From the list of available users, select the users you would like to add to a group.
3. Select **Groups** → **Add User(s) To Group** as shown in Figure 3-61.

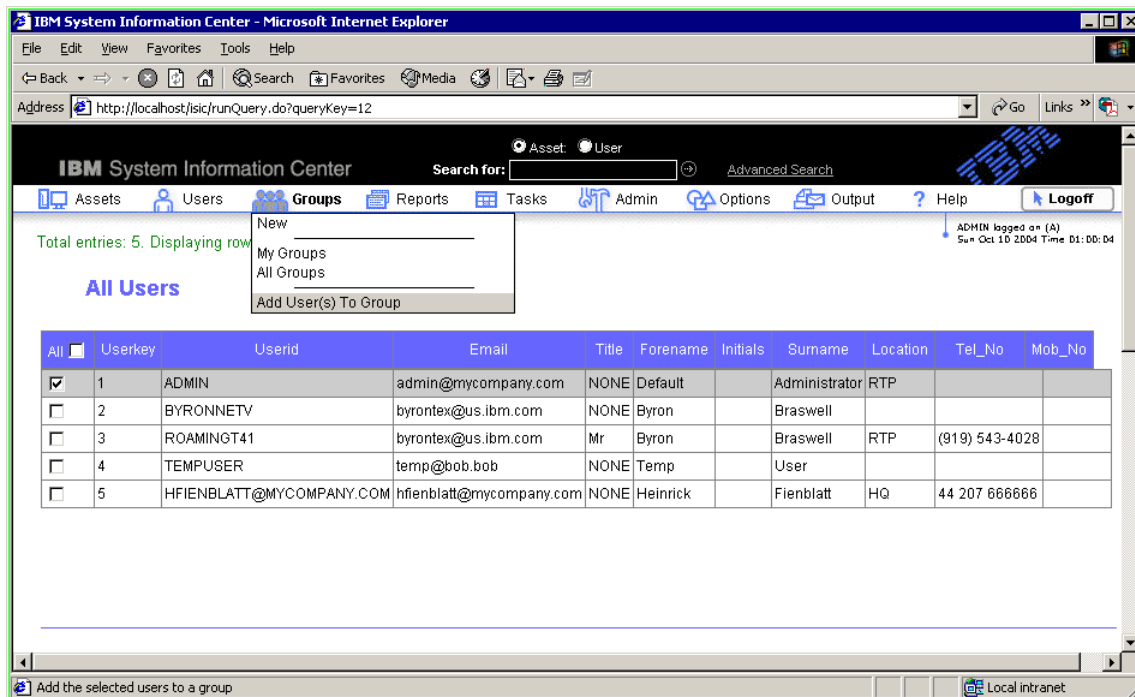


Figure 3-61 Add user(s) to a group page

This opens a new page (Figure 3-62).

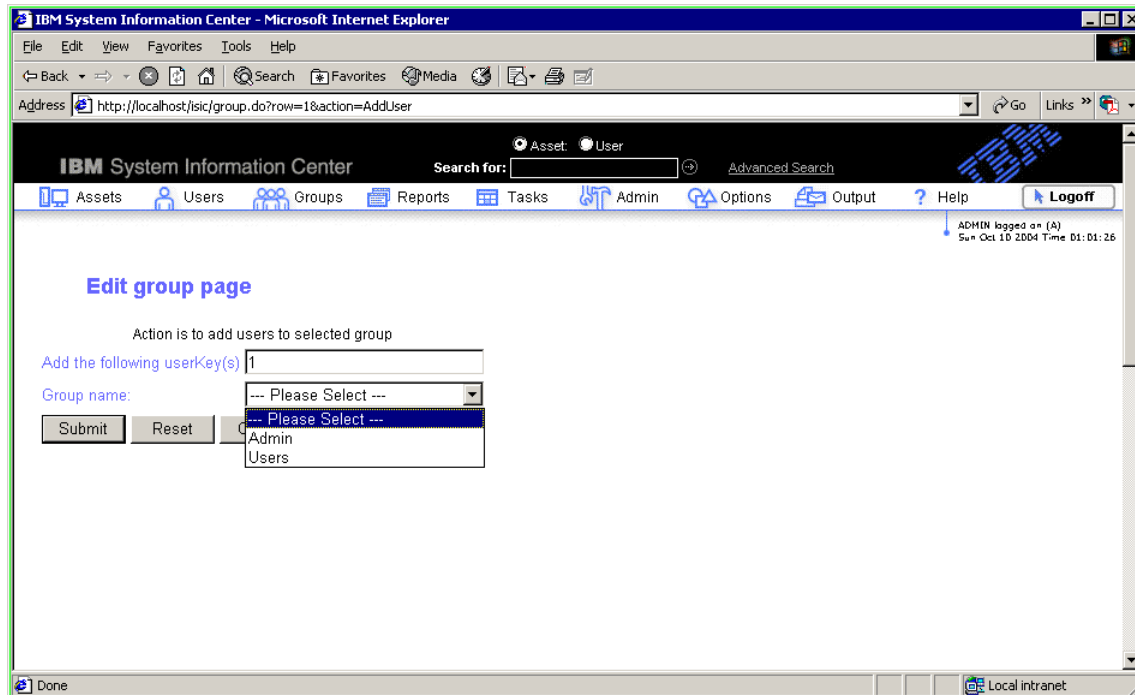


Figure 3-62 Add users to group

4. Select the group from the Group name menu.
5. Click **Submit** to add the user(s) to the group and return to the main page.

3.7.6 Delete Group

The procedure for deleting an existing group includes the following steps:

1. From the main page (Figure 3-59 on page 162), select **Groups** → **All Groups**.
2. From the list of groups, select the group you would like to delete.
3. Select **Groups** → **Delete Group**.

3.7.7 Edit Group

Edit the name of an existing group as follows:

1. From the main page (Figure 3-59 on page 162), select **Groups** → **All Groups**.

2. From the list of groups, select the group you would like to edit.
3. Select **Groups** → **Edit Group**. This opens a new page (Figure 3-63).
4. Enter the group name in the New group name field.
5. Click **Submit** to save the new group name and return to the main page.

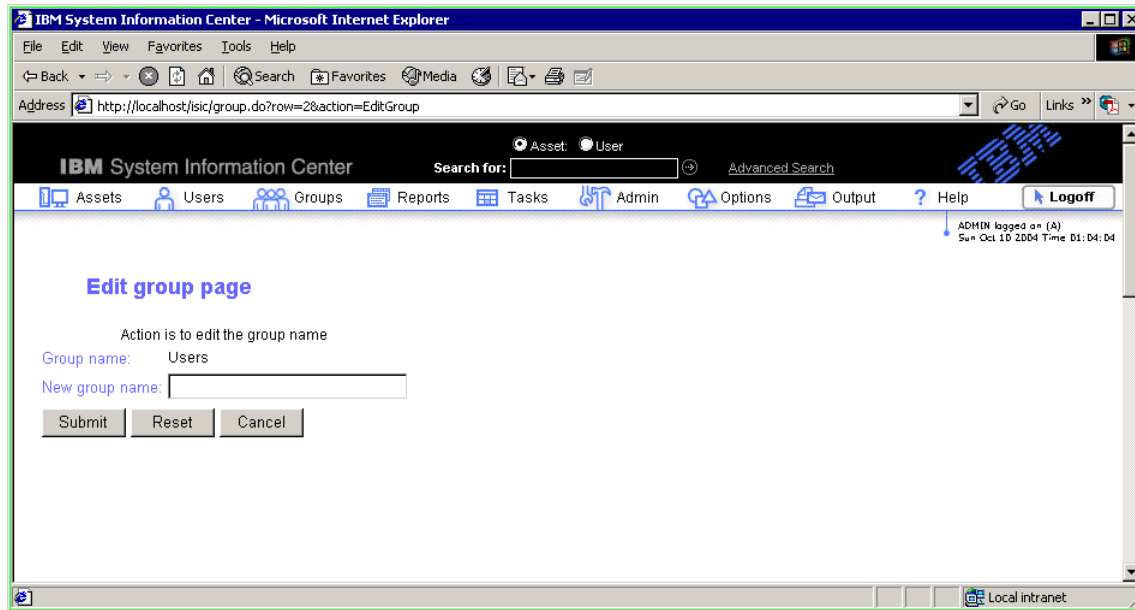


Figure 3-63 Edit group name

3.7.8 Remove All Group Members

The procedure for using this feature to remove all group members from a selected group includes the following steps:

1. From the main page Figure 3-59 on page 162), select **Groups** → **All Groups**.
2. From the list of groups, select the group you would like to edit.
3. Select **Groups** → **Remove All Group Members**.
4. All the users in the selected group are removed.

3.8 Reports

Reports are a powerful way to search the System Information Center database quickly for key information that is needed regularly. System Information Center supports two types of reports:

1. Common

These predefined reports are provided (predefined) with System Information Center. They are designed for generating general information from System Information Center database entries on a regular basis.

2. Custom

These are modified reports designed to generate information specific to your business requirements.

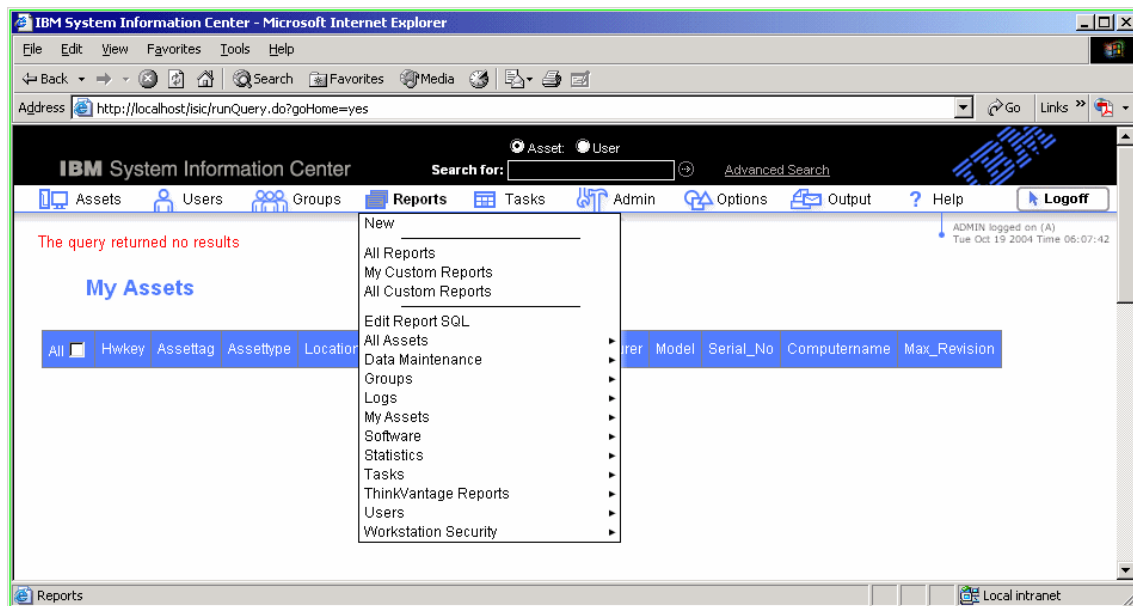


Figure 3-64 Reports menu on main page

The following reports are available from the Reports menu:

- ▶ New
- ▶ All Reports (see 3.8.12, “All Reports” on page 188)
- ▶ My Custom Reports
- ▶ All Custom Reports
- ▶ Edit Report SQL
- ▶ All Assets (see 3.8.1, “All Assets” on page 168)
- ▶ Data Maintenance (see 3.8.2, “Data Maintenance” on page 171)

- ▶ Groups (see 3.8.3, “Groups” on page 174)
- ▶ Logs (see 3.8.4, “Logs” on page 175)
- ▶ My Assets (see 3.8.5, “My Assets” on page 176)
- ▶ Software (see 3.8.6, “Software” on page 178)
- ▶ Statistics (see 3.8.7, “Statistics” on page 180)
- ▶ Tasks
- ▶ ThinkVantage Reports (see 3.8.9, “ThinkVantage Reports” on page 181)
- ▶ Users (see “Users” on page 184)
- ▶ Workstation Security (see 3.8.11, “Workstation Security” on page 186)
- ▶ Run (see 3.8.12, “All Reports” on page 188)

Reports are typically only used by administrator or super-user accounts. However, users within a group can be given access to custom reports that they otherwise would not be able to access with their individual user accounts.

In the following descriptions of System Information Center reports, we focus on the common reports provided with System Information Center. For more information about custom reports, see the *IBM System Information Center Administrator's Guide* installed with System Information Center in c:\ISIC\web\help\ISICADM.pdf, and the online help available from the System Information Center pages.

Attention: The columns shown in the System Information Center reports discussed in this section are the defaults supplied with the predefined System Information Center reports. The columns that are included in any predefined System Information Center report can easily be modified to include additional columns of data, or exclude data that is not needed. See 3.11.3, “Add Query Column” on page 198 for more information.

3.8.1 All Assets

Selecting **All Assets** from the Reports menu shown in Figure 3-64 on page 167 provides you with a list of common predefined asset reports. From the main page, select **Reports** → **All Assets**. This opens a page similar to the one shown in Figure 3-65 on page 169.

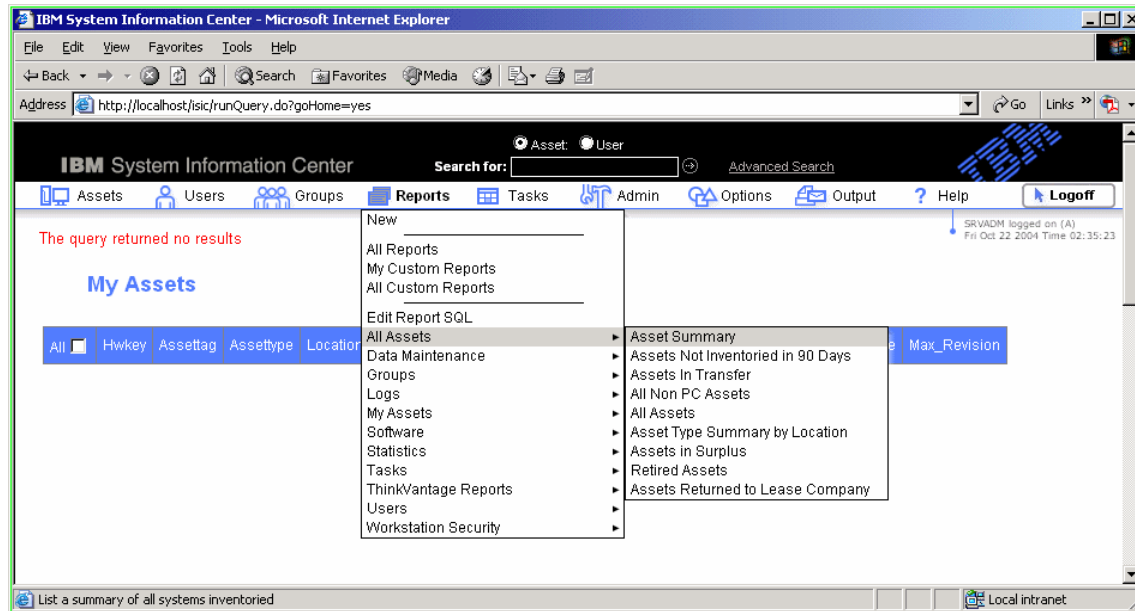


Figure 3-65 All Assets menu

The following types of asset reports types are available in **All Assets**:

- ▶ Asset Summary
- ▶ Assets Not Inventoried in 90 Days
- ▶ Assets In Transfer
- ▶ All Non PC Assets
- ▶ All Assets
- ▶ Asset Type Summary by Location
- ▶ Assets in Surplus
- ▶ Retired Assets
- ▶ Assets Returned to Lease Company

You can use these asset reports to create commonly requested reports for all assets or a subset of assets (depending on the type of report you select, in the System Information Center database.

For example, if you select **Reports** → **All Assets** → **Asset Summary**, you open the Asset Summary report shown in Figure 3-66.

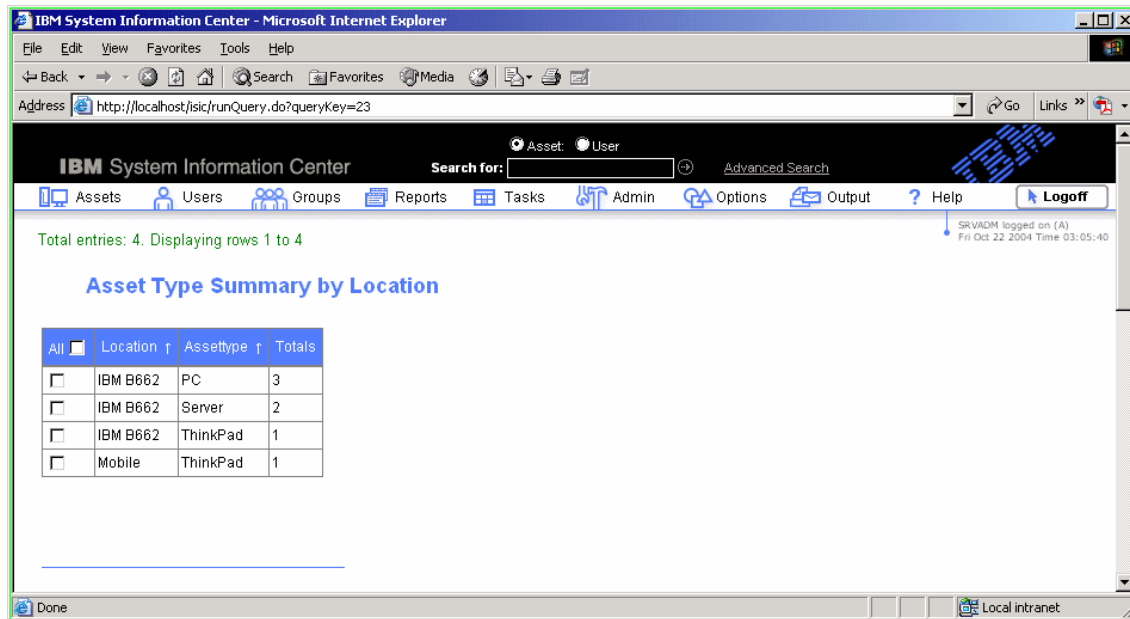
All	Hwkey	Owner	Assettag	Assettype	Manufacturer	Model	Serial_No	Os_Name	Computername	Max_Revision
<input type="checkbox"/>	1	Byron Braswell	999999	ThinkPad	IBM	23739HU	KP9Z511	Windows XP Professional	ROAMINGT41	2
<input type="checkbox"/>	2	Default Administrator	123456	PC	IBM	831048U	KADW039	Windows 2000 Terminal Server	BYRONNETV	3
<input type="checkbox"/>	3	Default Administrator		ThinkPad	IBM	2647T1U	78RCM98	Windows XP Professional	ITSOT21A	1
<input type="checkbox"/>	4	Default Administrator		PC	IBM	6792MHU	KA0KNHB	Windows 2000 Server	KA0KNHB	1
<input type="checkbox"/>	5	Default Administrator		Server	IBM	865861Y	23VNX72	Windows 2000 Server	ISICSERVER	1
<input type="checkbox"/>	6	Default Administrator		Server	IBM	865861Y	23VNX85	Windows 2000 Server	ISIC-MSSQL	1
<input type="checkbox"/>	7	Default Administrator		PC	VMware, Inc.	VMware Virtual Platform	VMware-56 4d eb ed b5 fb ca 86-49 bd 5f 6c 84 9e fb 80	Windows 2000 Terminal Server	DOMLDAP	1

Figure 3-66 Asset Summary page

This report provides a one line summary for all assets in the database.

Attention: The columns shown in the Asset Summary report in Figure 3-66 are the defaults supplied with the predefined System Information Center Asset Summary report. The columns that are included in any predefined System Information Center report can easily be modified to include additional columns of data or exclude unneeded data. See 3.11.3, “Add Query Column” on page 198 for information about how to modify the columns included in a System Information Center report.

If you select **Reports** → **All Assets** → **Asset Type Summary by Location**, a report similar to the one shown in Figure 3-67 provides a one-line summary for all assets in the database.



All	Location	Assettype	Totals
<input type="checkbox"/>	IBM B662	PC	3
<input type="checkbox"/>	IBM B662	Server	2
<input type="checkbox"/>	IBM B662	ThinkPad	1
<input type="checkbox"/>	Mobile	ThinkPad	1

Figure 3-67 Asset Type Summary by Location page

As can be seen from the report shown in Figure 3-67, thoughtful selection of names for asset location, asset type, and any other demographic information you choose to gather, along with consistent use of those names in your entire enterprise, is very important to insure useful report information.

Important: If you choose to require input of asset and user demographic information when System Information Center is installed (see Figure 3-19 on page 114), then it is a good idea to have a predefined list of accepted values for location, department, asset type, floor, description, and so on. The following section provides examples of the values used for selected demographic information.

3.8.2 Data Maintenance

Predefined data maintenance report types supplied with System Information Center allow a user to view information about asset status (such as surplus, retired, returned, and so on) and duplicate asset information. These reports also support viewing assets by selected demographic information.

From the main page (Figure 3-64 on page 167), select **Reports** → **Data Maintenance**. A window similar to the one shown in Figure 3-68 on page 172 opens.

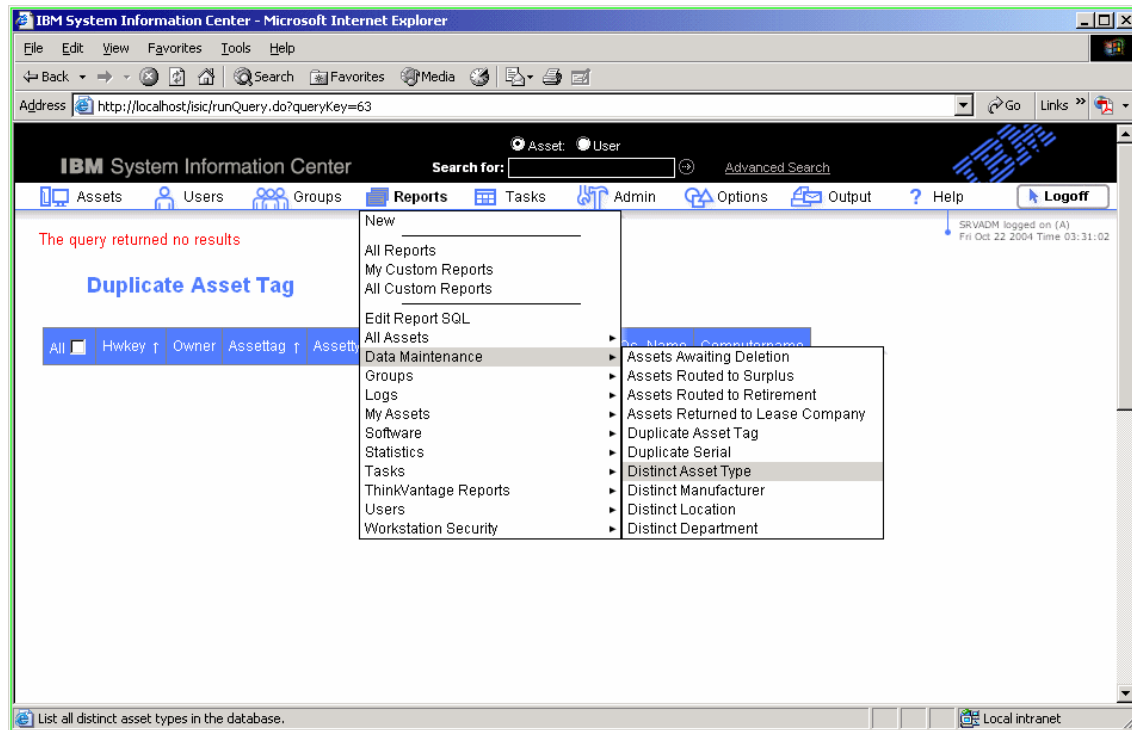


Figure 3-68 Data Maintenance menu

The following predefined types of reports are available in Data Maintenance:

- ▶ Assets Awaiting Deletion
- ▶ Assets Routed to Surplus
- ▶ Assets Routed to Retirement
- ▶ Assets Returned to Lease Company
- ▶ Duplicate Asset Tag
- ▶ Duplicate Serial
- ▶ Distinct Asset Type
- ▶ Distinct Manufacture
- ▶ Distinct Location
- ▶ Distinct Department

To learn how an asset can be deleted from the System Information Center database, see 3.5.12, “Delete” on page 150. For information about routing assets

to surplus, retired, or returned, see 3.5.18, “Surplus” on page 153; 3.5.16, “Retire” on page 152; and 3.5.17, “Return” on page 153.

The reports that list duplicate asset tags and serial numbers can help you find incorrect or duplicate entries in the System Information Center database.

Reports that list assets by distinctive demographic information are of special interest. Figure 3-69 illustrates a Distinct Asset Type report, and Figure 3-70 on page 174 shows a Distinct Location report. These reports are of interest because they summarize enterprise assets based on demographic information such as how many assets of each type a company owns and how many assets are at each company location.

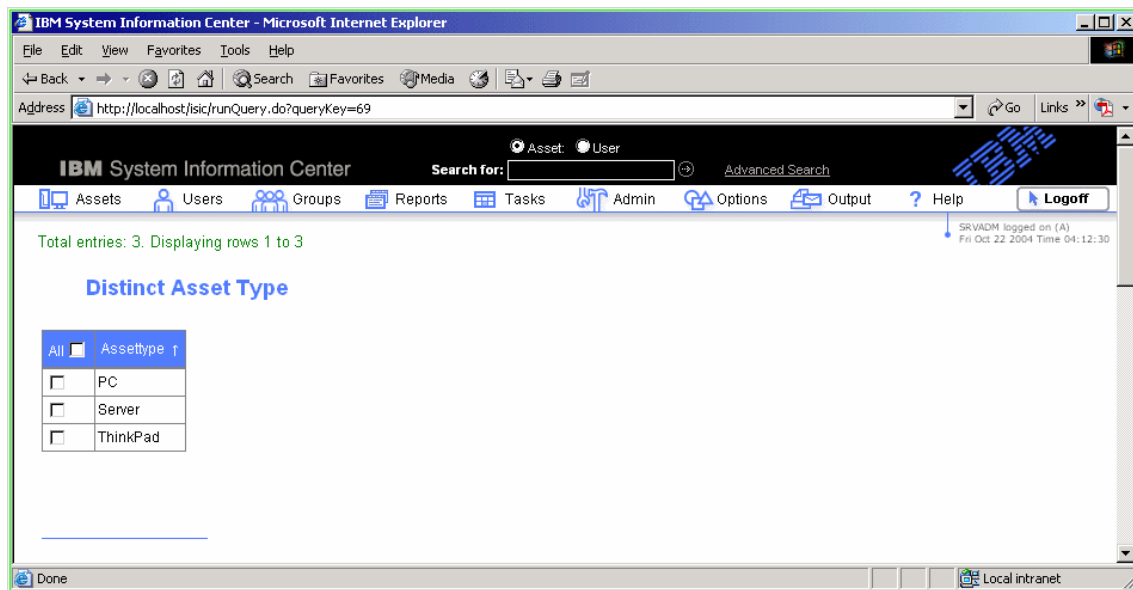


Figure 3-69 Distinct Asset Type page

These reports illustrate the importance of selecting meaningful names when registering users and assets and consistently using those names throughout the System Information Center database. For example, consider the effect the following scenarios might have on the report illustrated in Figure 3-69:

- ▶ One user registers a PC as a desktop
- ▶ One user registers a PC as a workstation
- ▶ One user registers a PC as a tower
- ▶ One user registers his or her PC asset as IBM PC

Because these are different registrations for the same asset, the Distinct Asset Type report might not be very useful.

You must determine the rules for naming assets early and ask questions such as: What kind of asset type is a ThinkPad? Is it a notebook, a mobile PC, or a portable PC?

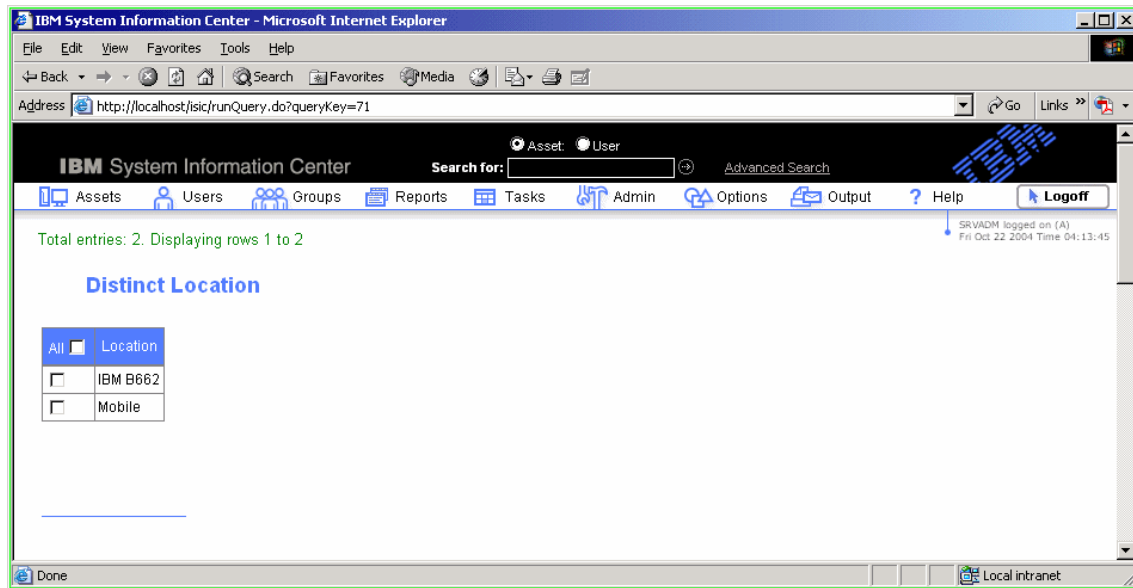


Figure 3-70 Distinct Location page

A location could be a building name or number, a campus, a geographic location, and so on. Consider the report format illustrated in Figure 3-70. Is Mobile a good choice for a location? Figure 3-70 also shows a location called IBM B662. However, building 662 is also part of the Tier Complex of IBM buildings. Should the location be IBM B662, Building 662, or Tier Complex?

Important: Predefined lists of accepted values for demographic information (such as location, department, asset type, floor, description, and so on) are mandatory for reports to be meaningful.

3.8.3 Groups

This report lists all the Groups that have been defined to System Information Center.

3.8.4 Logs

These predefined reports provide details of every user transaction and task performed within System Information Center. Two report types are defined:

- ▶ The transaction log, which includes date and time of each action, asset information, and user information
- ▶ The task log, which includes the task creator, what the task does, and when it was created

You can use these logs to track transactions that may have caused problems in the database or to ensure that specific tasks were performed. Figure 3-71 shows a partial transaction log.

The screenshot shows the IBM System Information Center interface in a Microsoft Internet Explorer browser. The address bar displays `http://localhost/sic/runQuery.do?viewPage=2`. The page title is "Transaction Log". Above the table, it states "Total entries: 142. Displaying rows 101 to 142". The table has columns for selection, Surname, Forename, Email, Hwkey, Manufacturer, Model, Serial_No, Tx_Data, Tx_Time, and Datetime. The transactions listed include asset information updates and EGXML xpaths processing for various IBM and VMware hardware, as well as a manual user addition for Braswell Byron.

All <input type="checkbox"/>	Surname	Forename	Email	Hwkey	Manufacturer	Model	Serial_No	Tx_Data	Tx_Time	Datetime
<input type="checkbox"/>	Administrator	Default	admin@mycompany.com	3	IBM	2647T1U	78RCM98	Added / updated asset information	2594	2004-10-22 13:07:08.25
<input type="checkbox"/>	Administrator	Default	admin@mycompany.com	3	IBM	2647T1U	78RCM98	Processed EGXML xpaths	12859	2004-10-22 13:07:21.375
<input type="checkbox"/>	Administrator	Default	admin@mycompany.com	4	IBM	6792MHU	KA0KNHB	Added / updated asset information	2890	2004-10-22 13:37:58.328
<input type="checkbox"/>	Administrator	Default	admin@mycompany.com	4	IBM	6792MHU	KA0KNHB	Processed EGXML xpaths	10860	2004-10-22 13:38:09.266
<input type="checkbox"/>	Administrator	Default	admin@mycompany.com	5	IBM	865861Y	23VNX72	Added / updated asset information	2469	2004-10-22 13:38:28.672
<input type="checkbox"/>	Administrator	Default	admin@mycompany.com	5	IBM	865861Y	23VNX72	Processed EGXML xpaths	11047	2004-10-22 13:38:40.203
<input type="checkbox"/>	Administrator	Default	admin@mycompany.com	6	IBM	865861Y	23VNX85	Added / updated asset information	1907	2004-10-22 13:44:29.719
<input type="checkbox"/>	Administrator	Default	admin@mycompany.com	6	IBM	865861Y	23VNX85	Processed EGXML xpaths	11610	2004-10-22 13:44:41.844
<input type="checkbox"/>	Administrator	Default	admin@mycompany.com	7	VMware, Inc.	VMware Virtual Platform	VMware-56 4d eb ed b5 fb ca 86-49 bd 5f 6c 84 9e fb 80	Added / updated asset information	2516	2004-10-22 13:44:58.078
<input type="checkbox"/>	Administrator	Default	admin@mycompany.com	7	VMware, Inc.	VMware Virtual Platform	VMware-56 4d eb ed b5 fb ca 86-49 bd 5f 6c 84 9e fb 80	Processed EGXML xpaths	10376	2004-10-22 13:45:08.938
<input type="checkbox"/>	Braswell	Byron	byrontex@us.ibm.com	null				ADDED USER	null	2004-10-22 13:53:40.328

Figure 3-71 Transaction log

3.8.5 My Assets

The My Assets report provides you with a list of all assets that are registered to you in the System Information Center database. You can obtain assets that are currently being transferred or that you have transferred that have not yet been received by the new owner. In addition, you can list any non-PC assets that have been manually entered and registered to you. Refer to 3.5.3, “Manually Add Asset” on page 142 to learn how to manually enter a non-PC asset.

From the main page (Figure 3-64 on page 167), select **Reports** → **My Assets**. This opens a page similar to the one shown in Figure 3-72.

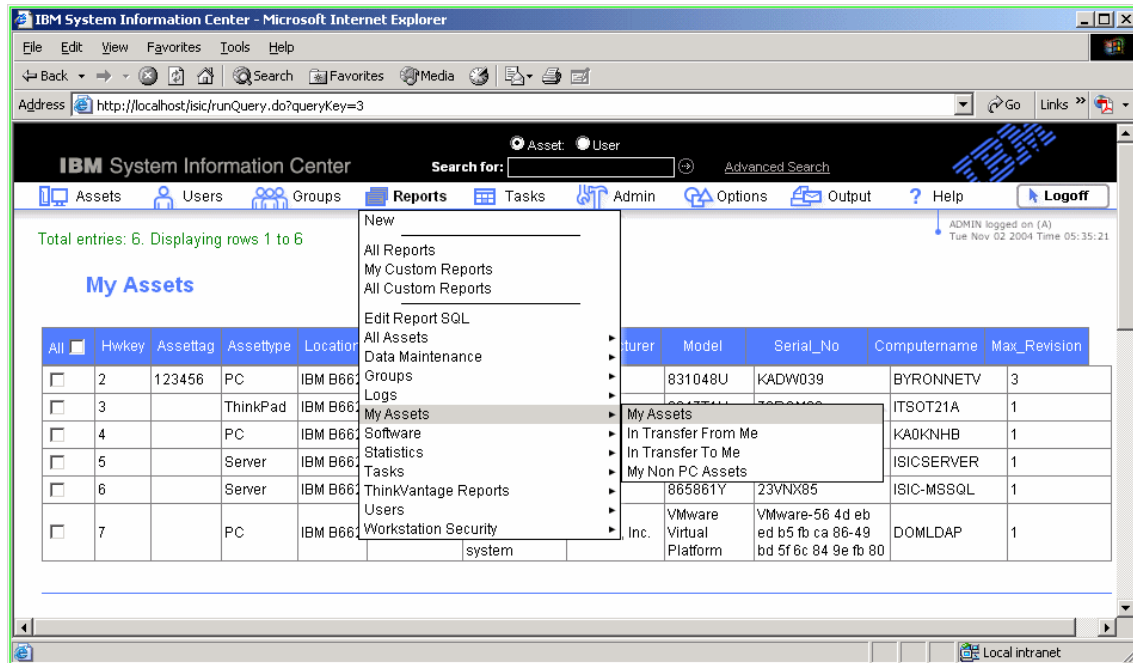


Figure 3-72 My Assets menu

To obtain the My Assets report, select **Reports** → **My Assets** → **My Assets**. This report also opens by default after a user logs in. See 3.11.1, “Set Current Query as Default” on page 198 to learn how to specify a different report as the default.

3.8.6 Software

The predefined Software reports allow you to list all or a subset of the software installed on all the clients registered in the IBM System Information Center database. See Figure 3-73.

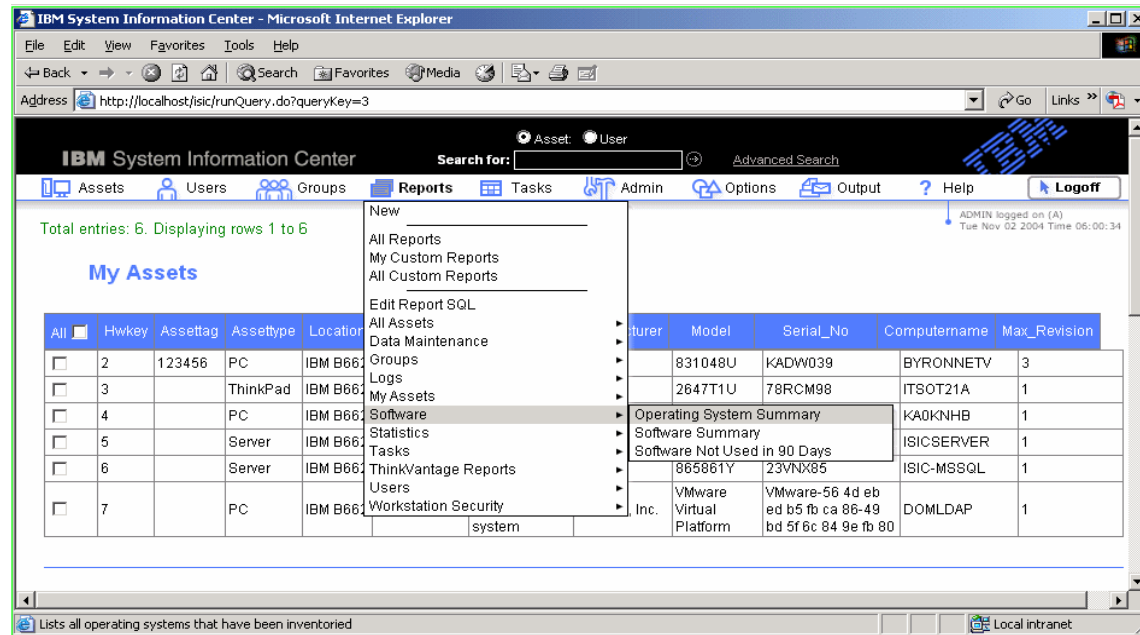


Figure 3-73 Software menu

As can be seen in Figure 3-73, there are three predefined software reports:

1. Operating System Summary
2. Software Summary
3. Software Not Used in 90 Days

The Operating System Summary report (Figure 3-74) provides a count of all operating system software by type installed on all clients. This report is very useful for tracking OS licensing and usage numbers.

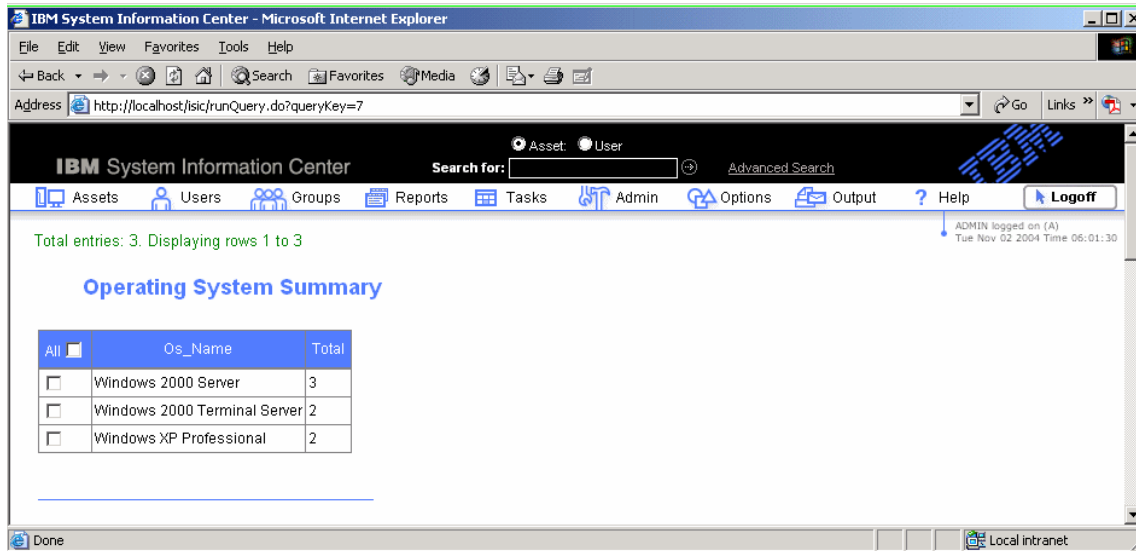


Figure 3-74 Operating System Summary report

Another predefined report that can be obtained from the Software menu is Software Not Used in 90 Days (Figure 3-75).

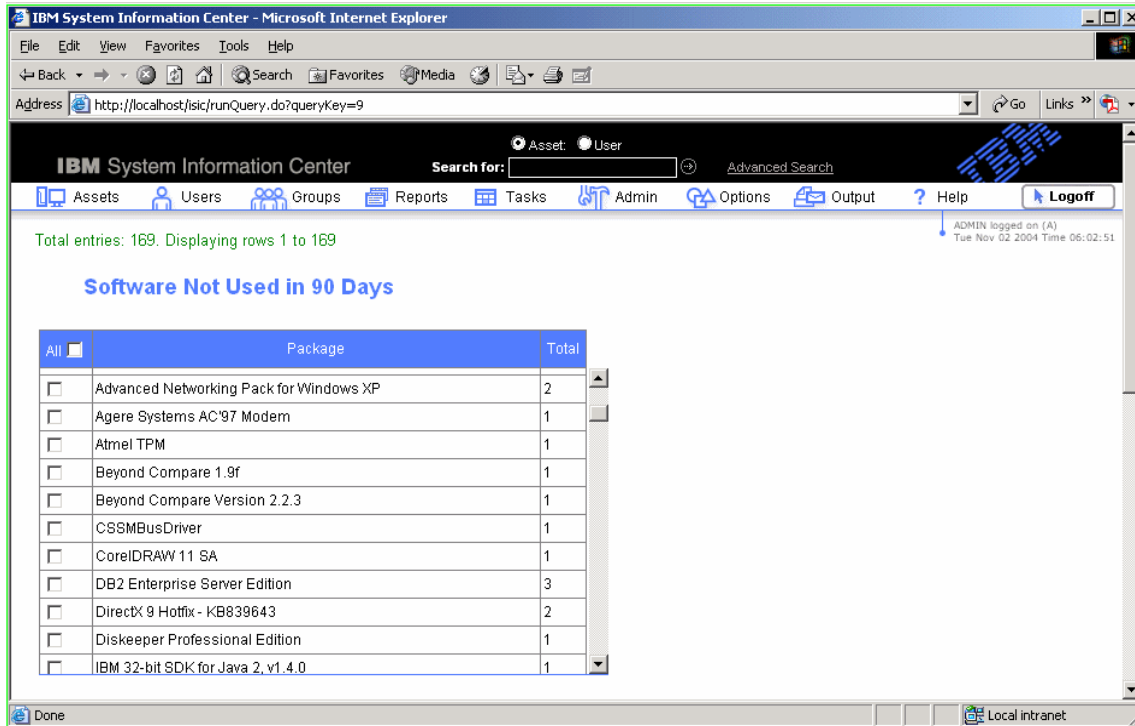


Figure 3-75 Software Not Used in 90 Days report

The information obtained from this report is very helpful in determining what installed software is not being used and can therefore be removed to reduce licensing fees.

3.8.7 Statistics

Selecting **Statistics** from the **Reports** menu results in a list of the three predefined statistics reports provided with System Information Center. These list counts for all assets, PC assets, and non-PC assets in the database.

3.8.8 Tasks

Predefined task reports supplied with System Information Center allow the user to view information about scheduled tasks, automatic tasks, manual tasks, and so on. These tasks are typically performed by an administrator or automatically by the System Information Center server.

From the main page (Figure 3-64 on page 167), select **Reports** → **Tasks**. This opens a page similar to the one shown in Figure 3-76.

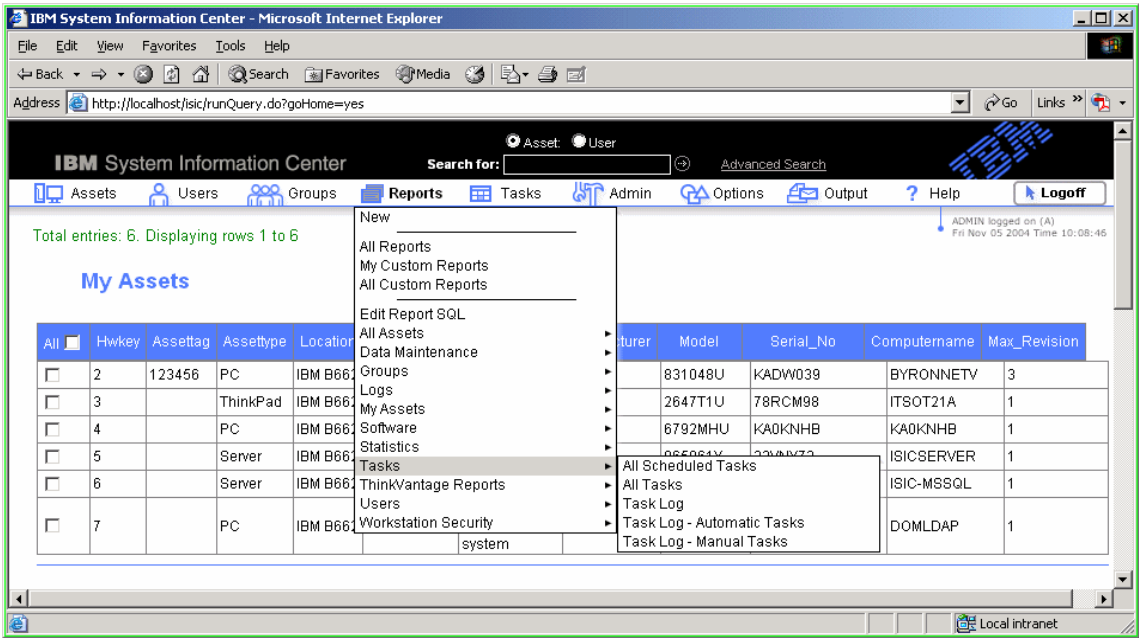


Figure 3-76 Tasks menu

3.8.9 ThinkVantage Reports

This series of reports provides information about assets deployed with ThinkVantage products and a log of Rapid Restore deployments.

From the main page (Figure 3-64 on page 167), select **Reports** → **ThinkVantage Reports**. A window similar to the one shown in Figure 3-77 opens.

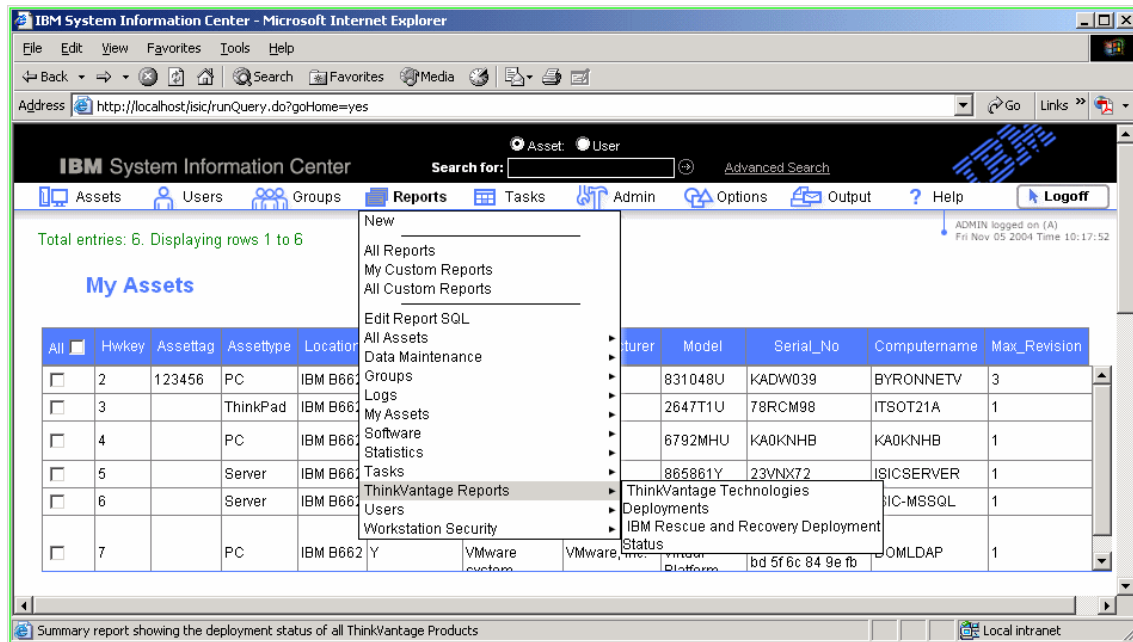


Figure 3-77 ThinkVantage Reports option

From the menus shown in Figure 3-77, we selected **ThinkVantage Technologies Deployments**. The window in Figure 3-78 opened.

All	Package	Version	Deployed_To	Percent_Of_Total	Ibm	Non_Ibm
<input type="checkbox"/>	Access IBM	4.0	1	15	1	0
<input type="checkbox"/>	Access IBM Cleanup Utility	1.00.0000	1	15	1	0
<input type="checkbox"/>	Access IBM Message Center	2.0.0	1	15	1	0
<input type="checkbox"/>	Access IBM Tools	4.0	1	15	1	0
<input type="checkbox"/>	AccessIBM	"4.1"	1	15	1	0
<input type="checkbox"/>	IBM Access Connections	1.00.000	1	15	1	0
<input type="checkbox"/>	IBM Access Connections	3.30	1	15	1	0
<input type="checkbox"/>	IBM Active Protection System	1.00.000	1	15	1	0

Figure 3-78 ThinkVantage Technologies Deployments report

The ThinkVantage Technologies Deployments report shown in Figure 3-78 is a summary of the status of all ThinkVantage products deployed in the enterprise including a count of IBM and non-IBM PCs with ThinkVantage products installed.

Attention: The columns shown in the ThinkVantage Technologies Deployments report in Figure 3-78 are the default column selections supplied with the predefined ThinkVantage Technologies Deployments report. The columns that are included in the ThinkVantage Technologies Deployments report (or any predefined System Information Center report) can easily be modified to include additional columns of data, or exclude unneeded data. See 3.11.3, “Add Query Column” on page 198 for information about how to modify the columns included in a System Information Center report.

3.8.10 Users

The User reports provided with System Information Center provide specific information about the users that have registered with System Information Center.

From the main page (Figure 3-64 on page 167), select **Reports** → **Users**. This opens a window similar to the one shown in Figure 3-79.

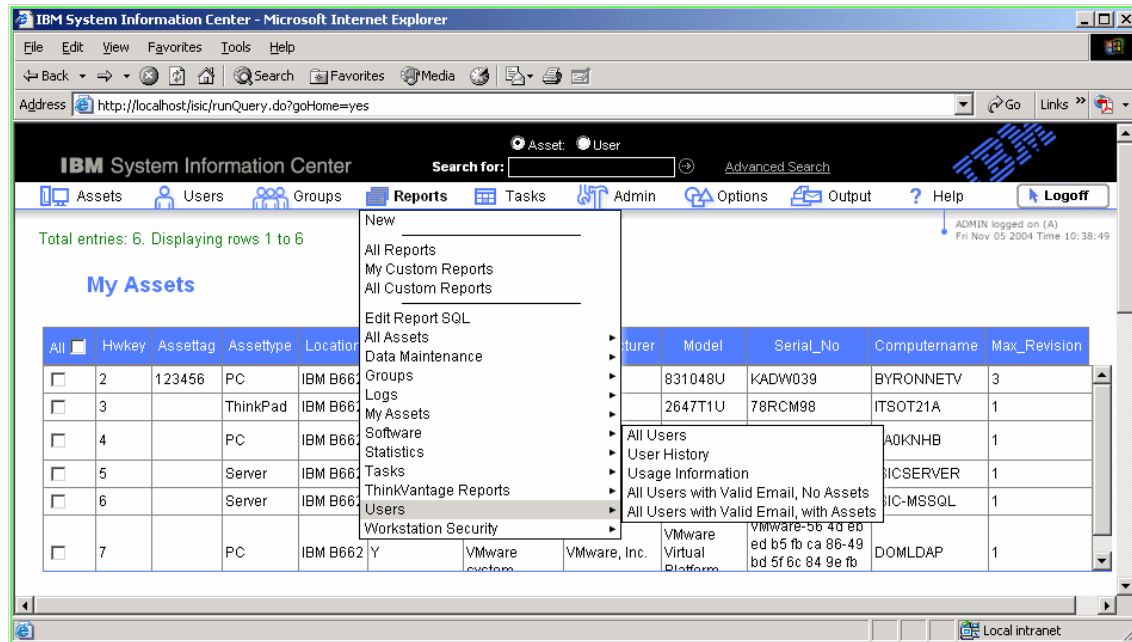


Figure 3-79 User reports menu

Selecting **All Users** from the Users menu (Figure 3-80) will result in a report that lists selected details for all registered System Information Center users.

All	Userkey	Userid	Email	Title	Forename	Initials	Surname	Location	Tel_No	Mob_No
<input type="checkbox"/>	1	ADMIN	admin@mycompany.com	Mr	Default		Administrator	Tier Complex	919 543 4028	
<input type="checkbox"/>	2	SRVADM	srvadm@us.ibm.com	Mrs	Server		Admin	Main Site	919 123 4567	
<input type="checkbox"/>	3	PCADM	pcadm@us.ibm.com	Mr	PC		Admin	ITSO	919 234-5678	
<input type="checkbox"/>	4	NONPCADM	nonpcadm@us.ibm.com	NONE	Nonpc		Admin	ITSO	919 345 6789	
<input type="checkbox"/>	5	BYRON	byrontex@us.ibm.com	Mr	Byron		Braswell	RTP	919 543-4028	

Figure 3-80 All Users report

Attention: The columns shown in the All Users report in Figure 3-80 are the default column selections supplied with the predefined System Information Center All Users report. The columns that are included in the All Users report (or any predefined System Information Center report) can easily be modified to include additional columns of data, or exclude unneeded data. See 3.11.3, “Add Query Column” on page 198 for information about how to modify the columns included in a System Information Center report.

The Usage Information report shown in Figure 3-81 was obtained by selecting **Reports** → **Users** → **Usage Information**. This is a convenient method for determining which users are using the System Information Center tool.

IBM System Information Center

Search for: Advanced Search

Assets Users Groups Reports Tasks Admin Options Output Help Logoff

ADMIN logged on (A)
Fri Nov 05 2004 Time 10:42:51

Total entries: 3. Displaying rows 1 to 3

Usage Information

All	Userkey	Userid	Name	Email	First_Access	Last_Access ↓	Visits ↓
<input type="checkbox"/>	1	ADMIN	Default Administrator	admin@mycompany.com	2004-10-14 16:32:42.891	2004-11-05 09:53:47.594	32
<input type="checkbox"/>	2	SRVADM	Server Admin	srvadm@us.ibm.com	2004-10-22 14:35:22.562	2004-10-29 14:21:42.594	7
<input type="checkbox"/>	4	NONPCADM	Nonpc Admin	nonpcadm@us.ibm.com	2004-10-22 17:41:26.578	2004-10-22 17:41:26.578	1

Figure 3-81 Usage Information report

3.8.11 Workstation Security

The Workstation Security report can be used to determine the security conditions of all client computers registered in System Information Center.

From the main page (Figure 3-64 on page 167), select **Reports** → **Workstation Security**. This opens a page similar to the one shown in Figure 3-82 on page 187.

IBM System Information Center - Microsoft Internet Explorer

Address: http://localhost/isc/runQuery.do?queryKey=120

IBM System Information Center Search for: Asset: User Advanced Search

Assets Users Groups Reports Tasks Admin Options Output Help Logoff

Total entries: 7. Displaying rows 1 to 7

ADMIN logged on (A) Sat Nov 06 2004 Time 03:14:22

Detailed Security Report

All	Hwkey	Userkey	Forename	Surname	Manufacturer	Model	Serial_No	Os_Name	Secure	Power_On_Pw	Hdd_Pw	Fileshare	Screensaver
<input type="checkbox"/>	1	5	Byron	Braswell	IBM	23739HU	KP9Z511	Windows XP Professional					
<input type="checkbox"/>	2	1	Default	Administrator	IBM	831048U	KADW039	Windows 2000 Terminal Server					
<input type="checkbox"/>	3	1	Default	Administrator	IBM	2647T1U	78RCM98	Windows XP Professional					
<input type="checkbox"/>	4	1	Default	Administrator	IBM	6792MHU	KA0KNHB	Windows 2000 Server					
<input type="checkbox"/>	5	1	Default	Administrator	IBM	865861Y	23VNX72	Windows 2000 Server					

Done Local intranet

Figure 3-82 Workstation Security report: Part 1

This report can provide additional security information (Figure 3-83 on page 188) such as:

- ▶ Power-on password
- ▶ Hardware password
- ▶ File sharing
- ▶ Screensaver
- ▶ User accounts
- ▶ Password length
- ▶ Password age
- ▶ Firewall

Model	Serial_No	Os_Name	Secure	Power_On_Pw	Hdd_Pw	Fileshare	Screensaver	User_Accounts	Pw_Length	Pw_Age	Antivirus	Firewall
23739HU	KP9Z511	Windows XP Professional										
831048U	KADW039	Windows 2000 Terminal Server										
2647T1U	78RCM98	Windows XP Professional										
6792MHU	KA0KNHB	Windows 2000 Server										
865861Y	23VNX72	Windows 2000 Server										

Figure 3-83 Workstation Security report: Part 2

The headings shown in Figure 3-83 correspond to the security settings that are configured when System Information Center is installed. See Figure 3-20 on page 115 for a list of the security settings that System Information Center can monitor.

If System Information Center is not configured to monitor a specific security setting, the corresponding column in the Workstation Security report will be empty. See 3.2.5, “Modifying the System Information Center installation” on page 124 for information about how to modify these settings after System Information Center has been installed.

3.8.12 All Reports

The All Reports report is a convenient way to view all the predefined and customized reports that exist within your System Information Center domain.

From the main page (Figure 3-64 on page 167), select **Reports** → **All Reports**. This opens a page similar to the one shown in Figure 3-84.

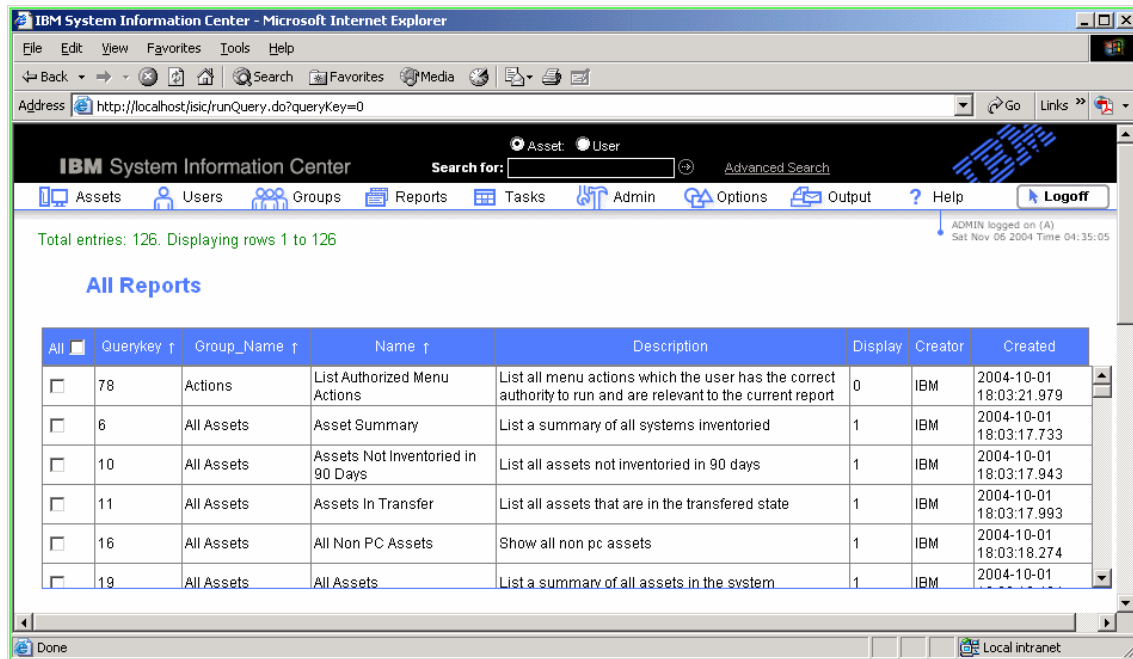


Figure 3-84 All Reports report

Each entry in the report lists:

- ▶ Group name (report type)
- ▶ Report name and a description of what it is
- ▶ Display type (0 indicates that the report is a subreport of a primary report, which is 1)

To obtain a specific report from the list shown in Figure 3-84, select the desired report, and select **Reports** → **Run** as shown in Figure 3-85 on page 190. This generates the requested report.

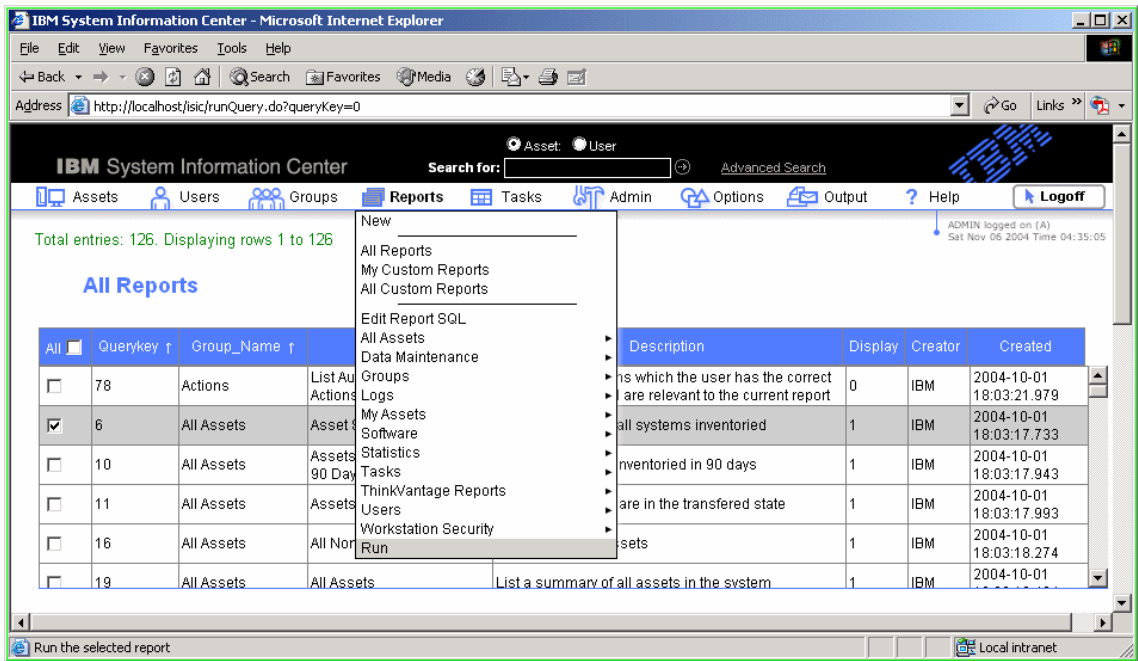


Figure 3-85 Selecting a specific report to run

Restriction: Subreports (display type of 0) work in conjunction with primary reports (display type of 1) and are dependent on the primary report. Therefore, some subreports cannot be run separately.

3.8.13 Rearrange report display output

Columns of data can easily be deleted or shifted left or right in the display output. For example, Figure 3-86 on page 191 is the output of the My Assets report.

IBM System Information Center - Microsoft Internet Explorer

Address: http://localhost/sic/runQuery.do?queryKey=3#

Search for: [] Advanced Search

Assets Users Groups Reports Tasks Admin Options Output Help Logoff

Total entries: 6. Displaying rows 1 to 6

My Assets

All	Hwkey	Assettag	Assettype	Location	Is_Pc_Asset	Description	Manufacturer	Model	Serial_No	Computername	Max_Revision
<input type="checkbox"/>	2	123456	PC	IBM B662	Y	ISIC Server	IBM	831048U	KADW039	BYRONNETV	3
<input type="checkbox"/>	3		ThinkPad	IBM B662	Y	LAB ThinkPad	IBM	2647T1U	78RCM98	ITSOT21A	1
<input type="checkbox"/>	4		PC	IBM B662	Y	Lab Pentium III	IBM	6792MHU	KA0KNHB	KA0KNHB	1
<input type="checkbox"/>	5		Server	IBM B662	Y	Lab Server	IBM	865861Y	23VNX72	ISICSERVER	1
<input type="checkbox"/>	6		Server	IBM B662	Y	Lab Server	IBM	865861Y	23VNX85	ISIC-MSSQL	1
<input type="checkbox"/>	7		PC	IBM B662	Y	2nd level VMware system	VMware, Inc.	VMware Virtual Platform	VMware-56 4d eb ed b5 fb ca 86-49 bd 5f 6c 84 9e fb 80	DOMLDAP	1

Done Local intranet

Figure 3-86 My Assets report output

Suppose you would like to delete or shift the **Hwkey** column of data. Place the cursor over the column heading and click. A group of manipulation icons is displayed as shown in Figure 3-87.

IBM System Information Center

Search for: [] Advanced Search

Assets Users Groups Reports Tasks Admin Options Output Help Logoff

Total entries: 6. Displaying rows 1 to 6

My Assets

All	Hwkey	Assettag	Assettype	Location	Is_Pc_Asset	Description	Manufacturer	Model	Serial_No	Computername	Max_Revision
<input type="checkbox"/>	2	123456	PC	IBM B662	Y	ISIC Server	IBM	831048U	KADW039	BYRONNETV	3
<input type="checkbox"/>	3		ThinkPad	IBM B662	Y	LAB ThinkPad	IBM	2647T1U	78RCM98	ITSOT21A	1
<input type="checkbox"/>	4		PC	IBM B662	Y	Lab Pentium III	IBM	6792MHU	KA0KNHB	KA0KNHB	1

Done Local intranet

Figure 3-87 Hwkey column selected

Figure 3-88 is a more detailed illustration of the column manipulation icons that appear when a column heading is selected.

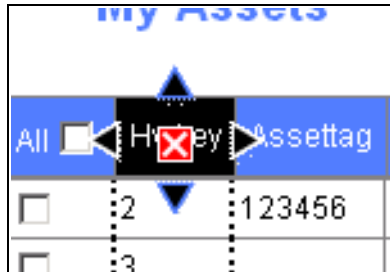


Figure 3-88 Column manipulation icons

Clicking on the column manipulation icons shown in Figure 3-88 performs the following actions:

- ▶ Clicking on the “X” in the center of the column heading will delete the column from the report.
- ▶ Clicking on the left or right arrows will shift the column in the direction of the arrow in the report.
- ▶ Clicking on the up or down arrows will sort the report rows in ascending or descending order based on the data in the selected column.

3.9 Tasks

Tasks are background processes that are run on the System Information Center server. An example of a task is an action that runs a specific report, attaches the report to an e-mail, and sends the report to a target user or group of users. Another example is the task that can automatically collect client computer asset data at specific intervals (see Figure 3-17 on page 112).

Tasks are typically performed by an administrator. They can be run once or be set to run automatically at set intervals. You can invoke them from the Tasks menu in the System Information Center menu bar or by using the Task Scheduler. The Task Scheduler automatically checks for scheduled tasks. See “Start Task Scheduler” on page 197 for more information.

From the main page, select **Tasks** to open the menu of functions (Figure 3-89 on page 193) that can be performed to manipulate and display System Information Center tasks.

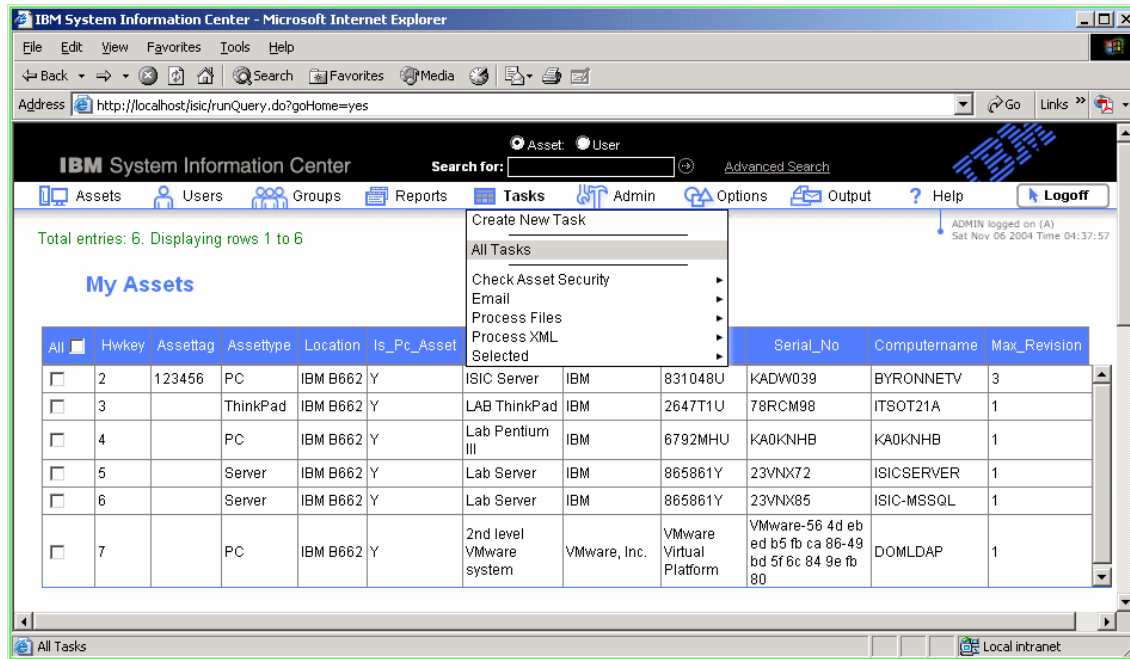


Figure 3-89 Tasks menu

For more information about creating and scheduling tasks, see the *IBM System Information Center Administrator's Guide* installed with System Information Center in c:\ISIC\web\help\ISICADM.pdf and the online help available from the System Information Center GUI.

3.10 Admin

The Admin feature of System Information Center is used to perform administrative tasks. This component is most often used to monitor the status of the system.

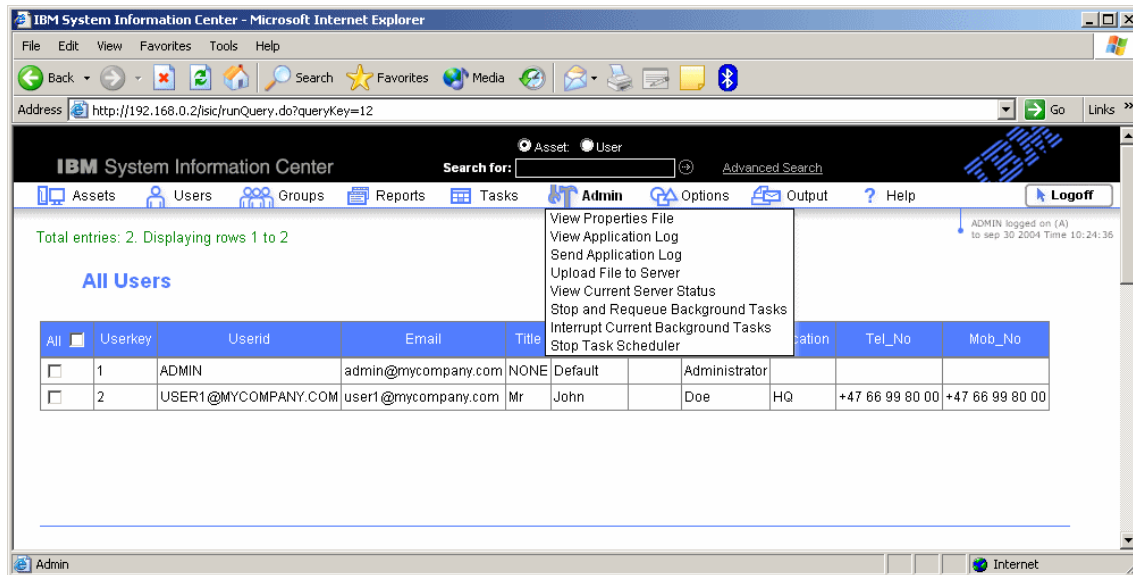


Figure 3-90 Admin menu on main page

From the Admin management menu, you can perform the following tasks:

- ▶ View the properties file for System Information Center
- ▶ View the application log for System Information Center
- ▶ Send the application log for System Information Center
- ▶ Upload a file to the server
- ▶ View current server status
- ▶ Stop and requeue background tasks
- ▶ Interrupt current background tasks
- ▶ Stop the task scheduler

You must be logged in to System Information Center with an administrator account to use this feature. Users and superusers will not see the Admin menu item when they log on to the System Information Center server (refer to 3.6, “User Management” on page 155 for a review of System Information Center user types).

3.10.1 View Properties File

Use the View Properties File feature to view the settings that System Information Center is currently using. You cannot make any changes to the configuration on this page, only look at it. The file is named `isic.properties`, which is typically stored in `c:\ISIC\web\WEB-INF\classes` on the System Information Center server. To make any changes to this file, you must edit file itself.

From the main page (Figure 3-90 on page 194), select **Admin** → **View Properties File**. A new page displays the current configuration.

3.10.2 View Application Log

The application log lists all the actions performed by System Information Center by date and time. It is useful for performing an analysis of failures or configurations.

From the main page (Figure 3-90 on page 194), select **Admin** → **View Application Log**. A new page displays the current application log for System Information Center.

3.10.3 Send Application Log

This menu item is used if you would like to save or look at the System Information Center server application log. It performs the same function as the View Application Log selection; however, no data is displayed in a window. Instead, it is displayed either as a text file in Notepad, or saved as a text file.

From the main page (Figure 3-90 on page 194), select **Admin** → **Send Application Log**. A dialog box opens that asks you if you would like to save or open the file. Click **Save** to save the file or **Open** to open it.

3.10.4 Upload File to Server

With this feature, you can upload a file to the server (such as a new WAR file) when other ports are blocked by a firewall or similar entity, as long as System Information Center has access to the network.

From the main page (Figure 3-90 on page 194), select **Admin** → **Upload File to Server**. A new page opens. Use the Browse feature to find the file you would like to upload to the server.

3.10.5 View Current Server Status

To obtain the current server status, select **Admin** → **View Current Server Status** from the main page (Figure 3-90 on page 194). A new page shows the current server status (Figure 3-91 on page 196).

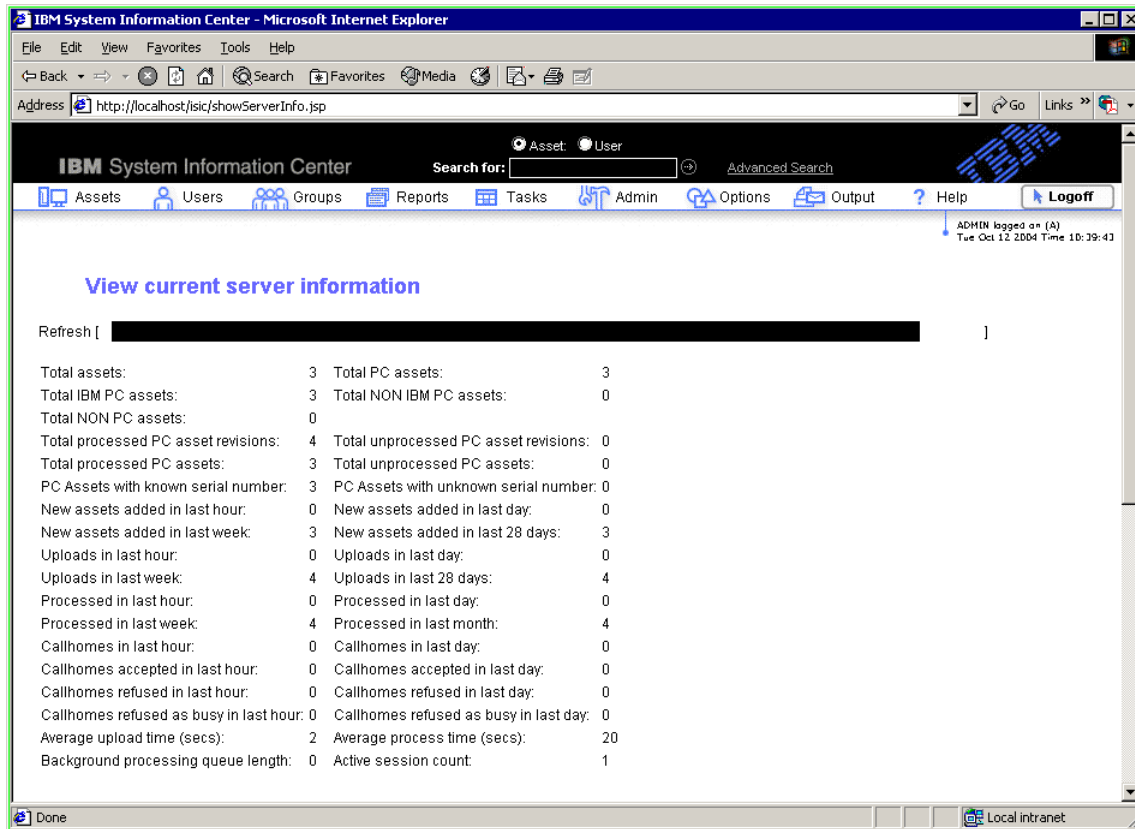


Figure 3-91 System Information Center server status

3.10.6 Stop and Requeue Background Tasks

Use this feature if you have added or modified background tasks and need to make them active. From the main page (Figure 3-90 on page 194), select **Admin** → **Stop and Requeue Background Tasks**. All the background tasks are requeued.

3.10.7 Interrupt Current Background Tasks

Use this feature to temporarily stop all background tasks to free up resources for other processing needs. From the main page (Figure 3-90 on page 194), select **Admin** → **Interrupt Current Background Tasks**. This interrupts background threads and then restarts them.

Start Task Scheduler

Use this feature to start the task scheduler. The tasks are configured through the **Task** button on the main page or by modifying the isic.properties file (c:\ISIC\web\WEB-INF\classes\isic.properties). To start the scheduler, select **Admin** → **Start Task Scheduler** from the main page.

3.11 Options

The Options menu (Figure 3-92) is used to change the way a user will see the report that is selected. For example, you can change the columns and tables that are included as well as how many lines are in a report.

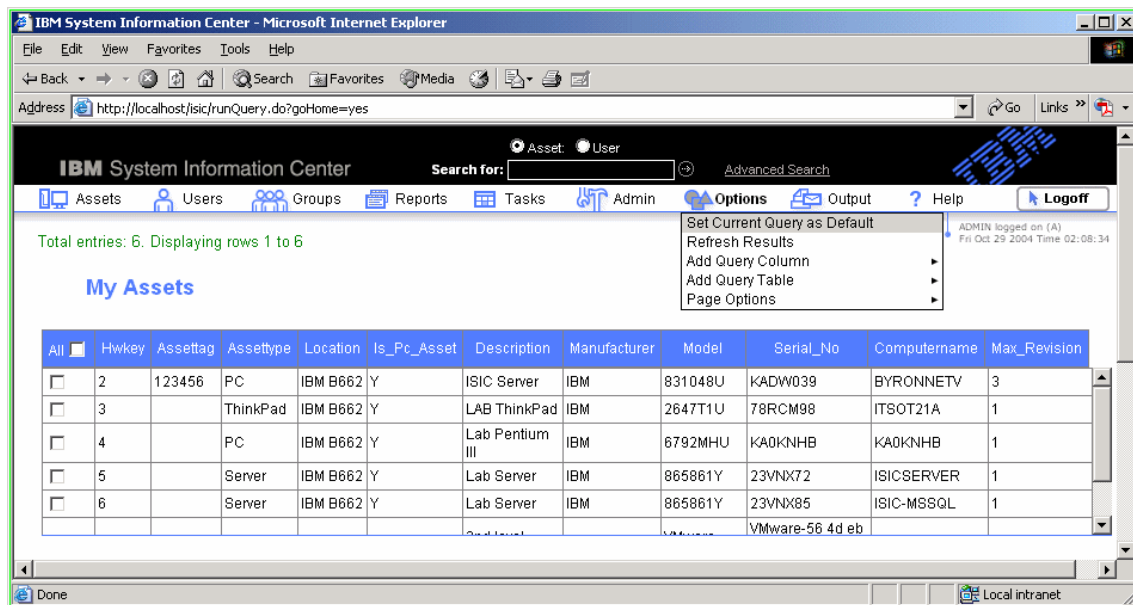


Figure 3-92 Options menu on main page

You can perform the following tasks from the Options menu:

- ▶ Set a query as an default query
- ▶ Refresh the query results
- ▶ Add query columns
- ▶ Add query tables
- ▶ Set page options

The options available will vary depending on the rights of the user.

3.11.1 Set Current Query as Default

To set the default report that appears when a user logs in to System Information Center, follow these instructions:

1. Log on to System Information Center with the user name and password of the user for whom you would like to change the default.
2. Open the report that you wish to be the default. (For more information about opening reports, see 3.8, “Reports” on page 167.)
3. From the main page (Figure 3-92 on page 197), select **Options** → **Set Current Query as Default**. The selected report will now be the default.

3.11.2 Refresh Result

Use this feature to refresh the data that is displayed after running a query. From the main page (Figure 3-92 on page 197), select **Options** → **Refresh Results**. This updates the data.

3.11.3 Add Query Column

You can temporarily add a column to the currently selected report to see more enhanced information during a query by selecting additional columns for display. Which columns you can select depends on the type of report.

To add a query column temporarily:

1. Open a report that you would like to modify. See 3.8, “Reports” on page 167. For our example, we opened the Asset Summary report (Figure 3-93 on page 199).

IBM System Information Center - Microsoft Internet Explorer

Address: http://localhost/jsic/runQuery.do?queryKey=6

IBM System Information Center Search for: Asset: User Advanced Search

Assets Users Groups Reports Tasks Admin Options Output Help Logoff

Total entries: 7. Displaying rows 1 to 7

ADMIN logged on (A) Fri Oct 29 2004 Time 02:44:07

Asset Summary

All	Hwkey	Owner	Assettag	Assettype	Manufacturer	Model	Serial_No	Os_Name	Computename	Max_Revision
<input type="checkbox"/>	1	Byron Braswell	999999	ThinkPad	IBM	23739HU	KP9Z511	Windows XP Professional	ROAMINGT41	2
<input type="checkbox"/>	2	Default Administrator	123456	PC	IBM	831048U	KADW039	Windows 2000 Terminal Server	BYRONNETV	3
<input type="checkbox"/>	3	Default Administrator		ThinkPad	IBM	2647T1U	78RCM98	Windows XP Professional	ITSOT21A	1
<input type="checkbox"/>	4	Default Administrator		PC	IBM	6792MHU	KA0KNHB	Windows 2000 Server	KA0KNHB	1
<input type="checkbox"/>	5	Default Administrator		Server	IBM	865861Y	23VNX72	Windows 2000 Server	ISICSERVER	1
<input type="checkbox"/>	6	Default Administrator		Server	IBM	865861Y	23VNX85	Windows 2000 Server	ISIC-MSSQL	1
<input type="checkbox"/>	7	Default Administrator		PC	VMware, Inc.	VMware Virtual Platform	VMware-56 4d eb ed b5 fb ca 86-49 bd 5f 6c 84 9e fb 80	Windows 2000 Terminal Server	DOMLDAP	1

Figure 3-93 Asset Summary report

- From the report page, select **Options** → **Add Query Column** as shown in Figure 3-94.

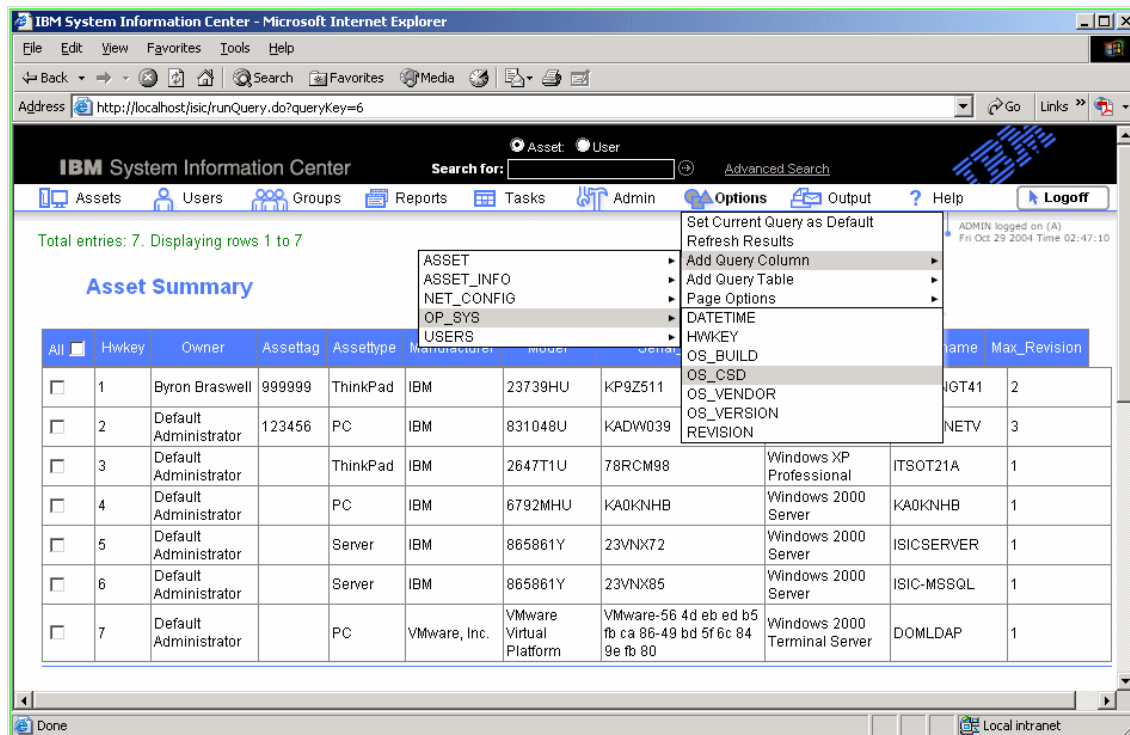


Figure 3-94 Selecting a column to add

As shown in Figure 3-94, when you select **Add Query Column**, another menu opens that lists the types of columns that can be added to the Asset Summary report. For an Asset Summary report, the additional column selections are:

- ASSET
- ASSET_INFO
- NET_CONFIG
- OP_SYS
- USERS

In our example, we selected **OP_SYS**. When **OP_SYS** is selected, another menu opens that allows you to further refine the type of column to be added to the report. For our example, we selected **OP_CSD** as the column to be added to the Asset Summary report.

- The column is added to the report and the page refreshes as shown in Figure 3-95.

The screenshot shows the IBM System Information Center interface in a Microsoft Internet Explorer browser. The address bar displays the URL: `http://localhost/isic/runQuery.do?appendColumn=OP_SYS.OS_CSD`. The page title is "IBM System Information Center". Below the title bar, there is a search bar and a navigation menu with options: Assets, Users, Groups, Reports, Tasks, Admin, Options, Output, and Help. A "Logoff" button is also present. A green message at the top left states: "Added column OP_SYS.OS_CSD to query". The main content area is titled "Asset Summary" and displays a table with 12 columns: All, Hwkey, Owner, Assettag, Assettype, Manufacturer, Model, Serial_No, Os_Name, Computername, Max_Revision, and Os_Csd. The table contains 6 rows of data, each with a checkbox in the "All" column.

All	Hwkey	Owner	Assettag	Assettype	Manufacturer	Model	Serial_No	Os_Name	Computername	Max_Revision	Os_Csd
<input type="checkbox"/>	1	Byron Braswell	999999	ThinkPad	IBM	23739HU	KP9Z511	Windows XP Professional	ROAMINGT41	2	Service Pack 1
<input type="checkbox"/>	2	Default Administrator	123456	PC	IBM	831048U	KADW039	Windows 2000 Terminal Server	BYRONNETV	3	Service Pack 4
<input type="checkbox"/>	3	Default Administrator		ThinkPad	IBM	2647T1U	78RCM98	Windows XP Professional	ITSOT21A	1	Service Pack 1
<input type="checkbox"/>	4	Default Administrator		PC	IBM	6792MHU	KA0KNHB	Windows 2000 Server	KA0KNHB	1	Service Pack 4
<input type="checkbox"/>	5	Default Administrator		Server	IBM	865861Y	23VNX72	Windows 2000 Server	ISICSERVER	1	Service Pack 4
<input type="checkbox"/>	6	Default Administrator		Server	IBM	865861Y	23VNX85	Windows 2000 Server	ISIC-MSSQL	1	Service Pack 4

Figure 3-95 Asset Summary report with added OS-CSD column

Compare Figure 3-94 on page 200 with Figure 3-95 and note that an additional column was added on the right. Also note the comment added in the upper left above the report name in Figure 3-95.

Note: The number and selection of available menu items depend completely on what report is currently displayed.

To add additional items, you must select a new table from the Add Query Table menu. This is described in the following section.

3.11.4 Add Query Table

This menu item is associated with the Add Query Column and allows you to add additional menu items in the Add Query Column menu to those that are available by default. This may be done as follows:

1. Open a report that you would like to modify. (See 3.8, “Reports” on page 167.) For our example, we opened the Asset Summary report as shown in Figure 3-93 on page 199.
2. On the Asset Summary report page, select **Options** → **Add Query Table** as shown in Figure 3-96.

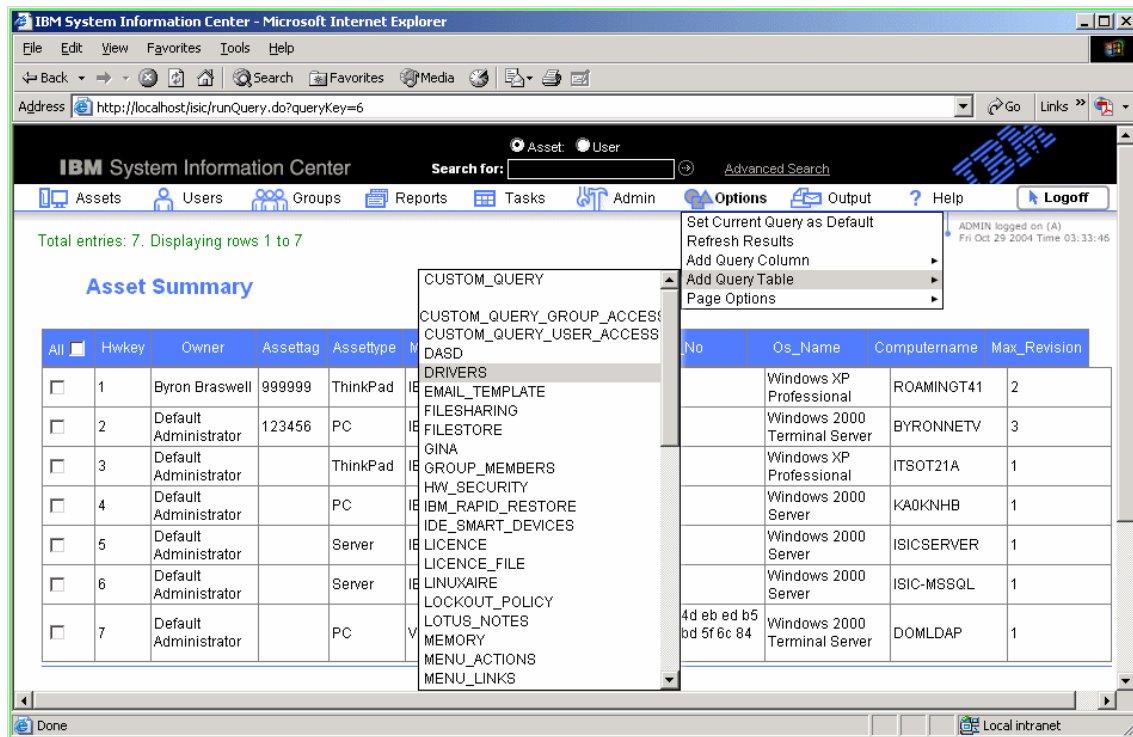


Figure 3-96 Selecting a query table to add

In the example shown in Figure 3-96, we selected **DRIVERS**. The Asset Summary report page refreshes.

Note: The query table addition will be available for selection only for the current report being displayed.

- On the Asset Summary report page, select **Options** → **Add Query Column** as shown in Figure 3-97.

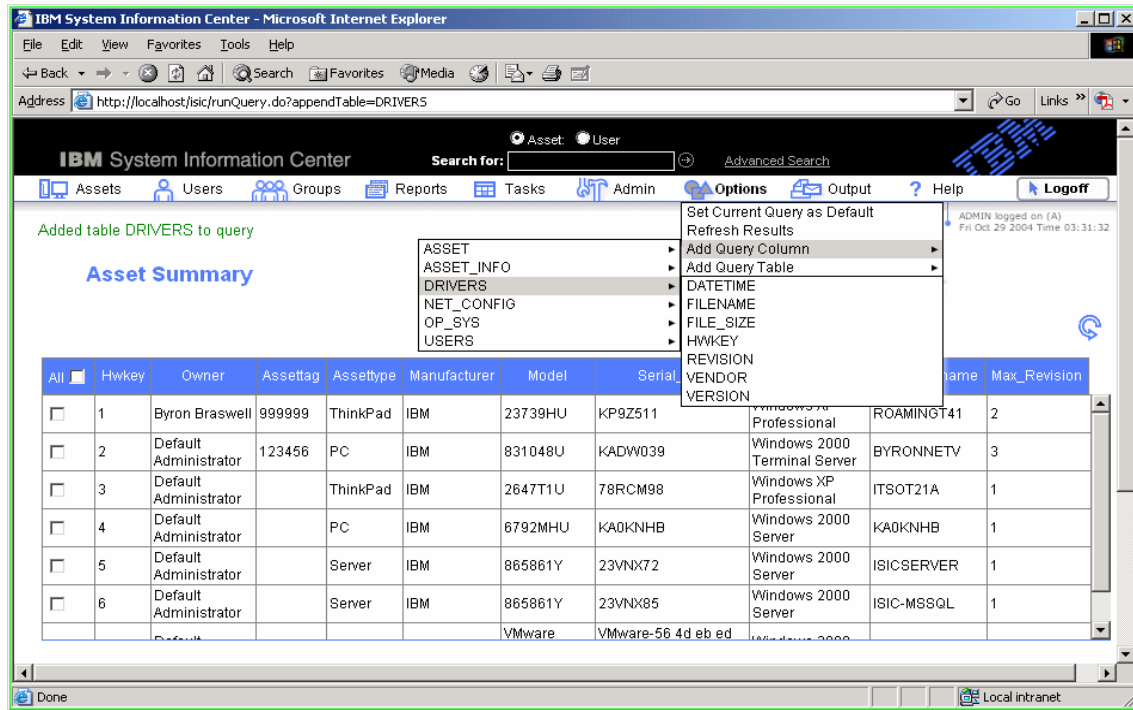


Figure 3-97 Selecting a column to add

Compare Figure 3-94 on page 200 with Figure 3-97 and notice that the **DRIVERS** selection has been added to the Add Query menu. Also note that selecting **DRIVERS** opens another menu for further refining the specific driver column to add to the Asset Summary report.

See the *IBM System Information Center Administrator's Guide* installed with System Information Center in \ISIC\web\help\ISICADM.pdf for additional information.

3.11.5 Page Options

This feature is used to select how many rows appear on a report page before you must page forward for additional output. To take advantage of Page Options:

- Open a report as described in 3.8, "Reports" on page 167. For our example, we opened the All Reports report as shown in Figure 3-98. Note from the report output that there are 126 lines to be displayed.

IBM System Information Center - Microsoft Internet Explorer

Address: http://localhost/sic/runQuery.do?pageRows=0

IBM System Information Center

Search for: [] Advanced Search

Assets Users Groups Reports Tasks Admin Options Output ? Help Logoff

Total entries: 126. Displaying rows 1 to 126

ADMIN logged on (A)
Fri Oct 29 2004 Time 04:03:26

All Reports

All	Querykey ↑	Group_Name ↑	Name ↑	Description	Display	Creator	Created
<input type="checkbox"/>	78	Actions	List Authorized Menu Actions	List all menu actions which the user has the correct authority to run and are relevant to the current report	0	IBM	2004-10-01 18:03:21.979
<input type="checkbox"/>	6	All Assets	Asset Summary	List a summary of all systems inventoried	1	IBM	2004-10-01 18:03:17.733
<input type="checkbox"/>	10	All Assets	Assets Not Inventoried in 90 Days	List all assets not inventoried in 90 days	1	IBM	2004-10-01 18:03:17.943
<input type="checkbox"/>	11	All Assets	Assets In Transfer	List all assets that are in the transfered state	1	IBM	2004-10-01 18:03:17.993
<input type="checkbox"/>	16	All Assets	All Non PC Assets	Show all non pc assets	1	IBM	2004-10-01 18:03:18.274
<input type="checkbox"/>	19	All Assets	All Assets	List a summary of all assets in the system	1	IBM	2004-10-01 18:03:18.434
<input type="checkbox"/>	23	All Assets	Asset Type Summary by Location	List a summary of asset quantity by type and location	1	IBM	2004-10-01 18:03:18.975
<input type="checkbox"/>	24	All Assets	Asset Info by Location	Show detail of all assets by location	0	IBM	2004-10-01

Done Local intranet

Figure 3-98 All Reports output

- From the All Reports page, select **Options** → **Page Options** as shown in Figure 3-99.

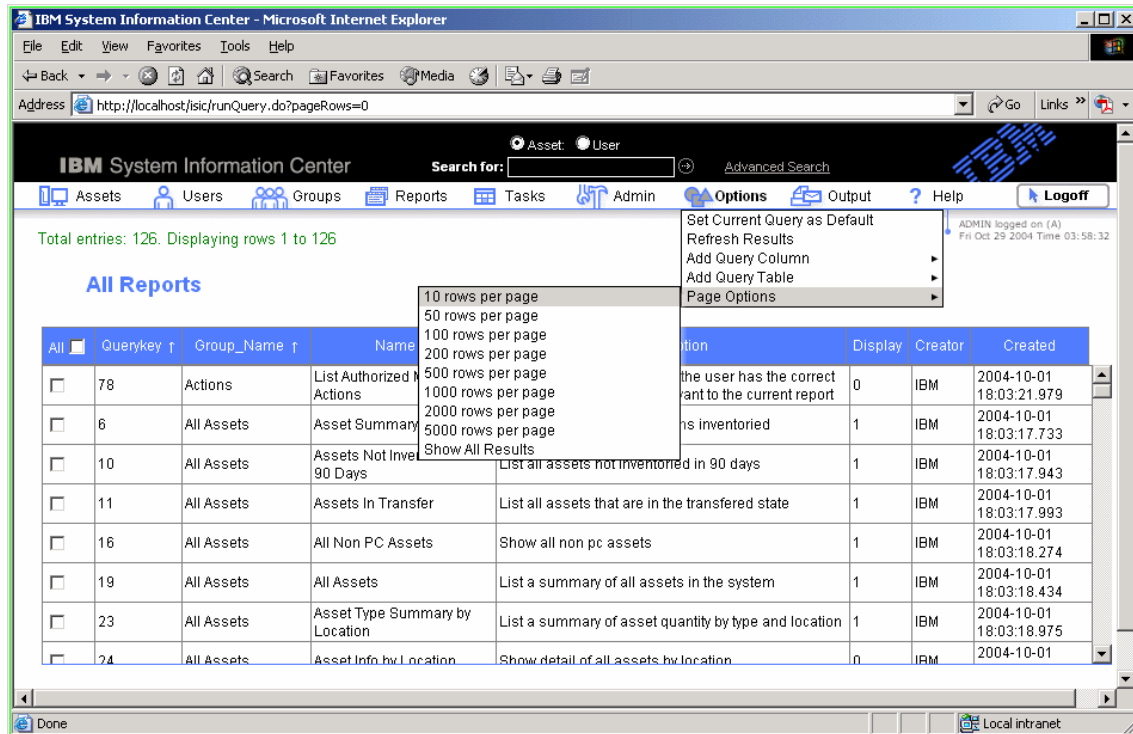


Figure 3-99 Page Options menu

- From the Page Options list, select the number of lines you would like to view before you must page forward. In our example, we selected 10 lines per page.

- The selected report is refreshed to show the amount of rows that you selected. See Figure 3-100 on page 206.

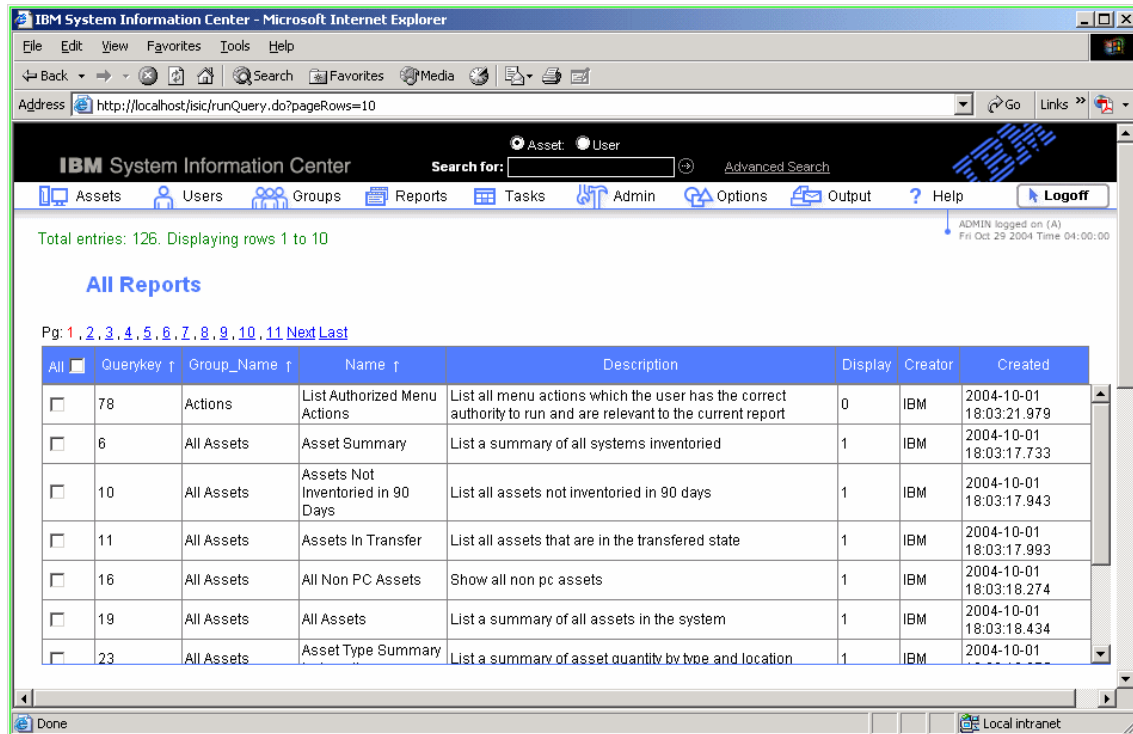


Figure 3-100 Refreshed All Reports page with new row limits

Note the comment above the report name that states which line numbers are currently displayed. Also note the addition of page selection hot spots to navigate through the output.

3.12 Output

You can perform the following tasks with the Output menu (Figure 3-101 on page 207):

- Save or open the information as a comma separated value (CSV) file
- E-mail reports
- Make the reports suitable for printing

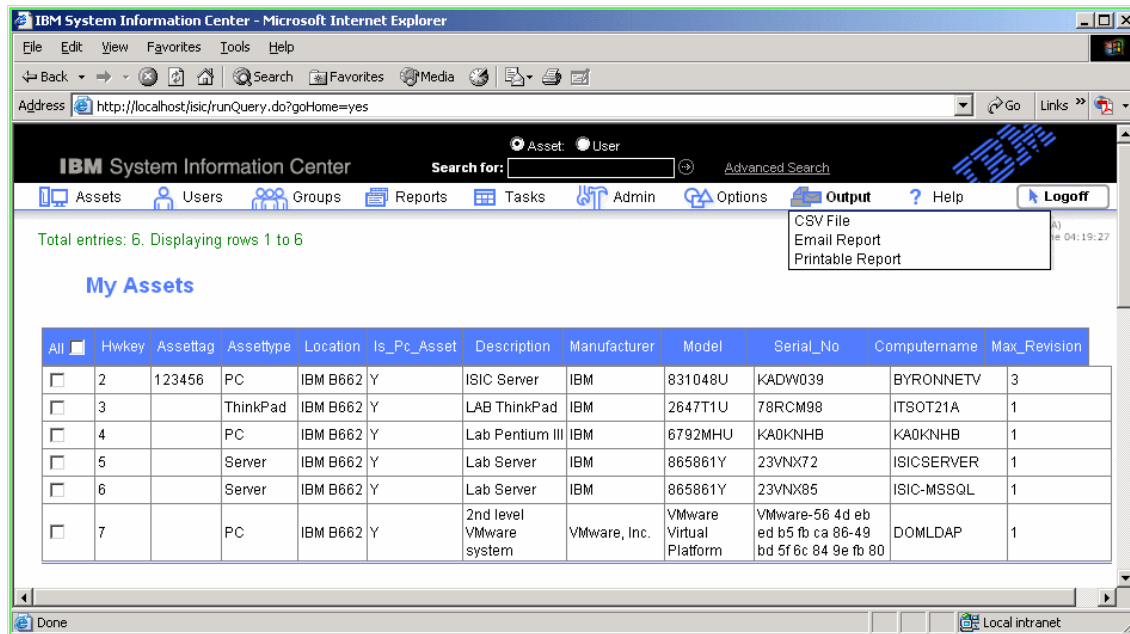


Figure 3-101 Output menu on main page

CSV File

This menu item is used if you would like to download and save the displayed report as a CSV file.

1. Open the report that you would like to save as described in 3.8, "Reports" on page 167.
2. From the report page, select **Output** → **CSV File**.
3. A dialog box (Figure 3-102 on page 208) asks you if you would like to save or open the CSV file. Click **Save** to save the file or **Open** to open it.

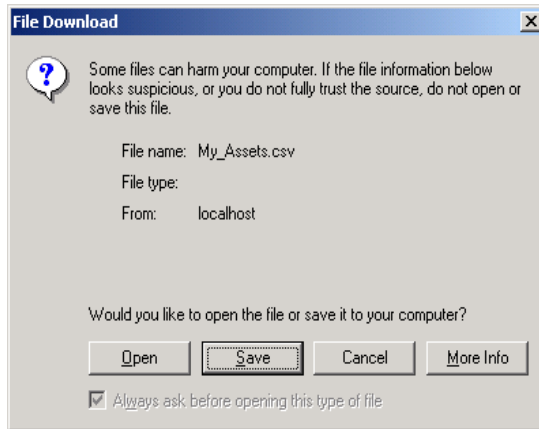


Figure 3-102 File Download window

Email Report

You can use this feature to send a report to an e-mail address, if System Information Center has already been configured for e-mail.

1. Open the report that you would like to e-mail.
2. Select **Output** → **Email Report** to open the window shown in Figure 3-103 on page 209.

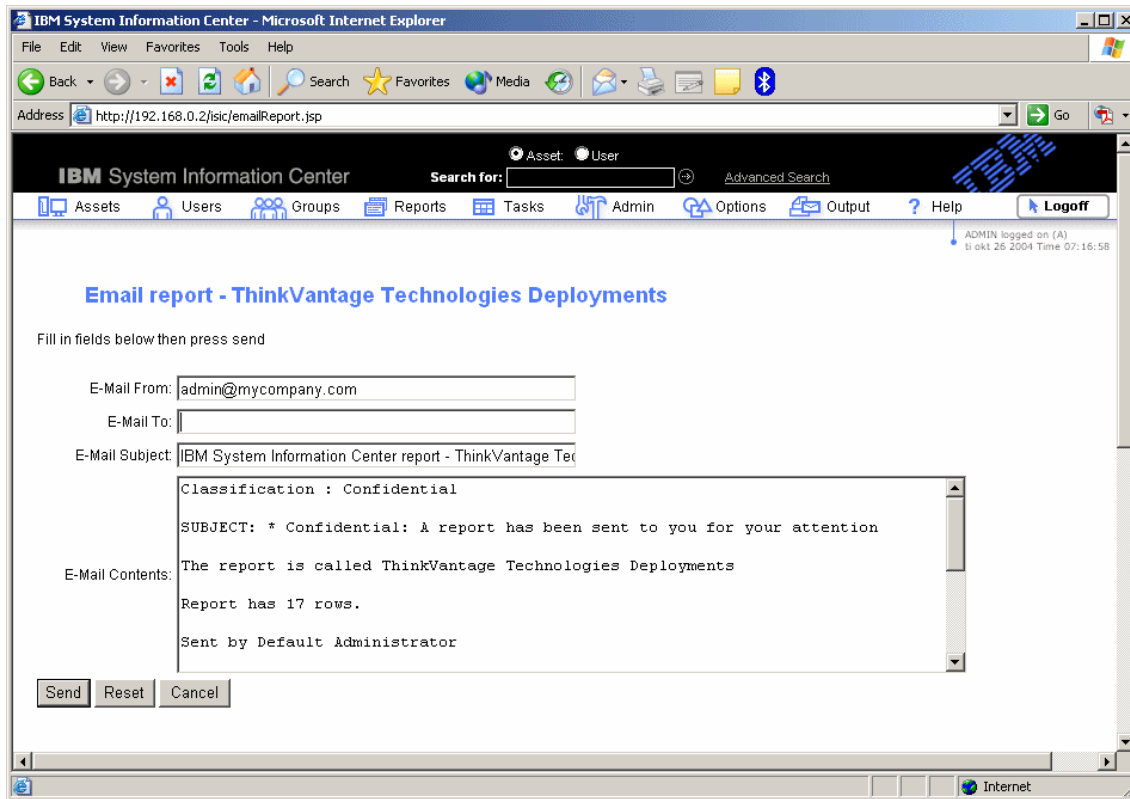


Figure 3-103 Email Report window

3. Enter an e-mail address and other information in the fields provided.
4. Click **Send**. The e-mail is sent and the report page opens again.

Printable Report

You may find it easier to study a long report when it is printed. Use this feature to print out a report as follows:

1. Open the report that you would like to print.
2. Select **Output** → **Printable Report**. This opens a new page that shows the selected report in a more appropriate form for printing.
3. To print the report, select the new page. Press CTRL+P or right-click the page and select **Print**.

3.13 IBM System Information Gatherer

IBM System Information Gatherer is an agent that runs on client machines. It gathers all the client information (drivers, operating system level, installed software, and so on) that is used to populate the System Information Center server database with information specific to this client. Refer to Figure 3-1 on page 96 for a graphical overview. See 3.1.2, “System Information Center components” on page 94 for more information on System Information Gatherer.

System Information Gatherer can be temporarily or permanently installed on client machines. The client machine must meet the following minimum requirements:

- ▶ Microsoft Windows 2000 or Microsoft Windows XP operating system
- ▶ Microsoft Internet Explorer 6.0 or higher
- ▶ TCP/IP and an Internet connection

The IBM System Information Gatherer program may be compatible with Microsoft Windows 98 and NT clients, however it is not normally supported in those environments. Support can be provided from IBM Global Services through an IT Specialist during on-site visits. These additional customization services are also available through IBM Global Services:

- ▶ Creation of new reports
- ▶ Customization of Web pages
- ▶ Integration with other solutions

Contact Gavin Cameron at gcameron@uk.ibm.com or Goran Wibran at wibran@us.ibm.com.

Refer to the *IBM System Information Center Administrator's Guide* on the System Information Center product CD for more information.

3.13.1 Temporarily installed client agent

System Information Gatherer is temporarily installed on the client during a user-initiated asset registration (see 3.5.2, “Register Asset” on page 140) or an asset upload (see 3.5.1, “Upload Asset Scan” on page 135). It is removed after the asset scan is completed and information is uploaded to the System Information Center server.

Client computers with this temporary installation cannot be prompted by the System Information Center server to perform scheduled scans.

3.13.2 Permanently installed client agent

System Information Gatherer can be installed permanently in one of the following ways:

- ▶ From the product CD (IBM and non-IBM computers)
- ▶ From the Web (IBM computers only)
- ▶ From the System Information Center GUI (IBM and non-IBM computers; see 3.5.19, “Download Agent Installer” on page 154 for more information).

Computers with a permanent installation can be prompted by the System Information Center server to perform scheduled scans. Information gathered during these scheduled scans is uploaded and updated in the System Information Center database.

3.13.3 Installation from product CD

To install System Information Gatherer (isig_oem.exe) from the product CD, make sure you know your server address and proceed as follows:

1. Insert the product CD into the CD drive on the client computer.
2. On the Windows desktop, select **Start** → **Run**.
3. If you are installing from the System Information Center CD, use the following command (where D is your CD drive):

d:\client\isig_oem.exe

4. If you are installing from the System Information Gatherer CD, use the following command (where D is your CD drive):

d:\isig_oem.exe

5. Click **OK**. This begins the installation of the System Information Gatherer client and opens the wizard illustrated in Figure 3-104 on page 212.



Figure 3-104 First installation window

6. Click **Next**.

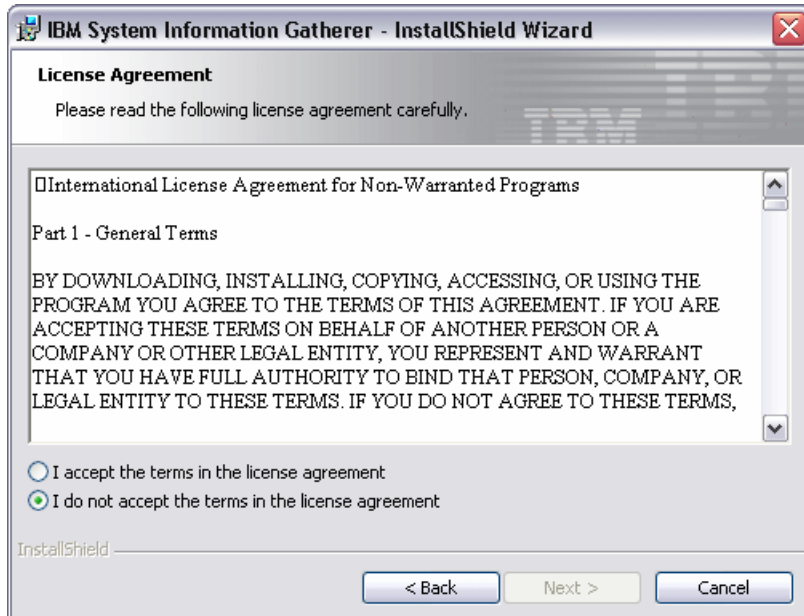


Figure 3-105 License Agreement window

7. Read the license agreement shown in Figure 3-105.
8. Select **I accept the terms in the license agreement** and click **Next** to open the Server address page (Figure 3-106).

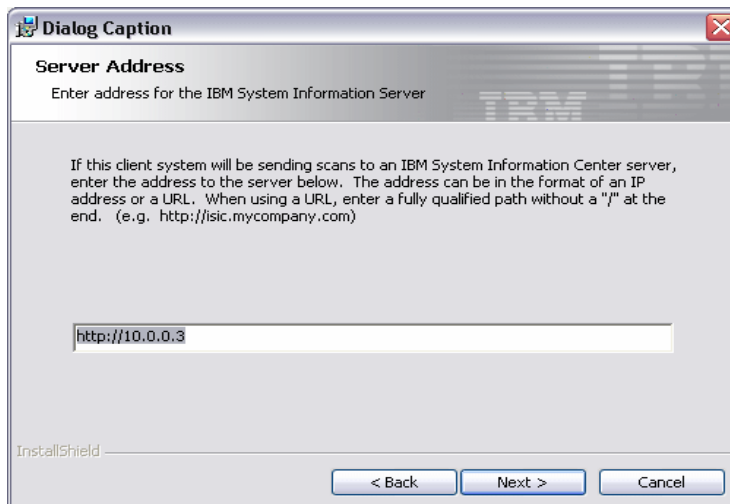


Figure 3-106 Server Address window

9. In the Server Address window shown in Figure 3-106, it is very important that you know the Web or intranet address of your System Information Center server.

In the field in this window, enter your System Information Center server address. You must include `http://` at the beginning of the System Information Center server address. You can use either an IP address or a DNS name for the server address.

Do not use `/` at the end of the address. Do not add `/isic` to your address. Only type in the base address (for example, `http://10.0.0.3`).

When you have typed in the address correctly, click **Next** to open the installation wizard (Figure 3-107).

Important: If you do not enter the address of your System Information Center server in this window (leave the input field blank), you will not be able to perform automatic scheduled uploads to the System Information Center server.



Figure 3-107 Ready to Install

10. Click **Install** to begin the installation.



Figure 3-108 InstallShield Wizard Completed

11. The installation process installs the System Information Gatherer client code in a directory named C:\IBMT00LS\ISIC\ on the client machine. When the installation is complete, the window illustrated in Figure 3-108 opens. The client can now communicate with the System Information Center server.

3.13.4 Installation from the Web (IBM computers only)

A version of the IBM System Information Center Gatherer program is available on the Web at:

<http://www.ibm.com/pc/support/site.wss/documentn.do?Indocid=MIGR-56187>

This version of the client agent is intended for IBM computers only, and is named `isig_ibm.exe`. The installation process is the same as documented in 3.13.3, “Installation from product CD” on page 211.

3.14 Customization and advanced usage

This section provides an outline of some typical enterprise scenarios that may use System Information Center. The *IBM System Information Center Administrator's Guide* provided with the installation files is a critical resource when deploying System Information Center in an enterprise environment.

Additional support and customization of System Information Center can be obtained from the IBM System Information Center development and support staff located in Greenock, UK. Contact Gavin Cameron at gcameron@uk.ibm.com or Goran Wibran at wibran@us.ibm.com.

3.14.1 Enterprise environment considerations

Enterprise environments present two different scenarios:

1. Asset information must be gathered automatically. An agent is installed as a service with Windows operating systems. This agent is able to run under a locked-down desktop. Using System Information Center, this agent can send the asset information, scheduled on a weekly or monthly basis, to the System Information Center server. To match the user information with an inventoried asset, the asset information can be configured to work with the Directory Services used by the enterprise.
2. Enterprise environments often have thousands of assets, which results in a very large detailed report. Locating a single asset in such a report can be very difficult. Using System Information Center, these report views can be customized to meet the needs of the user. For example, a report can be created that lists all assets assigned to a specific department or it can be structured based on a company, unit, division, team, users, and computers.

3.14.2 Deployment scenarios

This section describes several deployment scenarios for System Information Center. To fully implement these scenarios, however, you must import additional information from existing enterprise systems and databases.

The scenarios discussed in this section have the following requirements:

- Unattended activation of the probe (without user interventions or windows)
If the System Information Center client is packaged with IBM Software Distribution Assistant or other tools and distributed to all clients, it must be configured to suppress user dialog boxes during installation. It should also be configured to send inventory data back to System Information Center using the client Call Home feature.

- ▶ Collection of user identification such as e-mail address, Windows account, or user logon

Enterprise users must be populated in the System Information Center database so that it is not necessary to create accounts manually.

Tip: It is recommended that the enterprise e-mail address be used to identify users. The e-mail address should be used to populate the User ID field in System Information Center. See Figure 3-55 on page 157 for an example. This field must be globally unique.

- ▶ Previous population of System Information Center properties file fields where applicable

Data relevant to System Information Center contained in the import source data should populate the corresponding System Information Center fields. For example, if a user's e-mail address is entered in the User ID field, then the same information should populate the e-mail address field. The user's first name should go into the Forename field and the user's last name should go into the Surname field. All fields that have been designated as required fields need to be populated to ensure each user entry is valid.

- ▶ Agent/probe behavior
 - When first scanned, the probe executable should stay in the client hard disk [Optional/IT configurable].
 - The Call Home feature should check for a newer version on the server. If one is found, it should be downloaded if necessary and used.

Inventory only

In this case, the enterprise is only using System Information Center to maintain a either a hardware inventory, software inventory, or both. The user demographics are not to be collected or correlated to the inventory information. This is the most limited use of System Information Center in an enterprise. There is no need for advance user demographics. All clients are owned by the default user.

Full function (manual user setup)

In this case, each enterprise user logs into the System Information Center site, creates a user account, and uploads their assets. The user then enters demographics information.

The benefit of this scenario is that the System Information Center database does not need to be populated by outside data. The System Information Center database populates with relevant location, department, and asset type data as users create accounts and enter assets.

The disadvantage of this approach is that the consistency of entries and completeness of the asset inventory depends on the individual user. Some of these issues can be minimized by customizing the input screens and providing the end users with instructions to follow.

Tip: By default, System Information Center does not have prepopulated values for fields in the user and asset demographics forms. A manual workaround is to have the administrator populate these fields beforehand by selecting **Other** and entering the values that the company would like to be available to the end users. All values added in this manner become available to all users immediately after the asset is added to the database.

Full function (Automated user setup)

In this scenario, there is no user input. The user account is created based on a full e-mail address selected from user identification provided by the inventory scan described in “Inventory only” on page 217. The System Information Center password will expire and is reset by user after the initial login. An e-mail prompting a user to update user information is sent by System Information Center after the initial scan has been completed to ensure that each user’s asset information is current.

The benefit of this scenario is the consistency of initial data. It guarantees that all users in the source data will be added to the System Information Center database.

The disadvantage of this solution is that an outside source such as LDAP or an HR record system must be able to provide the required data to System Information Center in a usable format.

3.14.3 Secure access

The configuration of System Information Center for secure access through LDAP or other Directory Services can be configured as well as utilization of SSL via the editing of the C:\ISIC\tomcat\jakarta-tomcat-4.1.30\conf\server.xml file.



IBM Software Delivery Center

IBM Software Delivery Center is a software delivery solution that uses Web-based tools and technology to deliver software components to computers distributed throughout a corporate enterprise.

The following topics are covered in this chapter:

- ▶ Introduction
- ▶ Architecture considerations
- ▶ IBM Software Delivery Center server installation details
- ▶ Installing the Software Delivery Center client
- ▶ Building your Software Library
- ▶ Setting up your Software Delivery Center infrastructure
- ▶ Using the IBM Software Delivery Center administrator's console
- ▶ Using the IBM Software Delivery Center software catalog
- ▶ Troubleshooting

4.1 Introduction

For the past several years, customers have been migrating their environments to Web-based environments and want products and services to integrate with them. With the proliferation of corporate TCP/IP and Web-based intranets, it is logical to use them to deliver software to and manage software on enterprise computers. Web-enabled applications have the following advantages:

- ▶ Single interface for all clients and platforms
- ▶ Consistent, easily learned interface
- ▶ On demand availability
- ▶ Low cost of implementation and ownership

Many of the software delivery products in the marketplace are not Web based or Web enabled. The few Web-based software delivery solutions that do exist provide minimal functionality with a high degree of cost and complexity. They generally do not incorporate all the necessary requirements or they are too expensive to implement just for distributing software.

IBM Software Delivery Center is a cost-effective, full function, on demand, Web-based software distribution solution that delivers software updates and patches to networked and non-networked clients. Software Delivery Center helps administrators deliver to and manage software for a user, a group of users, or an entire organization through a single interface.

Software Delivery Center also can distribute software on CD for users who are not connected to the network or do not have access to the Software Delivery Center server.

4.1.1 Software Delivery Center benefits and features

Software Delivery Center has many valuable features that work together to satisfy current customer requirements and provide the following benefits:

- ▶ Ease of integration into the enterprise environment

The Software Delivery Center components (such as the Java Runtime Environment, Apache Tomcat server, and IBM HTTP Server) are reliable, industry-standard components and use cutting-edge Java and Web-based technologies.

- ▶ Ease of management

Software Delivery Center is easy to implement, use, and manage. An administrator can use a Web browser to access the administrator's console to push software packages and updates to one or multiple Software Delivery Center clients.

- Familiar interface

The Software Delivery Center user interface is a standard Web browser. This familiar end-user interface helps enhance usability and shorten learning time.

- Low cost and immediate return on investment

Software Delivery Center components provide a cost-effective solution. By contrast, planning, designing, devising naming conventions, and purchasing hardware and proprietary software for other software delivery solutions requires a big investment of time and money.

- Scalable solution

Software Delivery Center can be used by small, medium, and large enterprise environments.

Software Delivery Center includes the following features:

- Simple packaging requirements

The Software Delivery Center process works with various industry-standard packaging tools and utilities, such as InstallShield, Wise InstallManager, WinZip Self-Extractor, and Microsoft Software Installer (MSI). Software and data files also can be distributed in an unpackaged format.

- Incompatible installation prevention check

You can restrict each software package to one or more operating system environments. As you build each software package, you specify which platforms are supported and restrict the software package from being installed on computers with incompatible operating systems. If a software package is designed only for installation on a Windows XP computer, a user with a Windows 2000 computer will not be permitted to install it.

- Free-space checking

Before a software package is installed on a client computer, adequate free space must exist. Software Delivery Center checks the amount of free space to help ensure enough storage is available before the software package is delivered to a user.

- Locked-down desktop support

Software Delivery Center provides software installation to an environment where the user does not have the necessary access rights or privileges to install software.

- Checkpoint restart

Software Delivery Center program supports a byte-level checkpoint restart. If the delivery of a software package is interrupted because the network disconnects, only the missing data is sent when the network connection resumes.

- ▶ Self-updating agent

The Software Delivery Center client agent periodically checks the server for updates and automatically installs the required updates.

- ▶ Detailed logging

Detailed information about each software package installed through the Software Delivery Center process is available. If a problem occurs, the logs show which client had the error.

- ▶ Security and access control

Managing access to software packages in the Software Delivery Center process is simple. Based on your requirements, you set up groups to see catalogs of different software packages. Access is based on the organization, job function, or any other criterion that is viable in your company

4.1.2 Software Delivery Center components

Software Delivery Center consists of two parts: the server and the client.

Server

The server is the control center that manages software packages, groups, users, logs, and schedules. The server has three main areas of functionality:

- ▶ Server management

This area provides the group, user, packaging and bundling, and distribution management.

- ▶ Client communication

Clients can access the server using:

- Applet login check
- Query for scheduled push packages
- Log information sent back to the server

- ▶ Data persistence layer

The data persistence layer isolates data to provide independent database access.

Server components

The Software Delivery Center server has the following components:

- ▶ Cloudscape

Cloudscape is an embedded relational database-management system. This component allows Software Delivery Center to store and maintain the package metadata and log information.

- ▶ Installation program: SDC-SRVINST.EXE
SDC-SRVINST.EXE installs Software Delivery Center components on the server.
- ▶ Administrator's console
Administrators use this browser-based interface to manage the Software Delivery Center process. Administrators can manage multiple catalogs for different groups or business units. They can also add, delete, and modify software packages.
- ▶ IBM Java 2 SE SDK Version 1.4.2
This industry-standard, platform-independent programming language is part of the Software Delivery Center server.
- ▶ IBM HTTP Server, Version 2.047
This HTTP server software application is powered by industry-standard Apache Web Server Version 2.0.

Software Delivery Center also has provisions for downloading and installing Apache Tomcat Version 4.1.30 on the server. Apache Tomcat is a servlet container for Java servlet and JavaServer Pages technologies and is required by Software Delivery Center.

Note: Although the Software Delivery Center installation process installs the Apache Tomcat program, you are responsible for downloading the Apache Tomcat Version 4.1.30 zipped file from the Apache Web site and copying it to a specific folder. See 4.3, "Software Delivery Center server installation details" on page 231 for details. At the time this redbook was published, version 4.1.30 could be downloaded from the following Web site:

<http://archive.apache.org/dist/jakarta/tomcat-4/v4.1.30/bin/>

Client

Software Delivery Center has two main features: the client agent and the client applet. The client agent runs as a service that checks the server periodically at specified intervals to find the next scheduled installation package. It is also a local installer for the Software Delivery Center client applet if a software package needs secure installation.

Note: The Software Delivery Center client agent runs in the background. There is no administrator or user interface. Because the client agent runs as a service, it can be disabled through the Administrator's Tools function of the Windows Control Panel. By default, the client agent is set to start automatically. The client agent is listed as *SDCAgent* in the list of services.

The client applet runs either from the browser as a Java application or as a stand-alone Java Web Start application. It presents all software packages for which a particular user has access privileges. Users can select and install software packages from an online catalog. When the user selects a software package, the client applet shows detailed data about the software package.

If the software package the user selected meets the user's needs, the user clicks the **Install** button. The install procedure starts automatically. If the user does not have the rights or privileges to install the software package on that computer, the client applet passes the software package to the client agent to be installed

Client components

The components of the Software Delivery Center client are:

- ▶ Software Delivery Center client applet
This Java-based applet presents a catalog of software packages to the user. From this catalog, the user can select a software package for installation. The software package is downloaded to the client and automatically installed.
- ▶ Software Delivery Center client agent
The Software Delivery Center client agent controls the installation of software pull packages that require administrative rights to install and schedule pushes of software.
- ▶ IBM Java 2 Runtime Environment (JRE) Version 1.4.2
This is an industry-standard, platform-independent programming language.
- ▶ Installation program: SDCSETUP.EXE
This software package installs the JRE, the Software Delivery Center client agent, and the Software Delivery Center client applet on the client.

4.2 Architecture considerations

In this section, sample high level architecture overview diagrams are provided for small, medium, and large environments.

This section includes the following topics:

- ▶ "Architecture considerations" on page 225
- ▶ "Customization considerations" on page 229
- ▶ "Hardware specifications and recommendations" on page 230

4.2.1 Architecture considerations

You must consider several factors when designing and deploying a Software Delivery Center infrastructure. These factors include:

- ▶ Number of packages that you will be managing
- ▶ Average package size
- ▶ Number of distributions
- ▶ Hardware configurations
- ▶ Network topology
- ▶ Network bandwidth

As with any software-distribution solution, you should pay careful attention to the network topology. Place the Software Delivery Center server or servers as close to the clients as possible. The servers should be connected to the fastest backbone available, preferably 100 Mbps Ethernet or 1 Gbps Ethernet.

The following sections describe typical architectures for sample small, medium, and large network environments using Software Delivery Center.

Small and medium environments

The typical architecture for small and medium environments that handle up to 1500 clients consists of a single server dedicated to Software Delivery Center. The Software Delivery Center server pushes out software packages to clients that have the Software Delivery Center client agent installed or allows clients to pull packages and install them through a client application.

Figure 4-1 on page 226 shows a typical architecture for a small environment that can handle up to 1500 clients.

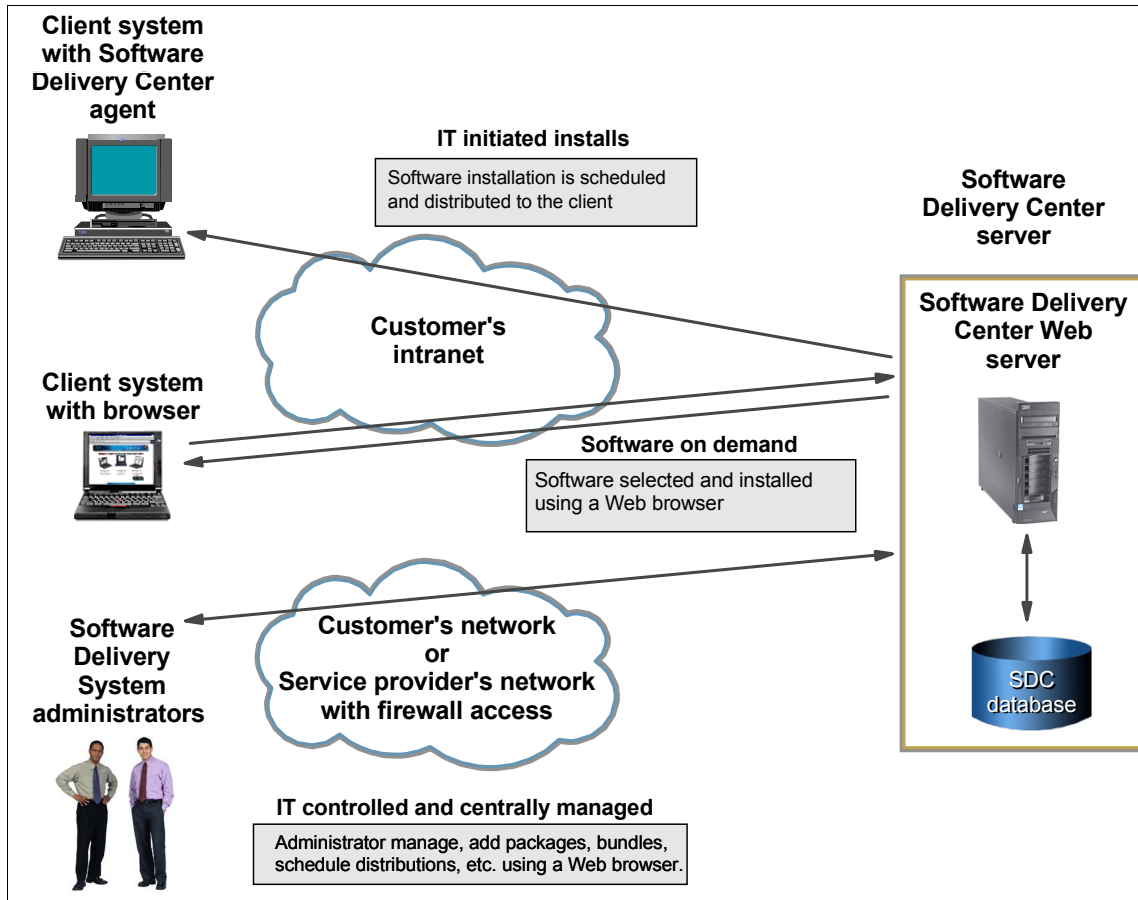


Figure 4-1 Sample Software Delivery Center architecture for small environment

If network bandwidth over a wide area network is an issue, Software Delivery Center provides the ability to store the software packages on remote files shares that are geographically close to the clients. A sample architecture overview diagram using this type of infrastructure is shown in Figure 4-2.

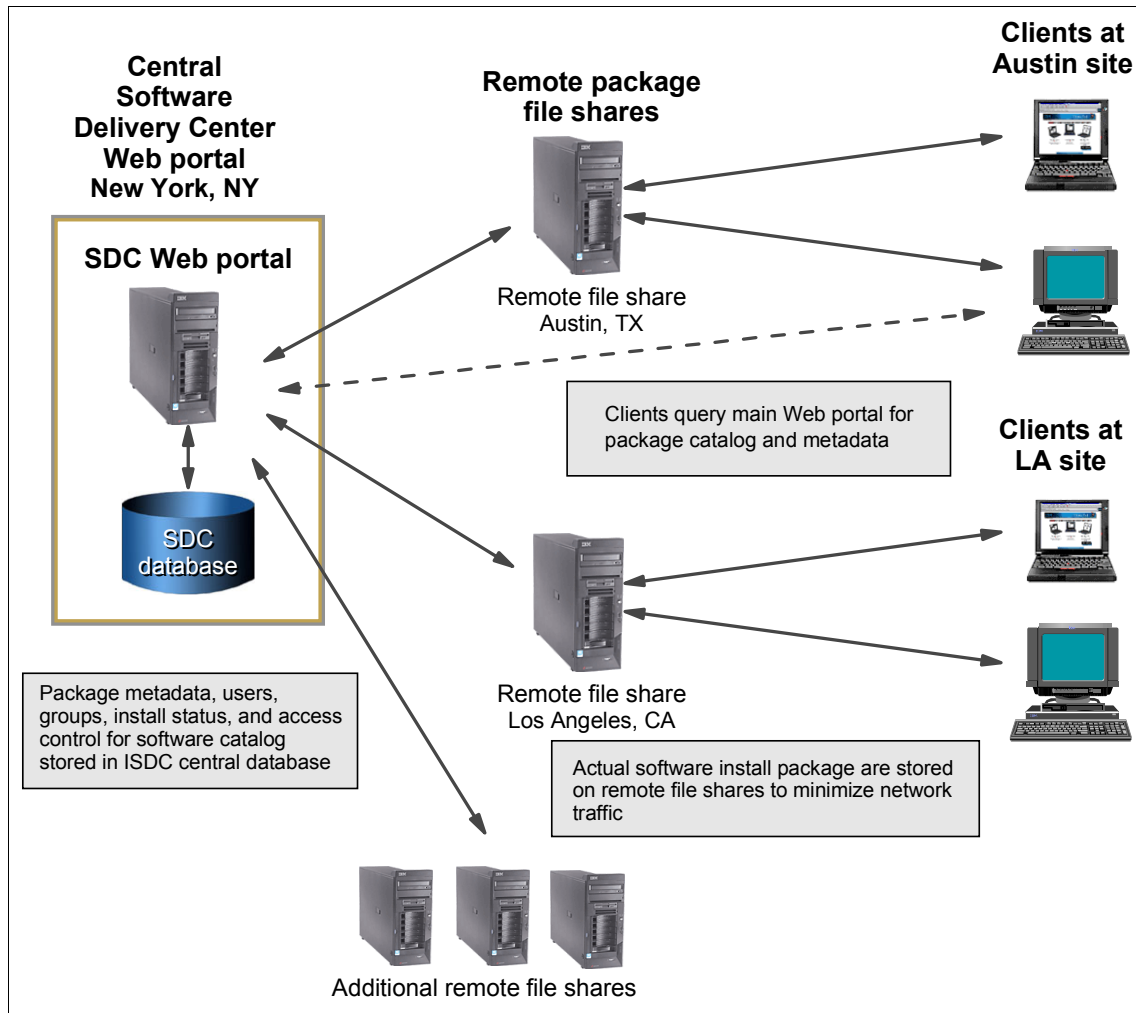


Figure 4-2 Sample Software Delivery Center architecture using remote file shares

Large environments

For larger environments, you can use multiple installations of Software Delivery Center servers. Segmented groups of users can be configured to use the server that is physically closest. Software Delivery Center provides export and import features to simplify the replication of the metadata associated with software packages and bundles from one server to another. This type of implementation is shown in Figure 4-3.

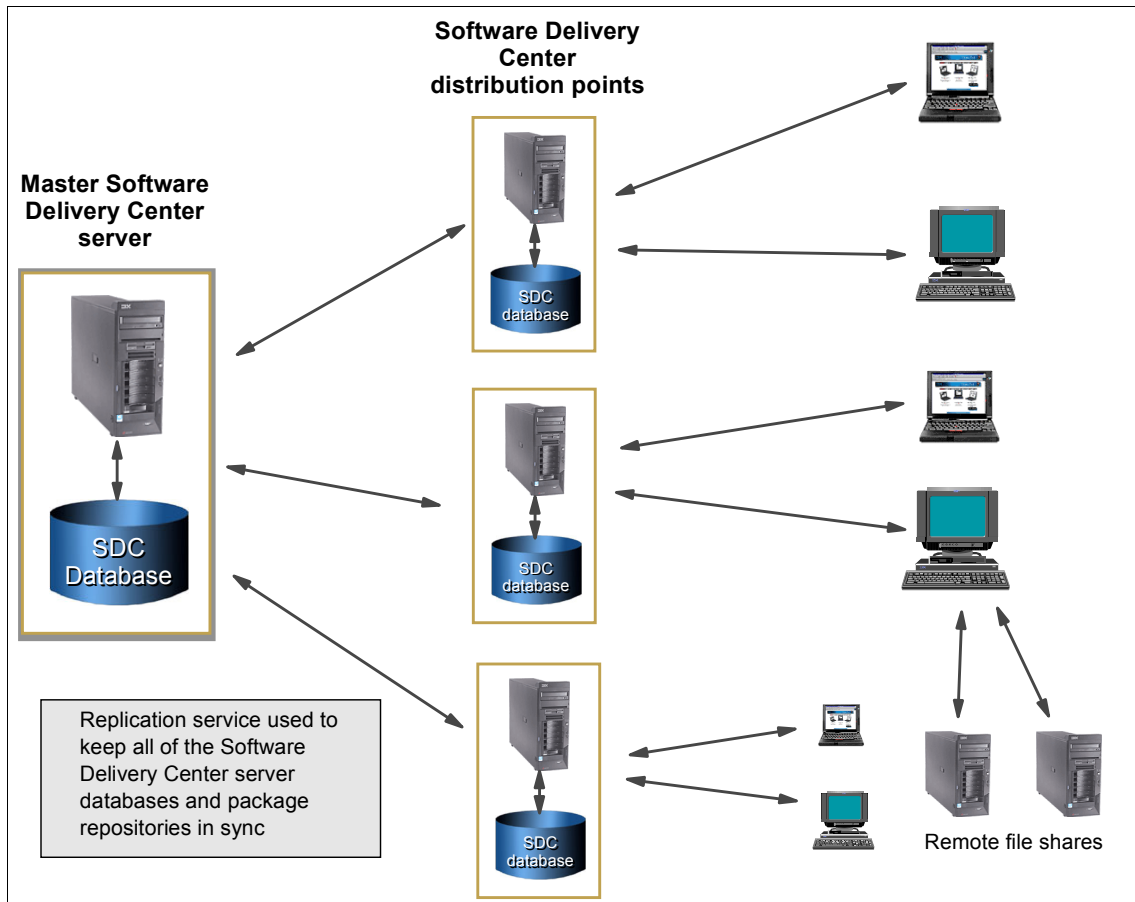


Figure 4-3 Sample tiered Software Delivery Center architecture

Another option is to use multiple Software Delivery Center servers and a load balancing solution as shown in Figure 4-4. For large enterprise environments, we recommend either IBM WebSphere Edge Server V2 or WebSphere Application Server V5 Edge Components (which both include IBM Network Dispatcher) to provide load balancing among several Web servers.

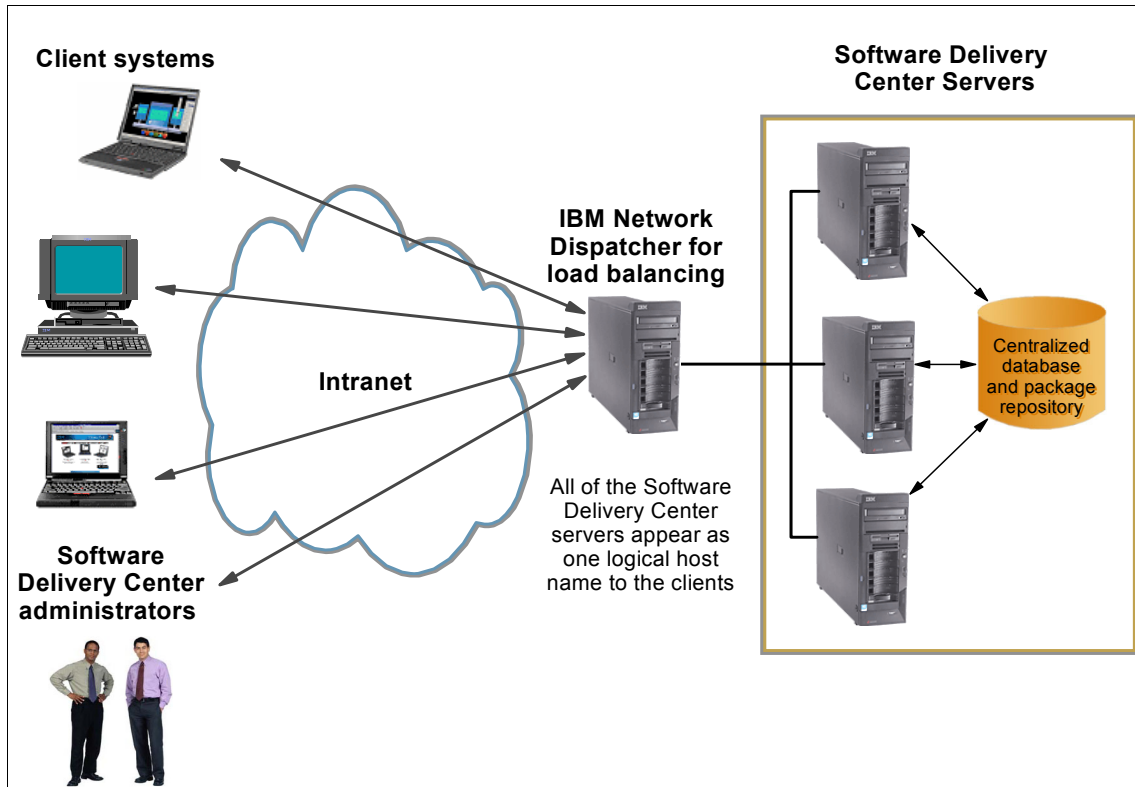


Figure 4-4 Sample Software Delivery Center architecture with load balancing

Note: If the architecture shown in Figure 4-4 is used, customization will be required on the server side so that only one instance of the Software Delivery Center database exists.

4.2.2 Customization considerations

It should be noted that while Software Delivery Center ships with a specific version of the IBM HTTP server, IBM Java, and the Cloudscape database, Software Delivery Center can easily be customized to integrate into an existing

customer's infrastructure. In general, all that is required to integrate Software Delivery Center into an existing infrastructure is:

- ▶ An HTTP server
- ▶ Java programming language version 1.4.2 or greater
- ▶ Apache Tomcat or equivalent
- ▶ A relational database system supporting SQL and JDBC

Each of these prerequisites is available on a large number of platforms and from several different vendors. IBM Global Services offers the following services to help customers integrate Software Delivery Center into specific environments:

- ▶ Architecture design and implementation
- ▶ Installation and setup
- ▶ Customization of Web pages
- ▶ Custom LDAP integration
- ▶ Custom database integration
- ▶ Custom software entitlement integration
- ▶ Customized sdcsetup.exe program
- ▶ Alternate Java Virtual Machine support.
- ▶ Agent integration and rollout
- ▶ Software packaging
- ▶ Software distribution management
- ▶ Non-Windows platform support
- ▶ Premium support services

For more information about these service offerings, send an e-mail to isdc@us.ibm.com.

4.2.3 Hardware specifications and recommendations

For best performance, the following minimum system requirements are recommended for the Software Delivery Center server computer:

- ▶ Dual Intel® Xeon® processors
- ▶ 2 GB of ECC RAM
- ▶ 15,000 RPM ultra320 SCSI hard drives with RAID controller
- ▶ CD-RW drive
- ▶ 200MB free hard disk space for server installation
- ▶ Additional space as required for package repository.
- ▶ One of the following operating systems:
 - Windows 2000 Server with Service Pack 4 or higher
 - Windows Server 2003
- ▶ Multiple NIC cards

4.3 Software Delivery Center server installation details

This section describes how to install and configure the server portion of Software Delivery Center on the Windows 2000 Server and Windows Server 2003 operating systems.

This section includes the following topics:

- ▶ “Installing a Windows operating system on the server” on page 231
- ▶ “Installing Software Delivery Center” on page 233
- ▶ “Testing the IBM Software Delivery Center server” on page 244
- ▶ “Providing security for the packages on the file server” on page 249

4.3.1 Installing a Windows operating system on the server

This section describes how to install the Windows 2000 Server and Windows Server 2003 operating systems.

Installing Windows 2000 Server

Install the Windows 2000 Server operating system on the computer you intend to use as the Software Delivery Center server. During the installation, perform the following tasks:

- ▶ Accept all of the default Windows component settings.
- ▶ When the Configure Your Server window opens, select **I will configure this server later** and clear the **Show this service at startup** check box.

Note: Depending on the networking card, video controller, and other hardware devices installed in your computer, you may have to acquire and install updated device drivers. Make sure all devices are working correctly before you continue.

When the operating-system installation is complete, continue by obtaining Windows 2000 Server critical updates and service packs.

Obtaining Windows 2000 Server critical updates and service packs

Go to the following Microsoft Web site:

<http://www.microsoft.com>

Download and install all of the critical updates and Service Packs for Windows 2000 Server. After you have installed all critical updates and Service Packs, continue by disabling IIS.

Disabling IIS

Software Delivery Center is designed to use port 80, which conflicts with the Internet Information Services (IIS) provided by the operating system.

To determine if IIS is installed, do the following:

1. Select **Start** → **Settings** → **Control Panel**. The Control Panel opens.
2. Double-click **Add/Remove Programs**. The Add/Remove Program window opens.
3. Click **Add/Remove Windows Components**. The Windows Components Wizard opens.
4. Locate the Internet Information Services (IIS) entry in the list of components.
 - If IIS is not installed, **Internet Information Services (IIS)** is not selected. To complete the installation process, click **Next**, and then click **Finish**.
 - If IIS is already installed, **Internet Information Services (IIS)** is selected. Disable IIS on your server by clearing the **Internet Information Services (IIS)** check box. (Disabling IIS also disables the DHCP and DNS servers, which interfere with Apache Tomcat). Click **Next**. The Completing the Windows Contents Wizard opens.
5. Click **Finish**.
6. Close all open windows.

When the installation is complete, you can install Software Delivery Center. For more information, refer to 4.3.2, “Installing Software Delivery Center” on page 233.

Installing Windows Server 2003

Install the Windows Server 2003 operating system on the computer you intend to use as the Software Delivery Center server. During the installation, perform the following tasks:

- ▶ Accept all of the default Windows component settings.
- ▶ When the Manage Your Server window opens, select **Don't display this page at logon**.
- ▶ Close the window.

Note: Depending on the networking card, video controller, and other hardware devices installed in your computer, you may have to acquire and install updated device drivers. Make sure all devices are working correctly before you continue.

When the operating-system installation is complete, continue by obtaining Windows Server 2003 critical updates and service packs.

Obtaining Windows Server 2003 critical updates and service packs

Go to the following Microsoft Web site:

<http://www.microsoft.com>

Download and install all of the critical updates and Service Packs for Windows Server 2003. After you have installed all critical updates and Service Packs, continue by disabling IIS.

Disabling IIS

Software Delivery Center is designed to use port 80, which conflicts with Internet Information Services (IIS) provided by the operating system.

To see whether IIS is installed:

1. Click **Start** → **Settings** → **Control Panel**. The Control Panel opens.
2. Double-click **Add/Remove Programs**. The Add/Remove Program window opens.
3. Click **Add/Remove Windows Components**. The Windows Components Wizard opens.
4. Locate the Internet Information Services (IIS) entry in the list of components.
 - If IIS is not installed, **Internet Information Services (IIS)** is not selected. To complete the installation process, click **Next**, and then click **Finish**.
 - If IIS is already installed, **Internet Information Services (IIS)** is selected. Disable IIS on your server by clearing the **Internet Information Services (IIS)** check box. (Disabling IIS also disables the DHCP and DNS servers, which interfere with Apache Tomcat). Click **Next**. The Completing the Windows Contents Wizard opens.
5. Click **Finish**.
6. Close all open windows.

When the installation is complete, you can install Software Delivery Center. For more information, refer to 4.3.2, “Installing Software Delivery Center” on page 233.

4.3.2 Installing Software Delivery Center

After you have installed the Windows server operating system, obtained critical updates and service packs, and disabled IIS, you can install Software Delivery Center from the installation CD.

During this installation process several events take place:

- ▶ You are prompted to download the Apache Tomcat 4.1.30 zipped file to the c:\tomcat4 folder.
- ▶ Apache Tomcat is installed.
- ▶ The IBM HTTP Server is installed.
- ▶ IBM JRE is installed.
- ▶ The Java home environment variable is created.
- ▶ The IBM Software Delivery Center Web application is installed, along with the IBM Cloudscape 5.1 database.

Complete the following procedures to install Software Delivery Center program.

Apache Tomcat Web server

1. Download Apache Group's Tomcat Java web server version 4.1.30 from this Web site:

<http://archive.apache.org/dist/jakarta/tomcat-4/v4.1.30/bin/>

2. Create a directory in the root of the C: drive named tomcat4.
3. Copy the jakarta-tomcat-4.1.30.zip to C:\tomcat4.

Important: The Software Delivery Center installation process detects jakarta-tomcat-4.1.30.zip in C:\tomcat4 directory. Do not change it.

The folder structure should resemble that shown in Figure 4-5

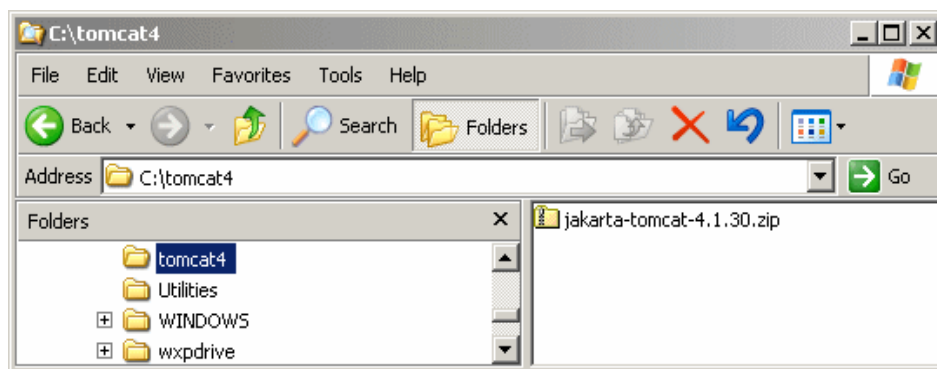


Figure 4-5 Tomcat file location

Note: During the IBM Software Delivery Center installation, the Tomcat zipped file will be extracted to \IBMSDC\TOMCAT413. At the end of the installation the c:\tomcat4\jakarta-tomcat-4.1.30.zip file will be deleted.

SDC, Cloudscape database, Java JDK, IBM HTTP server

The installation process for Software Delivery Center also installs the default Cloudscape database, IBM HTTP Server, and the required IBM Java JDK.

1. Insert the Software Delivery Center installation CD. The Software Delivery Center Installation wizard starts. If the wizard does not start, take the following steps:
 - a. From the Windows desktop, click **Start**.
 - b. Click **Run**.
 - c. Type `d:\sdc-srvinst.exe` (where *d* is the drive letter of the drive that contains the Software Delivery Center CD).
 - d. Click **OK**.
2. The window shown in Figure 4-6 opens.

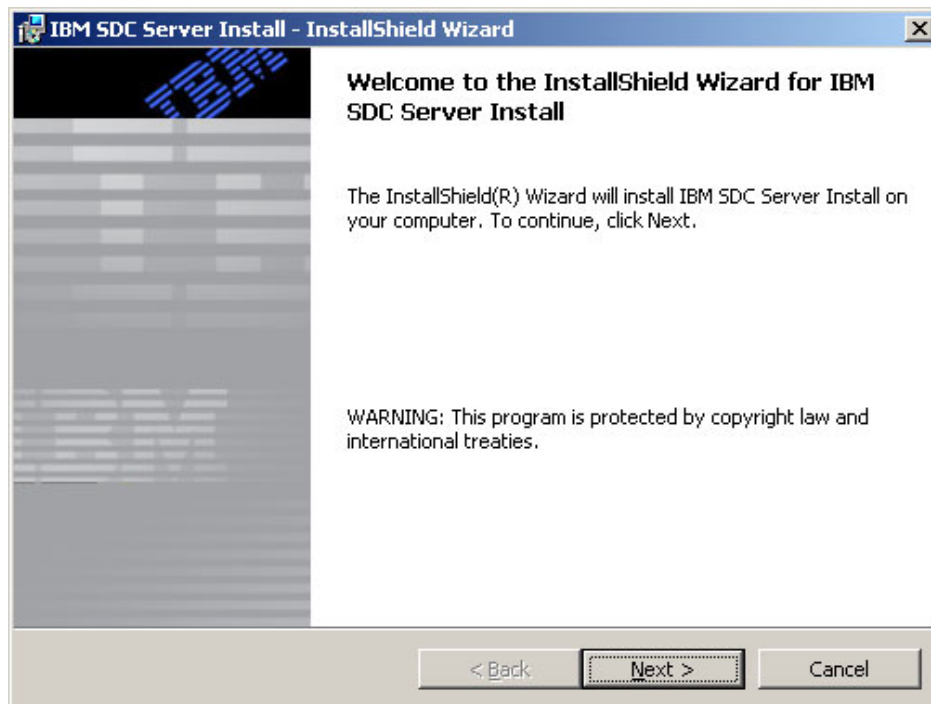


Figure 4-6 Software Delivery Center setup welcome window

3. Click **Next**. The window shown in Figure 4-7 opens.

This is the Apache Tomcat 4.1.30 Required window. It reminds the installer of the Tomcat version and file location requirement for proper Software Delivery Center installation. The correct version of the Tomcat zip file must be in the location shown in this window (a directory named C:\tomcat4) before proceeding with the installation of IBM Software Delivery Center.

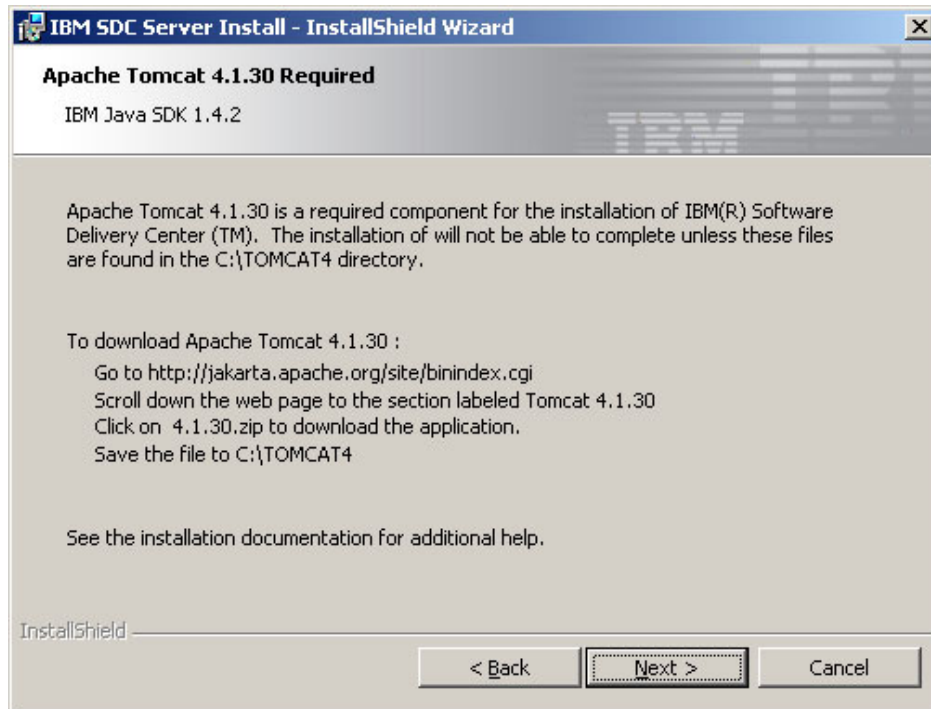


Figure 4-7 Apache Tomcat 4.1.30 warning

Note: The link to download Apache Tomcat 4.1.30 on the Apache Tomcat 4.1.30 Web site mentioned in Figure 4-7 has been changed to:

<http://archive.apache.org/dist/jakarta/tomcat-4/v4.1.30/bin/jakarta-tomcat-4.1.30.zip>

4. Click **Next**.
5. The Software Delivery Center installation process detects jakarta-tomcat-4.1.30.zip in the C:\tomcat4 directory. If the Software Delivery Center installation process detects a problem with the Tomcat 4 installation file, the window shown in Figure 4-8 on page 237 opens. Click **Back**. The

Tomcat version and file location requirement window shown in Figure 4-7 on page 236 will be displayed. Correct the problem and click **Next**.

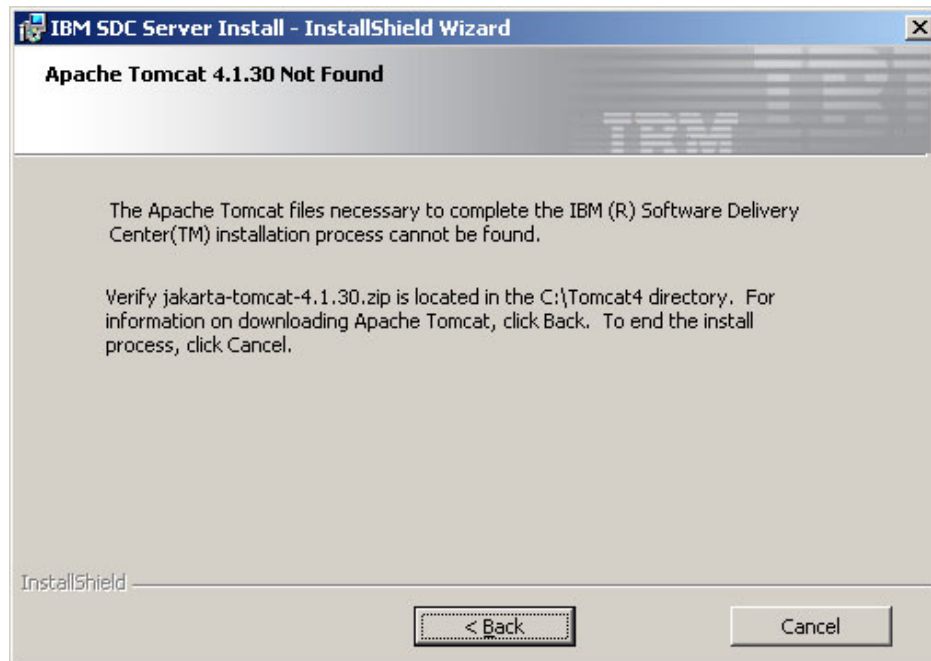


Figure 4-8 Tomcat installation file problem

6. If all prerequisites have been met or you have corrected any problem detected, the window shown in Figure 4-9 on page 238 opens.

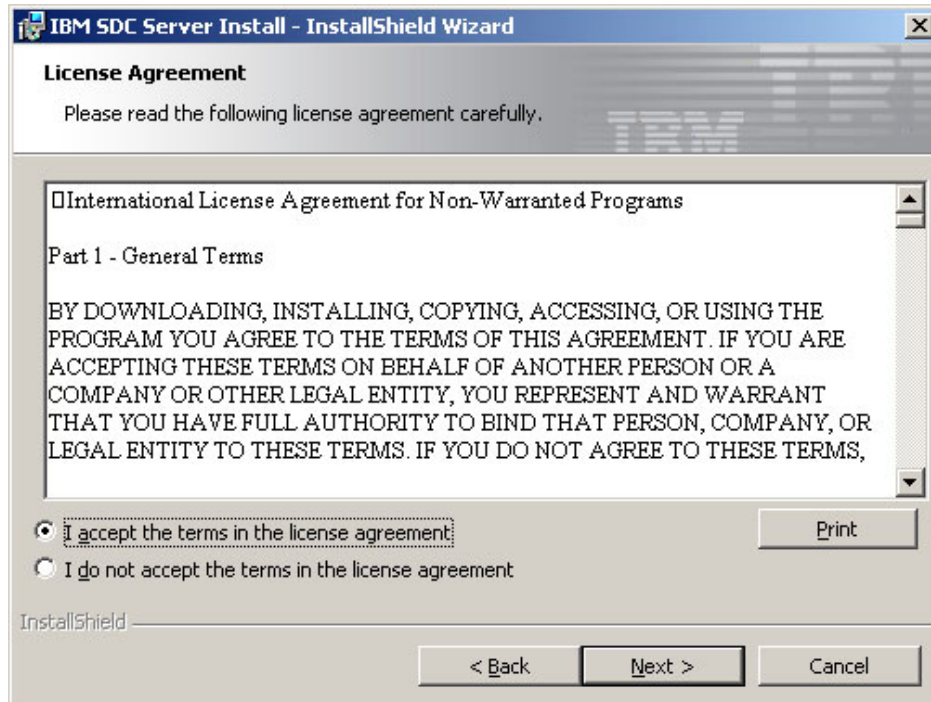


Figure 4-9 Software Delivery Center License Agreement

7. Read the license agreement and if you agree, select **I accept the terms in the license agreement** and click **Next**.

8. The Software Delivery Center URL and IP Address window shown in Figure 4-10 opens.

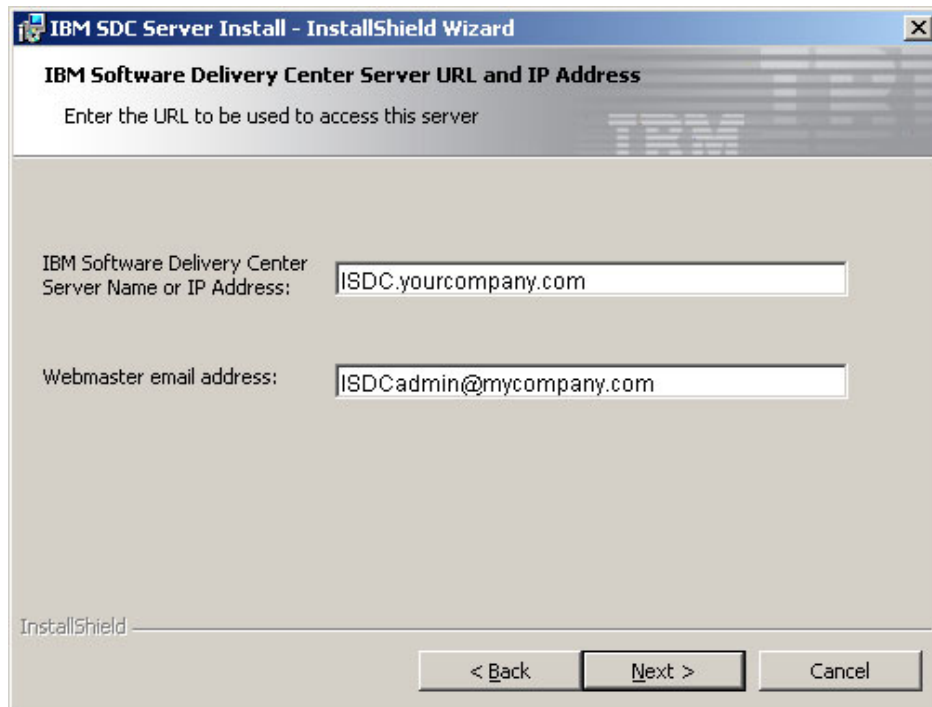


Figure 4-10 Software Delivery Center Web site settings

9. Type the URL or the IP address that will be used to access the server.

Note: In Figure 4-10, the box labeled **IBM Software Delivery Center Server name or IP Address** is the fully qualified domain name of the Software Delivery Center server from which you wish to launch the Software Delivery Center welcome page. This URL will be used as the *server name*.

10. Enter the e-mail address of the Software Delivery Center administrator in the Webmaster email address field.
11. Click **Next**.

12. The window shown in Figure 4-11 opens. This window gives you the option of specifying which folder the IBM Software Distribution Center code will be installed in.

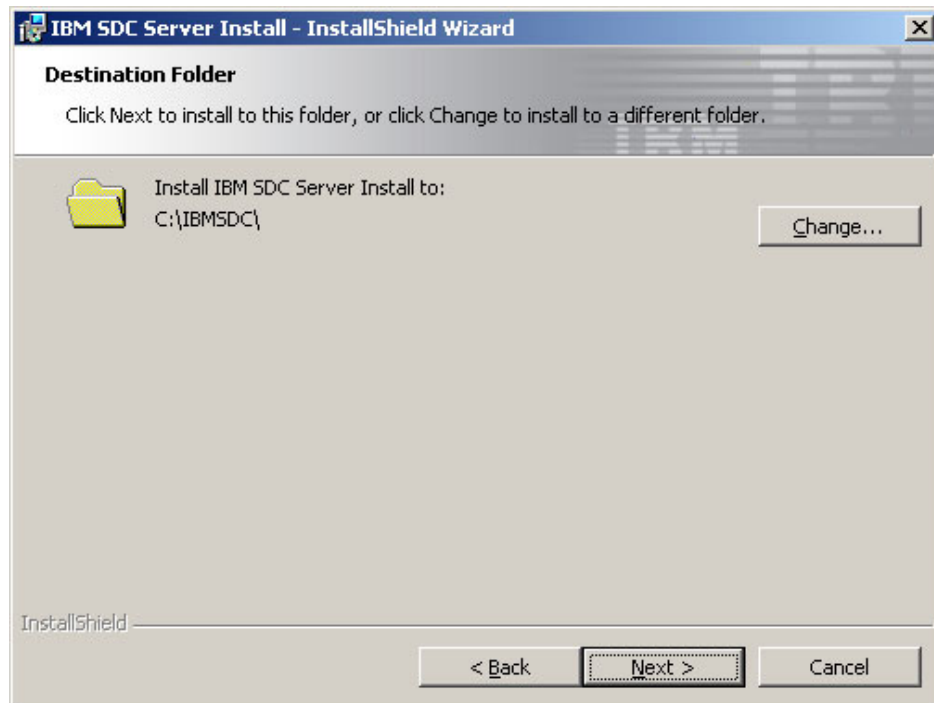


Figure 4-11 Software Delivery Center select location window

13. Either accept the default folder (C:\IBMSDC) or use the **Change** button to select a different folder.
14. Click **Next**.

15. The Ready to Install the Program window shown in Figure 4-12 opens.

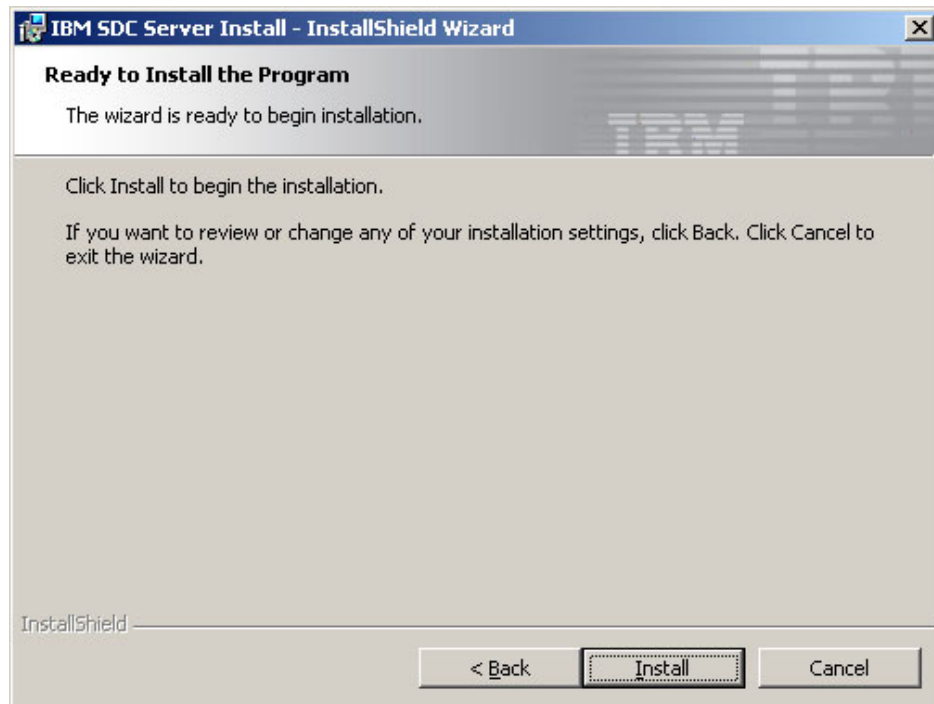


Figure 4-12 Software Delivery Center Ready to Install the Program window

16. Click **Install**.

17. The Setup Status window shown in Figure 4-13 opens and the indicator shows the progress of the setup.

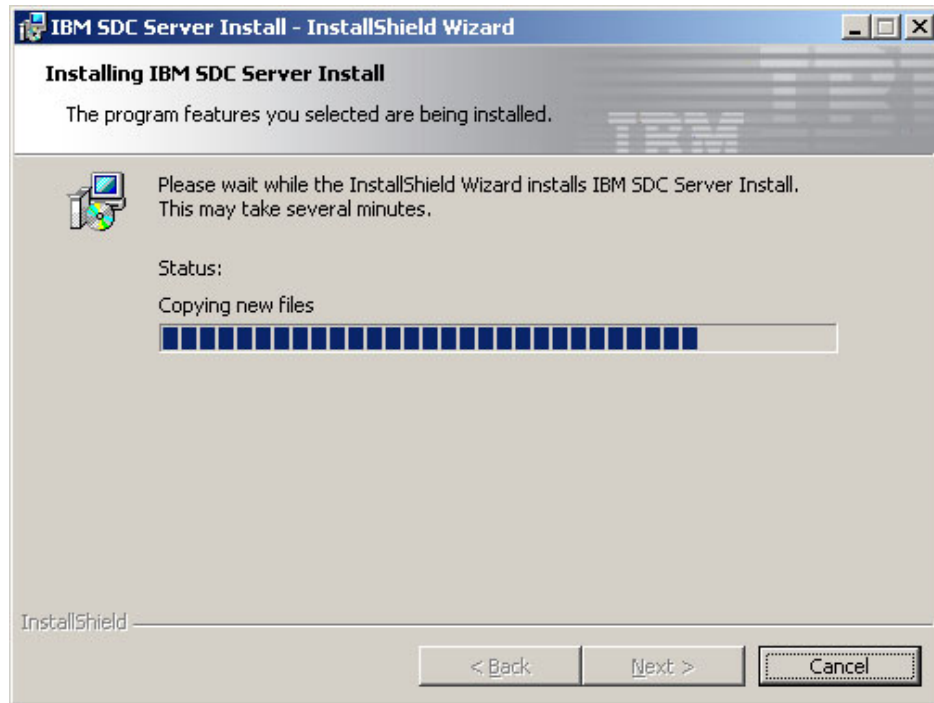


Figure 4-13 Software Delivery Center install status

18. The window shown in Figure 4-14 opens when the installation has completed.

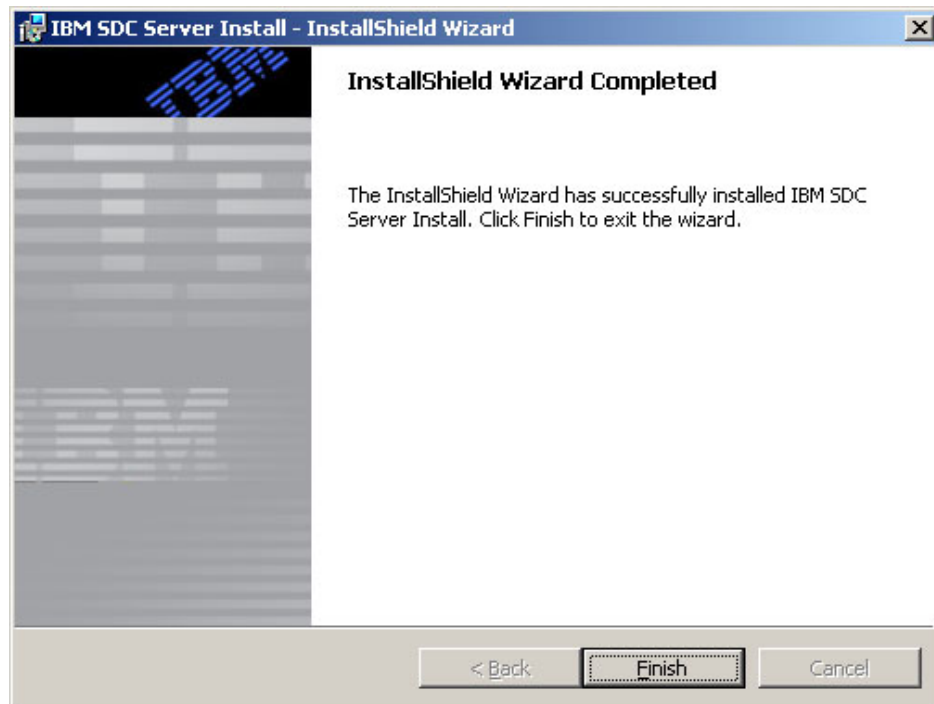


Figure 4-14 Software Delivery Center finished message

Note: It may take few seconds for the window shown in Figure 4-14 to open.

19. Click **Finish**. The window shown in Figure 4-15 on page 244 opens.

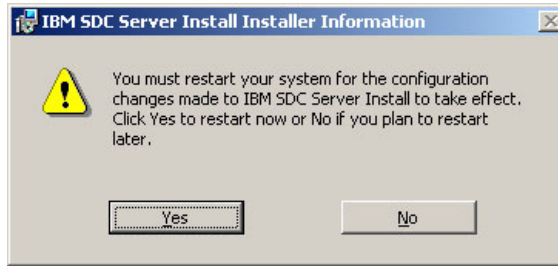


Figure 4-15 Software Delivery Center Restart System window

Note: When prompted to restart your computer, close any open programs and remove any disks (CDs, diskettes, DVDs, and so on) from their drives; then, click **Yes**. Or, if you do not want to restart your computer at this time, you can click **No**; however, you must restart your computer before Software Delivery Center will be fully installed.

20. You must now verify the Java environment variable PATH. The install program inserts the following text into the PATH variable:

```
;;%JAVA_HOME%bin;%JAVA_HOME%\jre\bin
```

You must insert two backslashes and delete one semicolon as shown:

```
;%JAVA_HOME%\bin;%JAVA_HOME%\jre\bin
```

This installation of Software Delivery Center on the server is complete.

4.3.3 Testing the IBM Software Delivery Center server

To test the IBM Software Delivery Center server, perform the following steps:

1. Make sure that the Tomcat service is running by opening the **Administrative Tools** → **Services** window. Locate the Apache Tomcat service shown in Figure 4-16 on page 245.

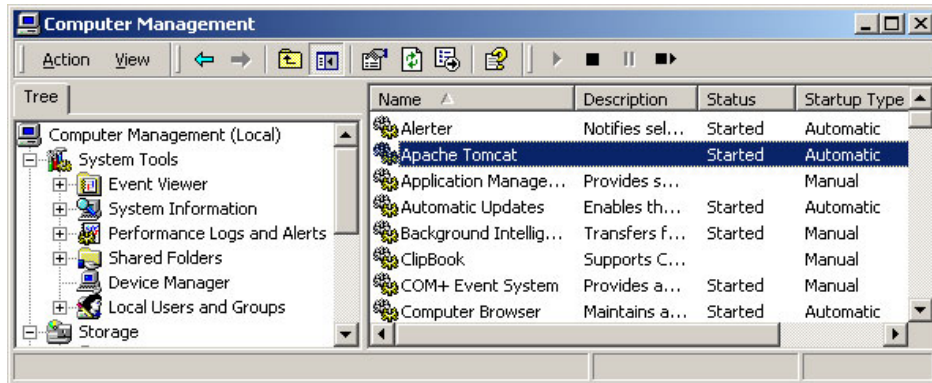


Figure 4-16 Software Delivery Center Tomcat service

2. Ensure that the IBM HTTP Server service is running by selecting **Administrative Tools** → **Services**. Locate the IBM HTTP Server 2.0 service as shown in Figure 4-17.

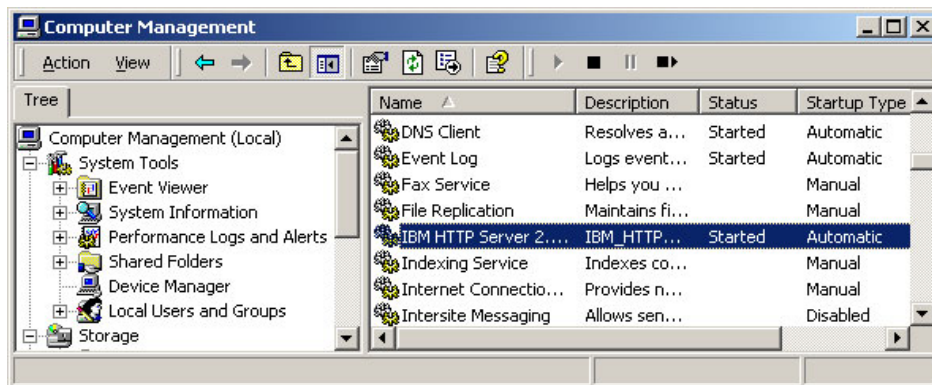


Figure 4-17 Software Delivery Center IBM HTTP Server service

3. Make sure that the Software Delivery Center Apache Tomcat and IBM HTTP Server service is set to **Automatic** and that it is started.
4. Close the services utility.

5. Start your browser and type `http://localhost` or `http://server_name` (where `server_name` is the name of the IBM Software Delivery Center server) in the Address field; then press **Enter**. If the installation was successful, the Software Delivery Center home page shown in Figure 4-18 opens.

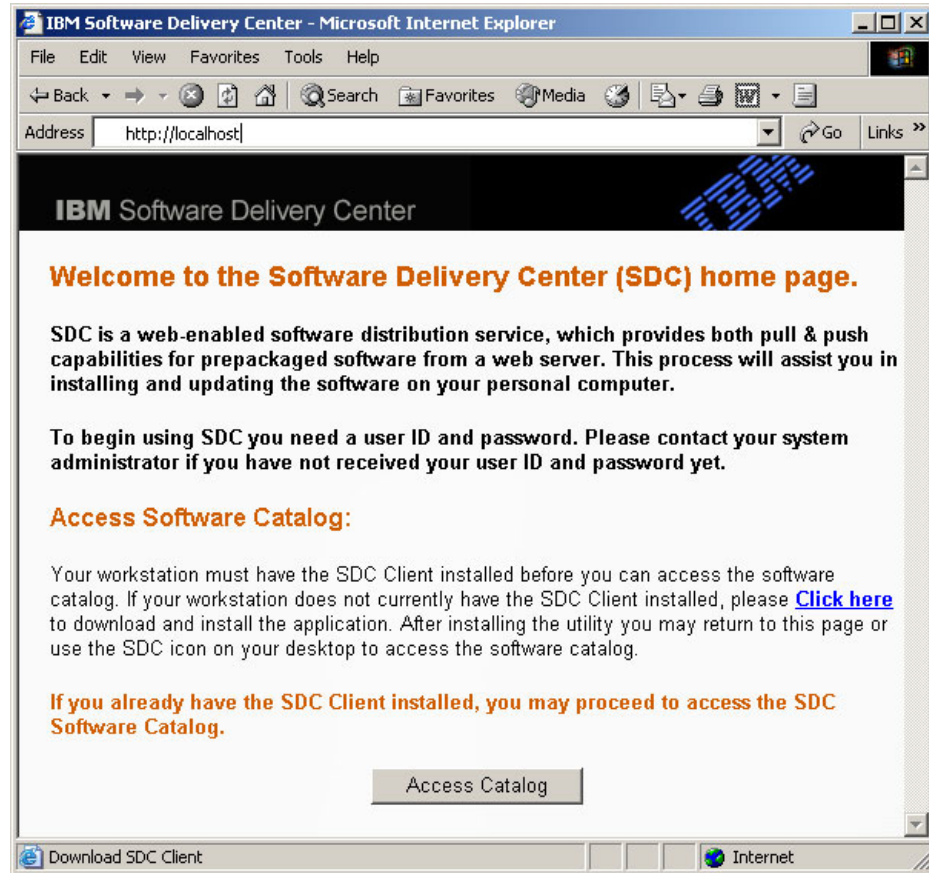


Figure 4-18 Software Delivery Center welcome message

To test the Software Delivery Center administrator console, perform the following steps:

1. Start your browser and type `http://localhost:8080` or `http://server_name:8080` (where `server_name` is the name of the Software Delivery Center server) in the Address bar; then press **Enter**.

2. The Loading SDC Admin Console page shown in Figure 4-19 opens.

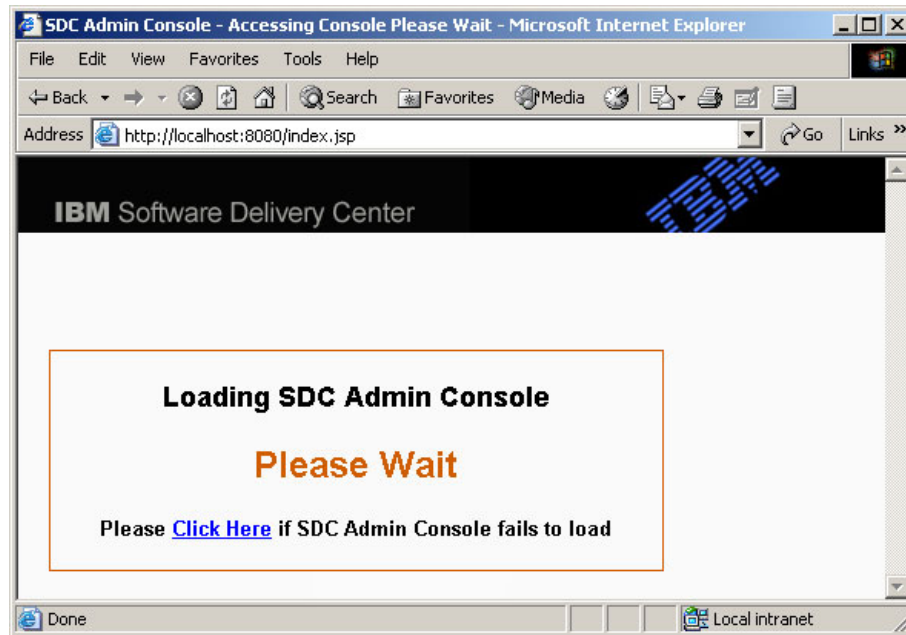


Figure 4-19 Software Delivery Center Loading SDC Admin Console page

Note: By default, the Software Delivery Center Loading SDC Admin Console login page will load automatically. At first launch, it may take few seconds for IBM Software Delivery Center Admin console page to load.

3. The IBM Software Delivery Center Administration Login page shown in Figure 4-20 opens.

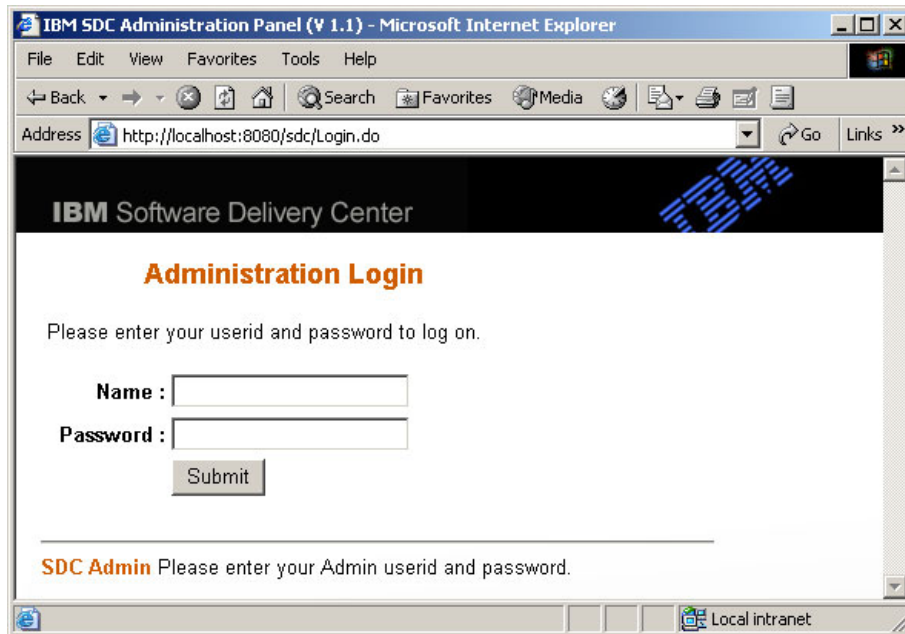


Figure 4-20 Software Delivery Center Administration Login page

Note: The Web address used to access Software Delivery Center is case sensitive.

4. Enter sdc in the Name field, sdc in the Password field, and click **Submit**. The Group Management page shown in Figure 4-21 on page 249 opens.

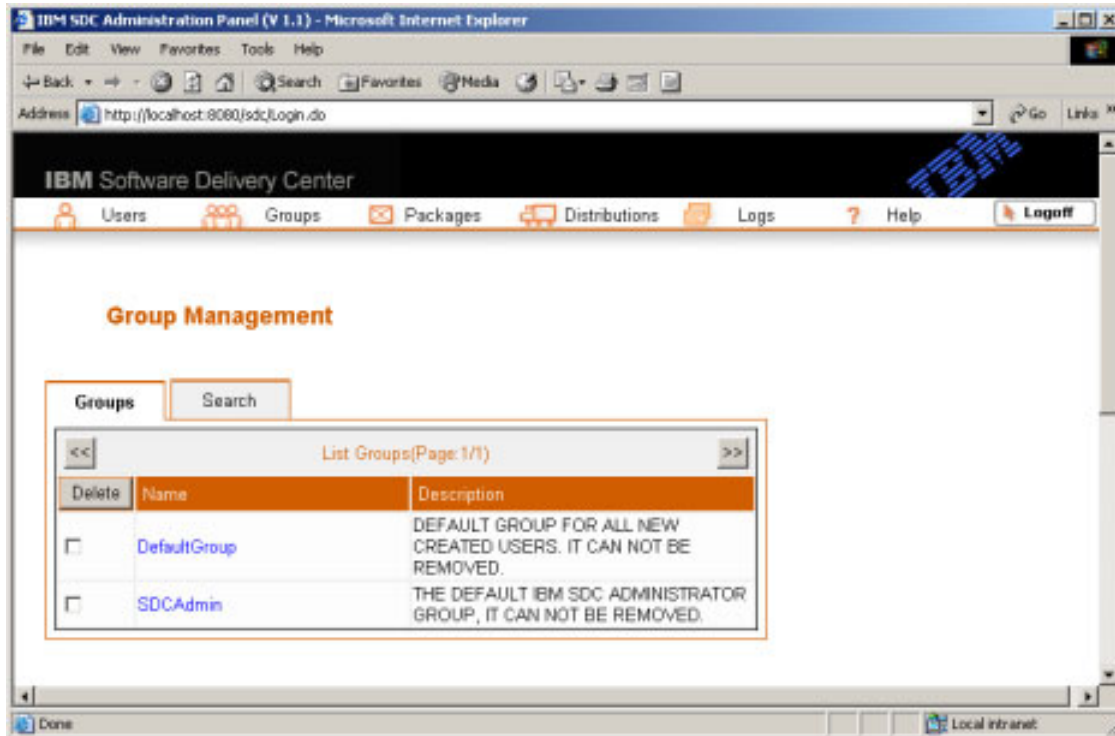


Figure 4-21 Software Delivery Center Group Management page

You have completed the installation of Software Delivery Center, Apache Tomcat, Cloudscape, and the required JDK when the Admin Console Login page appears.

To obtain information about using the Software Delivery Center administrator's console or changing the default administrator password, refer to 4.7.1, "Accessing Software Delivery Center administrator's console" on page 293.

4.3.4 Providing security for the packages on the file server

For the LogicalDrive(Secure) packages to work, the following registry key changes are needed on the server where the logical drive share is located.

1. Select **Start** → **Run**.
2. Type regedt32 and click **OK**.

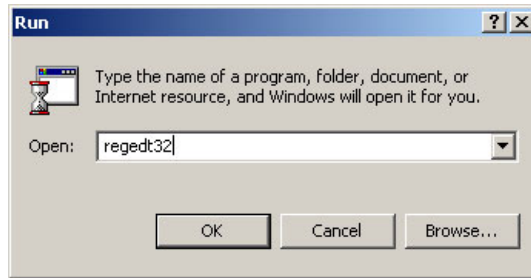


Figure 4-22 Software Delivery Center open program window

3. In the Registry Editor window, expand HKEY_LOCAL_MACHINE as shown in Figure 4-23.

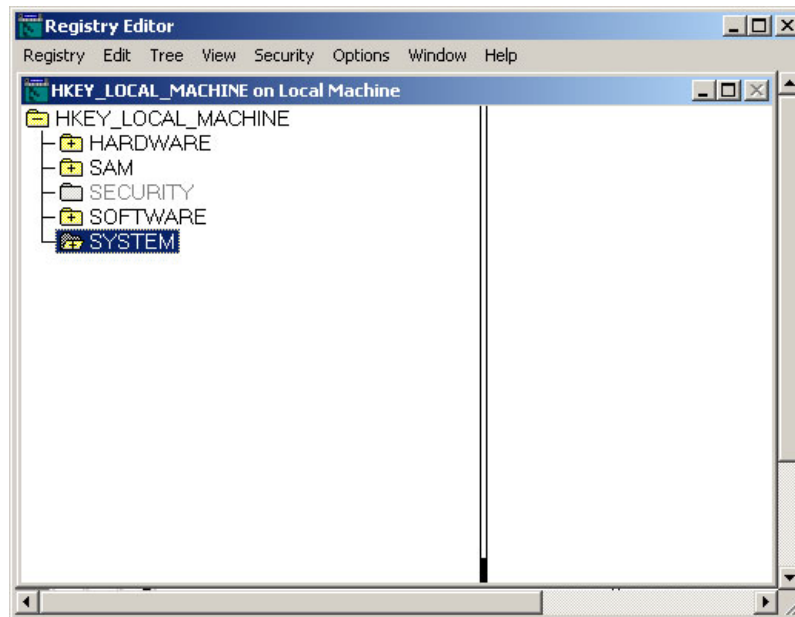


Figure 4-23 Expanding HKEY_LOCAL_MACHINE

4. Double-click **SYSTEM** to expand the folder as shown in Figure 4-24 on page 251.

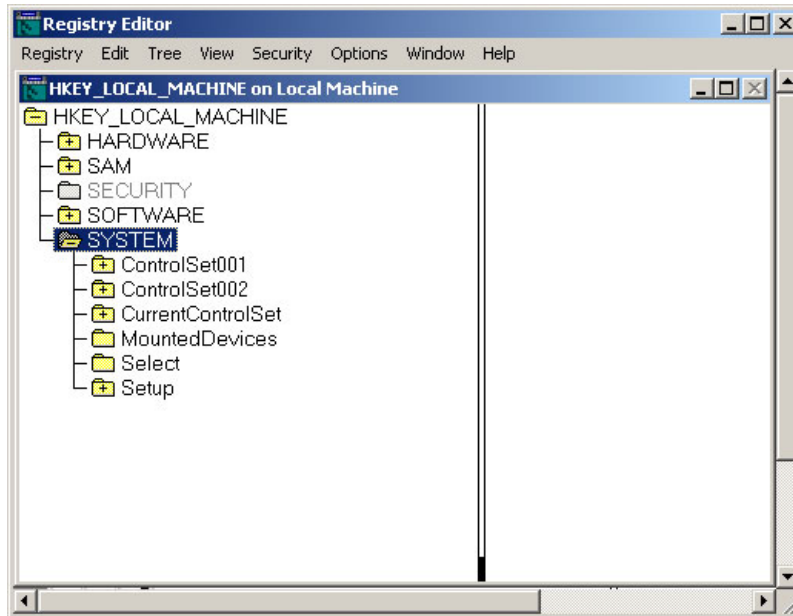


Figure 4-24 Expanding SYSTEM

5. Double-click **CurrentControlSet** to expand it as shown in Figure 4-25.

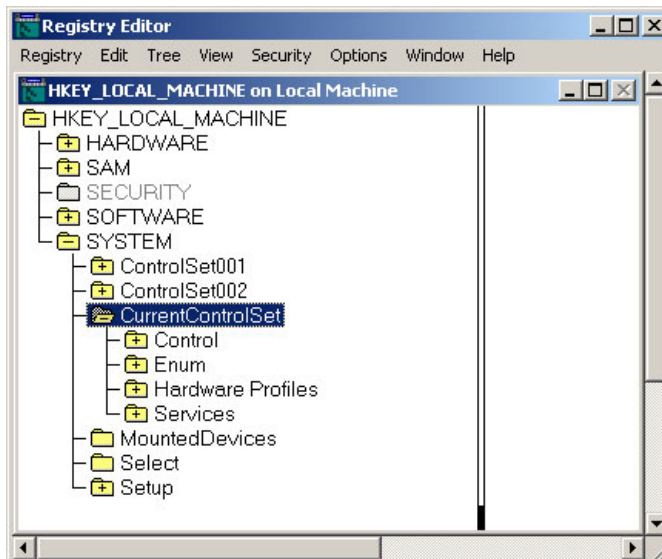


Figure 4-25 Expanding CurrentControlSet

6. Double click **Services** to expand the folder as shown in Figure 4-26.

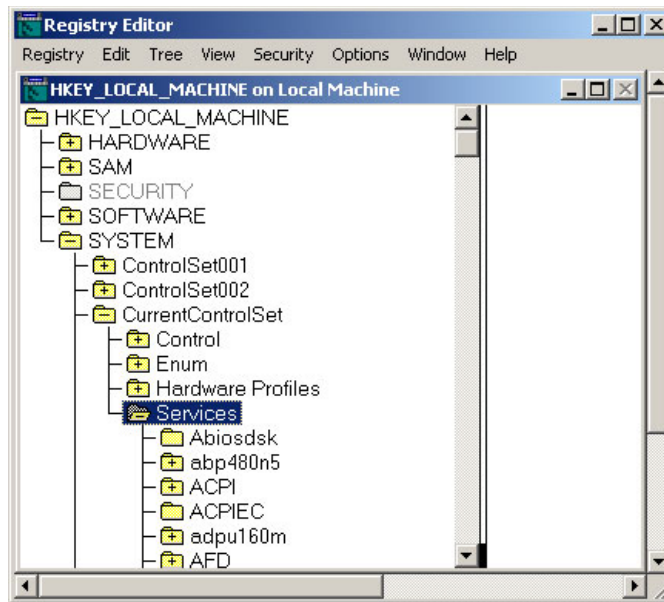


Figure 4-26 Expanding Services

7. Scroll down and double-click **lanmanserver** to expand the folder as shown in Figure 4-27.

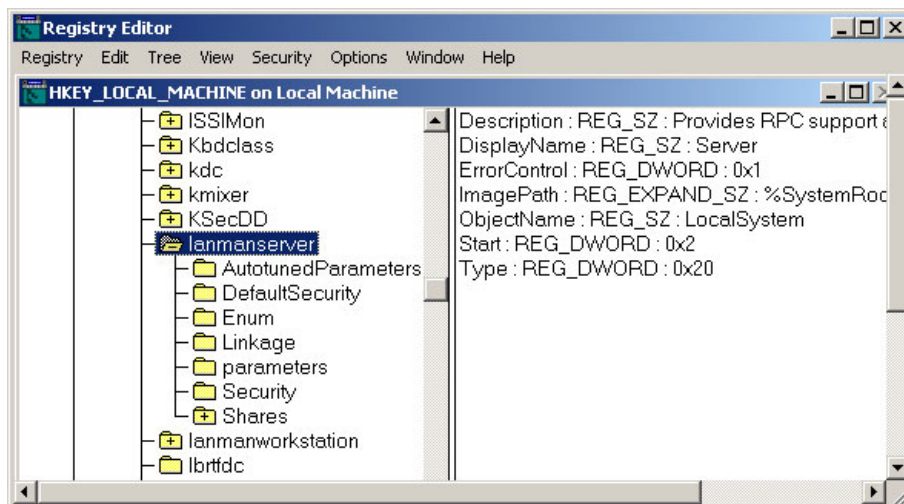


Figure 4-27 Expanding lanmanserver

8. Double-click **parameters** to expand the folder as shown in Figure 4-28.

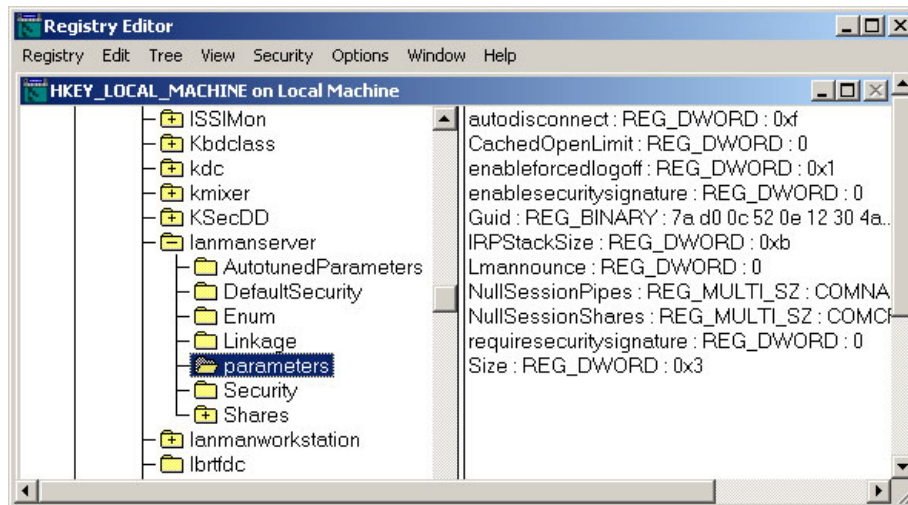


Figure 4-28 Expanding parameters

9. Move your cursor to the right window and double-click **NullSessionShares: REG_MULTI_SZ:COMFG DFS\$** (Figure 4-28).

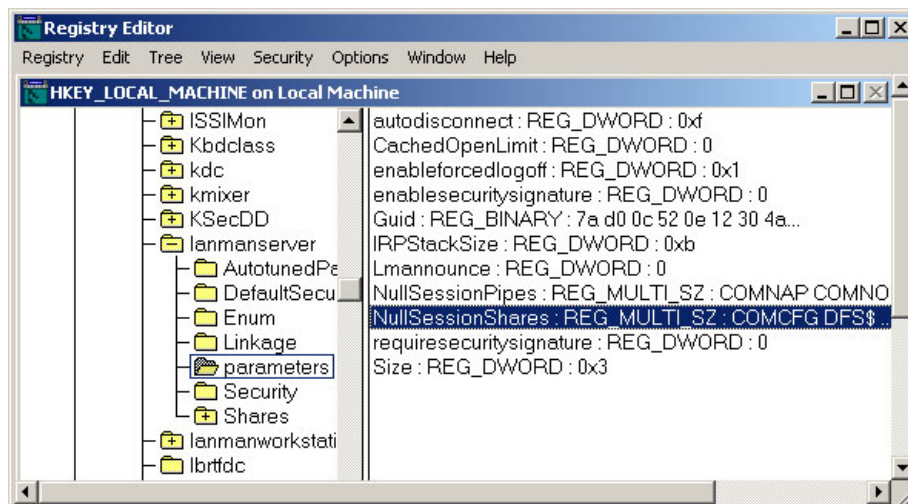


Figure 4-29 NullSessionShares

10. In the Multi-String Editor window (Figure 4-30 on page 254), click the empty row under DFS\$ and type the name of the share where the LogicalDrive(Secure) packages reside.

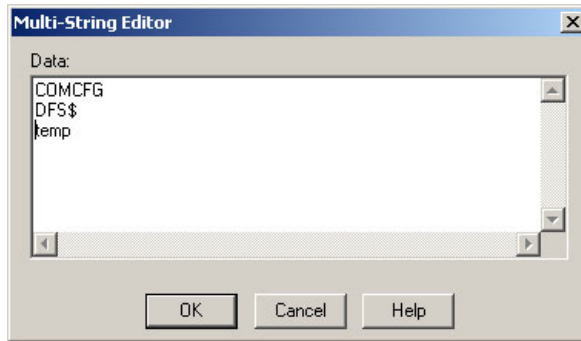


Figure 4-30 Software Delivery Center regedt32 Multi-String Editor window

Note: The file share server is the server where your software packages reside. The following is an example using the Software Delivery Center server as your file share server: `c:\IBMSDC\SDCServer\sdc\temp` (where *c* is the drive letter on which the software packages will be stored and *temp* is the logical drive share.)

11. Click **OK** to save the changes.
12. Navigate to:
 `\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`
13. Make sure that `restrictanonymous: REG_DWORD : 0` is there (Figure 4-31 on page 255).

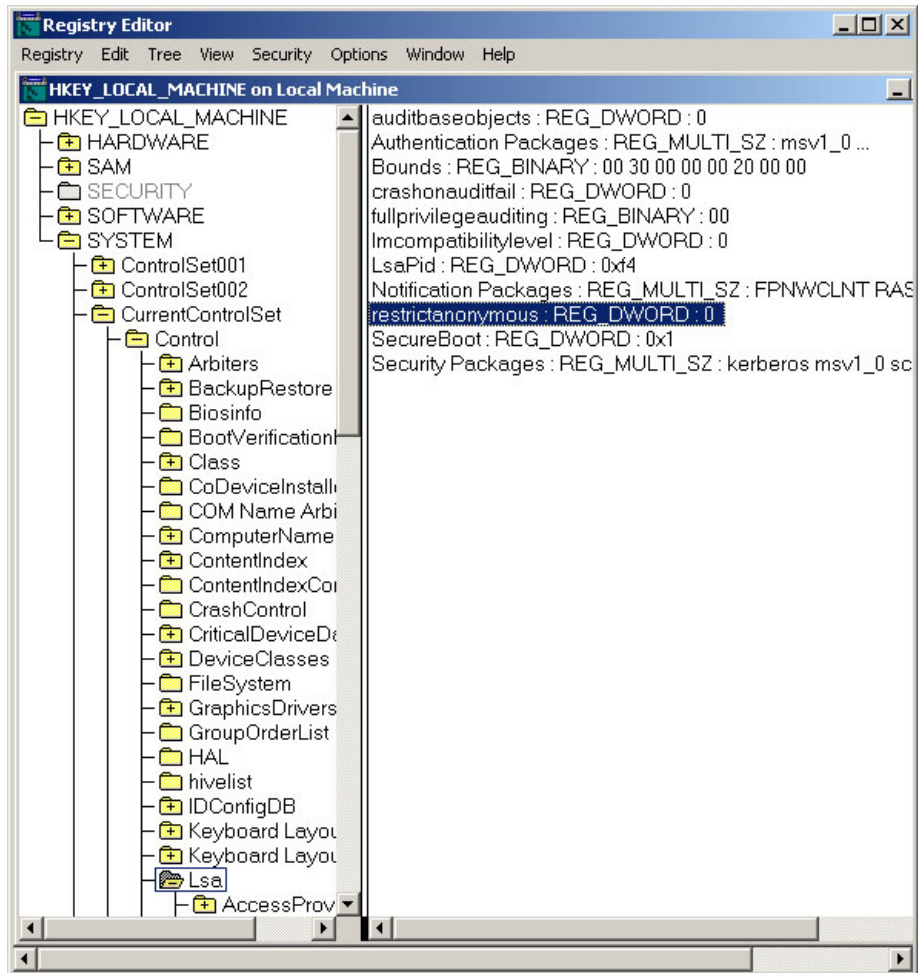


Figure 4-31 Software Delivery Center regedt32 restrictanonymous setting

14. If this entry is missing, do the following to add it:

- a. Windows 2003 Server
 - i. From the menu, select **Edit** → **New** → **DWORD Value** as shown in Figure 4-32 on page 256.

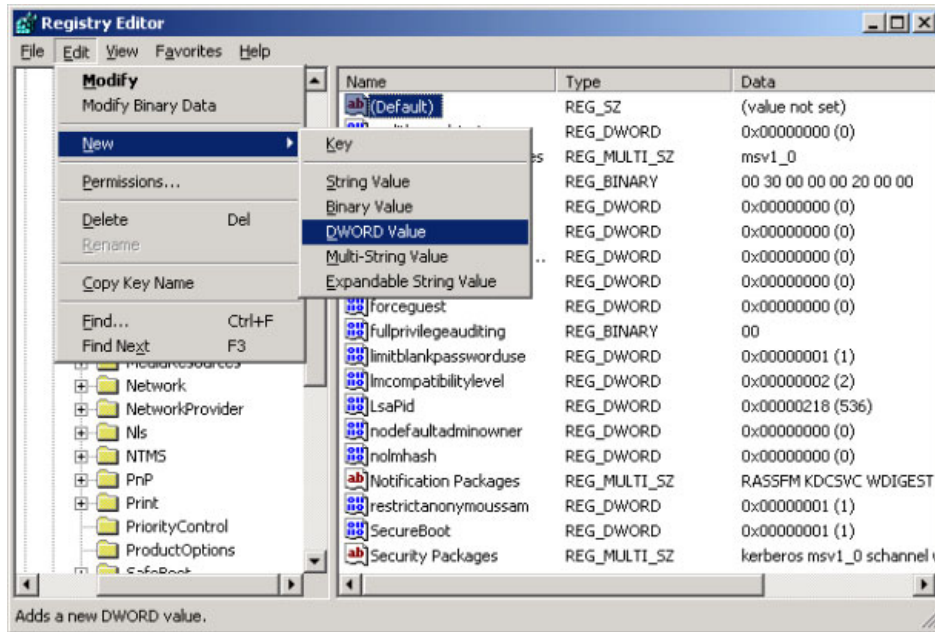


Figure 4-32 Selecting DWORD Value

- ii. In the Value Name field, type restrictanonym (Value Data=0) as shown in Figure 4-33 on page 257.

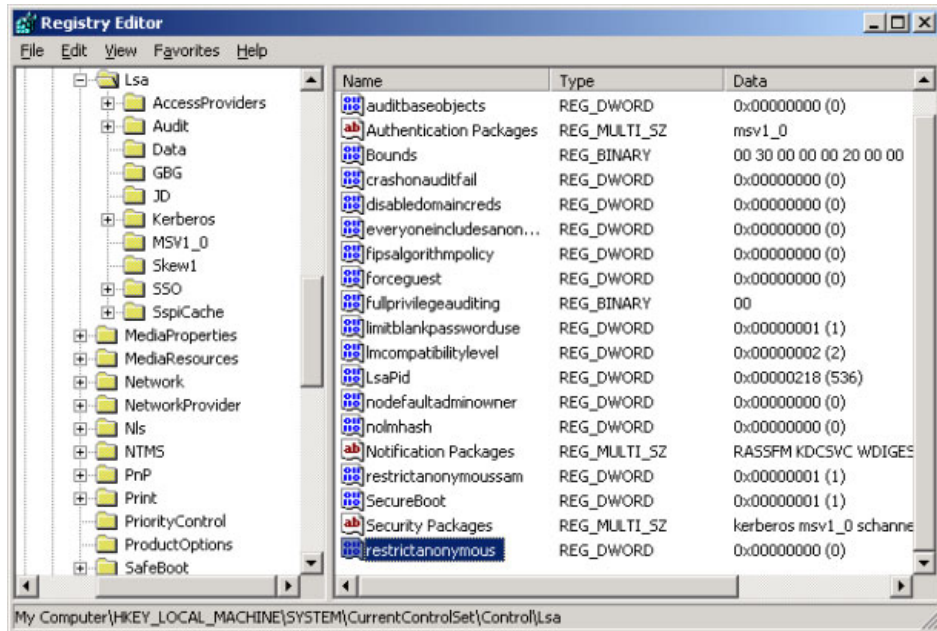


Figure 4-33 Software Delivery Center server Registry Editor window

iii. Press **Enter**.

b. Windows 2000 Server

i. From the menu, select **Edit** → **Add Value** as shown in Figure 4-34.

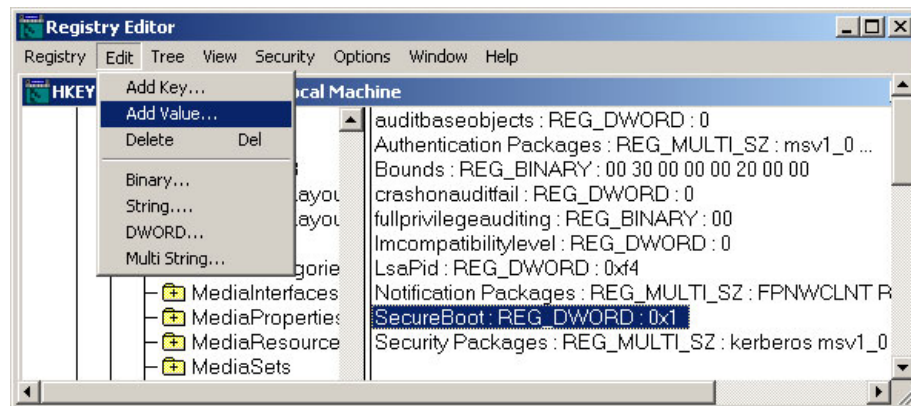


Figure 4-34 Selecting Add Value

ii. The Add Value window shown in Figure 4-35 on page 258 opens.

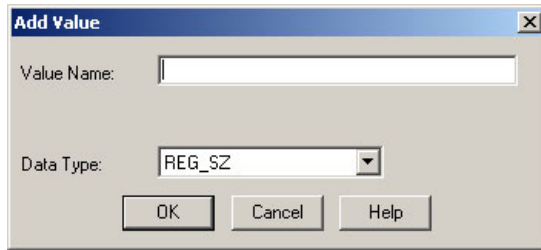


Figure 4-35 Software Delivery Center Add Value window

- iii. In the Value Name field, type restrictanonymous and select **REG_DWORD** from the Data Type menu as shown in Figure 4-36.

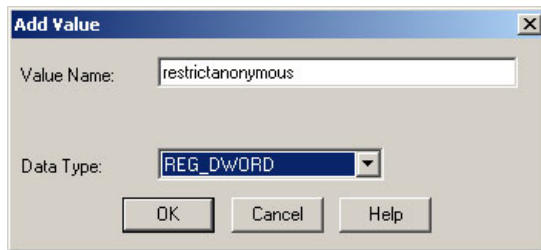


Figure 4-36 Selecting REG_DWORD

- iv. Click **OK**. The DWORD Editor window shown in Figure 4-37 should open.

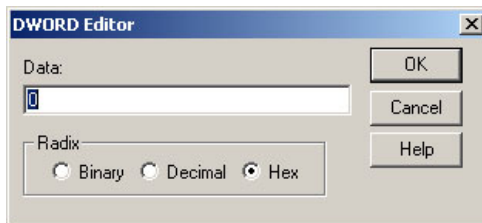


Figure 4-37 Software Delivery Center DWORD Editor window

- v. In the Data field, type 0 and Click **OK**.
- vi. The restrictanonymous : REG_DWORD : 0 value shown in Figure 4-38 on page 259 should display.

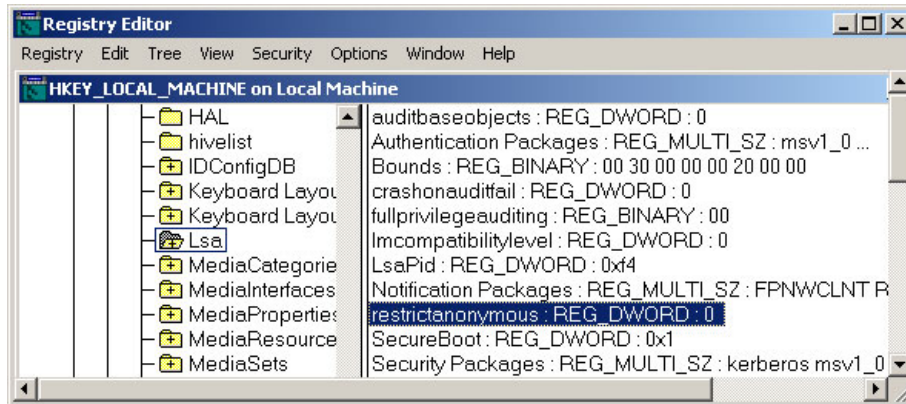


Figure 4-38 Software Delivery Center Registry Editor window

15. Close the Registry Editor window.

16. Close all the windows and restart the server.

4.4 Installing the Software Delivery Center client

This section describes how to install three components on the client:

- ▶ The client agent, which runs as a service granting software installation rights to the administrator, not to the user
- ▶ The client applet, which gives users access to the Software Delivery Center catalogs
- ▶ The JRE, which provides Java programming language support

This section includes the following topics:

- ▶ “Prerequisite software” on page 259
- ▶ “Supported types of installations” on page 260
- ▶ “Testing the Software Delivery Center client” on page 273

4.4.1 Prerequisite software

You can install the Software Delivery Center client components on any client computer that meets the following prerequisites:

- ▶ One of the following operating systems:
 - Windows 2000 Professional with Service Pack 4 or higher
 - Windows XP with Service Pack 1 or higher

- ▶ A Web browser (Internet Explorer 6.0 or higher)
- ▶ A network connection (for registration on the Software Delivery Center server)

Note: Additional platforms can be supported with a service offering from IBM Global Services. For additional information please send an e-mail to isdc@us.ibm.com.

4.4.2 Supported types of installations

The client portion of Software Delivery Center can be installed in either of the following ways:

- ▶ **Attended installation**

This is the default method of installation from the Software Delivery Center CD. The person installing the program is prompted to provide information during the installation process. See “Performing an attended installation of the client SDCSETUP.exe” on page 260 for more information.

- ▶ **Unattended installation**

For this method of installation, the administrator must customize the client so that no user interaction is required during the installation process. This method is very useful if you want to include the client portion as part of an image or if you intend to distribute it to non-technical users. See “Customizing the client SDCSETUP.EXE for an unattended installation” on page 269 for more information.

Performing an attended installation of the client SDCSETUP.exe

The attended installation requires the user to provide information as part of the installation process. Before beginning the installation, make sure the user has the following information:

- ▶ The Software Delivery Center server name or IP address
- ▶ Whether or not a desktop icon should be created on the client desktop to access the Software Delivery Center server

Note: Before you begin, make sure the installer is provided with the Software Delivery Center server name or IP address.

Continue with one of the following tasks:

- ▶ Default installation from a CD (see “Performing a default installation from CD” on page 261)

- ▶ Interactive installation from the command prompt (see “Performing an interactive installation from the command prompt” on page 267)
- ▶ Interactive installation from Windows (see “Performing an interactive installation from Windows” on page 267)
- ▶ Installation from the server (see “Installing the client portion from the server” on page 267)

Performing a default installation from CD

If you are installing directly from the Software Delivery Center CD, perform the following procedure:

1. Insert the Software Delivery Center CD.
2. If the installation program starts automatically, close it. This installation program is for the server portion only.
3. From the Windows desktop, select **Start**.
4. Select **Run**.
5. Type `d:\client\sdccsetup.exe` (where *d* is the drive letter of the drive that contains the Software Delivery Center CD as shown in Figure 4-39).

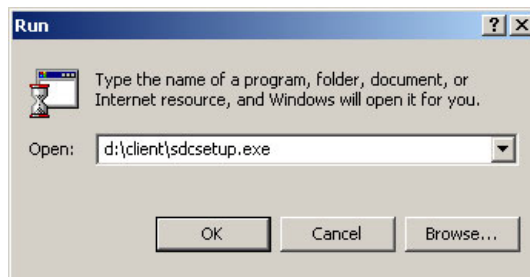


Figure 4-39 Starting the default installation from CD

6. Click **OK**. The window shown in Figure 4-40 on page 262 opens.

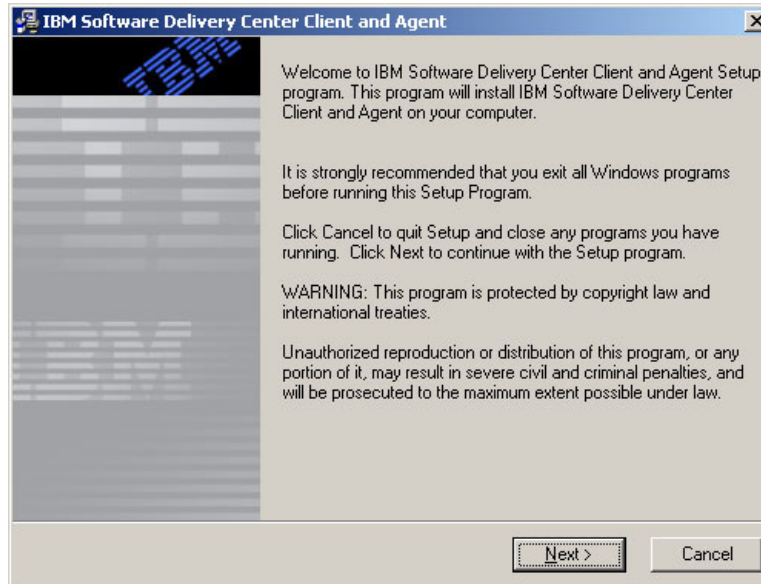


Figure 4-40 Software Delivery Center agent setup window

7. Click **Next**. The window shown in Figure 4-41 opens.

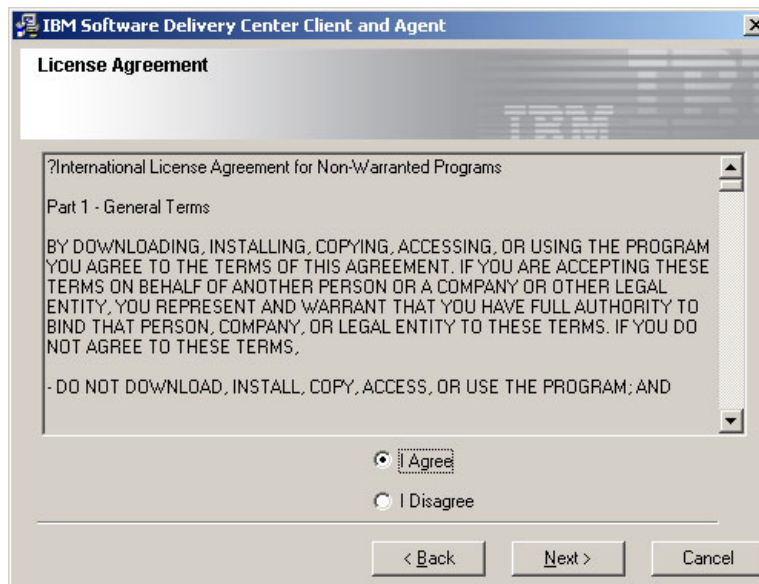


Figure 4-41 Software Delivery Center client license agreement

8. Read the license agreement and if you agree, click **I Agree** and then click **Next**. The Destination Location window shown in Figure 4-42 will be displayed.

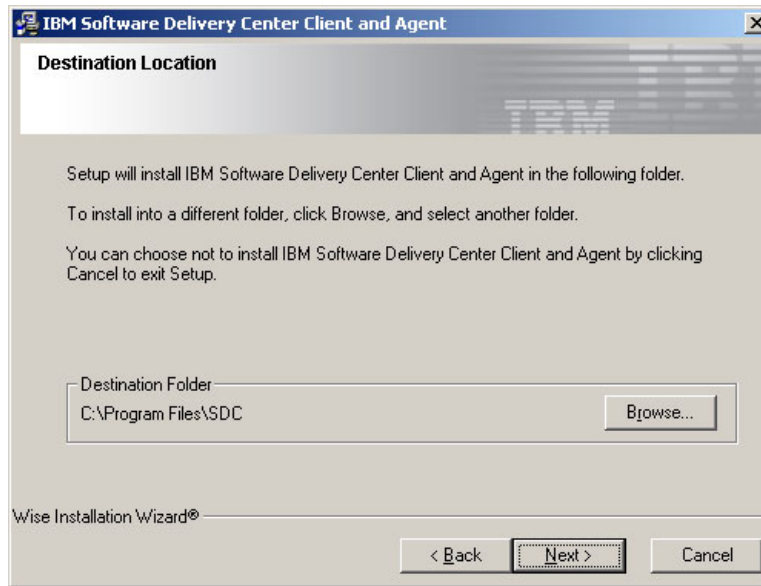


Figure 4-42 Software Delivery Center Destination Location window

9. Either accept the default folder (c:\Program Files\SDC) or use the **Browse** button to select a different folder.
10. Click **Next**.

11. The Server Name or IP Address window shown in Figure 4-43 opens.

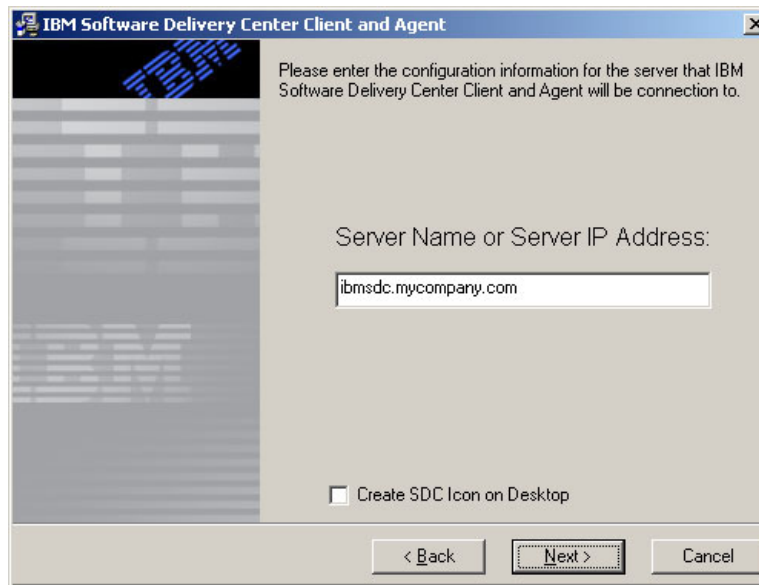


Figure 4-43 Software Delivery Center client Server Name window

12. Type the fully qualified domain name of the Software Delivery Center server or the IP address that will be used to connect to Software Delivery Center server.
13. Click **Create SDC Icon on Desktop** and then click **Next**.

Note: You may choose not create an Software Delivery Center icon on the desktop. If this is your choice, the user is asked to create a Software Delivery Center catalog icon at the second launch of the Software Delivery Center software catalog by the Java Webstart application.

14. The Start Installation window shown in Figure 4-44 opens.

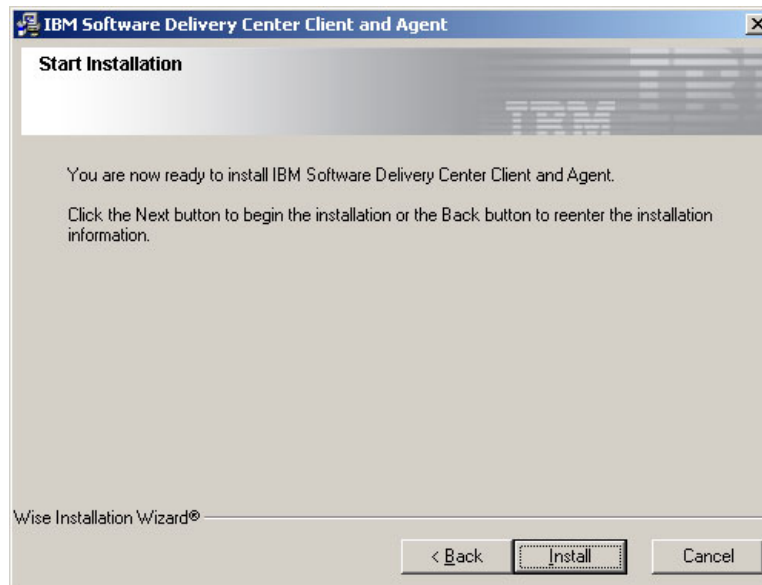


Figure 4-44 Software Delivery Center Start Installation window for the client

15. Click **Install**.

16. The Installing window shown in Figure 4-45 on page 266 displays the progress of the setup.

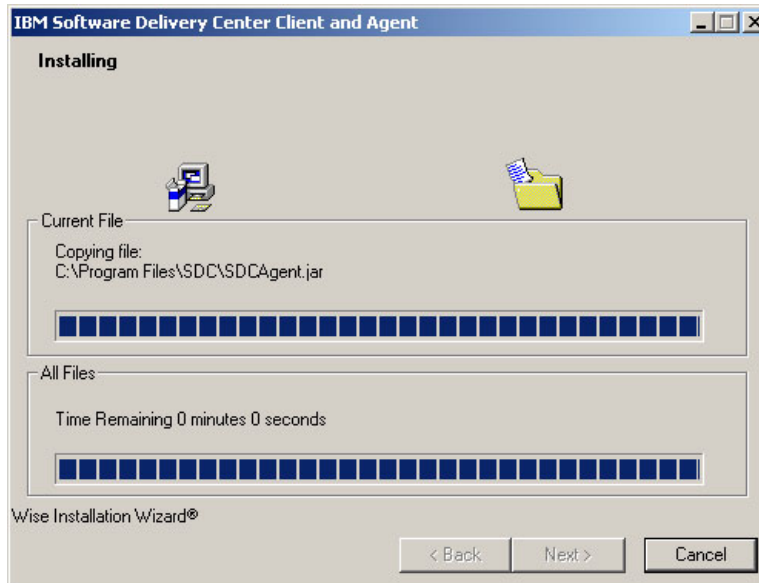


Figure 4-45 Software Delivery Center Install Progress window for the client

17. The window shown in Figure 4-46 opens when the installation is complete.

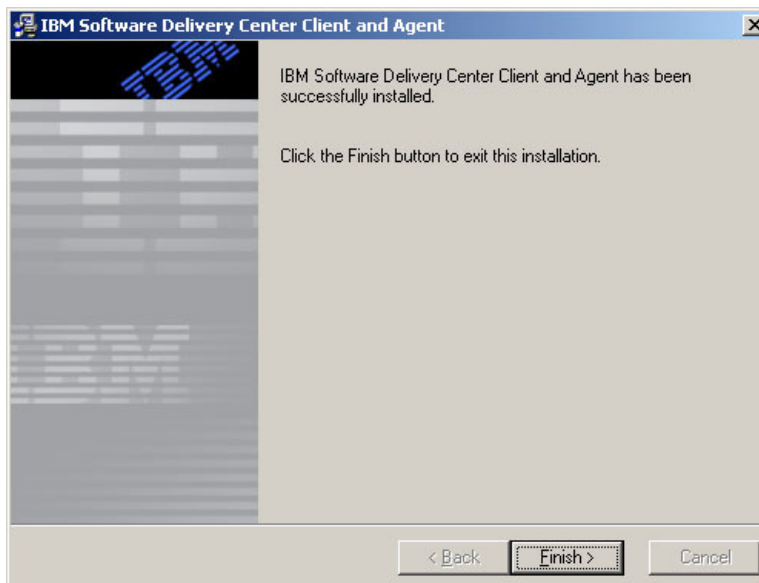


Figure 4-46 Software Delivery Center successful client installation message

18. Click **Finish**.

This concludes the installation of the Software Delivery Center client components on a workstation.

Performing an interactive installation from the command prompt

If you copied the client SDCSETUP.EXE file to a network drive or portable media, you can use the following procedure to perform an interactive installation from the command prompt:

1. Open a command prompt window.
2. Change to the folder containing the client SDCSETUP.EXE file. If you are installing directly from the Software Delivery Center CD, the client SDCSETUP.EXE file is in the client folder.
3. Run the following command: SDCSETUP.EXE
4. Follow steps 6 on page 261 through 18 on page 267 in “Performing an attended installation of the client SDCSETUP.exe.”

Performing an interactive installation from Windows

If you copied the client SDCSETUP.EXE file to a network drive or portable media, you can use the following procedure to perform an interactive installation from Windows Explorer or My Computer:

1. Open Windows Explorer or My Computer.
2. Change to the folder that contains the client SDCSETUP.EXE file. If you are installing directly from the Software Delivery Center CD, the client SDCSETUP.EXE file is in the client folder.
3. Double-click the SDCSETUP.EXE file.
4. Follow steps 6 on page 261 through 18 on page 267 in “Performing an attended installation of the client SDCSETUP.exe.”

Installing the client portion from the server

If you have client computers at remote locations with no access to the Software Delivery Center CD, you can install the client portion of Software Delivery Center from the Software Delivery Center server as follows:

1. Open a Web browser.
2. In the Address bar, type one of the following:
 - `http://server_name` (where *server_name* is the name of the Software Delivery Center Server)
 - `http://server_IP_address` (where *server_IP_address* is the IP address of the Software Delivery Center Server)

3. Press **Enter**. The Software Delivery Center home page shown in Figure 4-47 opens.



Figure 4-47 Software Delivery Center welcome page

4. In the Access Software Catalog section, click **Click here**. The File Download - Security Warning window shown in Figure 4-48 on page 269 opens.

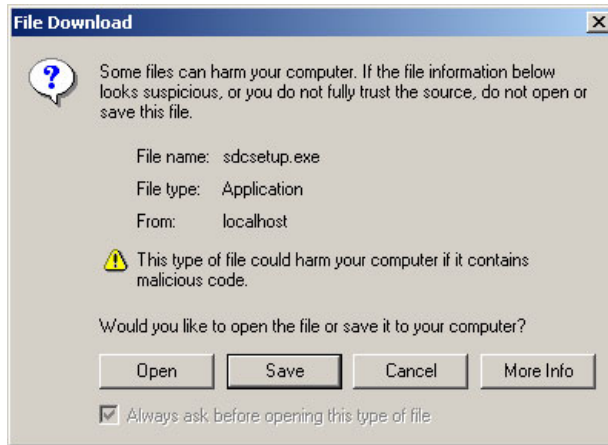


Figure 4-48 Software Delivery Center security warning window

5. Click **Open**. The Software Delivery Center installation wizard opens.
6. Follow steps 6 on page 261 through 18 on page 267 in “Performing an attended installation of the client SDCSETUP.exe.”

Customizing the client SDCSETUP.EXE for an unattended installation

You can customize the client SDCSETUP.EXE file to perform an unattended installation on a client computer, meaning no direct user intervention is required. The SDCSETUP.EXE file was created in a Microsoft Software Installer (MSI) format, which enables the administrator to perform or set up an unattended installation using command-prompt options, including:

- ▶ `/s`
Installs the application silently (unattended). To use this option, at a minimum, you also must include the `/ip:xxxxxx` option.
- ▶ `/?`
Displays the command-prompt options only. This command-prompt option does not install the application.
- ▶ `/ip:xxxxxx` (where `xxxxxx` specifies the Software Delivery Center server name or IP address)
This command-prompt option is required for an unattended installation.
- ▶ `/serverport:xxxxxx` (where `xxxxxx` specifies the Software Delivery Center server TCP/IP port)
This command-prompt option overrides the default setting of 8080.

- ▶ `/refreshinterval:xxxxxx` (where `xxxxxx` specifies the interval (0 - 99999 minutes) at which Software Delivery Center will poll the Software Delivery Center server for available push packages)

This command-prompt option overrides the default setting of 60 (for example, `/refreshinterval:120`).

- ▶ `/createdesktopicon:xxx` (where `xxx` specifies whether to create or not create a desktop icon to the Software Delivery Center server)

This command-prompt option is required for an unattended installation. Use Y or Yes to create a desktop icon; use No, any value other than Y or Yes, or no value to indicate that you do not want create a desktop icon.

If no command-prompt options are specified other than `/ip:xxxxxx`, the defaults for a silent installation are used. Any options specified on the command prompt override these defaults. Any command-prompt options specified for an attended installation merely become the default values and the user can manually override them during the installation. No spaces are allowed within a command-prompt option; however, spaces must be used to separate the individual command-prompt options. For example:

```
sdccsetup.exe /s /ip:www.myserver.com
```

Setting up an unattended installation from a shortcut

You can create a shortcut that enables users to perform an unattended installation from a network drive using the following procedure:

1. Create a folder on a network drive or CD for the client SDCSETUP.EXE file; then, copy the client SDCSETUP.EXE file to that folder.
2. Create a shortcut to the SDCSETUP.EXE file.
3. Rename the shortcut to something easily understood by the user. In these instructions Software Delivery Center Client Install is used.
4. Modify the properties of the shortcut as follows:
 - a. Right-click the **Software Delivery Center Install** shortcut file and then click **Properties**. The Properties window is displayed.
 - b. In the Target field, add the following to the end of the command (where *cmd_line_option* is one of the command-prompt options supported by the client SDCSETUP.EXE file):

```
/s /cmd_line_option /cmd_line_option
```

For example, if the client SDCSETUP.EXE file is in `x:\IBM\SDC`, the Software Delivery Center server IP address is 123.456.789, and a desktop icon is to be created, the target field would look like this:

```
x:\IBM\SDC\SDCSETUP.EXE /s /ip:123.456.789 /createdesktopicon:yes
```


This is illustrated in Figure 4-49.

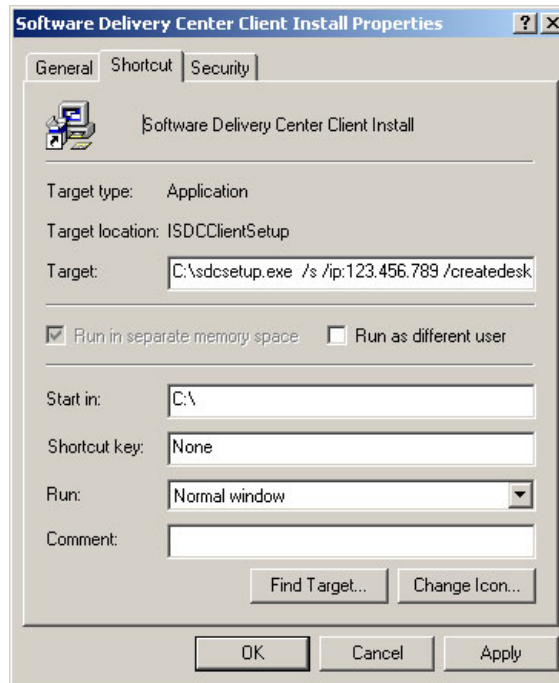


Figure 4-49 Software Delivery Center client setup shortcut window

c. Click **OK**.

Note: For more information about the command-prompt options supported by the client SDCSETUP.EXE file, see “Customizing the client SDCSETUP.EXE for an unattended installation” on page 269.

5. Instruct your users to map this location and to select the **Software Delivery Center Install** shortcut.

Performing an unattended installation of the client SDCSETUP.EXE from a command prompt

To perform an unattended installation of the client SDCSETUP.EXE file from a command prompt, complete the following procedure:

1. Open a command prompt window.
2. Change to the folder containing the client SDCSETUP.EXE.

3. Run the following command: `SDCSETUP.EXE /s /cmd_line_option /cmd_line_option` (where *cmd_line_option* is one of the command-prompt options supported by the client SDCSETUP.EXE file).

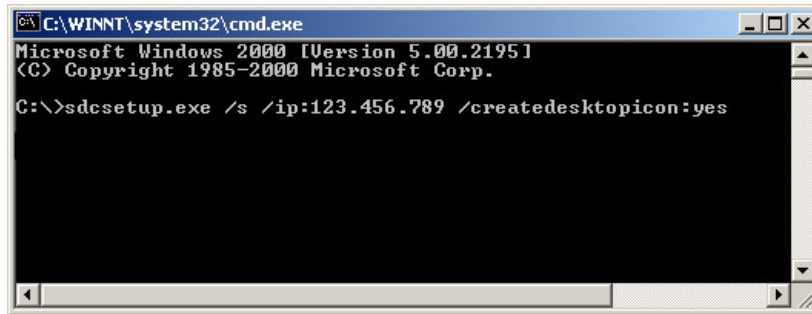


Figure 4-50 Software Delivery Center client command prompt setup

Note: For more information about the command-prompt options supported by the client SDCSETUP.EXE file, see “Customizing the client SDCSETUP.EXE for an unattended installation” on page 269.

Post deployment customizations of the client using the sdc.conf file

You can reconfigure the operation of the agent after it has been deployed by simply updating the `sdconf` file and restarting the SDCAgent service. The default location of the `sdconf` file is `c:\Program Files\sdc\sdc.conf`. The contents of a sample `sdconf` file are shown in Example 4-1.

Example 4-1 Sample sdc.conf file contents

```
com.ibm.sdc.server.protocol=http
com.ibm.sdc.server.host=ibmsdc.mycompany.com
com.ibm.sdc.server.port=8080
com.ibm.sdc.agent.offset=60
com.ibm.sdc.agent.clientHost=myhostname
```

The agent will query the server for available packages at regular time intervals. This interval is specified in minutes by the `offset` parameter above.

The agent will record status and error messages in a log file located in the `C:\program Files\sdc` directory.

The installation of the IBM Software Delivery Center client is complete.

4.4.3 Testing the Software Delivery Center client

To test the Software Delivery Center client, perform the following steps:

1. Open the Windows Services applet.
2. Make sure that the SDCAgent service is running. This can be checked by opening the Administrative Tools → Services window. Locate the SDCAgent service as shown in Figure 4-51.

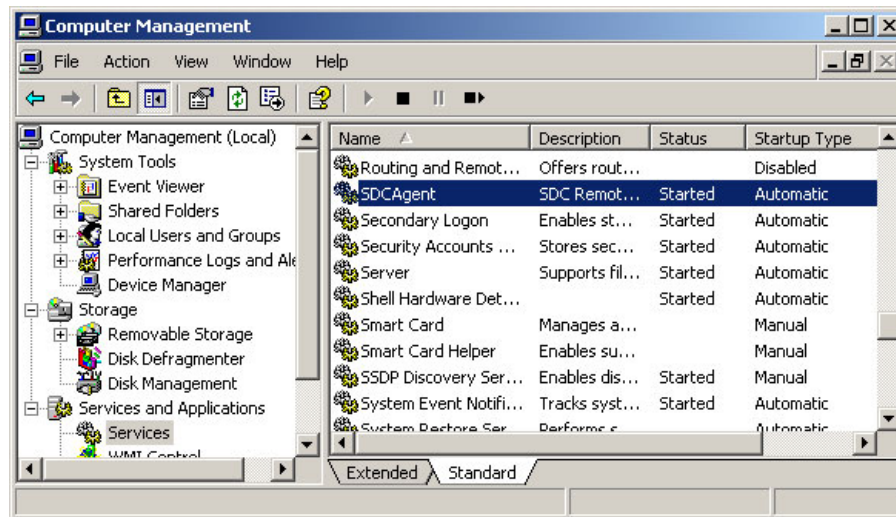


Figure 4-51 Locating SDCAgent

3. Make sure that the SDCAgent service is set to **Automatic** and that it is started.
4. Close the services utility.

The following procedures may be used to access a Software Delivery Center catalog:

1. If you have the Software Delivery Center Catalog desktop icon, double-click it. The Software Delivery Center Client Login window (see Figure 4-54 on page 275) opens.
2. If you do not have the Software Delivery Center Catalog desktop icon:
 - i. Open a Web browser.
 - ii. In the Address bar, type one of the following:
 - `http://server_name` (where `server_name` is the name of the Software Delivery Center server)

- `http://server_IP_address` (where `server_IP_address` is the IP address of the Software Delivery Center server)
- iii. Press **Enter**. The Software Delivery Center home page shown in Figure 4-52 opens.

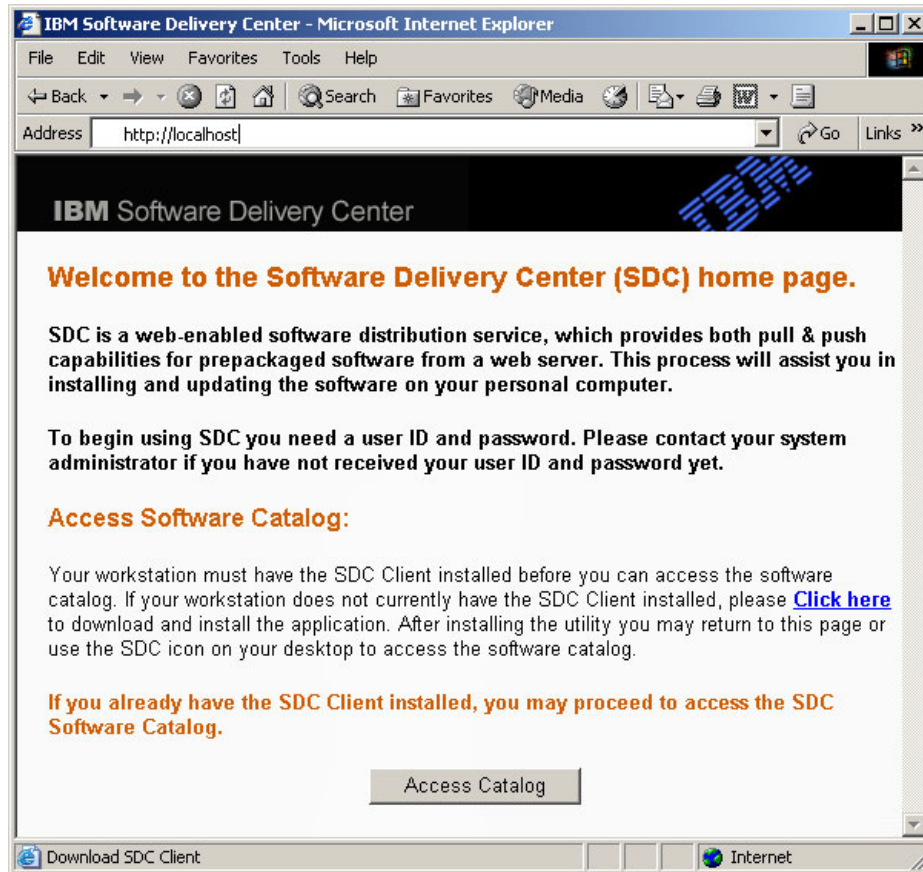


Figure 4-52 Software Delivery Center welcome page

Note: You can save the Software Delivery Center home page as one of your browser favorites for future use.

3. Click **Access Catalog**. The Security Warning window (Figure 4-53 on page 275) opens.

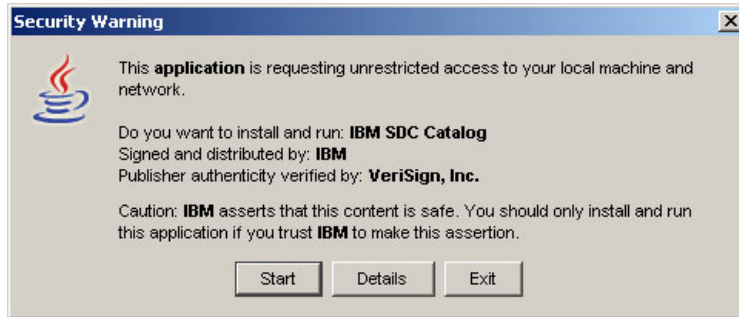


Figure 4-53 Software Delivery Center catalog security warning window

Note: Verify that the security warning window displays IBM and that the publisher authenticity is verified by VeriSign, Inc.

4. Click **Start**. The Software Delivery Center Login window (Figure 4-54) opens.

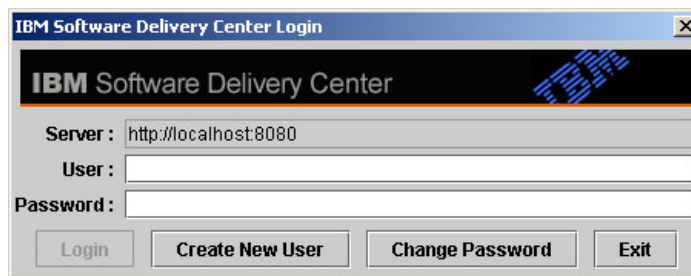


Figure 4-54 Software Delivery Center client login window

5. However, you may see the IBM SDC Catalog - Desktop Integration window shown in Figure 4-55.

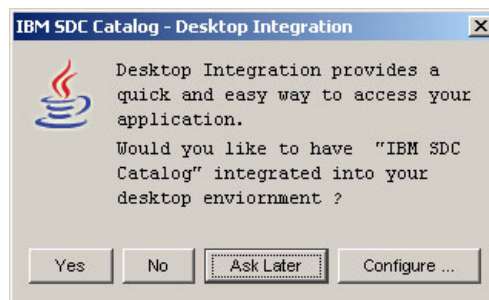


Figure 4-55 Software Delivery Center client desktop icon window

6. Click **Yes** to place an Software Delivery Center Catalog icon on desktop for easier access. Click **No** if icon is already present on your desktop. Click **Ask Later** to defer it to later time.

Note: Software Delivery Center uses Java Web Start technology to launch Software Delivery Center Software Catalog. The software catalog can be launched either from an icon on the desktop or from Software Delivery Center welcome page by clicking **Access Catalog**.

You have completed the installation of the Software Delivery Center client when the login window shown in Figure 4-54 on page 275 opens.

You can further test the client by following one of these steps:

- ▶ If the administrator has provided you with a user name and password for a Software Delivery Center catalog, type the user name and password in the fields provided and click **Login**. A catalog opens.
- ▶ If the administrator has instructed you to create your own user name and password, do the following:
 - a. Click **Create New User** shown in Figure 4-54 on page 275. The window shown in Figure 4-56 opens.

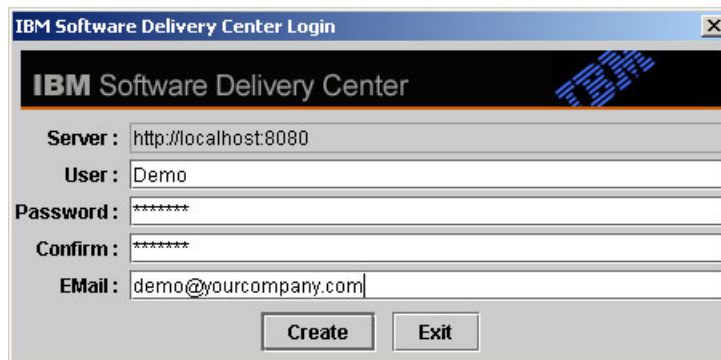


Figure 4-56 Software Delivery Center client new user window

- b. In the User field, type the user name you want to use.
- c. In the Password field, type the password you want to use.
- d. In the Confirm field, type your password again. You must type the password exactly as you typed it in the Password field.
- e. In the EMail field, type your e-mail address.
- f. Click **Create**. A catalog opens.

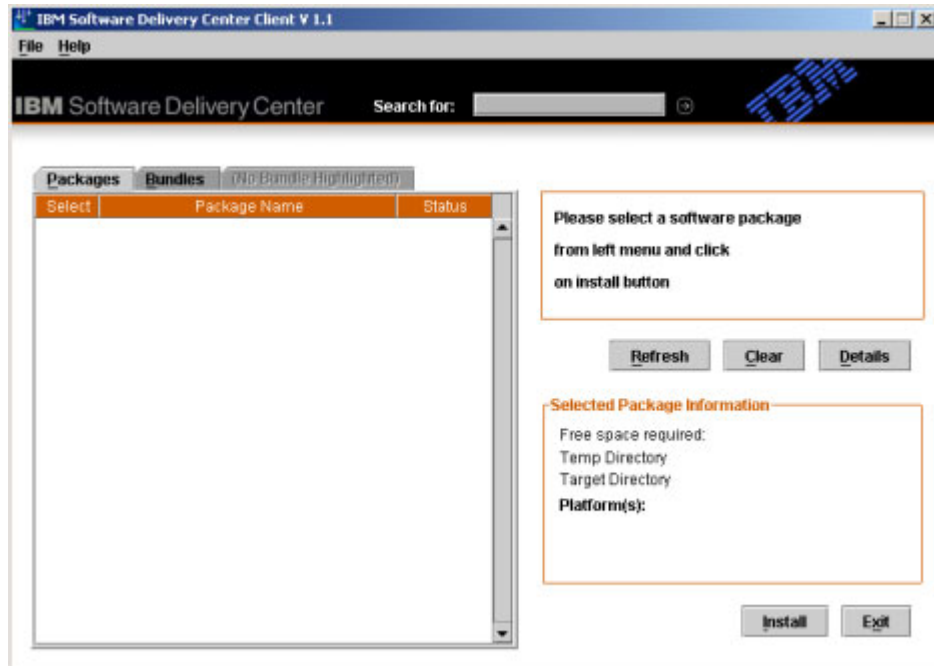


Figure 4-57 Software Delivery Center software catalog

Note: Catalogs for new users might not have any software packages or bundles listed. In most cases, the administrator must assign a new user to a specific group before the user can install software from a catalog.

You have completed the testing of IBM Software Delivery Center client when the window shown in Figure 4-57 opens.

Using the command prompt to launch the catalog

The install program provided with Software Delivery Center uses Java Web Start to launch the catalog. However, it is also possible to bring up the pull process catalog with the following command-prompt syntax:

```
Java -jar sdcclient.jar -h hostname -p 8080
```

This allows the Software Delivery Center application to run without the aid of a Web browser.

Note: You will need two files on the client to use this command prompt interface: `sdccclient.jar` and `win32registry.dll`. The file `sdccclient.jar` can be found in the `sdcc\apps` directory on the Software Delivery Center server. The file `win32registry.dll` resides inside the jar file named `win32native.jar` which can also be found in the `sdcc\apps` directory.

If the pull process is launched from the command prompt, the server line be available as shown in Figure 4-58.

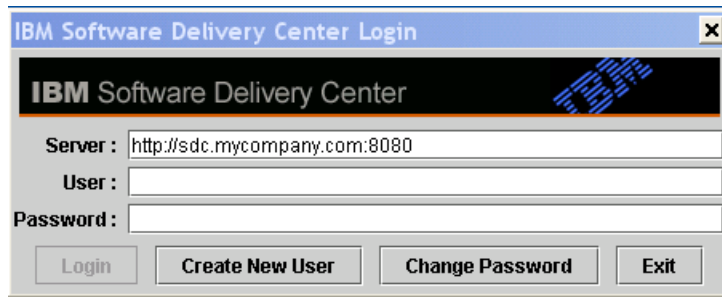


Figure 4-58 Login dialog when command prompt used

4.5 Building your software library

This section provides an overview of the tasks required to create a software package or bundle and check it into your Software Delivery Center library. The Software Delivery Center library is the main repository for software packages and bundles. Software packages and bundles referenced in the library are not made available to users until the administrator creates catalogs for the pull software-delivery method or schedules a push software delivery. See 4.6, “Setting up Software Delivery Center infrastructure” on page 287 for more information.

This section includes the following topics:

- ▶ “Creating a folder structure for your library” on page 279
- ▶ “Creating a software package” on page 280
- ▶ “Creating a software bundle” on page 285
- ▶ “Creating a portable catalog” on page 285
- ▶ “Using a portable catalog” on page 285
- ▶ “Importing files from another server” on page 286

4.5.1 Creating a folder structure for your library

Any package, folder, or file intended for distribution that is stored on the Software Delivery Center server must be stored under the document root. The default document root is `c:\IBMSDC\SDCSERVER\SDC`. Your document root might be different depending on the options you selected during installation.

In most cases, it is beneficial to use the `\PACKAGES` folder under the document root to help you organize the files associated with your packages. You might want to organize your packages in the `\PACKAGES` folder by operating system, type of application, or any other characteristic that meets the needs of your organization. It is a good idea to plan for your long-term organizational needs before designing your folder structure. The sample folder structure below provides guidance for creating your folder structure.

Sample folder structure

The following folder structure is a sample that you can use as a reference to set up a folder structure on your Software Delivery Center server. All software packages, detail files, and icon files stored on the Software Delivery Center server must be stored under the document root, which by default is `c:\IBMSDC\SDCSERVER\SDC`.

Note: The document root on your server may be different depending on the options you chose during installation. Sample folder structures in this appendix show the default document root.

The folder structure you implement is entirely up to you as long as it resides under the document root. You can organize your files by operating system, type of application, or any other characteristic that meets the needs of your organization.

The following sample shows separate folders for each operating system. In them are folders for each software package to be used for that operating system. The `COMMON` folder shown in this example contains folders for software packages that can be installed on either Windows XP or Windows 2000.

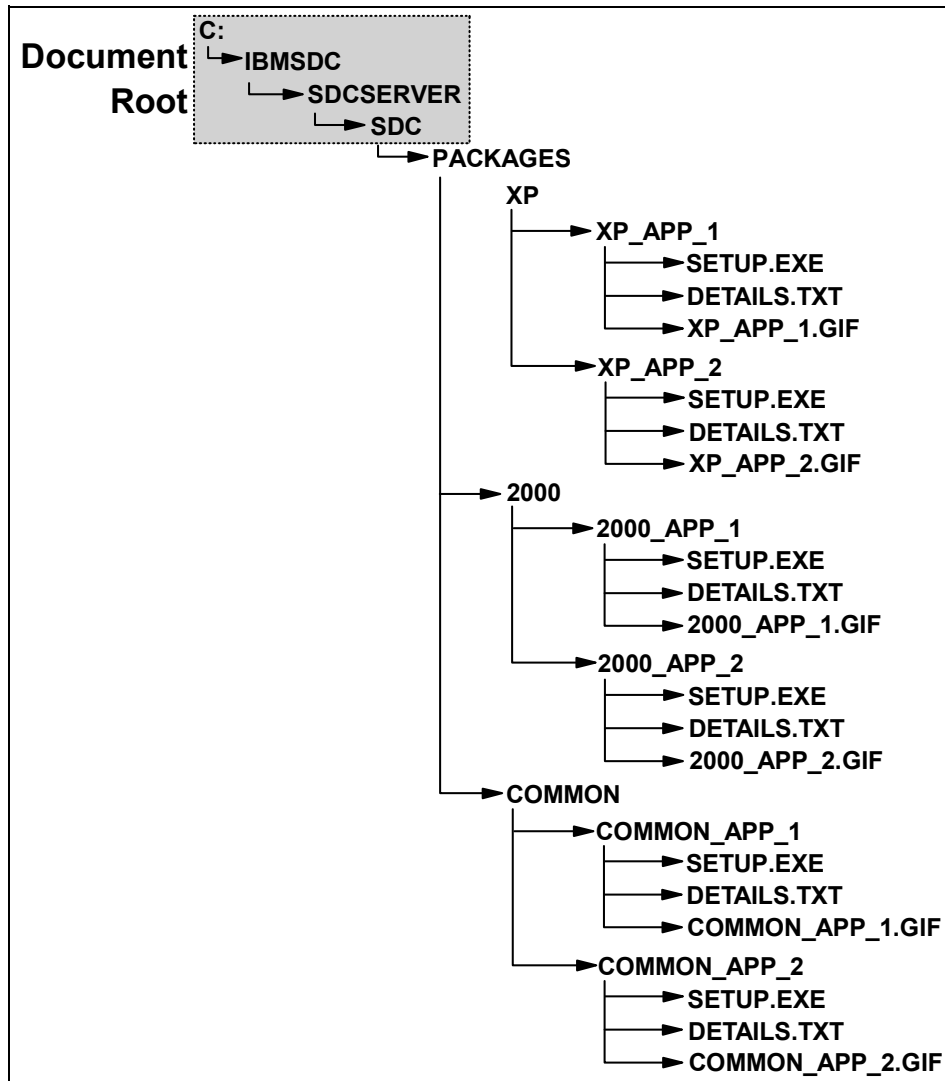


Figure 4-59 Software Delivery Center folder structure

4.5.2 Creating a software package

Creating a software package involves the following tasks:

1. Creating the source files. See “Creating the source files” on page 281 for more details.
2. Determining where you will store the source files for distribution. See “Determining where to store the source files” on page 282 for details.

3. Adding the software packages to the Software Delivery Center library through the administrator's console. See "Adding the software package to the Software Delivery Center library" on page 284 for details.

Creating the source files

The first step in creating a software package is creating the source files. The following are the source files associated with each package:

- The source software package (required)

This file typically is created using a third-party packaging tool. Software Delivery Center supports any software package created by the following packaging tools:

- InstallShield
- Wise InstallManager
- WinZip Self-Extractor
- Microsoft Software Installer (MSI)

Note: For best results, the source package should be developed so it installs silently (without user intervention).

For information about using these tools, refer to the documentation provided by the packaging tools.

Optionally, the source software package can be in an unpacked format that consists of a folder structure with all the files required for installation or data files for distribution.

- The icon file (optional)

When a user selects a package from a catalog, Software Delivery Center displays basic information about the program, such as the file size and amount of disk space required. If an icon file is provided, the icon shown in Figure 4-60 is displayed next to the basic information. The icon image can be either a .gif or .jpg file. Icons are 32 pixels by 32 pixels.

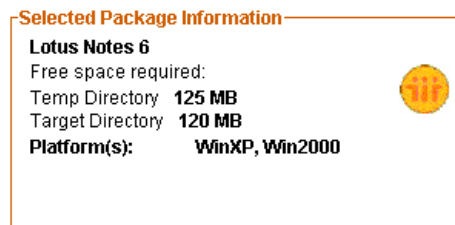


Figure 4-60 Software Delivery Center catalog information

- The details file (optional)

When a user selects a package from the catalog and wants more information than the basic information that is typically displayed, the user can click the **Details** button in the catalog to view the information in the details file shown in Figure 4-61.



Figure 4-61 Software Delivery Center package details window

Note: The details file must be in .txt format and can contain any information deemed useful by the administrator. For example, if a README.TXT file is provided by the software vendor, the administrator might choose to use the README.TXT file as the details file.

Determining where to store the source files

After you have created your source files, you need to determine where you will store them for distribution. You can store the source files on either of the following:

- On the Software Delivery Center server under the document root. The default document root is c:\BMSDC\SDC\SERVER\SDC. Your document root might be different depending on the options you selected during installation.

Packages stored on the Software Delivery Center server are always downloaded to the client before being installed. When you add these packages to the library with the administrator's console, you must assign one of the following package types to each package:

- Download(Open)

This type signifies a package that is created by a third-party packaging tool that is not identified by a digital signature.

- Download(Secure)

This type signifies a package that is created by a third-party packaging tool that is identified by a digital signature.

- DirectoryDownload

This type is assigned to an unpackaged set of files and folders. When this type of package is added to the library, Software Delivery Center automatically creates a compressed file containing these files and folders. It is important to note that unpackaged files and folders intended for distribution must reside on the Software Delivery Center server.

- ▶ On a shared network drive outside of the Software Delivery Center server. Throughout the remainder of this document, the term *logical drive* is used to describe this storage location. Packages stored on a logical drive are not downloaded to the client; they are installed directly from the logical drive. When you add these packages to the library through the administrator's console, you will have to assign one of the following package types:

- LogicalDrive(Open)

This type of package is created by a third-party packaging tool that is not identified by a digital signature.

- LogicalDrive(Secure)

This type of package is created by a third-party packaging tool that is identified by a digital signature.

Figure 4-62 is a high level overview of the different package types and where the source files reside.

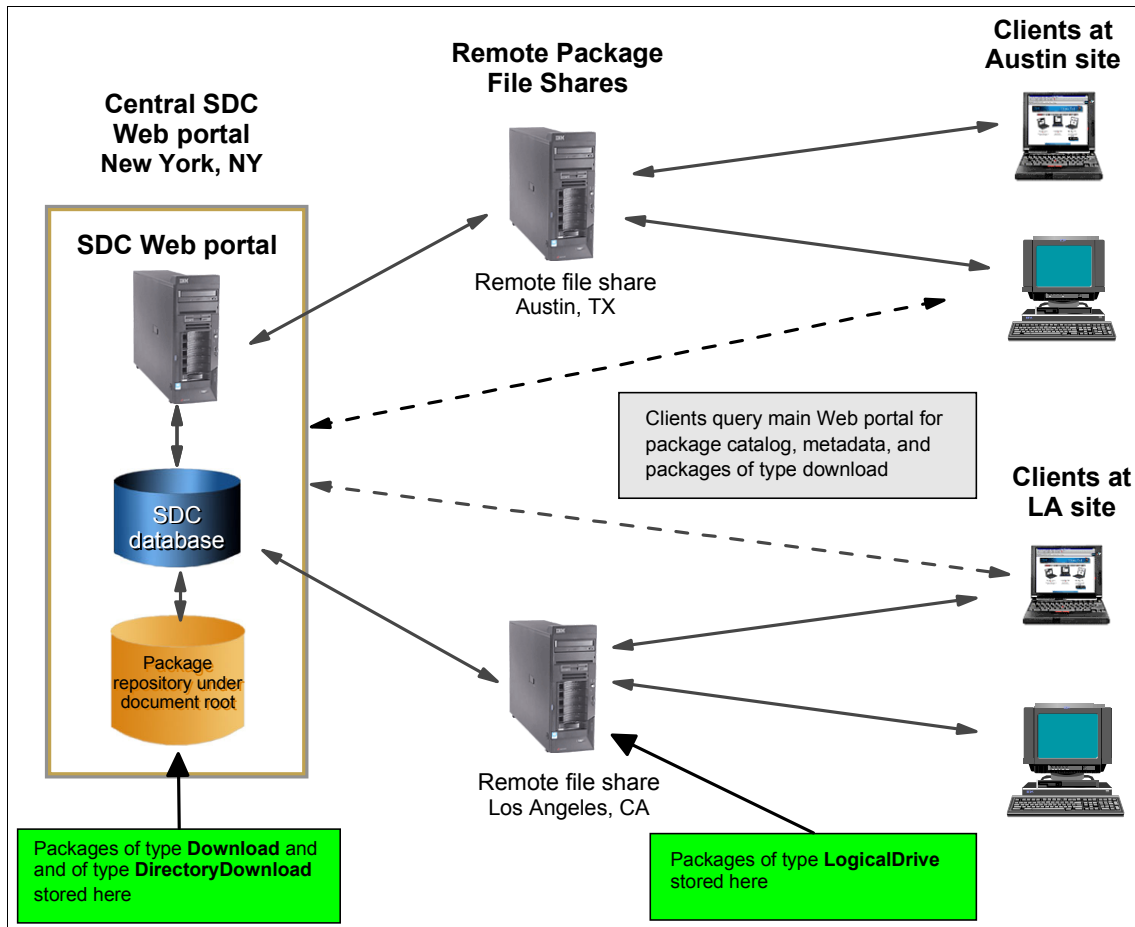


Figure 4-62 Storage of different package types

For more information about adding packages to the library, see “Adding the software package to the Software Delivery Center library”.

Adding the software package to the Software Delivery Center library

After the source package has been created, you must use the administrator’s console to add it to the Software Delivery Center library. This process adds information in a database that includes a pointer to the source files and the text that appears in a catalog. This process does not physically copy any source files

into the library; it simply creates database entries. If the source files need to be copied to the Software Delivery Center server, the administrator must copy the files before the packages are added to the library database. If the source files are deleted or moved from their original location after the entries have been added to the database, the administrator must modify the software package information in the library to update the database. For more information about adding a package to the library, see “Adding a new software package to the library” on page 312.

4.5.3 Creating a software bundle

A software bundle is a collection of software packages that is either made available for users to pull through a single catalog entry or pushed to users. After you have created the individual software packages, you can use the Software Delivery Center administrator's console to create a software bundle. Software bundles are optional. For more information about creating a software bundle, see “Adding a new software bundle to the library” on page 314.

4.5.4 Creating a portable catalog

You can use Software Delivery Center to create a portable catalog that can be run from a network drive, CD, or other portable media. This feature is useful for computers that are not connected to the network or computers that do not have access to the Software Delivery Center server. The portable catalog contains software packages and bundles and a Java-based application that displays the catalog and allows a user to select which software packages to install.

Creating a portable catalog is a two-step operation. First, you create an export group and select which software packages or bundles to include in the export group catalog. See “Creating an XML output file for an export group” on page 345 for details. Then, you invoke an export process that creates the portable catalog files and copies them to a folder. See “Importing Software Delivery Center files from another server” on page 348 for details.

4.5.5 Using a portable catalog

If the portable catalog is on a CD, in most cases it starts automatically when the CD is inserted into the drive. If the portable catalog does not start automatically or if the portable catalog is on a different type of media (such as network drive and USB memory key), you must use the following procedure:

1. Open Windows Explorer or My Computer and navigate to the folder where the portable catalog resides.
2. Double-click the **SETUP.bat** file.

Note: If a prompt asks if you want to install the Build CD and Verify program, click **Start**. You will see this prompt the first time you start a portable catalog on a computer. If a prompt asks if you want to create a desktop icon, click **No**. You will see this prompt the second time you start a portable catalog. When the portable catalog opens, make your selections from the **Packages** and **Bundles** tabs, then click **Install**.

4.5.6 Importing files from another server

Importing files from another Software Delivery Center server using the admin console is a process with three phases:

1. The first phase involves creating an export group, defining the packages and bundles to be exported, and exporting an XML output file from the source Software Delivery Center server. See “Creating an XML output file for an export group” on page 345.
2. The second phase adds the package entries to the target Software Delivery Center library database. This is accomplished by importing the XML output file that was exported by the source Software Delivery Center server. See “Importing Software Delivery Center files from another server” on page 348.
3. The third phase involves copying the software packages from the source Software Delivery Center server to the target Software Delivery Center server. Software packages residing on logical drives (shared network drives outside of the source Software Delivery Center server) do not have to be copied. See “Importing Software Delivery Center files from another server” on page 348.

Note: The folder structure for the package files must be the same on the target server as the source server. Otherwise, the package information must be updated for each package.

4.5.7 Command prompt Export/Import interface

The XML files used to exchange data between Software Delivery Center Servers can be created and imported using the command prompt interfaces illustrated in Example 4-2 on page 287 and Example 4-3 on page 287.

A single command on the source server creates the output.xml file that contains the information required to replicate all packages in the database. Another command on the target server can then use the output.xml to populate the database with the definitions for the entire package repository.

Example 4-2 Export XML command prompt syntax

```
Java -cp C:\IBMSDC\SDCServer\database\cloudscape\lib\db2j.jar:  
      C:\IBMSDC\SDCServer\sd\WEB-INF\lib\dom.jar:  
      C:\IBMSDC\SDCServer\sd\apps\sdctools.jar  
      com.ibm.webd.server.tools.CmdLine  
      -v -o c:\output.xml  
      -url jdbc:db2j:c:\IBMSDC\SDCServer\database\sd
```

Example 4-3 Import XML command prompt syntax

```
Net stop "Apache Tomcat"  
Java -cp C:\IBMSDC\SDCServer\database\cloudscape\lib\db2j.jar:  
      C:\IBMSDC\SDCServer\sd\WEB-INF\lib\jdom.jar:  
      C:\IBMSDC\SDCServer\sd\apps\sdctools.jar  
      com.ibm.webd.server.tools.CmdLine, -v -i C:\output.xml  
      -url jdbc:db2j:C:\IBMSDC\SDCServer\database\sd  
Net start "Apache Tomcat"
```

Note: The Apache Tomcat Service must be stopped and restarted before you can use the import command prompt interface. This could affect a production environment. In this case, it may be best to use the administrator's console, which does not require the Apache Tomcat service to be stopped.

4.6 Setting up Software Delivery Center infrastructure

Once you have installed the server portion of Software Delivery Center and created your software library, you must set up an infrastructure for the type of software delivery method you want to support:

- ▶ A pull software delivery method is one in which a user can select one or more software packages or bundles from an online catalog and initiate the installation process.
- ▶ A push software delivery method allows an administrator to remotely schedule, deliver, and install one or more software packages or bundles. If the software packages are configured for an unattended installation, the push operation can be achieved without any user intervention.

You can also support both methods of software delivery.

The instructions for setting up the delivery method or methods are in the following sections:

- ▶ "Setting up a pull infrastructure" on page 288
- ▶ "Setting up a push infrastructure" on page 288

4.6.1 Setting up a pull infrastructure

Setting up a pull infrastructure involves creating groups, assigning users to groups, and building software catalogs for each group. The packages that can be used in the pull process are determined by the group to which the user is assigned. For example, an administrator might establish separate groups based on department needs, such as a Finance group, Development group, Human Resources group, and Marketing group. Each of these groups has its own software catalog. When a user assigned to the Finance group opens Software Delivery Center from a client computer, that user will be able to install any of the software listed in the Finance group catalog.

If the software needs of all users in a company are similar, the administrator can simply set up a single group and assign all of the users to that group. Or, the administrator can set up different groups for management and non-management personnel if access to certain applications is restricted to management only. The number of groups you choose to implement and the granularity of groups is determined by the needs of your company.

To set up a pull infrastructure, perform the following tasks:

1. Evaluate the software needs of your company.
2. Set up groups. See “Adding a new group” on page 297 for details.
3. Assign users to each group. See “Adding a new user” on page 306 for details.
4. Build a software catalog for each group. See “Adding or deleting a software package or bundle in a specific export group” on page 343 for details.

4.6.2 Setting up a push infrastructure

Setting up a push infrastructure involves creating distribution groups, assigning computer names to the distribution groups, and setting up a schedule.

A distribution group is a distribution list of the computers to which the push packages or bundles will be made available. Each computer is identified by the computer name and its associated host name and IP address. Software Delivery Center maintains a list of all registered Software Delivery Center clients installed. Client registration automatically takes place when the client agent is installed. When you create a distribution group, you make selections from the registered clients list.

Note: Distribution lists used by the push process are different from the groups used by the pull process. User and group names used by the pull process are not used by any functions of the push process. Instead, the push process uses computer names and identifies the target computers by host name and IP address. There is no relationship between user names and machine names or between groups and distribution lists.

The schedule defines which software packages or bundles are to be installed and when and how long the software packages or bundles be available to the client computers defined in the distribution group.

Each client computer queries the server at scheduled intervals to determine if push packages or bundles have been made available. If they are available, the client agent automatically begins the installation process if the packages are configured for unattended installation or if the user is logged on. If the packages require user intervention during the installation process and the user is not logged on, the client agent delays installation until the user logs on.

The intervals at which the client queries the server are controlled by the client agent and are set when the client agent is installed. Therefore, the installation of the push package does not begin as soon as the push package is made available; instead, it is dependent upon when the client queries the server.

Note: The default interval for client queries is 60 minutes. If you want to change the interval length, edit the `sd.c.conf` file on the client computer with a text editor such as Notepad. Change the numeric value to any value in the range 0 to 99999.

Upon the successful installation of the push package, an entry is logged that prevents the client computer from installing the same push package again the next time it queries the server.

To set up a push infrastructure, perform the following tasks:

1. Evaluate the software needs of your company.
2. Compile a list of computer names and their respective users. You will need this information later when you assign machines to the distribution groups.
3. Set up distribution groups. See “Adding a distribution group” on page 354 for details.
4. Assign machines to the distribution groups. See “Adding or deleting machines for a specific distribution group” on page 361 for details.
5. Set up a schedule. See “Adding a schedule” on page 367 for details.

4.6.3 Software Delivery Center package directory replication tips

If more than one Software Delivery Center server is used or there are multiple distribution points for packages, an administrator may be required to keep several Software Delivery Center package repositories synchronized. Microsoft provides a command-prompt tool called Robocopy that can save administrative time and ensure that packages are available across all Software Delivery Center distribution points in an environment.

Robocopy is a 32-bit command-prompt tool used for file replication. This tool helps maintain identical copies of a directory structure on a single computer or in separate network locations. Robocopy can be found in the Windows 2003 Server administration kit. You can copy a single directory, or you can recursively copy a directory and its subdirectories with Robocopy. The tool classifies files based on whether they exist in the source directory, in the destination directory, or both. In the latter case, the tool further classifies files by comparing time stamps and file sizes between the source file and the corresponding destination file. You control which classes of files are copied. If a file exists in both the source and destination locations, by default Robocopy copies the file only if the two versions have different time stamps or different sizes. This saves time if the source and destination are connected by a slow network link. You can also specify that copies are restarted in the event of a failure, which saves even more time when network links are unreliable.

With Robocopy, you can:

1. Use file names, wildcard characters, paths, or file attributes to include or exclude source files as candidates for copying
2. Exclude directories by name or by path
3. Delete source files and directories after copying (that is, move rather than copy them)
4. Delete destination files and directories that no longer exist in the source
5. Control the number of times the program retries an operation after encountering a recoverable network error
6. Schedule copy jobs to run automatically
7. Specify when copying is to be performed
8. Monitor a directory tree for changes
9. Selectively copy file data.

Robocopy version XP010 system requirements are:

- Microsoft® Windows® Server 2003
- Microsoft® Windows® 2000

To run Robocopy, use the following syntax at the command prompt:

ROBOCOPY source destination [file [file]...] [options]

Table 4-1 defines these syntax elements.

Table 4-1 Robocopy syntax elements

Variable	Meaning	Comments
source	source directory	You can use drive:\path or \\server\share\path
destination	Destination directory	You can use drive:\path or \\server\share\path
file	Names of files to act upon	You can use wildcard characters (? and *). If no files are listed, Robocopy defaults to all files (*.*)
options	command-prompt options you wish to use	Available options are described later in this document.

Tip: To view brief usage instructions at the command prompt, run ROBOCOPY without specifying any command-prompt options.

Robocopy and Software Delivery Center

To use Robocopy, enter the following strings into a batch file:

```
robocopy <source> <destination> /E /R:x /NP /w:min /V /XD <directory>  
/LOG+:<logfile> /MOT:min /RH:hmm-hmm
```

The options are described in Table 4-2.

Table 4-2 Robocopy option descriptions

Option	Description
/E	Copies all subdirectories (including empty ones)
/R:x	Specifies the number of retries on failed copies (the default is 1 million)
/NP	Turns off copy progress indicator (% copied), otherwise log file gets very big
/w:min	Specifies the wait time between retries (the default is 30 seconds.)
/V	Produces verbose output (including skipped files), creating a record of all files copied or not in the log file

Option	Description
/XD <directory>	Excludes directories with the specified names, paths, or wildcard characters in case there are server specific packages
/LOG+:	Redirects output to the specified file, appending it to the file if it already exists
/MOT	Monitors the source directory for changes, and runs again when a further <i>n</i> minutes have elapsed, and the minimum number of changes specified by /MON have been detected (default for /MON is 1 if not specified)
/RH	Defines the time slot during which starting new copies is allowed, which is useful for restricting copies to certain times of the day. Both values must be 24 hour times in the range 0000 to 2359

Sample Robocopy batch file

The sample batch file in Table 4-4 first maps a drive to a target server. Once the drive is mapped, Robocopy monitors both the source package directory and package signature directories for any changes. Any changes will only be copied to the target server during the designated time window (2300 – 0300). Any changes will be logged in the c:\temp\sync.log log file.

Example 4-4 Robocopy batch file

```
@echo off
net use z: /d

net use z: \\157.235.3.231\d$

start robocopy D:\IBMSDC\SDCServer\sd\packages\win32
          Z:\IBMSDC\SDCServer\sd\packages\win32 /E /R:3 /NP /w:5 /V /XD
          webdagent /LOG+:c:\temp\sync.log /MOT:60 /RH:2300-0300

start robocopy D:\IBMSDC\SDCServer\sd\signatures
          Z:\IBMSDC\SDCServer\sd\signatures /E /R:3 /NP /w:5 /V
          /LOG+:c:\temp\sync.log /MOT:60/RH:2300-0300
```

4.7 Using the Software Delivery Center administrator's console

You can perform various administration tasks, such as managing software packages and bundles, creating schedules, and viewing error logs from the IBM Software Delivery Center administrator's console.

This section covers the following topics:

- ▶ “Accessing Software Delivery Center administrator’s console” on page 293
- ▶ “Managing groups” on page 296
- ▶ “Managing users” on page 306
- ▶ “Managing software packages and bundles” on page 312
- ▶ “Exporting and importing software packages and bundles” on page 336
- ▶ “Managing distributions” on page 354
- ▶ “Managing machines” on page 364
- ▶ “Managing schedules” on page 367
- ▶ “Using the IBM Software Delivery Center logs” on page 375
- ▶ “Finding help” on page 381
- ▶ “Logging out of the administrator’s console” on page 381

4.7.1 Accessing Software Delivery Center administrator’s console

With the administrator’s console, you use a Web browser to manage the Software Delivery Center process. Only authorized users who belong to the SDCAdmin group can access the Software Delivery Center administrator’s console. To authorize a Software Delivery Center administrator, another administrator must create a new user and assign the user name to the SDCAdmin group. See “Adding a new user” on page 306 for details.

To access the Administration Login panel:

1. Start your browser and type `http://localhost:8080` or `http://server_name:8080` (where *server_name* is the name of the Software Delivery Center server) in the Address bar; then press **Enter**. The Loading SDC Admin Console page shown in Figure 4-63 on page 294 opens.

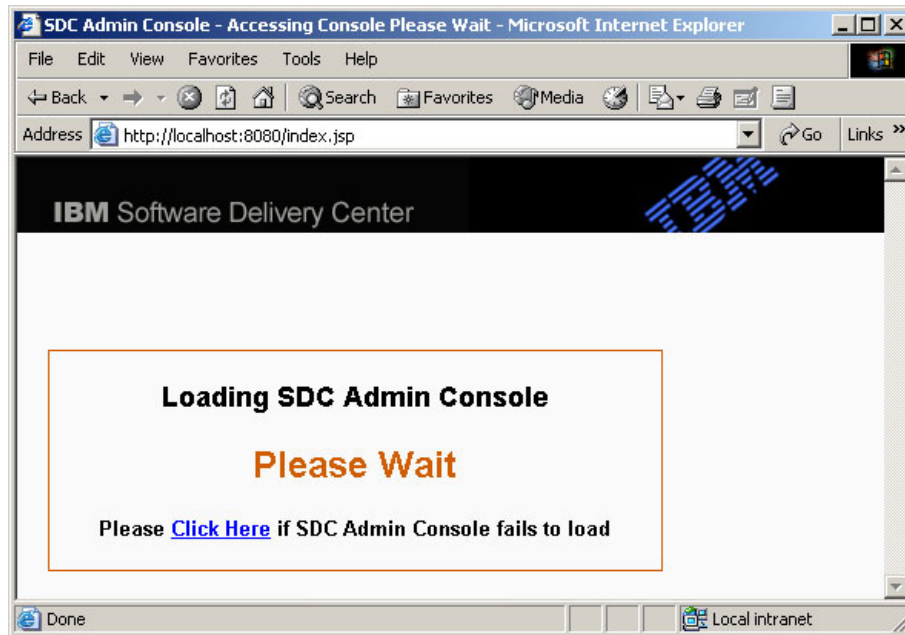


Figure 4-63 Software Delivery Center administrator's console launch message

Note: The administrator's console is always accessed from HTTP port 8080. By default, the Software Delivery Center Admin Console Login page loads automatically. At first launch, it may take a few seconds for the Software Delivery Center admin console page to load.

2. The Software Delivery Center Administration Console Login page shown in Figure 4-64 opens.

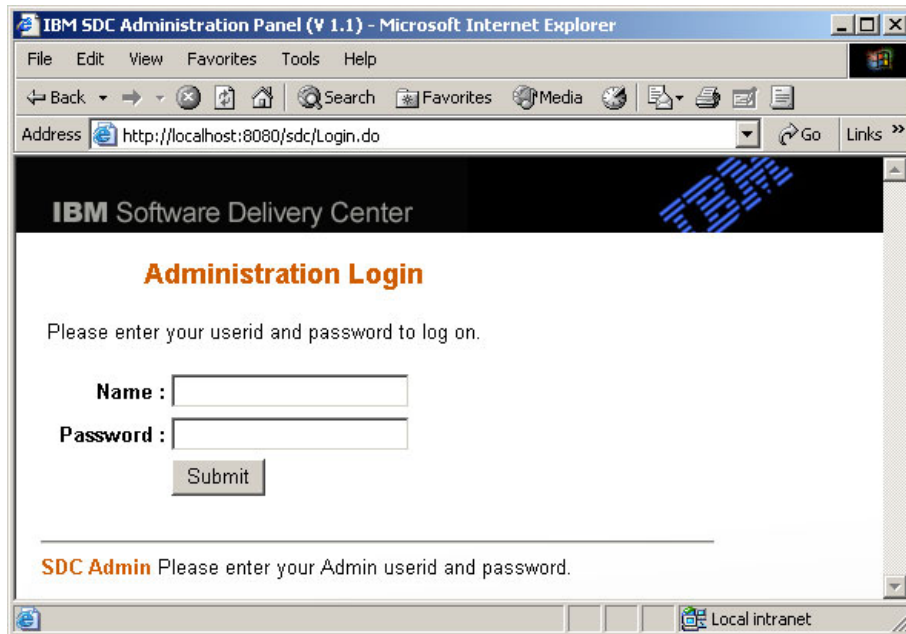


Figure 4-64 Software Delivery Center administrator login page

Note: The Web address used to access Software Delivery Center is case sensitive. The default administrator user name is *sdc* and the default password is *sdc*. If you want to change the user name and password, see “Managing users” on page 306

3. Enter *sdc* in the Name field, *sdc* in the Password field, and click **Submit**. The Group Management page shown in Figure 4-65 on page 296 opens.

Note: To access the administrator’s console, the user must belong to the SDCAdmin group. This means that an administrator must create a new user and assign the user name to the SDCAdmin group. For more information about creating a new user name, refer to “Adding a new user” on page 306.

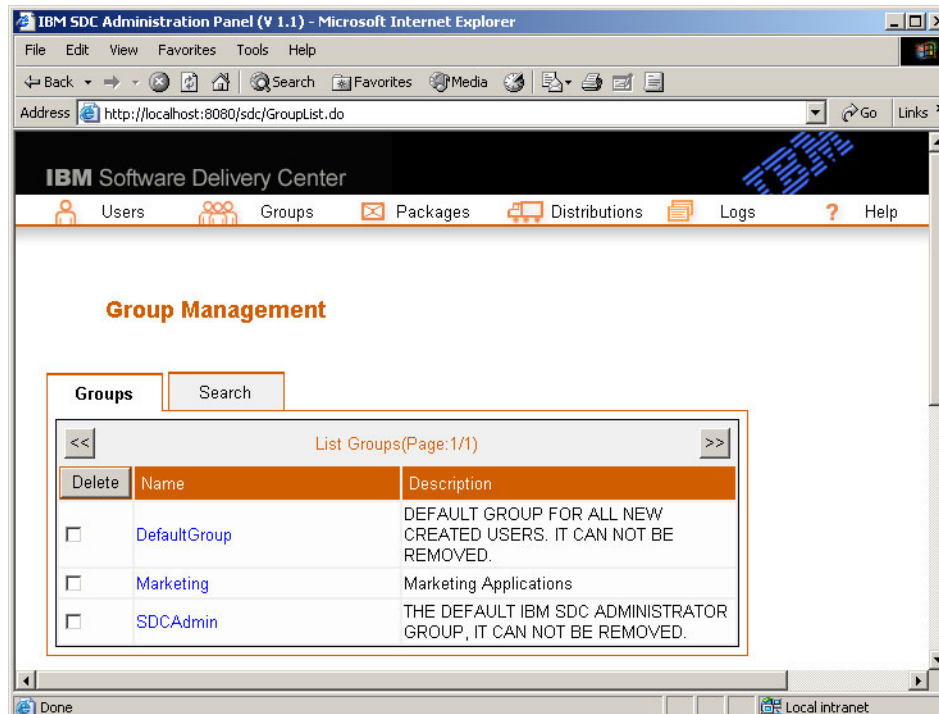


Figure 4-65 Software Delivery Center Group Management page

4.7.2 Managing groups

Groups are used to categorize users. A group is a set of users that are given access to a particular collection of software packages and bundles. The Group Management page shows a list of group names and their associated descriptions (List Groups table).

Adding a new group

To add a new group:

1. From the Software Delivery Center menu, select **Groups** → **New**. The Add Group page shown in Figure 4-66 opens.

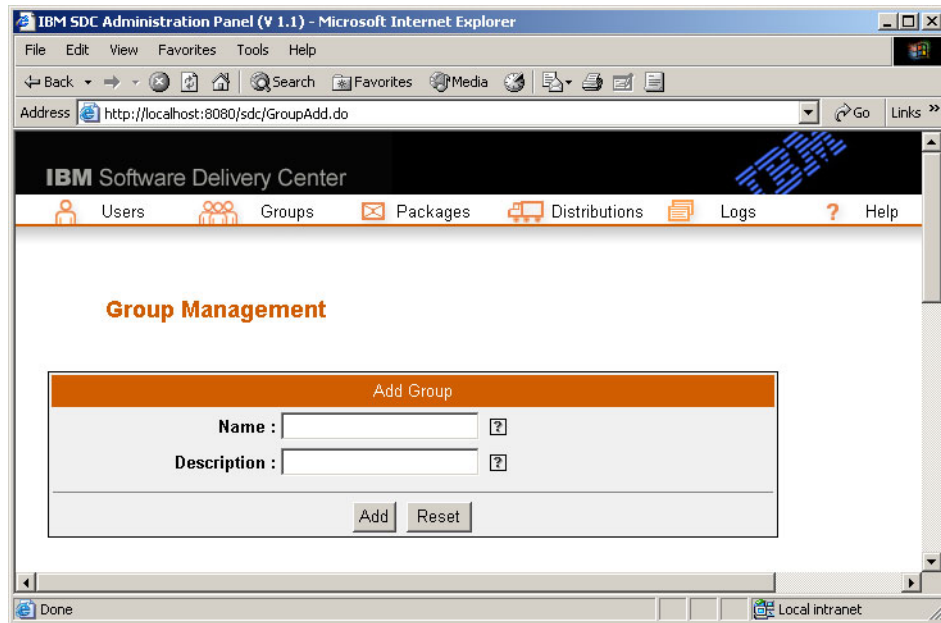


Figure 4-66 Software Delivery Center Add Group page

2. In the Name field, type the group name you want to add.
3. In the Description field, type the associated short description.
4. Click **Add**.

5. The Add Group page with a message that says “Group '<group name>' has been added successfully” (Figure 4-66 on page 297) opens.

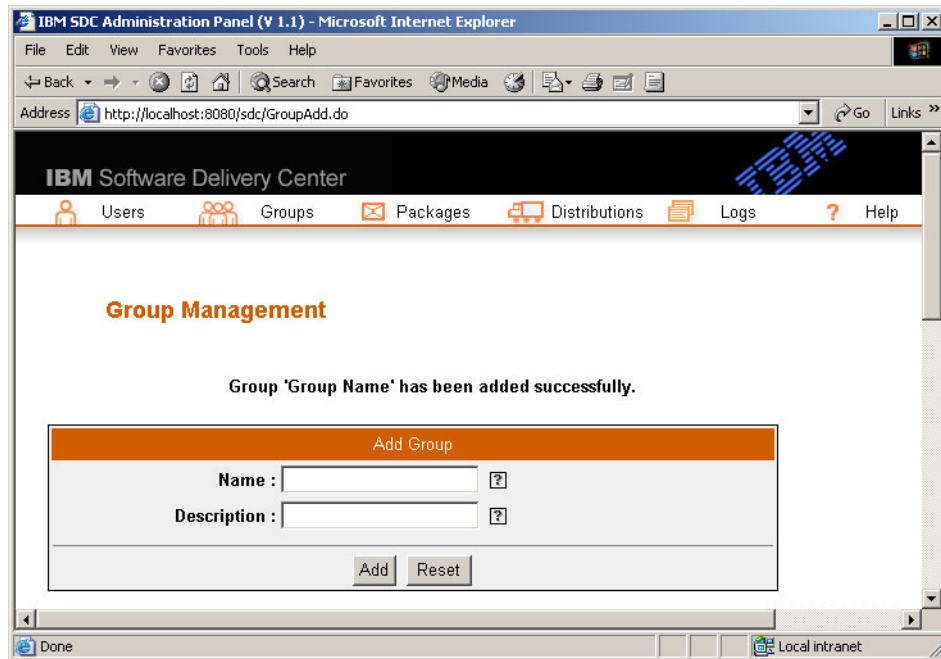


Figure 4-67 Software Delivery Center successful group addition message

Note: You cannot create multiple groups with the same name. The Name field has a limitation of 32 characters, uniquely defined to distinguish group definitions. In addition, the field will not accept apostrophes or quotation marks. The Description field is an alphanumeric field that has a limitation of 128 characters and is used to describe a group definition.

Deleting a group

To delete an existing group:

1. Select **Groups** → **All Groups**. The List Groups page shown in Figure 4-68 opens.

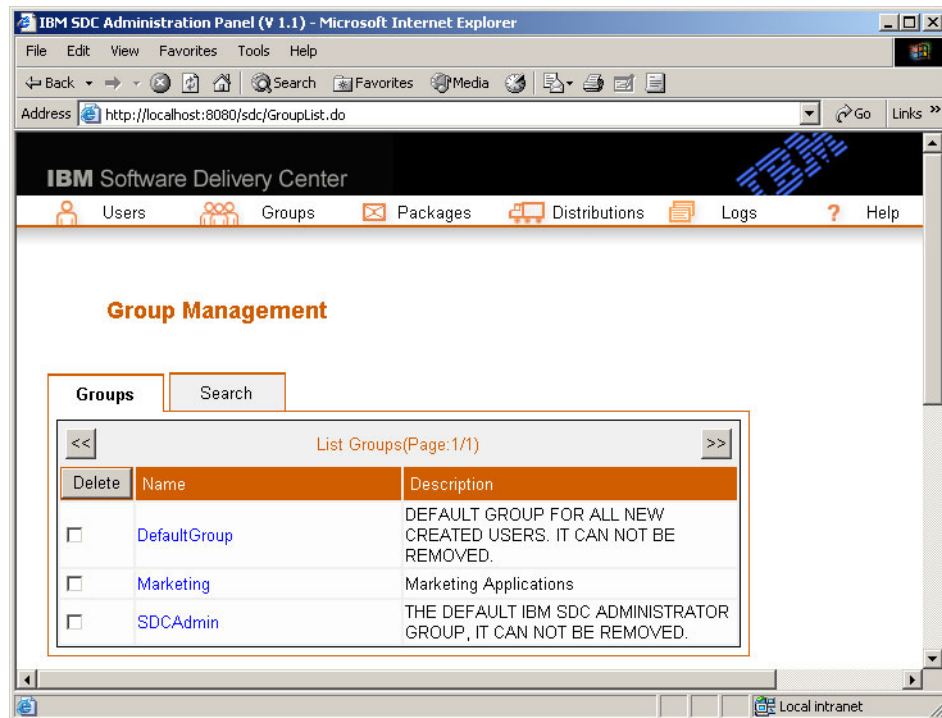


Figure 4-68 Software Delivery Center groups list

2. Select the check box beside the group name you want to delete.
3. Click **Delete**. The window shown in Figure 4-69 opens.

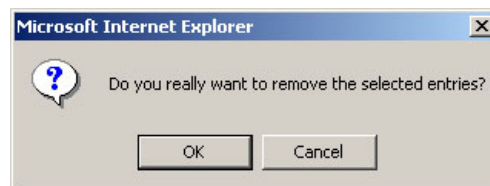


Figure 4-69 Software Delivery Center window

4. Click **OK** to delete the group or click **Cancel** to return without making any changes to the database.

Searching for a group

To search for a specific group name:

1. Select **Groups** → **All Groups**. The List Groups page shown in Figure 4-68 on page 299 opens.
2. Click **Search**. The Search page shown in Figure 4-70 opens.

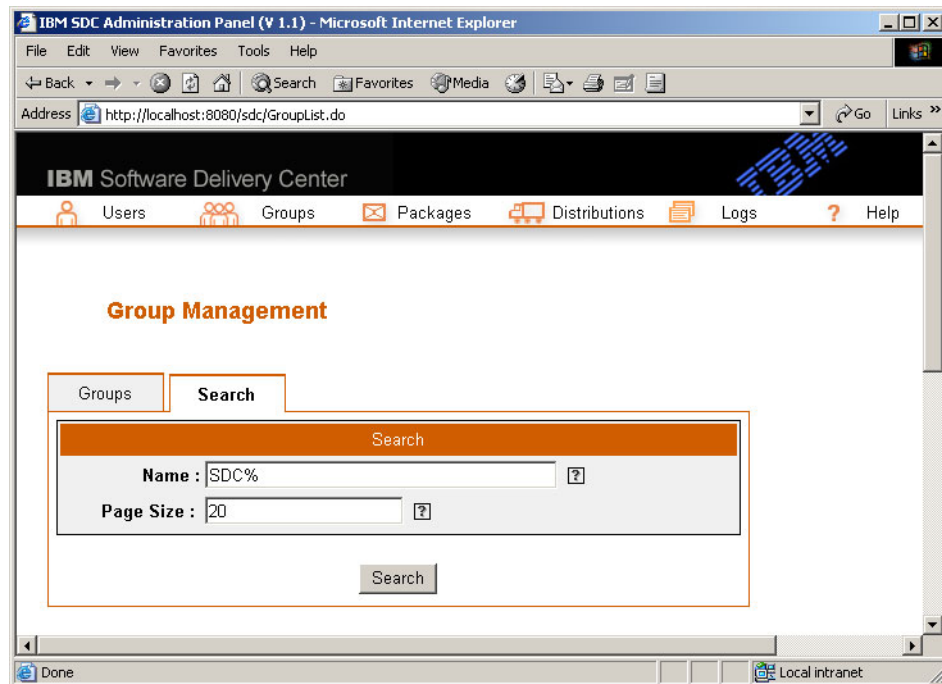


Figure 4-70 Software Delivery Center administration group search

3. In the Name field, type the group name.
4. In the Page Size field, type the maximum number of entries per page to display.

Note: The group name is case sensitive. Type the name exactly as the name is listed in the group list you are searching. If you are not sure of the spelling, you can use the percent symbol (%) as a wild card in place of one or more characters. (for example, A% or a%).

5. Click **Search**.

6. The selected group name and description is shown in the List Groups table (Figure 4-71).

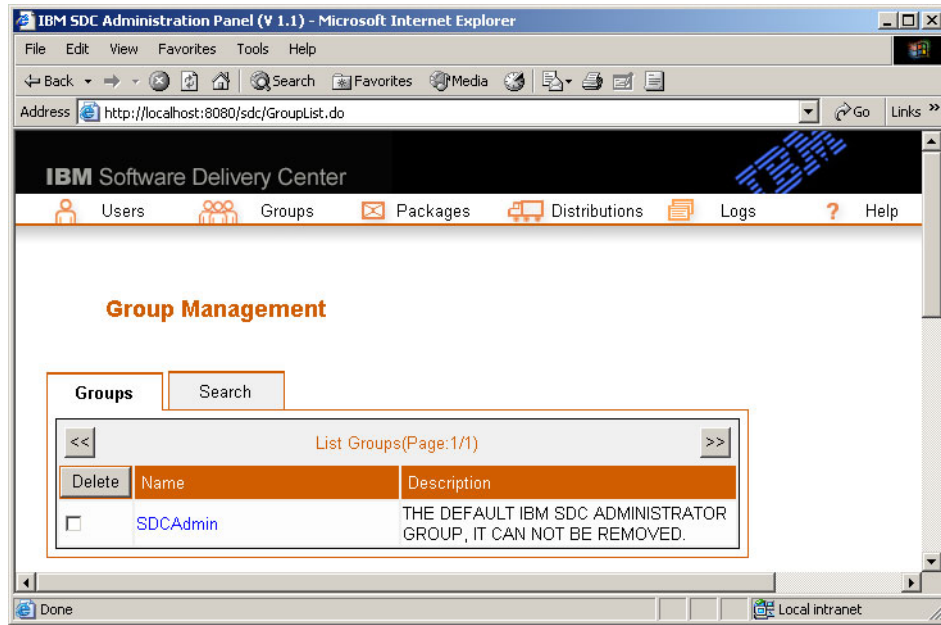


Figure 4-71 Software Delivery Center administration groups search results

Changing the group description

To change the group description:

1. Click **Groups** → **All Groups**. The List Groups page shown in Figure 4-68 on page 299 opens.

2. Click the group name. The Update Group page shown in Figure 4-72 opens.

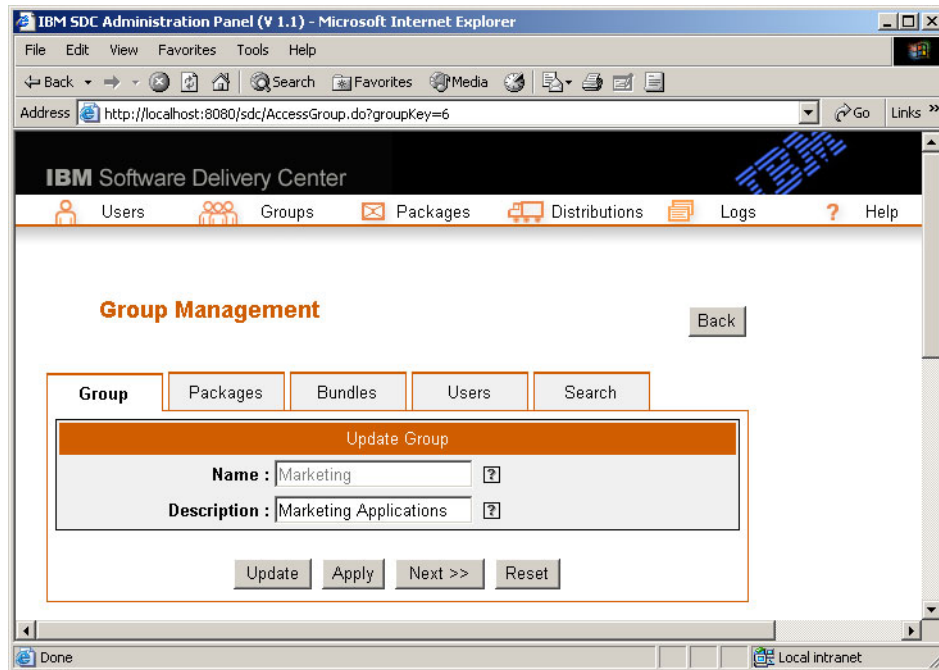


Figure 4-72 Software Delivery Center administration group description update

3. Make the changes to the description.
4. Click **Update**. The List Groups table shown in Figure 4-65 on page 296 is displayed.

Adding or deleting a software package or bundle for a specific group

To add or delete a defined software package or bundle for a specific group:

1. Select **Groups** → **All Groups**. The List Groups table shown in Figure 4-65 on page 296 appears.
2. Click the group name. The Update Group page shown in Figure 4-72 opens.
3. Click the **Package** or **Bundle** tab, depending on which one you want to add or delete. The Package Access List (Figure 4-73 on page 303) or the Bundle Access List for a specific group name appears.



Figure 4-73 Software Delivery Center administration group application packages list

4. Select or clear the check box for the software package or bundle that you want to add to or delete from the group.

Note: When adding packages or bundles from multiple pages, you must click **Apply** to save your changes before selecting the << arrow or >> arrow to navigate between the multiple pages.

5. Click **Update**. The List Groups table shown in Figure 4-65 on page 296 is displayed.

Updating user information in a specific group

To update user information for a specific group:

1. Select **Groups** → **All Groups**. The List Groups table shown in Figure 4-65 on page 296 is displayed.
2. Click the group name. The Update Group page shown in Figure 4-72 on page 302 opens.
3. Click **Users**. The User List for a specific group such as that shown in Figure 4-74 is displayed.

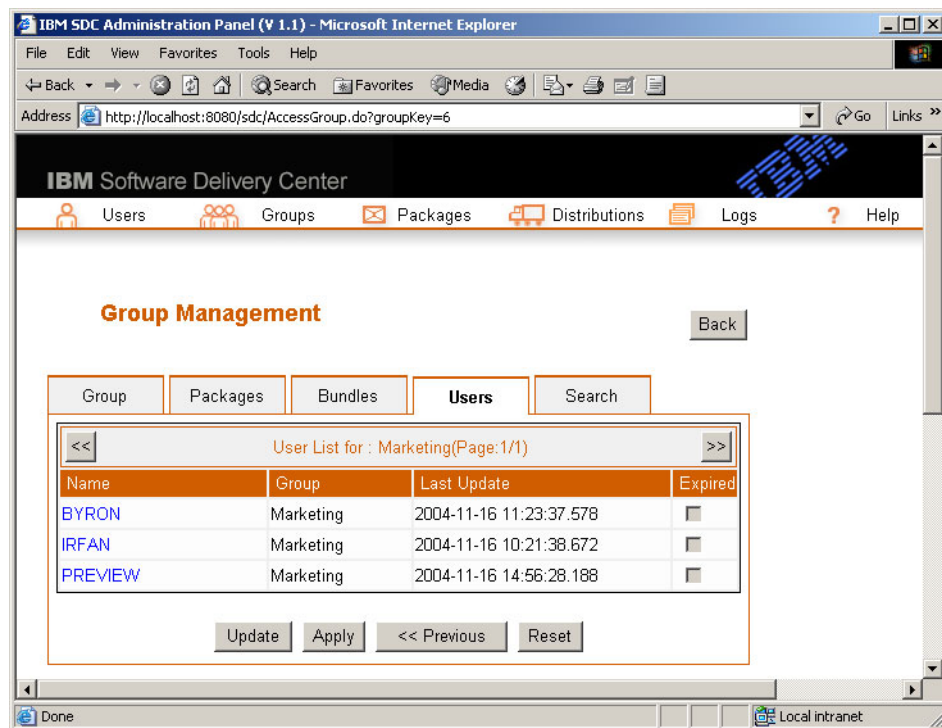


Figure 4-74 Software Delivery Center administration group user list

- Click the user name. The Update User page shown in Figure 4-75 opens.

IBM SDC Administration Panel (V 1.1) - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://localhost:8080/sdc/UserEdit.do?userid=PREVIEW Go Links

IBM Software Delivery Center

Users Groups Packages Distributions Logs Help

User Management Back

Update User

Name : PREVIEW ?

Reset Password : ☐ ?

New Password : ?

Confirm : ?

Expired : ☐ ?

EMail : ?

Group : Marketing ?

Created : 2004-11-16 14:56:28.188 ?

Last Update : 2004-11-16 14:56:28.188 ?

Update Reset

Done Local intranet

Figure 4-75 Software Delivery Center administrative user information update

- Make the changes to the user information. See “Updating user information” on page 312 for details.
- Click **Update**. The List Groups table shown in Figure 4-65 on page 296 will be displayed.

Note: The changes will be accepted even if there is an Unhandled Exception error. A fix for this unhandled exception will soon be available from IBM.

4.7.3 Managing users

Each user is required to obtain a user name and password before accessing the catalog. The User Management screen shows a list of user names, the group assignment, and the date that the user information was last updated.

Adding a new user

To add a new user:

1. Click **Users** → **New**. The Add User page shown in Figure 4-76 opens.

IBM SDC Administration Panel (V 1.1) - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media Print Mail

Address http://localhost:8080/sdc/UserAdd.do Go Links

IBM Software Delivery Center

Users Groups Packages Distributions Logs Help

User Management

Add User

Name : Demo ?

Password : ***** ?

Confirm : ***** ?

Group : DefaultGroup ?

EMail : demo@mycompany.com ?

Add Reset

Local intranet

Figure 4-76 Software Delivery Center Add User page

2. In the Name field, type the name of the user.
3. In the Password field, type the password.
4. In the Confirm field, type the password again to ensure that you have entered it as intended.
5. In the Group field, select the group to which you want the user to belong.
6. In the EMail field, type the user's e-mail address.

Note: **Name** and **E-Mail** fields are alphanumeric fields with a limitation of 70 characters. **Password** field is an alphanumeric field with a limitation of 15 characters.

7. Click **Add**. The page shown in Figure 4-77 opens.

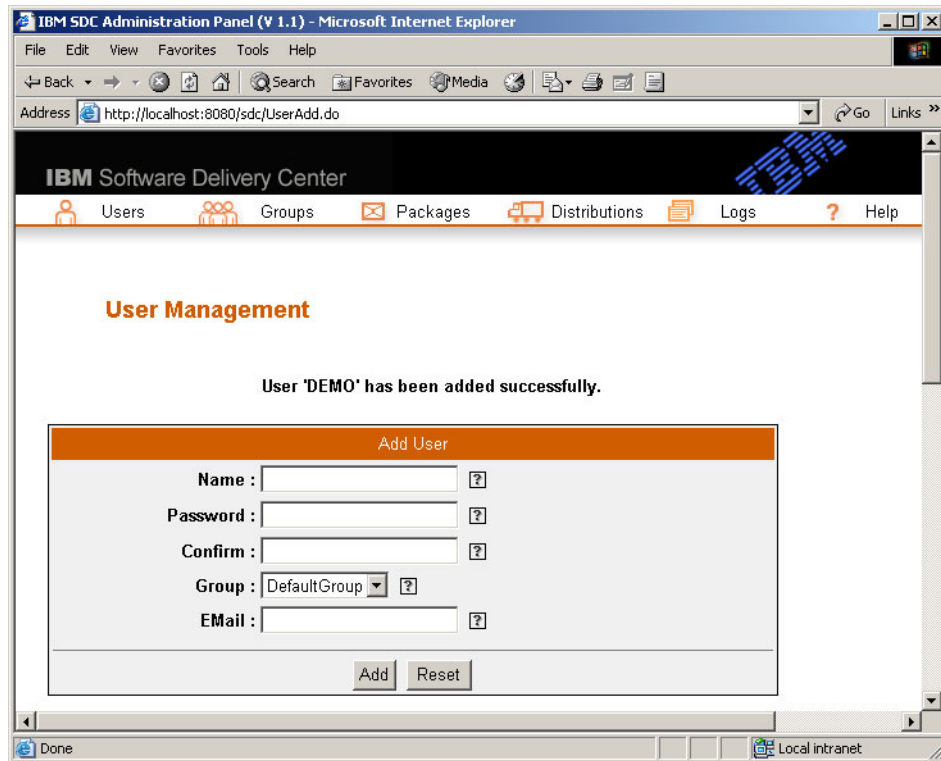


Figure 4-77 Software Delivery Center successful user addition message

Deleting a user

To delete a user:

1. Select **Users** → **All Users**. The List Users table shown in Figure 4-78 is displayed.

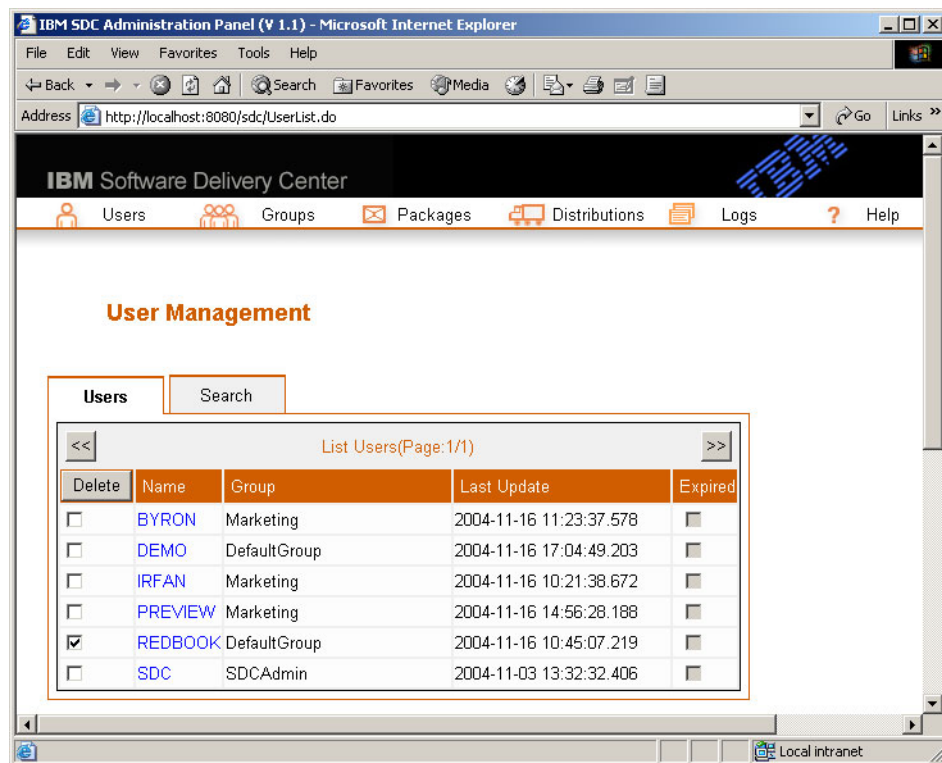


Figure 4-78 Software Delivery Center user list

2. Select the user name you want to delete as shown in Figure 4-78.
3. Click **Delete**. The window shown in Figure 4-79 opens.

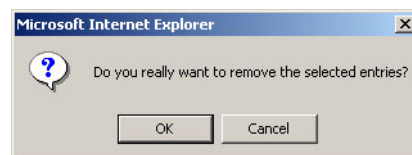


Figure 4-79 Software Delivery Center confirm user deletion window

4. Click **OK** to delete the user name or click **Cancel** for no action.

Searching for a user

To search for a specific user name:

1. Click **Users** → **All Users**. The List Users table shown in Figure 4-78 on page 308 is displayed.
2. Click **Search**. The Search page shown in Figure 4-80 opens.

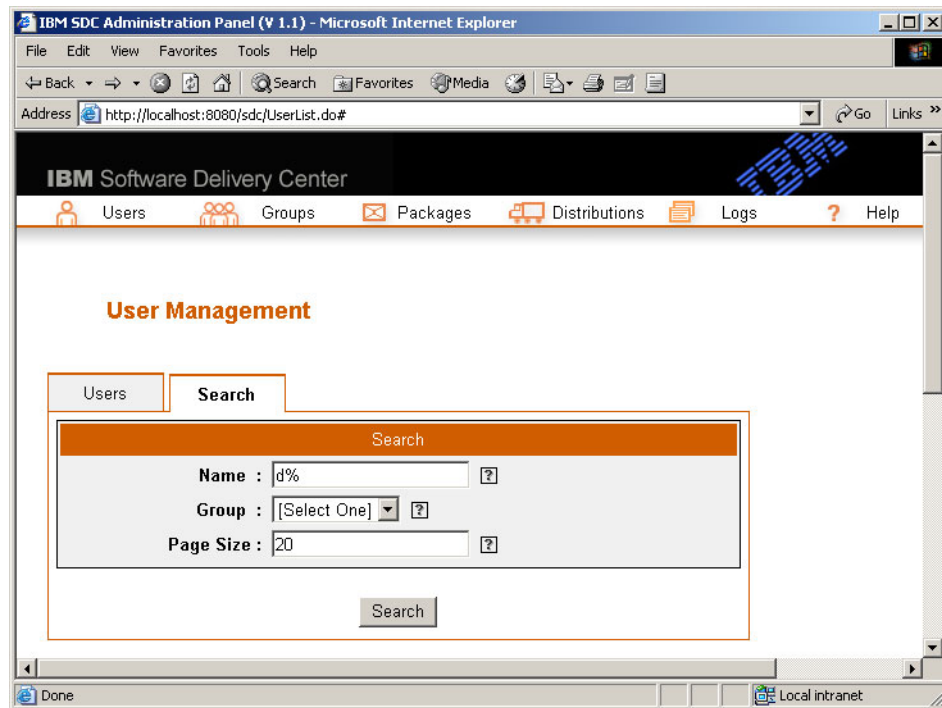


Figure 4-80 Software Delivery Center user search

3. You can search by user name or group. Do one or both of the following:
 - a. In the Name field, type the user name.
 - b. In the Group field, select the group name to which the user belongs.

Note: The user name text field is case sensitive. Type the name exactly as the name is listed in the user list you are searching. The text field can be searched with a wildcard (for example, A% or a%).

4. In the Page Size field, type the maximum number of entries per page to display.

5. Click **Search**. The selected user name and the description is shown in the List Users table (Figure 4-81).

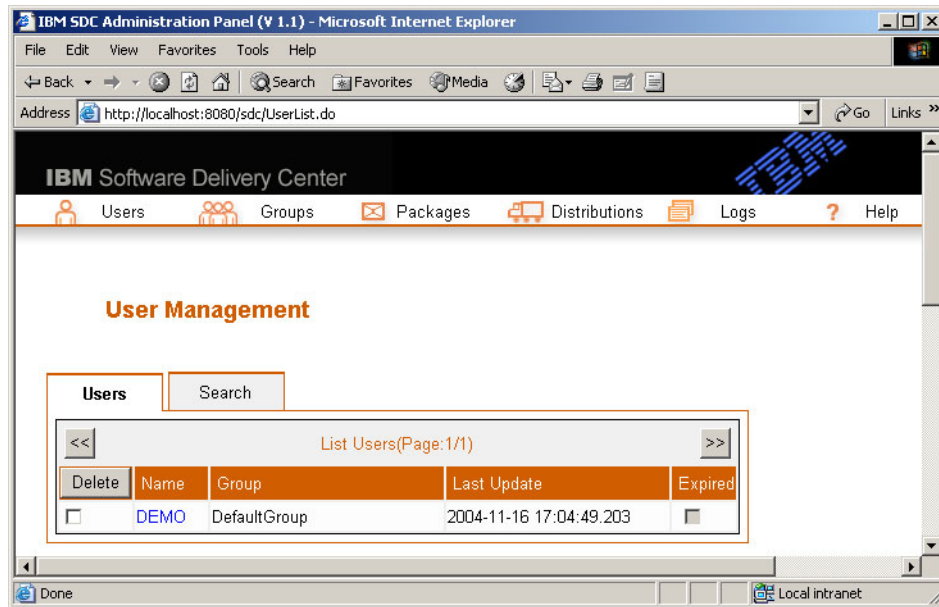


Figure 4-81 Software Delivery Center user search results

Changing a user to a different group

To change a user to a different group:

1. Click **Users** → **All Users** to obtain the List Users table (see Figure 4-78 on page 308).
2. Click the user name. The Update User page shown in Figure 4-82 opens.

IBM SDC Administration Panel (V 1.1) - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media Print

Address http://localhost:8080/sdc/UserEdit.do?userid=DEMO Go Links

IBM Software Delivery Center

Users Groups Packages Distributions Logs Help

User Management Back

Update User

Name : DEMO ?

Reset Password : ☐ ?

New Password : ?

Confirm : ?

Expired : ☐ ?

EMail : demo@mycompany.com ?

Group : DefaultGroup ?

Created : 2004-11-16 17:04:49.203 ?

Last Update : 2004-11-16 17:04:49.203 ?

Update Reset

Done Local intranet

Figure 4-82 Software Delivery Center Update User page

3. In the Group field, select the name of the group to which you want the user to belong.
4. Click **Update**. The List Users table shown in Figure 4-78 on page 308 opens with the group name updated.

Updating user information

To update user information:

1. Click **Users** → **All Users** to obtain the Users List shown in Figure 4-77 on page 307.
2. Click the user name. The Update User page shown in Figure 4-82 on page 311 opens.
3. Make the changes to the user information.

The following are the fields and descriptions used to update user information:

- Name: This field contains the user name. It cannot be modified.
- Reset Password: This field is used to reset user's password.
- New Password: This field is for entering a new password. The field is alphanumeric with a limitation of 15 characters.
- Confirm: You enter the new password again in this field.
- Expired: This field is used to terminate a user. If it is selected, the user cannot log in to the Software Delivery Center client applet.
- EMail: This field is used to update a user's e-mail. The field is alphanumeric with a limitation of 70 characters.
- Group: This menu allows the user to be a member of a different group.
- Created: This field contains the date the user account was created (system generated). It cannot be modified.
- Last Updated: This field shows the date the user account was last updated (system generated). It cannot be modified.

4. Click **Update** to obtain the List Users table shown in Figure 4-78 on page 308.

4.7.4 Managing software packages and bundles

Software packages are software files used to install a specific software application. Software bundles are groups of software packages. The Package Management page and the Bundle Management page show lists of software packages and bundles and their associated descriptions.

Adding a new software package to the library

If a software package file is stored on the Software Delivery Center server it must be placed in a folder under the document root (where `c:\ibmsdc\sdcserver\sdc` is the document root) as shown:

```
c:\ibmsdc\sdcserver\sdc\packages
```

If you have not already set up a folder structure for your library, see 4.5.1, “Creating a folder structure for your library” on page 279. For information about the source files (package file, details file, and icon file) used in this procedure, see 4.5.2, “Creating a software package” on page 280.

To add a new software package to the library:

1. Create your package file, details file, and icon file.
2. If you intend to store your package file, details file, and icon file on the Software Delivery Center server, create the folder structure for these files and then copy these files to the appropriate folder.
3. Open the administrator’s console and select **Packages** → **Packages** → **New**. The Add Package page shown in Figure 4-83 opens.

The screenshot shows the IBM SDC Administration Panel (V 1.1) in a Microsoft Internet Explorer browser window. The address bar shows <http://localhost:8080/sdc/PackageAdd.do>. The page title is "IBM Software Delivery Center". The navigation bar includes links for Users, Groups, Packages, Distributions, Logs, and Help. The main content area is titled "Package Management" and features four tabs: General, Install, Target, and Platform. The "General" tab is selected, displaying the "Add Package" form. The form contains the following fields and controls:

- Name:
- Version:
- Family:
- Details:
- Icon Path:
- Max Install Time(Min.):
- Silent: ☐
- Reboot: ☐

At the bottom of the form are three buttons: "Add", "Next >>", and "Reset".

Figure 4-83 Software Delivery Center admin Add Package page

4. Complete the software package definition information. See “Software package definition information” on page 322 for details.
5. Click **Add**.
6. If the package is to be used by the pull process, then you must associate it with one or more groups as described in “Adding or deleting a software package or bundle for a specific group” on page 302.

Note: If the package you added is a Download(Open), LogicalDrive(Open), or DirectoryDrive type, no further action is required. If the package is a Download(Secure) or LogicalDrive(Secure) type, you must create a digital certificate after you have granted the appropriate access. See 4.7.5, “Creating a digital signature for a secure package” on page 336 for details.

Adding a new software bundle to the library

To create a new software bundle:

1. Select **Packages** → **Bundles** → **New**. The Add Bundle window shown in Figure 4-84 on page 315 opens.

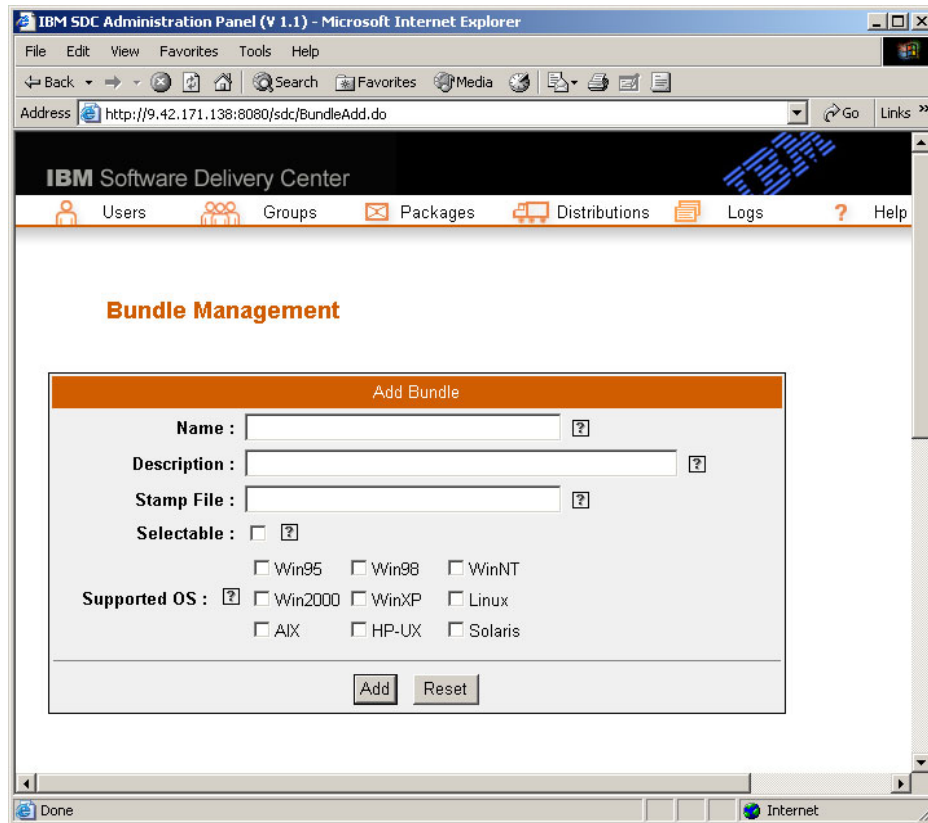


Figure 4-84 Software Delivery Center Add Bundle page

2. Complete the software bundle definition information. See “Software bundle definition information” on page 335 for details.
3. Click **Add**.
4. Click **Next** or **Packages**. The package list page shown in Figure 4-85 on page 316 opens.

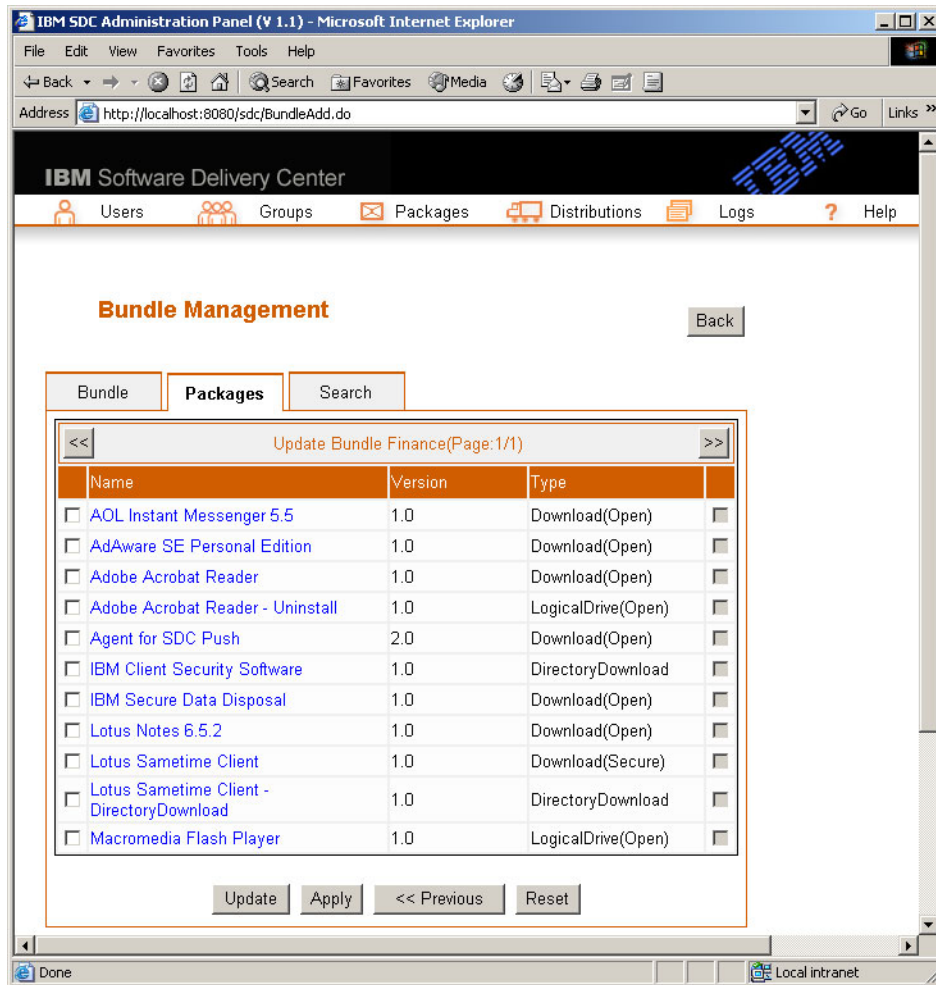


Figure 4-85 Software Delivery Center admin packages list window

5. Select the check box beside the software packages you want to add to the bundle.

Note: When adding packages to the bundle from multiple pages, you must select Apply to save your changes before selecting the << arrow or >> arrow.

- When you have selected the packages to be added to the bundle, click **Update**. You are then asked to select the order of installation for the packages in the bundle as shown in Figure 4-86.

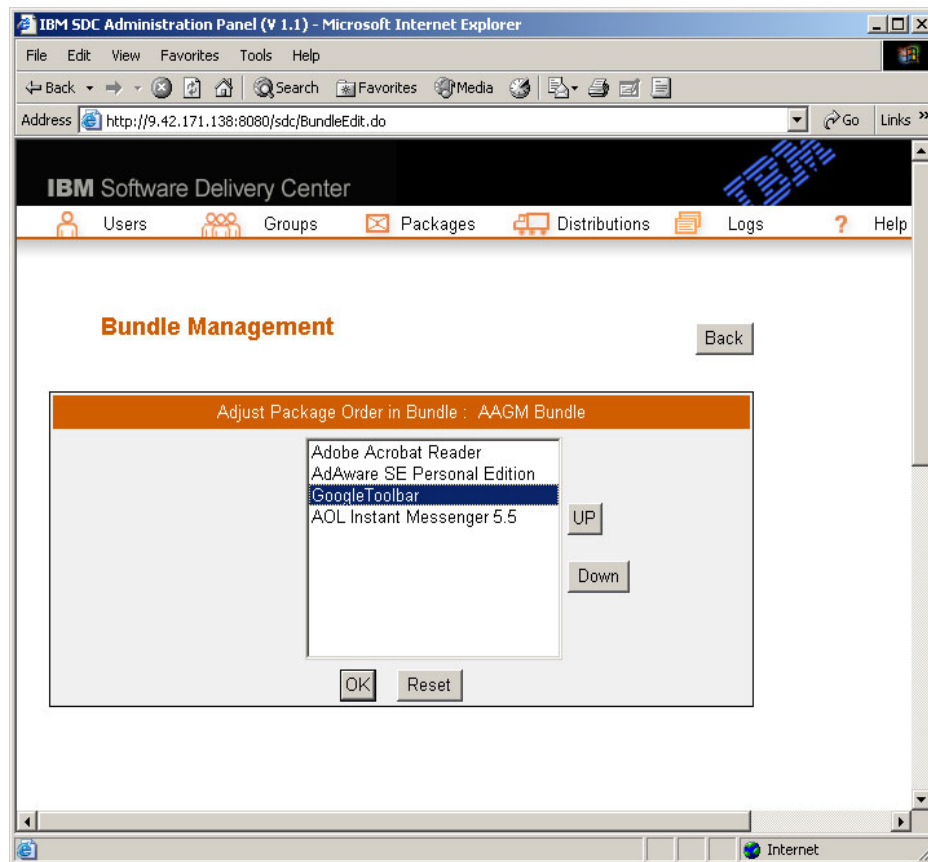


Figure 4-86 Software Delivery Center bundle order adjustment

- Select a software package name, and then click **UP** or **DOWN** to move the packages into the desired order.

Note: Packages that require a reboot should be the last package in the installation sequence.

- Click **OK** to add the bundle.
- If the bundle is to be used by the pull process, then it must be associated with one or more groups as described in “Adding or deleting a software package or bundle for a specific group” on page 302.

Deleting a software package or bundle from the library

To delete a software package or bundle:

1. Select **Packages** → **Packages** or **Packages** → **Bundles** depending on which you want to delete.
2. Click **Packages** or click **Bundles** to obtain the List Packages table or the List Bundles table (Figure 4-87).

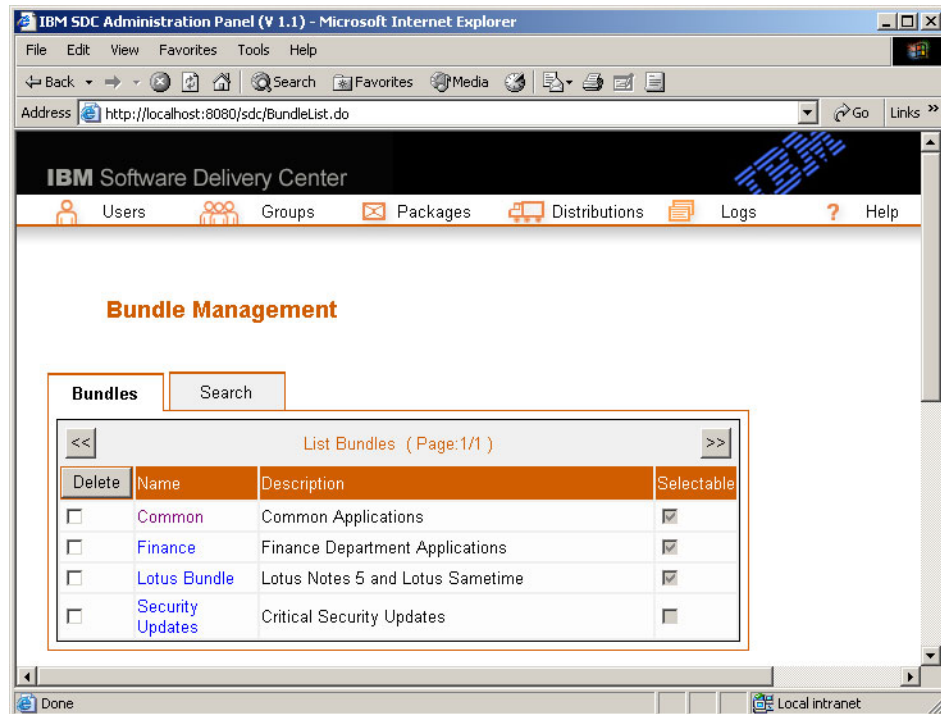


Figure 4-87 Software Delivery Center bundles list

3. Select the software package or bundle name you want to delete.

4. Click **Delete**. The window shown in Figure 4-88 opens.

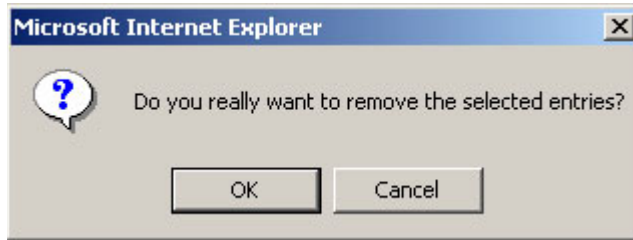


Figure 4-88 Software Delivery Center deletion confirmation window

5. Click **OK** to delete a software package or bundle name or click **Cancel** for no action.

Note: A software package can be deleted even if there are groups currently authorized to access the software package.

Searching the library for a software package or bundle

To search for a specific software package or bundle name:

1. Select **Packages** → **Packages** or **Packages** → **Bundles** depending on which you want to locate.
2. Click **Packages** or **All Bundles**. The List Packages table or List Bundles table (see Figure 4-85 on page 316) is displayed.

3. Click **Search**. The Search page shown in Figure 4-89 opens.

IBM SDC Administration Panel (V 1.1) - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media Print

Address http://localhost:8080/sdc/BundleList.do Go Links

IBM Software Delivery Center

Users Groups Packages Distributions Logs ? Help

Bundle Management

Bundles Search

Search

Name : [] ?

Supported OS : [Select OS] ?

Selectable : ☐ ?

Page Size : 20 ?

Search

Local intranet

Figure 4-89 Software Delivery Center bundle search

4. You can search by name, type or operating system. Do one or any combination of the following:
 - a. In the Name field, type the software package or bundle name.
- Note:** The software package or bundle name is case sensitive. Type the name exactly as the name is listed in the package or bundle list you are searching. If you are not sure of the spelling, you can use the percent symbol (%) as a wild card in place of one or more characters.
- b. In the Type field, select the file type.
 - c. In the OS field, select the operating system.
5. In the Page Size field, type the maximum number of entries per page to display.

6. Click **Search**. The selected software package or bundle name is displayed in the List Packages table or List Bundles table (see Figure 4-85 on page 316).

Updating software package information in the library

To update a software package:

1. Select **Packages** → **Packages** → **All Packages**. The List Packages table (see Figure 4-85 on page 316) is displayed.
2. Click the software package name. The Update Package page opens.
3. Make the changes to the software package definition information. See “Software package definition information” on page 322 for details.
4. Click **Update**.

Updating software bundle information in the library

To update a software bundle:

- ▶ Select **Packages** → **Bundles** → **All Bundles**. The List Bundles table (see Figure 4-87 on page 318) opens.
5. Click the software bundle name. The Update Bundle page opens.
6. Make the changes to the software bundle definition information. See “Software bundle definition information” on page 335 for details.
7. Click **Update**.
8. Click **Next** or **Packages** to obtain the list of available packages.
9. Select the software package name you want to add to the bundle.

Note: When adding machines from multiple pages, you must click **Apply** to save your changes before selecting the << arrow or >> arrow.

10. When all packages to be added to the bundle have been selected, click **Update**. You are prompted to select the order of installation for the packages in the bundle.
11. Select a software package name and click **UP** or **DOWN** to move the packages into the desired order.
12. Click **OK** to update the bundle.

Note: Packages that require a reboot should be the last packages in the installation sequence.

Software package definition information

The following sections cover the fields and descriptions required to create and edit software packages.

General

Figure 4-90 shows the General page for a sample Download(open) package type that installs Adobe Acrobat Reader.

The screenshot displays the IBM SDC Administration Panel (V 1.1) in a Microsoft Internet Explorer browser window. The address bar shows the URL: <http://9.42.171.138:8080/sdc/PackageEdit.do?packageKey=23>. The page title is "IBM Software Delivery Center". The navigation bar includes links for Users, Groups, Packages, Distributions, Logs, and Help. The main content area is titled "Package Management" and features a "Back" button. Below this, there are four tabs: General, Install, Target, and Platform. The "General" tab is selected, and within it, there is a sub-section titled "Update Package". This section contains several input fields with help icons (question marks):

- Name: Adobe Acrobat Reader
- Version: 1.0
- Family: Application
- Details: /sdc/packages/win32/Acrobat/adobe.txt
- Icon Path: /sdc/packages/win32/Acrobat/AcroRd32.c
- Max Install Time(Min.): 5
- Silent: ☐ ?
- Reboot: ☐ ?

At the bottom of the "Update Package" section, there are three buttons: "Update", "Next >>", and "Reset". The browser's status bar at the bottom shows the same URL and the "Internet" icon.

Figure 4-90 Package definition: General

The following fields are available:

- ▶ Name: This field provides the unique name of the software package.
- ▶ Version: This field contains the version number of the application.
- ▶ Family: This field has critical patch management information.

Note: This field is currently not used and is reserved for future use by Software Delivery Center.

- **Details:** This field shows the path to the details file that displays when the user clicks the Details button in the IBM Software Delivery Center catalog.

All warnings and relevant information about the software package should be put in this file.

Note: The path name to the details file must be relative to the document root of the server. The default document root is c:\ibmsdc\sdserver\sd. Your document root might be different depending on the options you chose during installation.

- **Icon Path:** This field shows the path to the software package icon in the Software Delivery Center catalog.

The icon must be a .gif or .jpg file. The use of an icon is optional.

Note: The path name to the file must be relative to the document root of the server. The default document root is c:\ibmsdc\sdserver\sd. Your document root might be different depending on the options you chose during installation.

- **Max Install Time (Min.):** This field shows the maximum amount of time in minutes the software package should take to install.

The software package installation will terminate if the installation does not complete within the specified time.

Note: Specify a large enough value to account for network congestion, slow processors, or both.

- **Silent:** This field indicates whether the software package will install unattended. Software Delivery Center uses this during a scheduled push operation as follows:
 - If the software package is silent, Software Delivery Center installs the software package, even if the user is not logged on to the client.
 - If the software package is not silent (requires user interaction) and the user is not logged on to the client, any scheduled push of the non-silent installation package will still be delivered, but installation is delayed until the user logs on to the client.

- Reboot: This field indicates that the software package requires a restart at the end of the installation.

Install

Figure 4-91 shows the Install page for the sample package.

Figure 4-91 Package definition: Install

This page has the following fields:

- Type: The package types are:
 - Download(Open)

This type of package consists of a single executable file that resides on the Software Delivery Center server and requires no administrator rights to run or install. When a Download(Open) package is pushed or pulled, the

complete package is downloaded to the client before the installation begins. Download(Open) is the default package type.

Note: When a pull process is used for a Download(Open) package type, the client agent is not involved with the installation process. The packages will install even if the client agent is disabled.

- Download(Secure)

This type of package consists of a single executable file that resides on the Software Delivery Center server and requires administrator rights to run or install. When a Download(Secure) package is pushed or pulled, the complete package is downloaded to the client before the installation begins.

This software package requires a digital signature. To create the digital signature, see 4.7.5, “Creating a digital signature for a secure package” on page 336.

- LogicalDrive(Open)

This type of package consists of one or more files that are stored on a logical drive (a shared network drive outside of the Software Delivery Center server) and requires no administrator rights to install. When a LogicalDrive(Open) package is pushed or pulled, the installation takes place directly from the logical drive without downloading the package first.

Note: The Software Delivery Center process does not do the actual mapping of the drive. The client must be mapped to the logical drive that contains the software package before the installation process is initiated.

When a pull process is used for a LogicalDrive(Open) package, the client agent is not involved in the installation process. The software packages install even if the client agent is disabled.

- LogicalDrive(Secure)

This type of package consists of one or more files that are stored on a logical drive (a shared network drive outside of the Software Delivery Center server) and requires administrator rights to install. When a LogicalDrive(Secure) package is pushed or pulled, the installation takes place directly from the logical drive without downloading the package first.

This software package requires a digital signature. To create the digital signature, see 4.7.5, “Creating a digital signature for a secure package” on page 336.

Note: The Software Delivery Center process does not do the actual mapping of the logical drive. The client must be mapped to the logical drive that contains the software package before the installation process is initiated.

– DirectoryDownload

This type of package consists of an unpackaged application or a set of data files. These files must reside on the Software Delivery Center server in the document root. When this type of package is created, Software Delivery Center creates a compressed package that contains the complete set of files in the original folder structure. During a push or pull operation, the compressed package is downloaded to the client. The client application decompresses it and restores the files and folders to their original condition as follows:

- If an installation command is defined in the Parameters field, an installation process takes place after the package is decompressed and the directory that was delivered is removed after the installation is completed.
- If a parameter is not defined, no action is taken after the package is decompressed. This type of package is useful for distributing data files and templates.

Note: If you make changes to the content of the DirectoryDownload package, you must delete the _IGS.SDC zipped file located in the source directory as specified in the Remote File field.

► Remote File: The definition of this field depends on the type of package you are defining:

- When it is used with a DirectoryDownload package, this is the relative path to the root folder of the application or data files stored on the Software Delivery Center server. Relative paths are relative to the document root. For example, suppose the full path to the root folder of a set of data files located on the Software Delivery Center server is:

`c:\IBMSDC\SDCServer\sdc\packages\FILES\TEMPLATES`

The relative path is:

`/sdc/packages/FILES/TEMPLATES`

It is also important to understand that the last folder in the relative path is the starting point of the directory structure that will be extracted to the

client. For example, suppose you specify the TEMPLATES folder as:
`\sdc\packages\FILES\TEMPLATES`

Then, all files in the TEMPLATES folder and all of its subfolders are extracted to the client.

- When it is used in conjunction with a Download(Open) or Download(Secure) package, this is the relative path to the software package executable file. This path must be relative to the document root of the Software Delivery Center server. For example, suppose the full path is:

`c:\IBMSDC\SDCServer\sdc\packages\XP\My_Package\SETUP.EXE`

Its relative path then is:

`/sdc/packages/XP/My_Package/SETUP.EXE`

Note: Path names are case sensitive. Make sure the path name you use matches the actual path name on your Software Delivery Center server exactly.

- Supported extensions for the remote files are:
 - .CMD
 - .EXE
 - .MSI
 - .RPM
 - .TAR
 - .VBS
 - Null (no extension)
- This field is not used for LogicalDrive(Open) and LogicalDrive(Secure) packages.
- Install Command: This field contains the command used to start the installation of the software package.

This field is required for LogicalDrive(Open) and LogicalDrive(Secure) packages.

This field is not used for Download(Open), Download(Secure), and DirectoryDownload packages.
- Parameters: This field contains the parameters that are passed to the software package executable.

They are required for the DirectoryDownload package, if an installation process is required.

Examples of parameters are:

 - /s for a silent installation of InstallShield and Wise InstallSystem

- /qn for a silent installation of Microsoft Software Installer packages (.msi file extension)

The actual parameters depend on the tool that was used to create the package. Refer to the documentation provided with the packaging tool for more information.

- **Windows RegKey:** This field contains the appropriate string that matches the program name displayed in the Add/Remove Programs window.

This field is used by Software Delivery Center to determine if a particular software package is already installed on the client. Software Delivery Center queries the Windows registry to determine what programs have been installed and also listed in the Add/Remove Programs window.

To view the string in Windows 2000, select **Start** → **Settings** → **Control Panel** and then click **Add/Remove Programs**. You must use the program name exactly as shown in the Add/Remove Programs window.

In some cases, when you look at the Add/Remove Programs window, you may not be able to determine whether there is an extra space at the end of the string or between words.

You can also cut and paste the required string from the Windows Registry into the Windows RegKey field. The following method ensures that the value you place in the Windows RegKey field matches the value in the Add/Remove Programs window:

- Install the application on a test computer or go to a computer where the application is already installed.
- From the Windows desktop, select **Start** → **Run**. The Run window opens. In the Open field, type `regedit`.

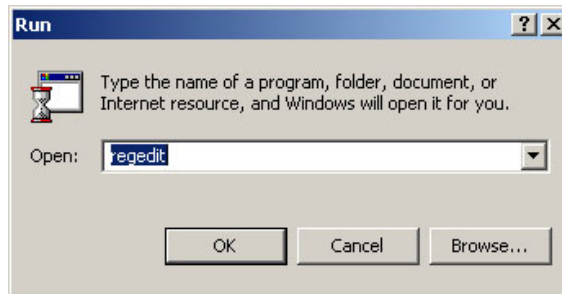


Figure 4-92 Software Delivery Center Run Regedit

- Click **OK**. The Registry Editor window opens as shown in Figure 4-93 on page 329.

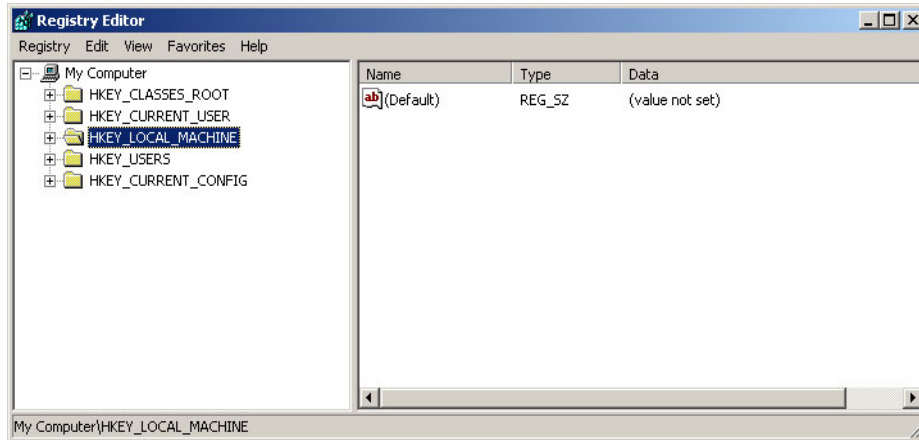


Figure 4-93 IBM Software Delivery Center regedit window

- d. In the Registry Editor window, navigate to the HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/Uninstall folder as shown in Figure 4-94.

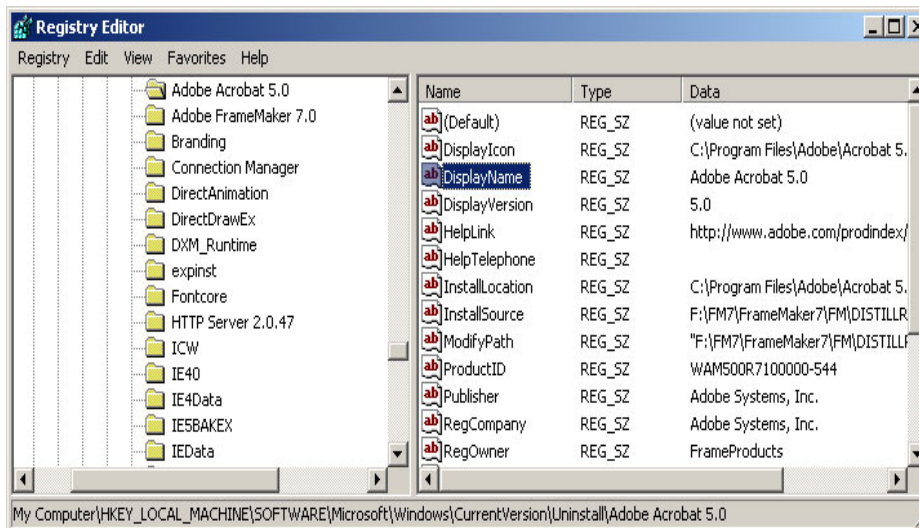


Figure 4-94 Navigating Windows RegKey

- e. In the left pane, click the appropriate application name.
 f. In the right pane, double-click **DisplayName**. The Edit String window opens.

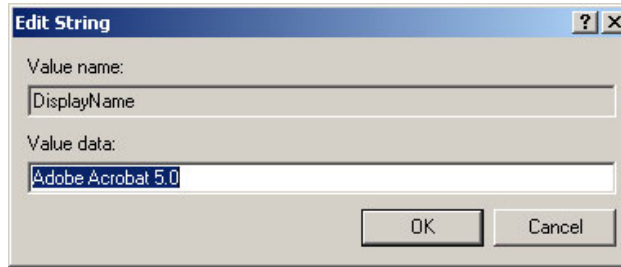


Figure 4-95 Edit String window

- g. The string highlighted in the Value field is the exact string you need to use in the Windows RegKey field.
- h. Cut and paste this value into the Windows RegKey field.

Note: You can specify either the Stamp File field or Windows RegKey field. Use the Windows RegKey field unless this software package does not register itself in the Add/Remove Programs window.

- **Stamp File:** The stamp file indicates that the software package installed successfully on the client.

The Software Delivery Center process checks for the existence of the stamp file after the completion of the software package installation. The stamp file is used as a means of obtaining a return code from the software package. The software package itself must create the stamp file after the software package has successfully installed. The software package cannot create the stamp file if the application does not successfully install.

The software package is responsible for writing the stamp file because there is no agreed upon standard among software vendors that indicates a particular installation was successful. Often, the installation program will return with a return code of zero for a successful installation, but this is not always the case. Therefore, each individual package must determine if the software installed successfully, and if so, create the software package stamp file. For this field, specify the full path for the stamp file for which to check.

Note: You can specify either the Stamp File field or Windows RegKey field. Use the Windows RegKey field unless the software package does not register in the Add/Remove Programs window.

- **Stamp Mode:** This field indicates the stamp file mode.

The stamp file mode must be set to one of the following types:

- Auto

The Software Delivery Center client applet automatically creates the stamp file after the installation program completes. Auto stamp file mode is provided for development and testing of software packages.

- Package

The software package itself creates the stamp file after the software package has successfully installed.

- Dated

Dated time stamp mode is used to instruct the Software Delivery Center process to check the time stamp of the stamp file in addition to the existence of the file.

- ▶ Stamp File Date: This field contains the time stamp (date and time of the target stamp file).

When you select **Dated** for the stamp mode, the software package passes the stamp file check only if the last modified date of the stamp file matches the date specified. The date is specified in Java-epoch milliseconds, the number of milliseconds since the Java epoch, defined as midnight, January 1, 1970 GMT. These are the number of milliseconds that have elapsed since January 1, 1970 00:00.

To generate the stamp file time stamp, run the following command from a Windows command prompt (where *filename* is the stamp file name):

```
java -jar printstamp.jar filename
```

Note: The `printstamp.jar` file is provided as part of the Software Delivery Center server software in the `c:\ibmsdc\sdserver\sd\apps\printstamp.jar` folder (where `c:\ibmsdc\sdserver\sd` is the default document root). Your document root might be different depending on the options you choose during installation.

Target

Figure 4-96 shows the Target page for the sample package.

The screenshot displays the IBM SDC Administration Panel (V 1.1) in a Microsoft Internet Explorer browser window. The address bar shows the URL: `http://9.42.171.138:8080/sdc/PackageEdit.do?packageKey=23`. The page title is "IBM Software Delivery Center". The navigation bar includes links for Users, Groups, Packages, Distributions, Logs, and Help. The main content area is titled "Package Management" and features a "Back" button. Below this, there are four tabs: General, Install, Target (selected), and Platform. The "Target" tab is active, showing a form titled "Update Package". The form contains the following fields:

Update Package	
Temp. Space Required(MB) :	<input type="text" value="20"/>
Target Space Required(MB) :	<input type="text" value="18"/>
Target Directory :	<input type="text" value="c:\\"/>
Prerequisite Program :	<input type="text"/>
Preinstall Program :	<input type="text"/>
Postinstall Program :	<input type="text"/>

At the bottom of the form are four buttons: "Update", "<< Previous", "Next >>", and "Reset".

Figure 4-96 Package definition: Target

This page has the following fields:

- Temp. Space Required (MB): This field contains the amount of temporary disk space (in megabytes) required to install the software package.

This is usually the temporary space required for unpacking a software package prior to installation. The drive that is checked is the same drive that the Java Runtime Environment on the client uses for temporary space and is usually specified by the *tmp* or *temp* environment variable.

Note: If the drive letter used by the Java runtime environment for temporary space is the same drive letter specified in the Target Directory field, then the values in the Temp. Space Required (MB) field and Target Space Required (MB) field are added together before the free space check is performed; otherwise, two separate free space checks are performed.

- ▶ **Target Space Required (MB):** This field contains the amount of disk space (in megabytes) required to install the software package.

The letter of the drive or logical volume on which to perform the free space check is specified by the entry in the Target Directory field.

- ▶ **Target Directory:** The definition of this field depends on the type of package you are defining:
 - When used with a DirectoryDownload package, this is the path to the folder in which the files in the package will be extracted. An example is:
c:\Documents and Settings\All Users
 - When used with Download(Open), Download(Secure), LogicalDrive(Open), or LogicalDrive(Secure) packages, this is the letter of the drive on which the software package will be installed. An example is:
c:\

This folder will be checked for the required amount of free disk space prior to the installation of the software package.

- ▶ **Prerequisite Program:** This field displays the path name of the prerequisite program that is run prior to installing the software package:
 - If this program returns with a return code of zero, Software Delivery Center assumes that all of the prerequisites for this software package have been met.
 - A return code of any value other than zero indicates to Software Delivery Center that the prerequisites have not been met and the software package will not install.
- ▶ **Preinstall Program:** This field contains the program or script that runs before the installation of the software package.

Note: If the Preinstall Program specified returns a return code of any value other than zero, the installation for the package will continue but subsequent packages in a bundle or multiple package selection will not be installed.

- **Postinstall Program:** This field contains the program or script that runs after the installation of the software package. If the software package is run from a software bundle, a return code of any value other than zero causes subsequent software packages in the software bundle not to run.

Note: If the Postinstall Program specified returns a return code with any value other than zero, then subsequent packages in a bundle or multiple section will not be installed.

Platform tab

Figure 4-97 shows the Platform page for the sample package.

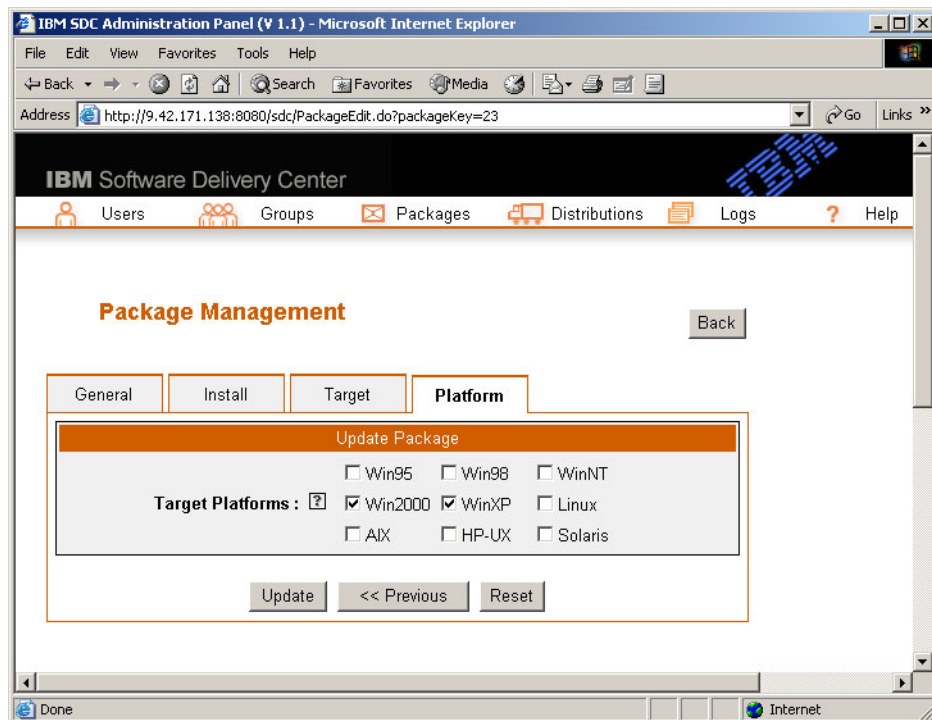


Figure 4-97 Package definition: Platform

This page has the following fields:

- **Target Platforms:** This field contains the operating-system platforms on which this software package can be installed. Software Delivery Center checks for the presence of the specified operating systems to determine if the software package should be displayed in the catalog. One or more operating systems can be specified by making the appropriate selection.

Software bundle definition information

Figure 4-98 shows the Bundle page.

IBM SDC Administration Panel (V 1.1) - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media Print

Address http://9.42.171.138:8080/sdc/BundleEdit.do?bundle.bundleKey=1 Go Links

IBM Software Delivery Center

Users Groups Packages Distributions Logs Help

Bundle Management Back

Bundle Packages Search

Update Bundle

Name : AAGM Bundle ?

Description : Bundle of AOL, AdAware, Google Toolbar, and Macromed ?

Stamp File : c:\progra~1\sdci\stampfiles\packageof4.tx ?

Selectable : ☐ ?

Win95 Win98 WinNT

Supported OS : ? ☒ Win2000 ☒ WinXP ☐ Linux

☐ AIX ☐ HP-UX ☐ Solaris

Update Apply Next >> Reset

http://9.42.171.138:8080/sdc/BundleEdit.do?bundle.bundleKey=1# Internet

Figure 4-98 Bundle definition information

The following are the fields and descriptions required to create and edit software bundles:

- ▶ Name: This field contains the unique name of the software bundle.
- ▶ Description: This field displays the description of the software bundle.
- ▶ Stamp File: The existence of the stamp file indicates that the software bundle installed successfully on the client. If all of the packages specified in the bundle install successfully then the stamp file specified will be created by

Software Delivery Center. For this field, specify the full path of the stamp file for which to check.

- ▶ **Selectable:** This file contains the indication that the software bundle can be selected.
- ▶ **Supported OS:** This file indicates the operating systems in which a software bundle can be installed.

Software Delivery Center checks for the presence of the specified operating systems to determine if the software package should be displayed in the catalog. One or more operating systems can be specified by selecting the appropriate check box.

4.7.5 Creating a digital signature for a secure package

You can create a digital certificate for Download(Secure) and LogicalDrive(Secure) packages using the following procedure:

1. Open a command prompt window.
2. Change to the \signatures folder located under the document root of the server.
3. Run the following command (where *executable* is the relative path name to the software package executable):

```
java -jar ..\apps\sdcsigner.jar executable
```

An example is:

```
java -jar ..\apps\sdcsigner.jar ..\packages\win32\winzip90\WinZip90M.exe
```

Note: The environment variable path must include the path name of the JRE bin directory for the above command to work. If necessary, you can specify the full path name of the java executable as shown in Example 4-5.

Example 4-5 Using full path name for java.exe

```
C:\IBMSDC\Java142\jre\bin\java.exe -jar ..\apps\sdcsigner.jar  
.. \packages\win32\winzip90\WinZip90M.exe
```

4.7.6 Exporting and importing software packages and bundles

You use the Export/Import function to do the following:

- ▶ Create a portable catalog containing software packages and bundles that can be distributed on CD or a network drive.

- Export an XML file from a source Software Delivery Center server that can be imported on a target Software Delivery Center server to update the library database.

For a more detailed description of the Export/Import function, see 4.5.4, “Creating a portable catalog” on page 285 and 4.5.6, “Importing files from another server” on page 286.

Adding a new export group

To create a new export group:

1. Select **Packages** → **Export/Import** → **New**. The Add Export page shown in Figure 4-99 opens.

IBM SDC Administration Panel (V 1.1) - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media Print Copy Paste

Address http://localhost:8080/sdc/ExportEdit.do Go Links

IBM Software Delivery Center

Users Groups Packages Distributions Logs ? Help

Export Management

Export Packages Bundles Search

Add Export

Name : Marketing ?

Description : Marketing Applications ?

OK Apply Next >> Reset

Done Local intranet

Figure 4-99 Software Delivery Center Add Export page

2. In the Name field, type the export group name.
3. In the Description field, type the associated export group name description.

Note: The Name field has a limitation of 64 text characters. The Description field is alphanumeric with a limitation of 128 characters.

4. Click **OK**. The Add Export message shown in Figure 4-100 is displayed.

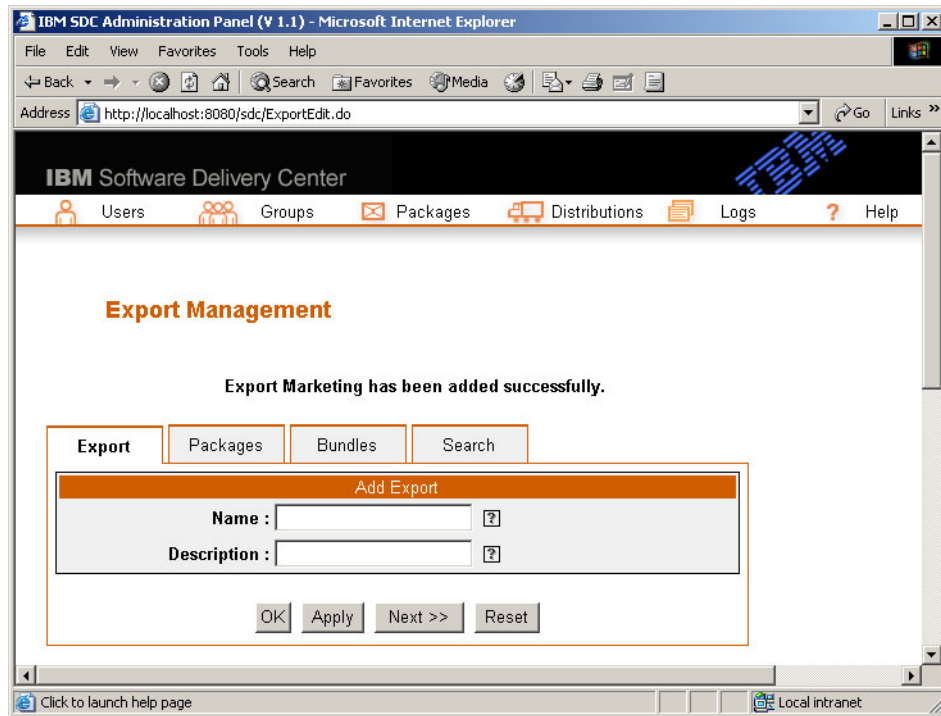


Figure 4-100 Software Delivery Center export message

Deleting an export group

To delete an export group:

1. Click **Packages** → **Export/Import** → **All Exports**. The List Exports table shown in Figure 4-101 on page 339 is displayed.

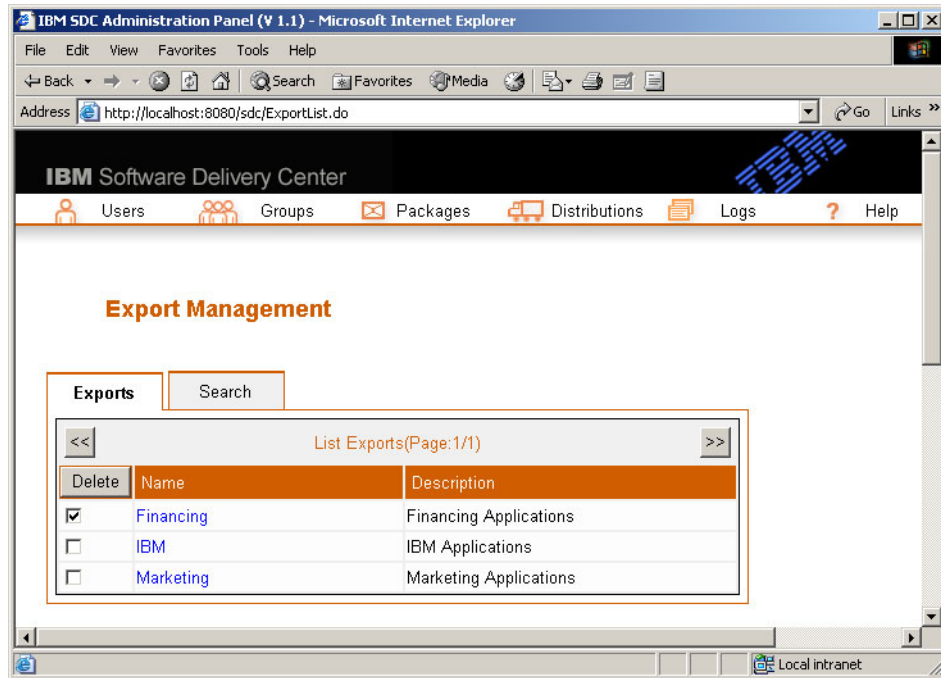


Figure 4-101 Software Delivery Center export list

2. Select the export group name you want to delete.
3. Click **Delete**. The window shown in Figure 4-102 opens.

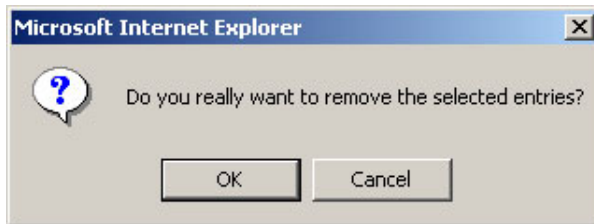


Figure 4-102 Software Delivery Center deletion confirmation window

4. Click **OK** to delete an export group or click **Cancel** for no action.

Searching for an export group

To search for a specific export group name:

1. Select **Packages** → **Export/Import** → **All Exports**. The List Exports table (see Figure 4-101) is displayed.

2. Click **Search**. The Search page shown in Figure 4-103 opens.

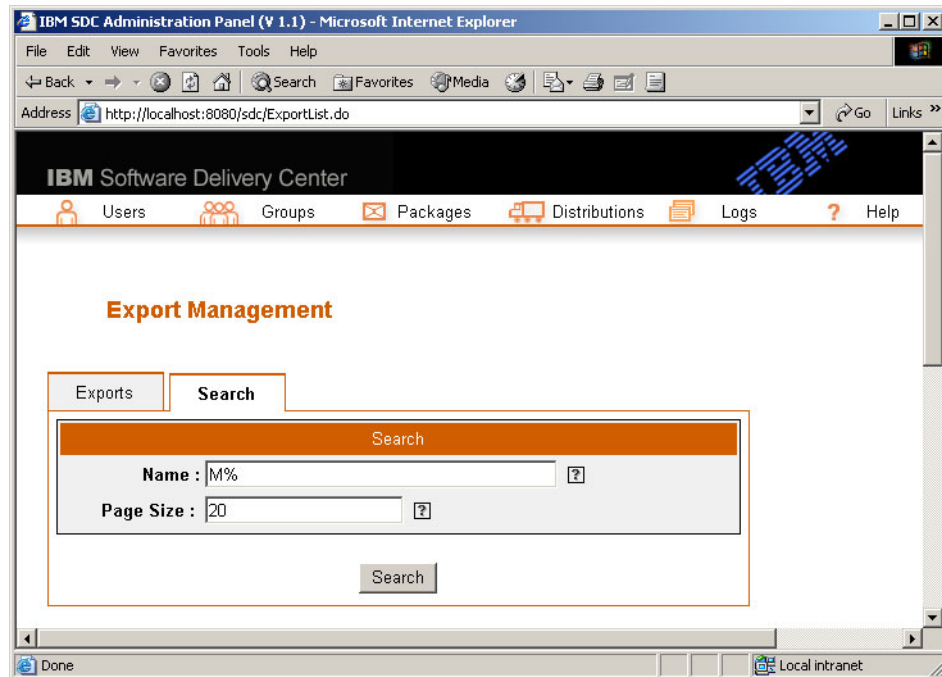


Figure 4-103 Software Delivery Center admin export search

3. In the Name field, type the group name.

Note: The Name field is case sensitive. Type the name exactly as the name is listed in the user list you are searching. The field can be searched with a wildcard (for example, A% or a%).

4. In the Page Size field, type the maximum number of entries per page to display.

5. Click **Search**. The selected export group name and description is displayed in the List Exports table shown in Figure 4-104.

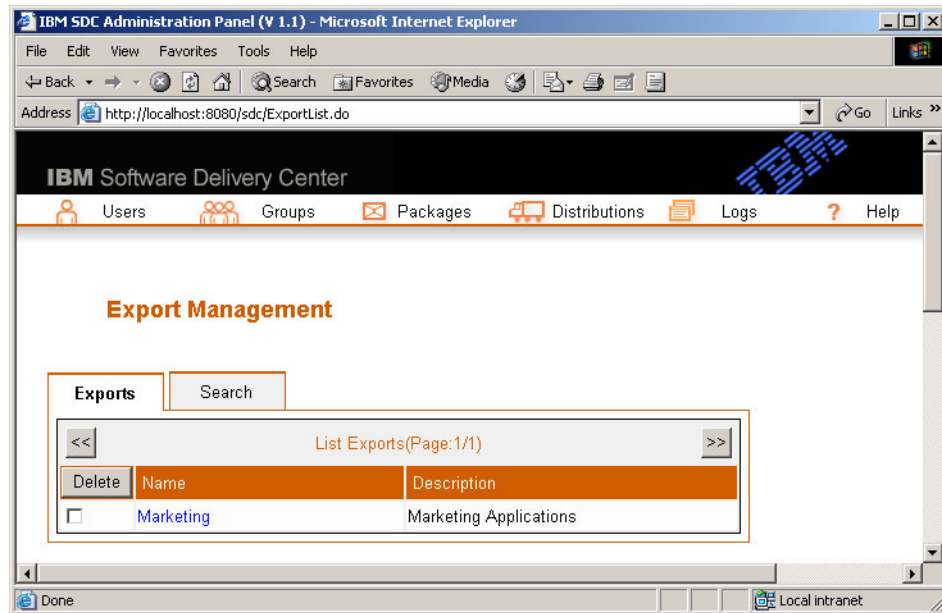


Figure 4-104 Software Delivery Center admin export search results

Changing the export description

To change the export description:

1. Select **Packages** → **Export/Import** → **All Exports**. The List Exports table (see Figure 4-101 on page 339) is displayed.
2. Click the export group name. The Edit Export page shown in Figure 4-105 on page 342 opens.

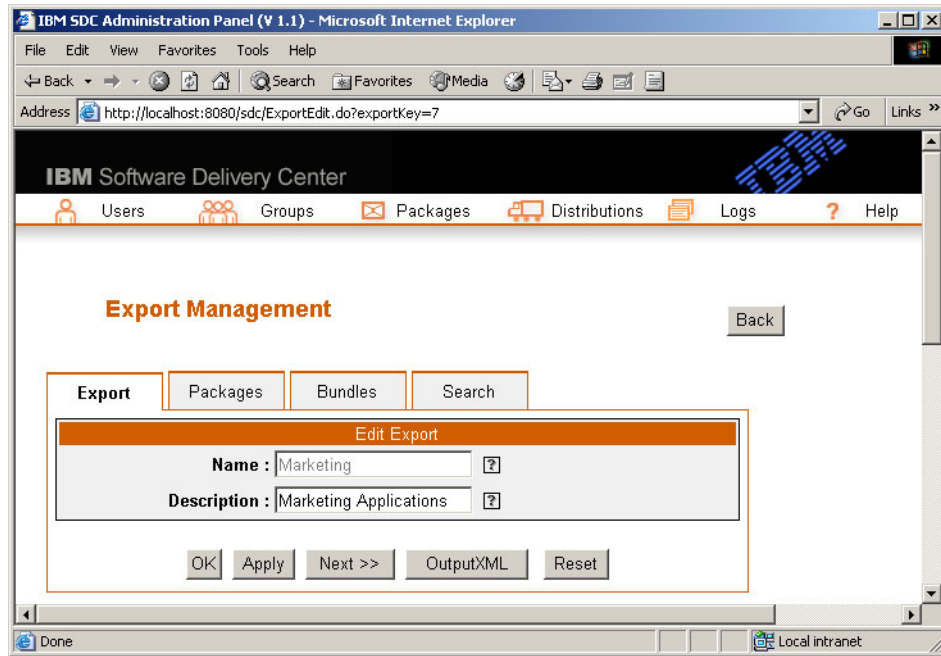


Figure 4-105 Software Delivery Center export editing

3. Make changes to the export description.
4. Click **OK** to update the information. The List Exports table shown in Figure 4-106 on page 343 opens with the updated description.

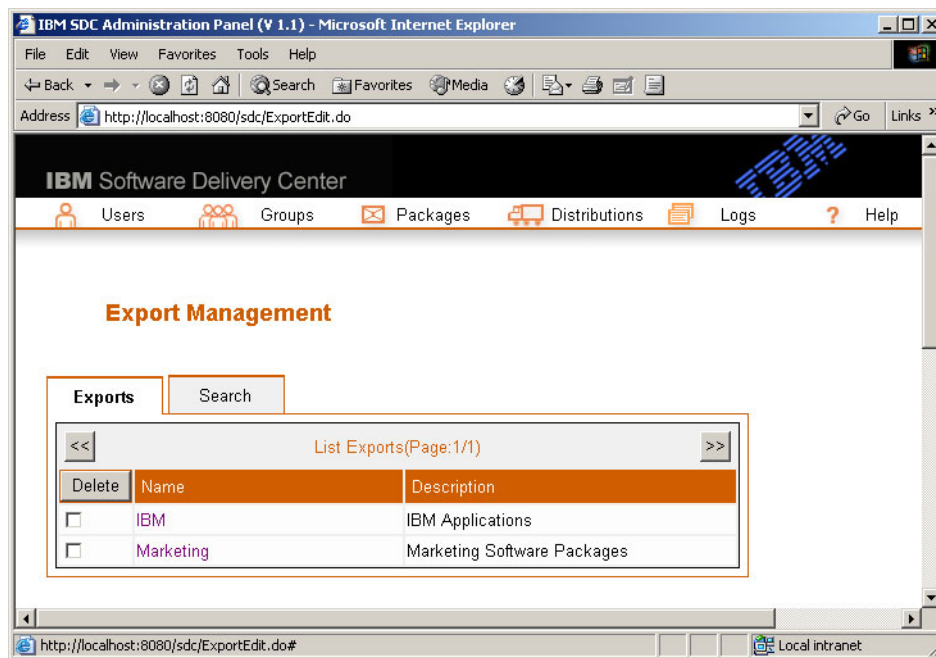


Figure 4-106 Software Delivery Center export edit results

Adding or deleting a software package or bundle in a specific export group

To add or delete a software package or bundle in a specific export group:

1. Select **Packages** → **Export/Import** → **All Exports**. The List Exports table (see Figure 4-101 on page 339) is displayed.
2. Click the export group name. The Edit Export page shown in Figure 4-105 on page 342 is displayed.

3. Click **Packages** or click **Bundles**. The Package List (Figure 4-107) or Bundle List table for a specific export group is displayed.

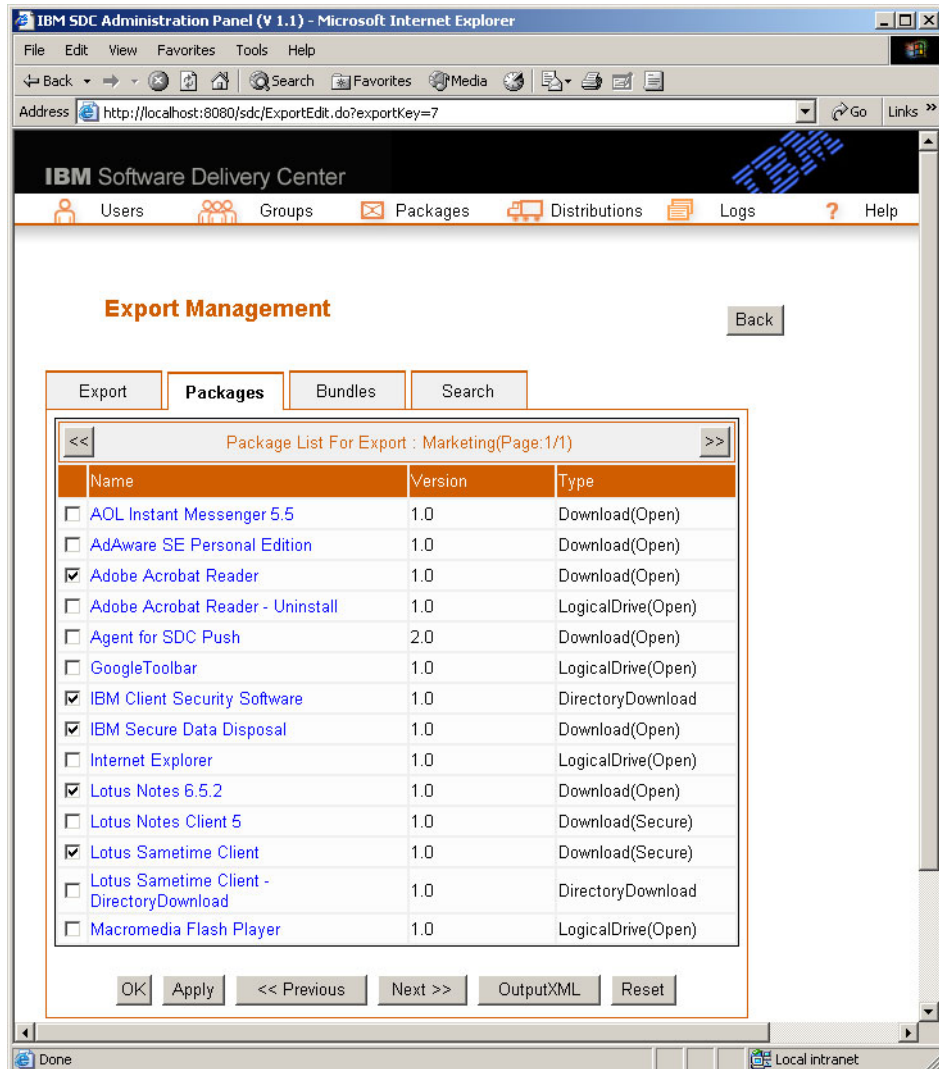


Figure 4-107 Software Delivery Center export packages list

4. Select or clear the check box for the software package or bundle name you want to include or delete.

Note: When adding packages or bundles from multiple pages, you must click **Apply** to save your changes before selecting the << arrow or >> arrow to move between pages.

5. Click **OK**. The List Exports table shown in Figure 4-101 on page 339 is displayed.

Creating an XML output file for an export group

This procedure creates XML output from the packages and bundles contained in the export group. It can be imported to another Software Delivery Center server to provide additional entries in a Software Delivery Center library.

To create XML output from packages and bundles in a specific group:

1. Select **Packages** → **Export/Import** → **New**. The Add Export page shown in Figure 4-108 opens.

IBM SDC Administration Panel (V 1.1) - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media Print Mail

Address http://localhost:8080/sdc/ExportEdit.do Go Links

IBM Software Delivery Center

Users Groups Packages Distributions Logs ? Help

Export Management

Export Packages Bundles Search

Add Export

Name : Marketing ?

Description : Marketing Applications ?

OK Apply Next >> Reset

Done Local intranet

Figure 4-108 Software Delivery Center admin add export

2. In the Name field, type the export group name.

3. In the Description field, type the associated export group name description.

Note: The Name field has a text limitation of 64 characters. Description field is alphanumeric with a limitation of 128 characters.

4. Click **Apply**.
5. Click **Packages**. The Package List for Export page shown in Figure 4-107 on page 344 opens.
6. Select the packages you want to add.
7. Click **Apply**.
8. Click **Bundles**. The Bundle List for Export page shown in Figure 4-109 opens.

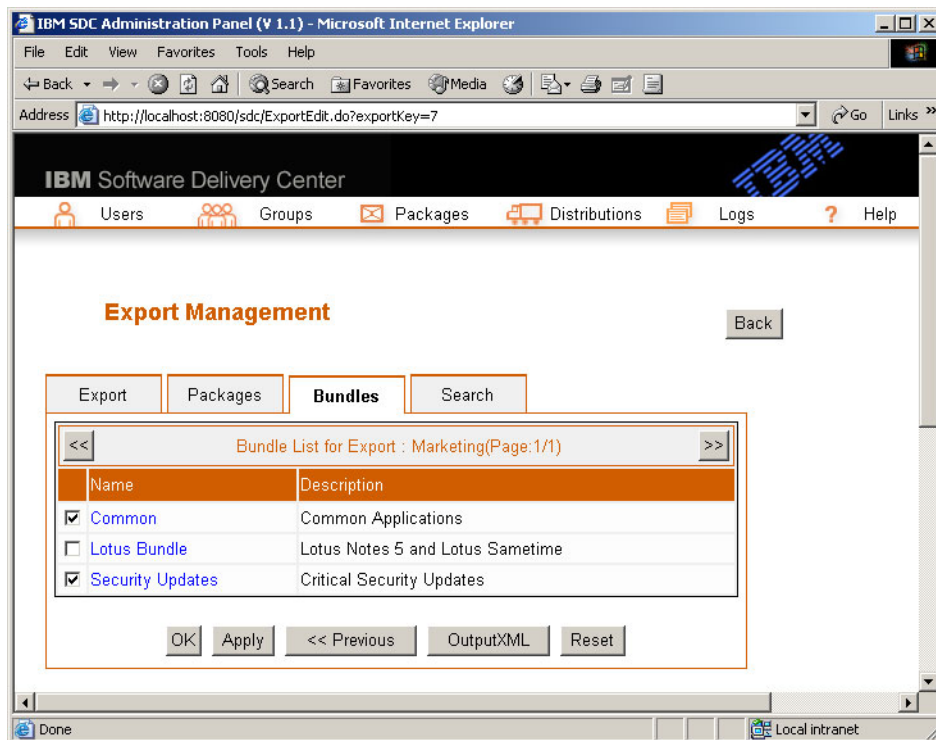


Figure 4-109 Software Delivery Center bundle list

9. Select the check box beside the bundles you want to add.
10. Click **Apply**.

11. Click **Output XML**. The XML output file shown in Figure 4-110 is displayed.

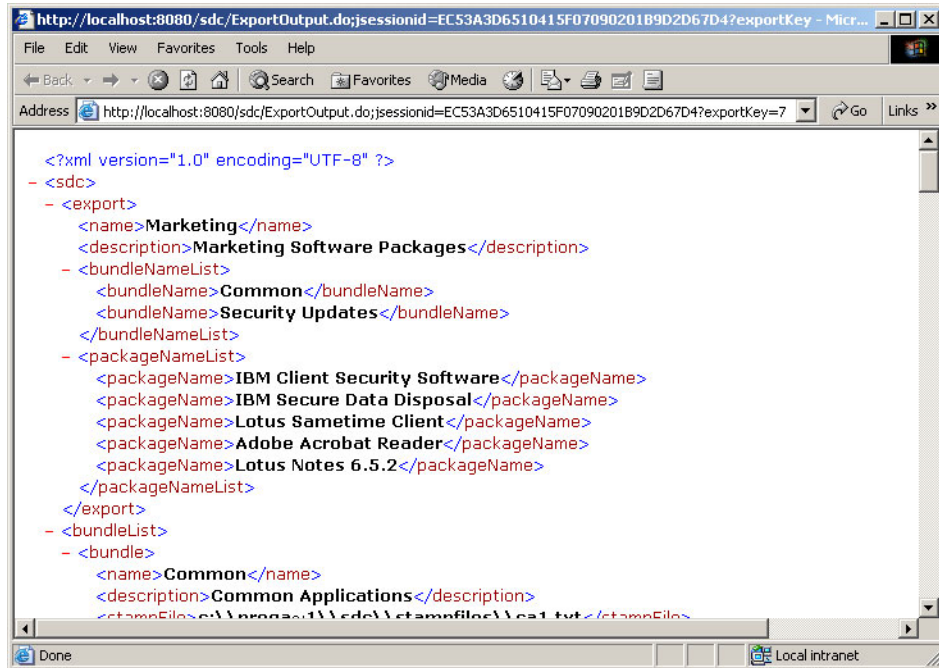


Figure 4-110 Software Delivery Center admin export output

12. Select **File** → **Save As**. The Save As window shown in Figure 4-111 opens.

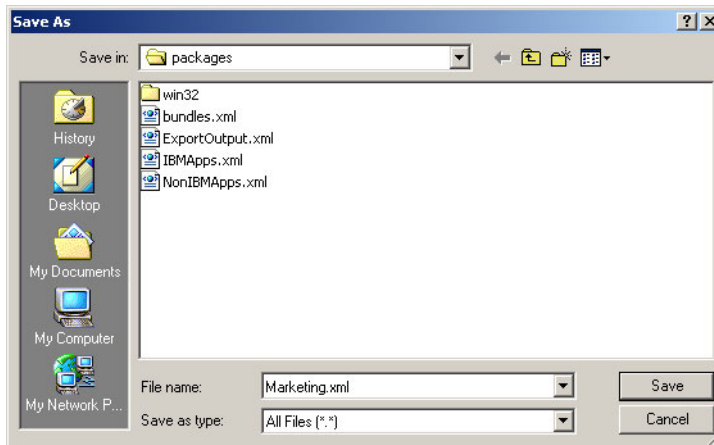


Figure 4-111 Software Delivery Center Save As window

13. Replace the text in the File name section with the XML output file name.
14. From the Save In menu, select the appropriate media, server, drive for storing the XML file.
15. Click **Save**.
16. Close the page with the XML output.

Importing Software Delivery Center files from another server

The following procedure assumes you have already created the XML output file from the source Software Delivery Center server. If you have not, export the XML file now before you start this procedure. See “Creating an XML output file for an export group” on page 345.

Throughout this procedure, the term *source server* is used to identify the Software Delivery Center server that currently contains the XML source file and software packages to be exported. The term *target server* is used to identify the Software Delivery Center server to which the files will be imported.

1. Copy the XML output file to the target server using one of the following methods:
 - From the target server map to the source server. Then, copy the XML output file from the source server to the target server.
 - At the source server, copy the XML output file to a portable medium. Then, bring the portable medium to the target server and copy the XML source file anywhere on the target server.
2. At the target server, open the Software Delivery Center administrator's console and do the following:
 - a. Select **Packages** → **Export/Import** → **Import XML**. The Select the XML File for Import page shown in Figure 4-112 on page 349 opens.

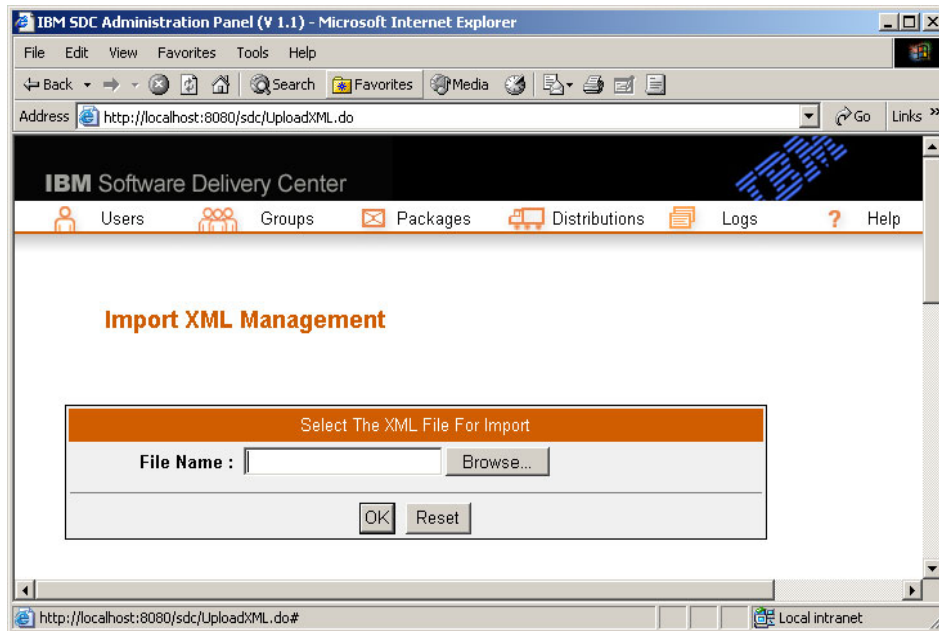


Figure 4-112 Software Delivery Center Import XML Management page

- b. In the File Name field, type in the XML source file name or click **Browse** to select the XML output file.
- c. Click **OK**. The Import Package window shown in Figure 4-113 on page 350 opens.

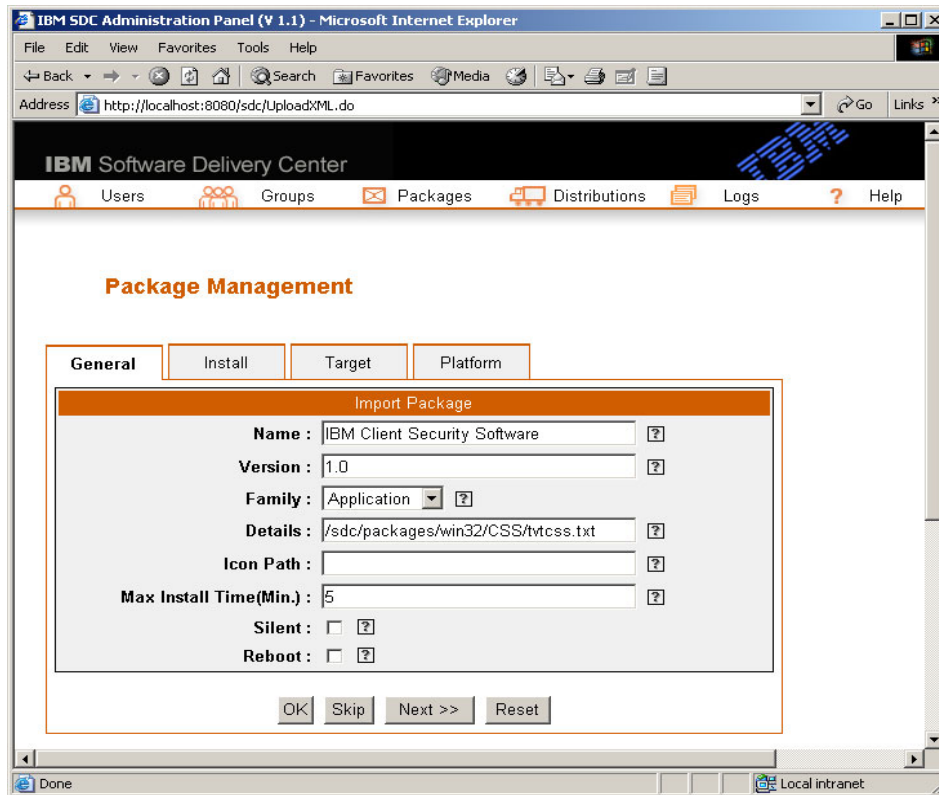


Figure 4-113 Software Delivery Center General page

- d. Click **OK** to accept each package. Click **Skip** to bypass any package you do not want to import. After all packages and bundles contained in the output XML have been added, you are prompted to add the export definition used to create the export XML output file.
 - e. Click **OK** to finish importing the XML output file.
3. If the physical package files, detail files, and icon files are on a logical drive (a shared network drive outside of the source server), no further action is required.
4. If the physical package files, details files, and icon files are stored on the source server, copy the files to the target server using one of the following methods:
 - From the target server, map to the source server. Then, copy the appropriate package files, detail files, icon files, and signature files to the target server.

- At the source server, copy the appropriate package files, detail files, icon and signature files to portable media (such as CD or DVD). Then, bring the portable media to the target server and copy the files on the target server.

Note: The folder structure for the package files, detail files, icon and signature files must be the same on the target server as the source server. Otherwise, you will have to update the package information for each imported package at the target server to specify the changed paths. The affected fields are the Details field and Icon Path field on the General page and the Remote file on the Install page.

4.7.7 Exporting a portable catalog

A portable catalog can reside on a CD, DVD, network drive, or other portable media.

Note: When exporting a portable catalog with LogicalDrive(Open) or LogicalDrive(Secure) package types, the IBM Software Delivery Center server must be mapped to the logical drive before the export operation is initiated.

This is useful for distributing software to computers that do not have network access or access to the Software Delivery Center server.

To export the portable catalog:

1. Click **Packages** → **Export/Import** → **CD Export**. The Java-based Import/Export Utility window shown in Figure 4-114 on page 352 opens.

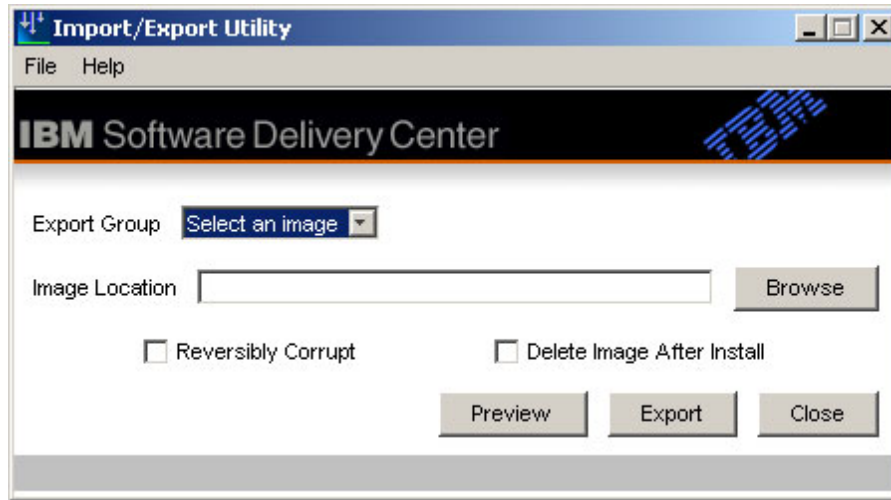


Figure 4-114 Software Delivery Center CD Export window

2. In the Export Group field, select an export name.
3. In the Image Location field, type in the file name or use **Browse** to select the folder where the portable catalog files and folders can be stored.

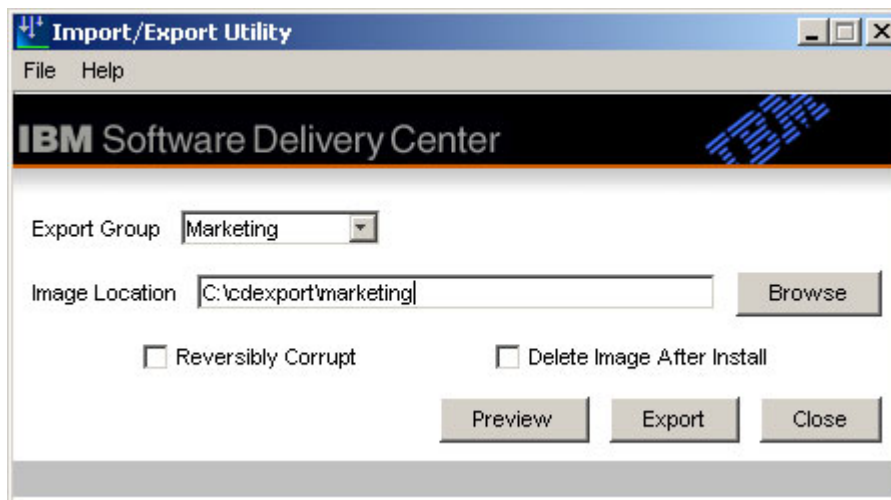


Figure 4-115 Software Delivery Center CD Export window

Note: The folder must be new or empty.

4. If the software packages must be installed only from the Software Delivery Center Client catalog, select **Reversibly Corrupt** (optional). These package executables must be installed through the Software Delivery Center client and cannot be installed outside of the client catalog.
5. If this is a one-time run of the client catalog, select **Delete Image After Install** (optional). All files and directories in the Image Location field are deleted after the client catalog is exited.
6. Click **Preview**. The space per package, a list of packages, the total space required, and the names of any missing files are displayed as shown in Figure 4-116.

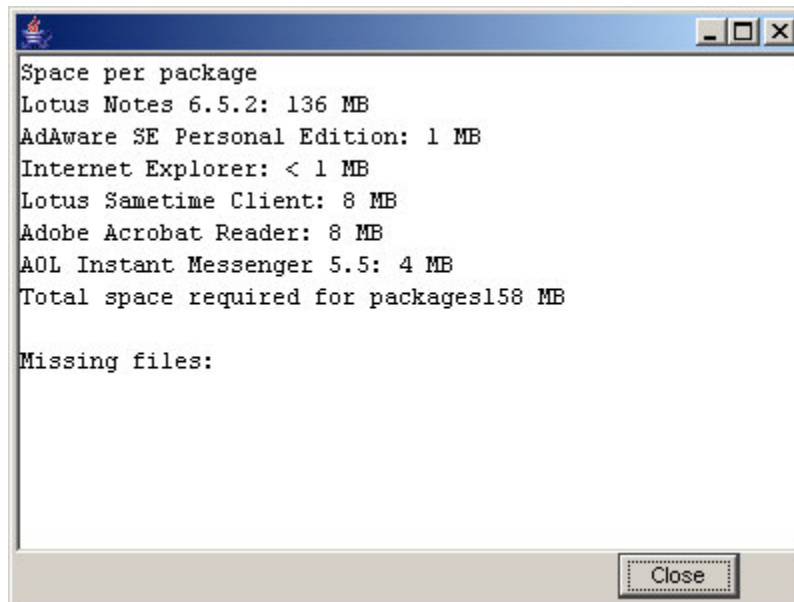


Figure 4-116 Software Delivery Center admin CD export information

7. Click **Export**. When the export process is complete, **Done** is displayed at the bottom of the window as shown in Figure 4-117.

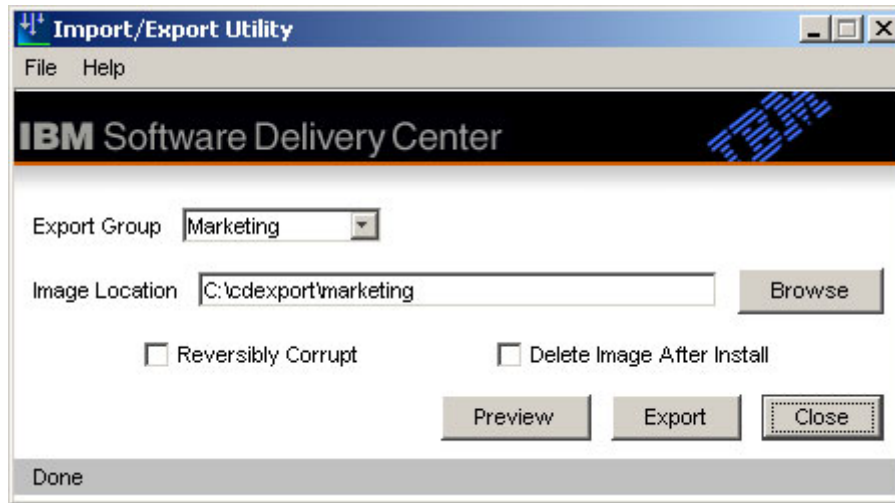


Figure 4-117 Software Delivery Center CD Export window

8. If you want to put the portable catalog on CD or DVD, use the CD/DVD recording software of your choice to copy the portable catalog files and folders to the CD or DVD. If you want to put the portable catalog on a network drive or other media, copy the files to the appropriate drive or media.

Note: Make sure you maintain the folder structure and include all of the files and folders.

4.7.8 Managing distributions

To schedule a software package for a push distribution, you must first create a distribution group and then add a distribution list of target machines. The Distribution Management screen shows a list of distribution groups (Distribution List table).

Adding a distribution group

To add a distribution group:

1. Select **Distributions** → **Distributions** → **New**. The Add Distribution page shown in Figure 4-118 on page 355 opens.

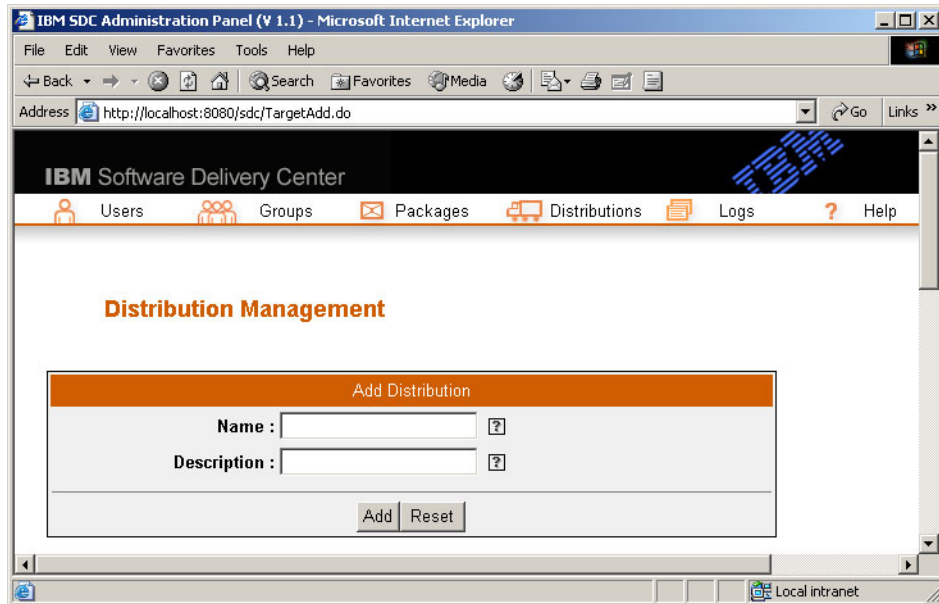


Figure 4-118 Software Delivery Center Distribution Management window

2. In the Name field, type the name of the distribution group.
3. In the Description field, type the associated distribution group description.

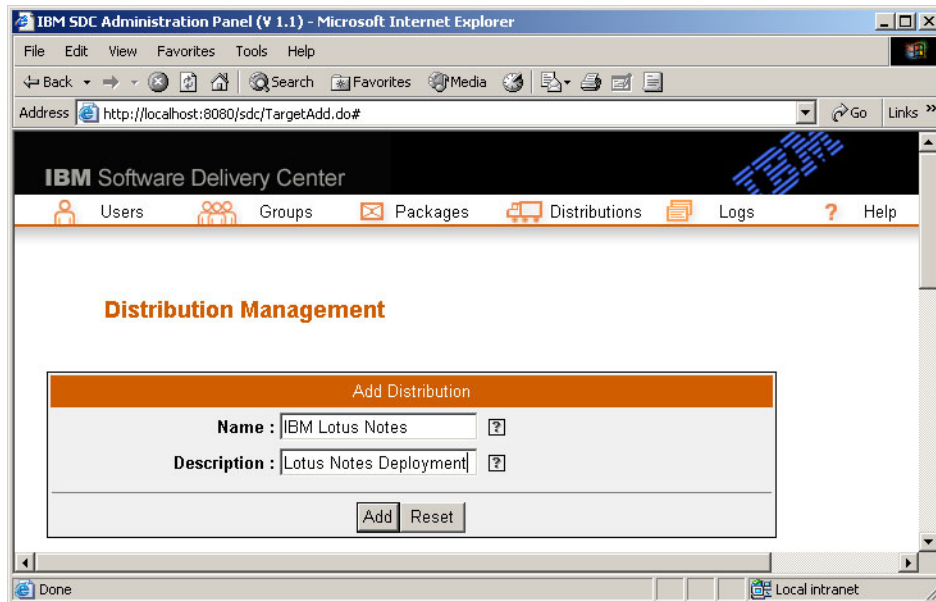


Figure 4-119 Software Delivery Center admin Distribution Management page

Note: The Name field is alphanumeric with a limitation of 32 characters. The Description field is alphanumeric with a limitation of 64 characters.

4. Click **Add**. The message shown in Figure 4-120 on page 357 is displayed.

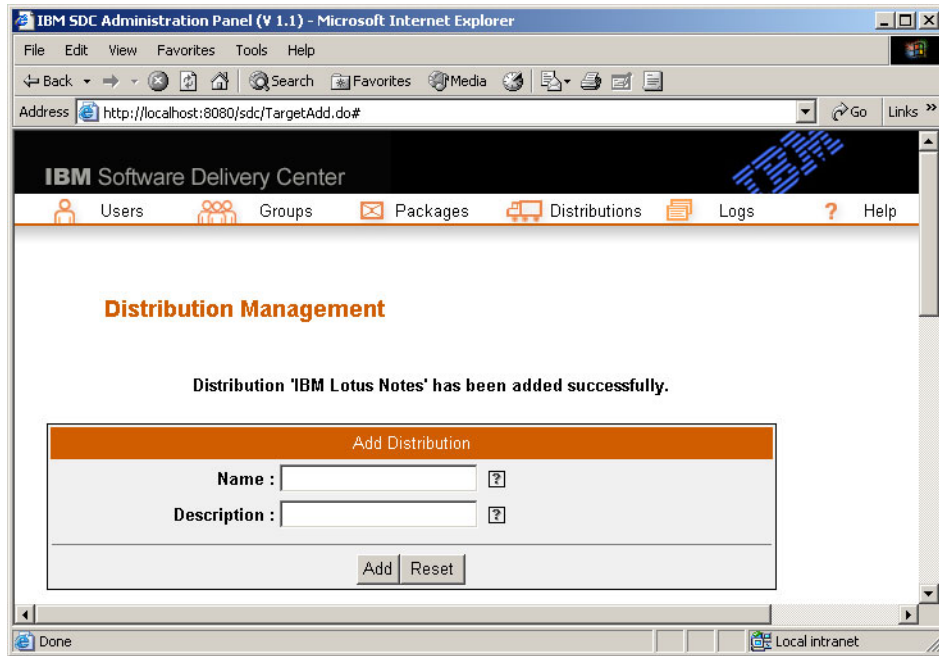


Figure 4-120 Software Delivery Center distribution management message

Note: You can add as many new distribution groups as you need.

Deleting a distribution group

To delete the distribution group:

1. Select **Distributions** → **Distributions** → **All Distributions**. The List Distributions table shown in Figure 4-121 on page 358 is displayed.

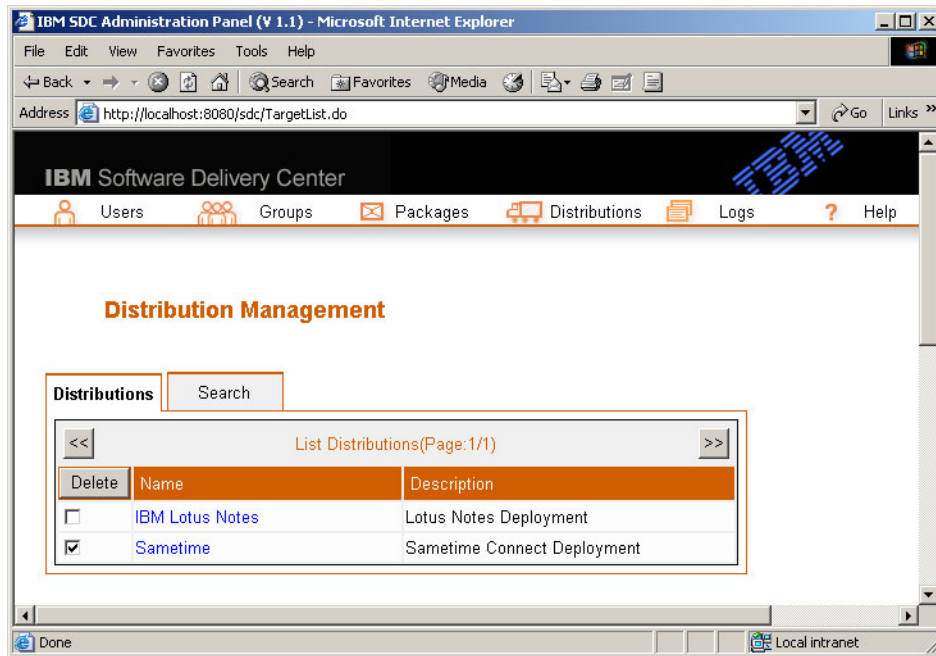


Figure 4-121 Software Delivery Center admin Distribution Management page

2. Select the distribution group you want to delete.
3. Click **Delete**. The window shown in Figure 4-122 opens.

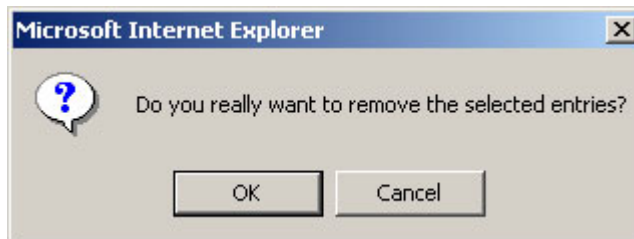


Figure 4-122 Software Delivery Center deletion confirmation window

4. Click **OK** to delete the distribution definition or click **Cancel** for no action.

Searching for a distribution group

To search for a specific distribution group name:

1. Select **Distributions** → **Distributions** → **All Distributions**. The List Distributions table shown in Figure 4-121 is displayed.

2. Click **Search**. The Search page shown in Figure 4-123 opens.

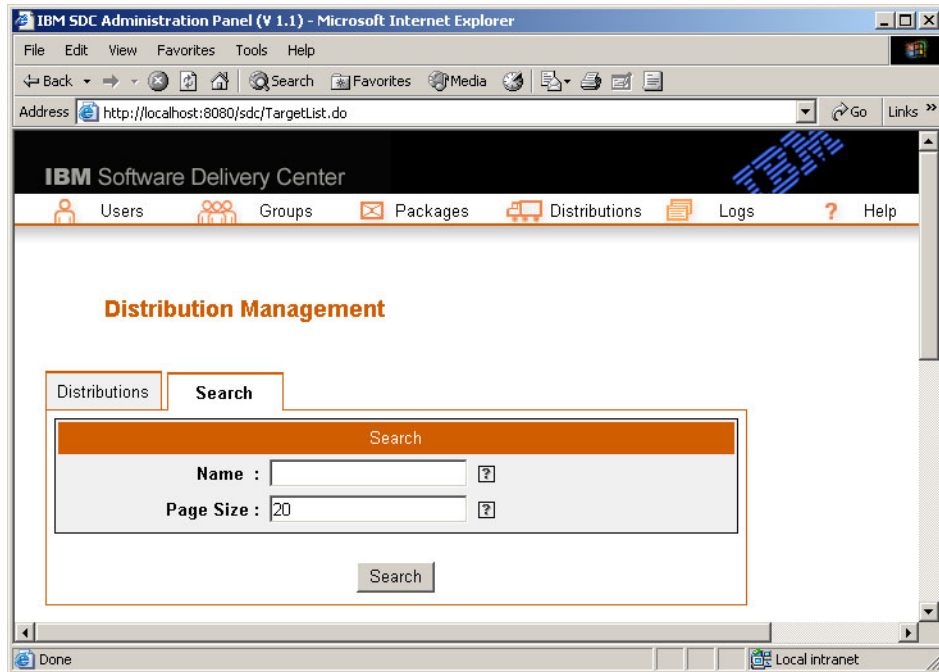


Figure 4-123 Software Delivery Center Distribution Search page

3. Type the distribution group name.
4. In the Page Size field, type the maximum number of entries per page to display. The default is 20 entries per page.

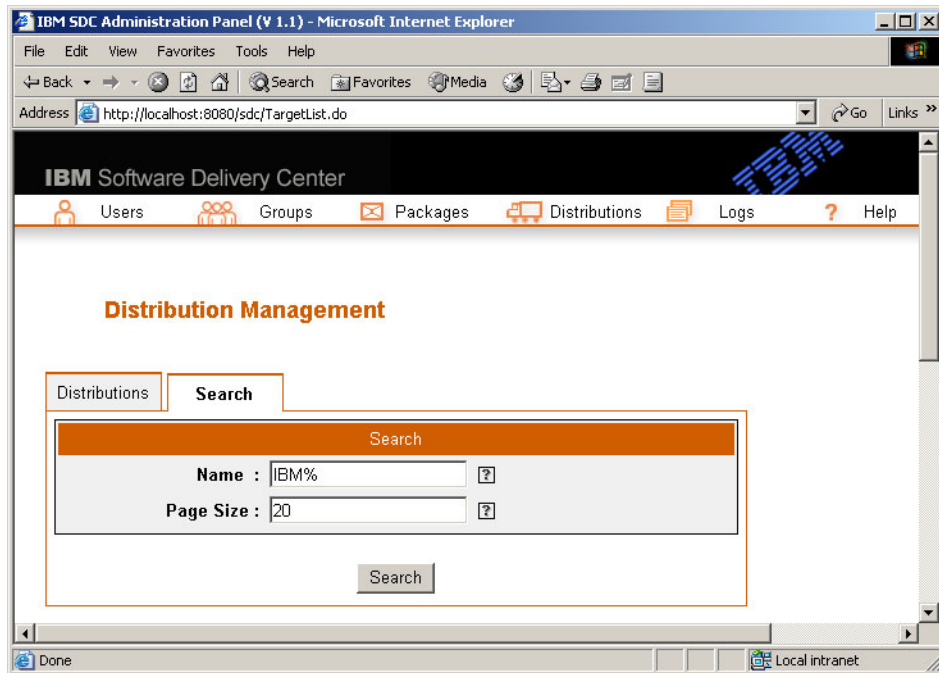


Figure 4-124 Completing the fields for a distribution search

Note: The Name field is case sensitive. Type the name exactly as the name is listed in the user list you are searching. The text field can be searched with a wildcard (for example, A% or a%)

5. Click **Search**. The selected distribution group name displays in the distribution group list.

Changing the distribution group description

To change a distribution group description:

1. Select **Distributions** → **Distributions** → **All Distributions**. The List Distributions table shown in Figure 4-121 on page 358 is displayed.
2. Select the name of the distribution group. The Edit Distribution page shown in Figure 4-125 on page 361 opens.

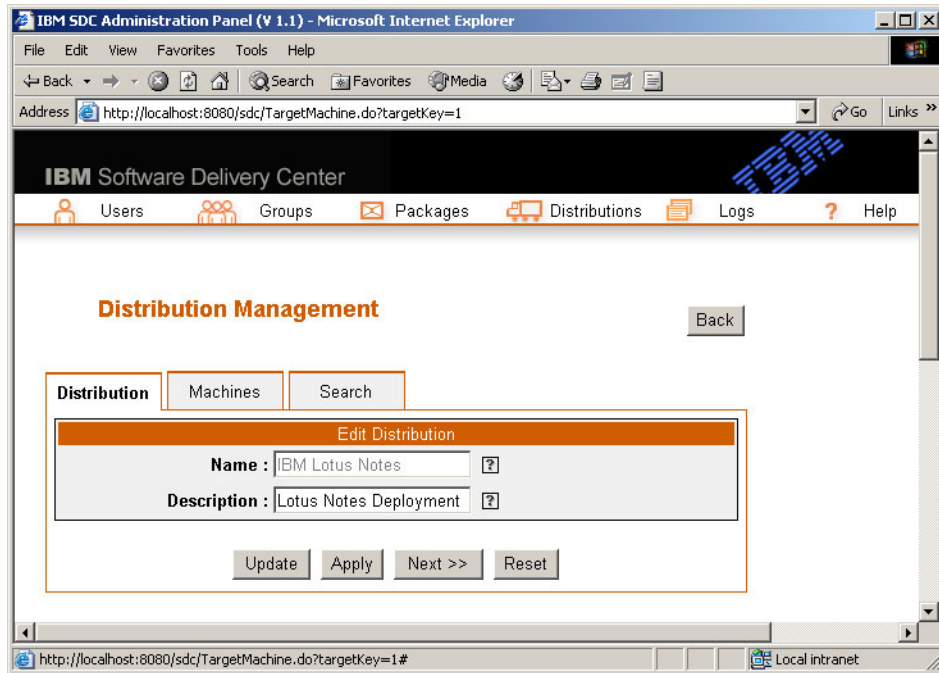


Figure 4-125 Software Delivery Center distribution editing

3. Make the changes to the distribution description.
4. Click **Update**. The List Distributions table shown in Figure 4-121 on page 358 opens.

Adding or deleting machines for a specific distribution group

To add or delete a target machine for a specific distribution group:

1. Select **Distributions** → **Distributions** → **All Distributions**. The List Distributions table shown in Figure 4-121 on page 358 is displayed.
2. Click the distribution group name. The Edit Distribution page shown in Figure 4-125 opens.
3. Click **Machines**. The Machine List for Distribution page shown in Figure 4-126 on page 362 opens.

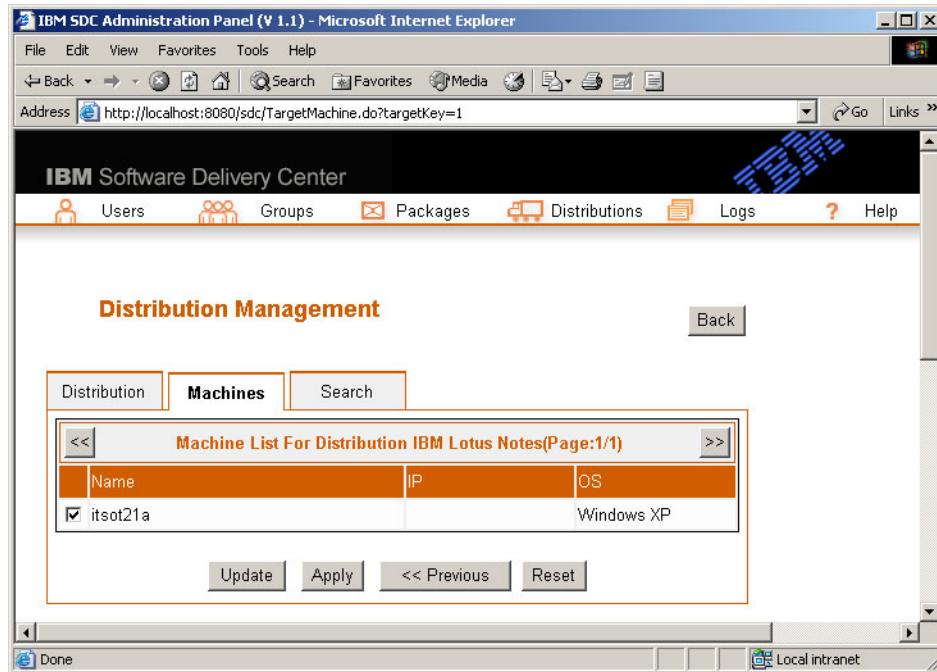


Figure 4-126 Software Delivery Center Distribution Machine Add window

4. Do one of the following:
 - To add a machine, select the machines you want to add.
 - To delete a machine, clear the check box for the machines you want to delete.
5. Click **Update**. The List Distributions table shown in Figure 4-121 on page 358 is displayed.

Note: When adding machines from multiple pages, you must click **Apply** to save your changes before selecting the << arrow or >> arrow to navigate between multiple pages.

When the administrator performs a push operation to a specific distribution group, all machines defined for that group will receive the push packages.

Searching for a machine in a specific distribution group

To search for a machine in a specific distribution group:

1. Select **Distributions** → **Distributions** → **All Distributions**. The List Distributions table shown in Figure 4-121 on page 358 is displayed.

2. Click the distribution group name.
3. Click **Search**. The Search page shown in Figure 4-127 opens.

IBM SDC Administration Panel (V 1.1) - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print

Address http://localhost:8080/sdc/TargetMachine.do Go Links

IBM Software Delivery Center

Users Groups Packages Distributions Logs Help

Distribution Management Back

Distribution Machines Search

Search

Name : it% ?

OS : [Select OS] ?

IP : ?

Selected Only : ☐ ?

Page Size : 20 ?

Search

http://localhost:8080/sdc/TargetMachine.do# Local intranet

Figure 4-127 Software Delivery Center distribution machine search

4. You can search by machine name, operating system, IP address, or selected machines. Do one or any combination of the following:

- a. In the Name field, type the machine name.

Note: The Name field is case sensitive. Type the name exactly as the name is listed in the user list you are searching. The text field can be searched with a wildcard (for example, A% or a%).

- b. In the OS field, select the operating system.
- c. In the IP field, type the IP address.
- d. Select **Selected Only** to restrict the search to selected machines for the distribution group only.

5. In the Page Size field, type the maximum number of entries per page to display.
6. Click **Search**. The page shown in Figure 4-126 on page 362 with the machine name opens.

Note: The user has access to each machine with a mark in the check box in the machine distribution list.

4.7.9 Managing machines

In the Software Delivery Center database, self-registration occurs the first time the machine is started after the Software Delivery Center client agent has been installed. All machines that are self-registered with the Software Delivery Center server are listed in the Machine Management table shown in Figure 4-128.

Deleting a machine

To delete a machine:

1. Select **Distributions** → **All Machines**. The List Machines table shown in Figure 4-128 is displayed.

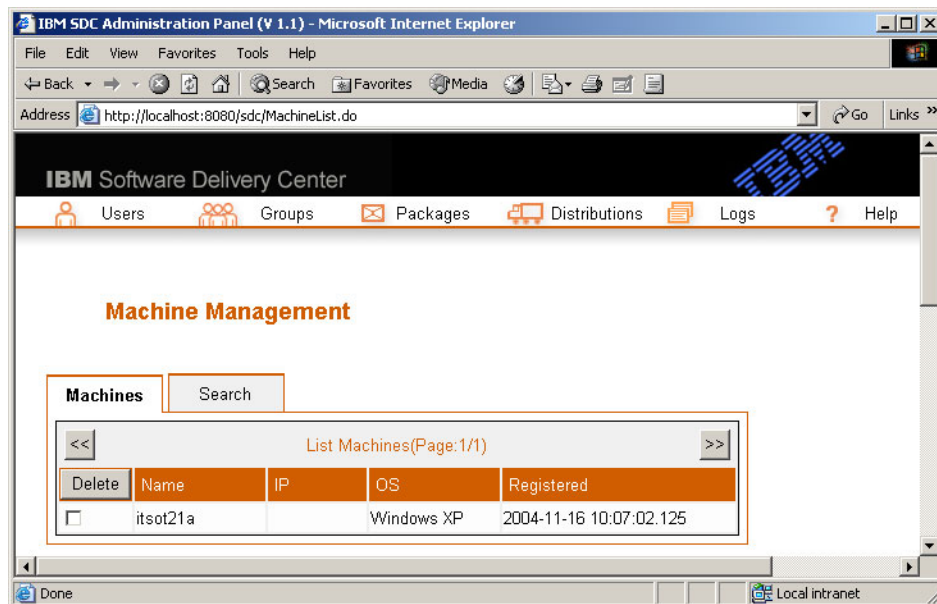


Figure 4-128 Software Delivery Center admin Machines Management page

2. Select the machine you want to delete.

3. Click **Delete**. The window shown in Figure 4-129 opens.

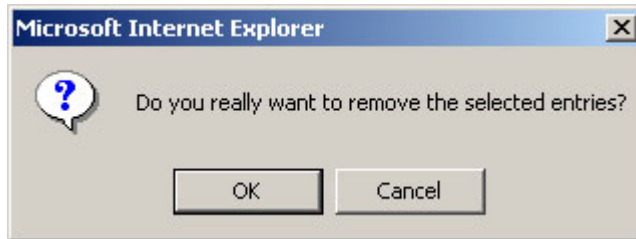


Figure 4-129 Software Delivery Center admin machine Confirm Delete window

4. Click **OK** to delete the machine name or click **Cancel** for no action.

Searching for a machine

To search for a specific machine:

1. Select **Distributions** → **All Machines**. The List Machines table shown in Figure 4-128 on page 364 is displayed.
2. Click **Search**. The Search page shown in Figure 4-130 on page 366 opens.

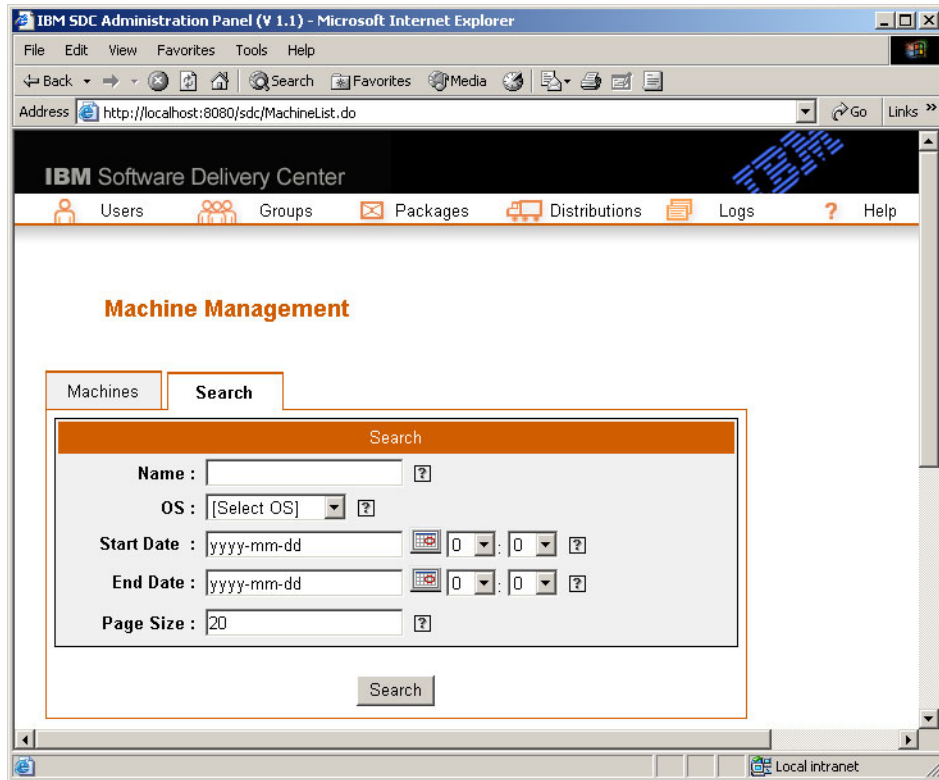


Figure 4-130 Software Delivery Center machine search

3. You can search by machine name, operating system, and schedule start or end date. Do one or of any combination of the following:
 - a. In the Name field, type the machine name.

Note: The Name field is case sensitive. Type the name exactly as the name is listed in the user list you are searching. The text field can be searched with a wildcard (for example, A% or a%).

- b. In the OS field, select the operating system.
 - c. In the Start Date field, select the schedule start date and time.
 - d. If the End Date field, select the schedule end date and time.
4. In the Page Size field, type the maximum number of entries per page to display. The default is 20 entries per page.

5. Click **Search**. The selected machine name and associated information (IP address, operating system, and date machine was registered) display in the machine list page shown in Figure 4-128 on page 364.

4.7.10 Managing schedules

A schedule is a time window for when a software package will be pushed to a set of clients. The Schedule Management page shows a list of schedules, distribution names, start dates, and end dates, and whether each schedule is enabled for distribution.

Adding a schedule

To add a schedule:

1. Select **Distributions** → **Schedules** → **New**. The Add Schedule page shown in Figure 4-131 opens.

IBM SDC Administration Panel (V 1.1) - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://localhost:8080/sdc/ScheduleAdd.do>

IBM Software Delivery Center

Users Groups Packages Distributions Logs Help

Schedule Management

General Package

Add Schedule

Schedule : ?

Description : ?

Enable : ☐ ?

Distribution Name : [For All] ?

Daily Start Time : : ?

Daily End Time : : ?

Start Date : ?

End Date : ?

Add Next >> Reset

Figure 4-131 Software Delivery Center Schedule Management page

2. Complete the schedule information fields on the General page and the Package or Bundle page.

The following fields are available:

- General page (Figure 4-132 on page 369)
 - **Schedule:** This field is for the name of the schedule. It has a limitation of 32 characters and does not except apostrophes or quotation marks.
 - **Description:** This field is for short description of the scheduled distribution. It is an alphanumeric text field, with a limitation of 64 characters
 - **Enable:** If this is selected, the schedule is enabled for push distribution.
 - **Distribution Name:** This field is used to select the distribution group assigned to this schedule.
 - **Daily Start Time:** This field is for the start time for software package distribution. The format is HHMM (using the 24-hour format: 9:00 p.m. is 2100).
 - **Daily End Time:** This is the end time for software package distribution. The format is HHMM (using the 24-hour format: 9:00 p.m. is 2100).
 - **Start Date:** This is the start date for software package distribution. The format is YYYY-MM-DD.
 - **End Date:** This field is used to specify the end date for software package distribution. The format is YYYY-MM-DD.

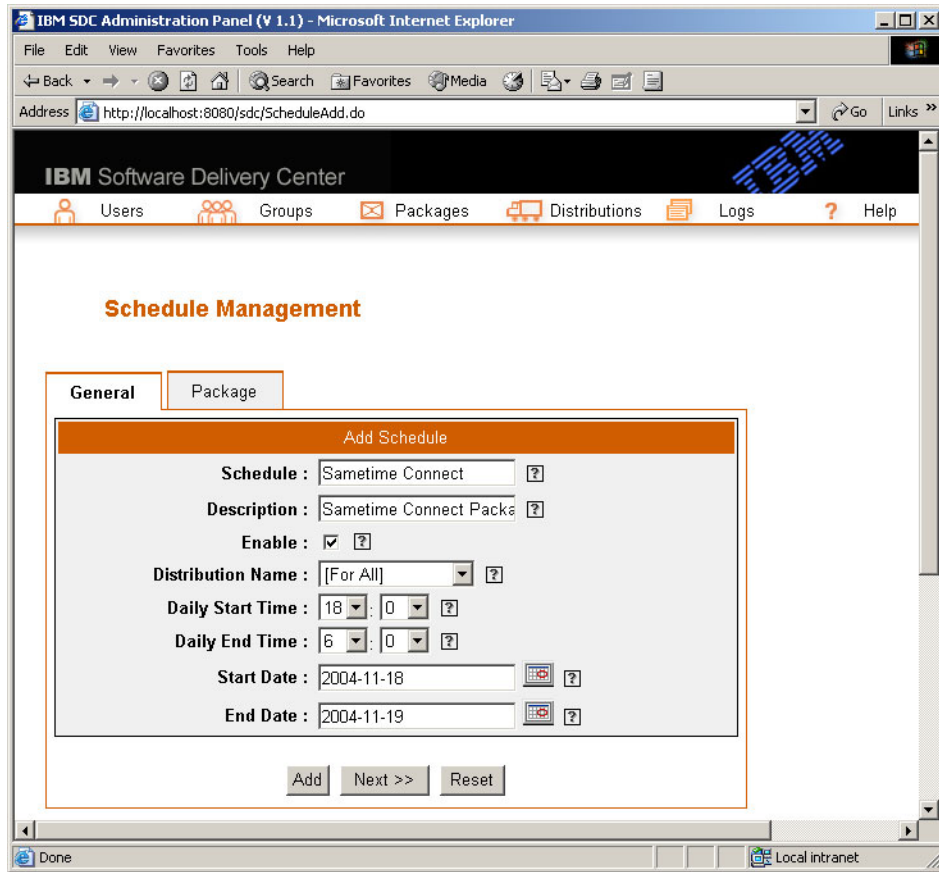


Figure 4-132 Software Delivery Center Schedule Management: General page

- Package or Bundle page (Figure 4-133 on page 370)
 - Query Packages/Bundles: This query is used to filter available software packages by package or bundle name. A menu is provided for selecting an application from a completed search. Click **Search** to obtain the list of packages or bundles.
 - The Package/Bundle query has a Name field, a Type field, and an OS field.

The Name field is used to specify the name of a software application. This field is case sensitive, and it is used to search the database for a specific application or bundle. The text field can be searched with a wildcard (for example, A% or a%).

The Type field is used to specify the software package type. A menu is provided for restricting the search to one of these specific package types:

- Download(Open)
- Download(Secure)
- LogicalDrive(Open)
- LogicalDrive(Secure)
- DirectoryDownload

The OS field provides a menu for restricting the package or bundle search to a specific operating system.

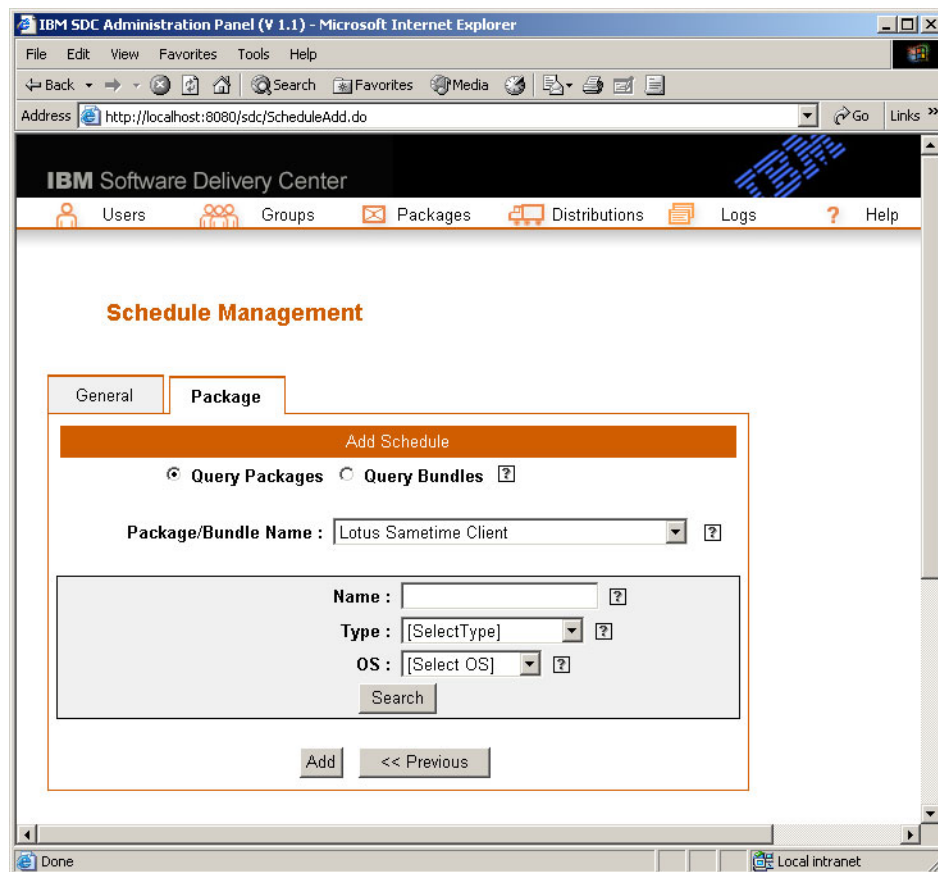


Figure 4-133 Software Delivery Center Schedule Management: Package page

3. Click **Add**. The message shown in Figure 4-134 on page 371 is displayed.

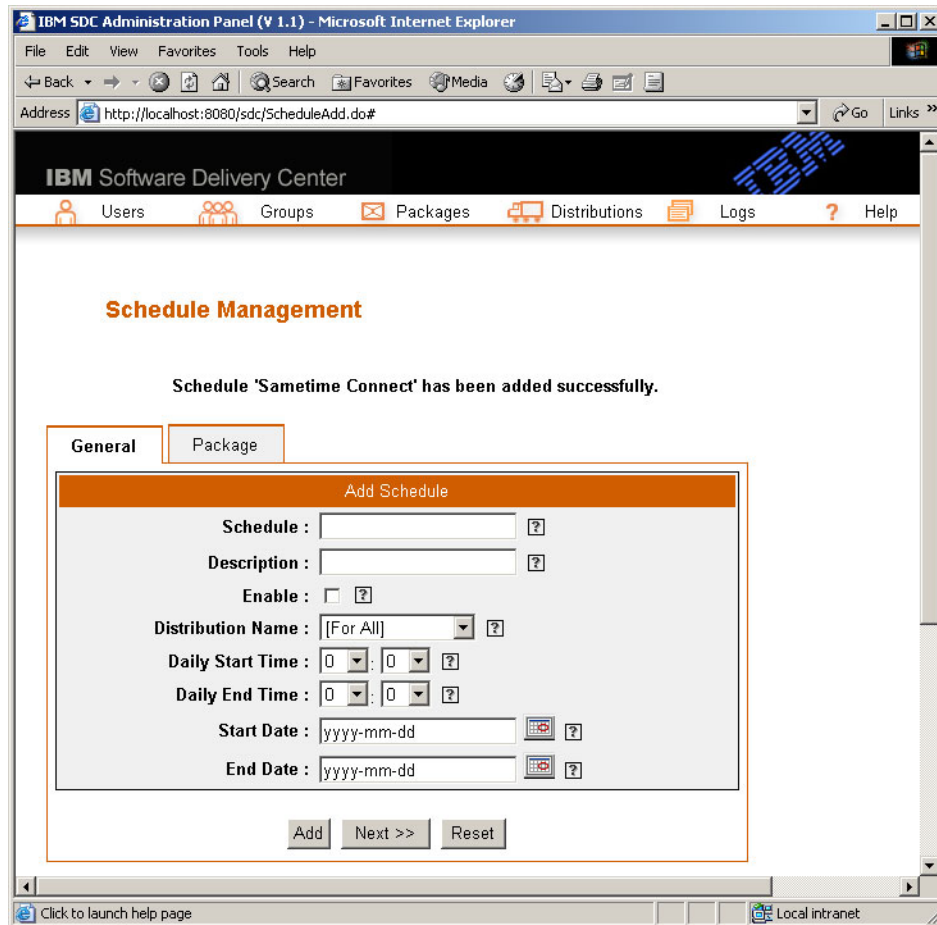


Figure 4-134 Software Delivery Center schedule message

Deleting a schedule

To delete the schedule:

1. Select **Distributions** → **Schedules** → **All Schedules**. The List Schedules table shown in Figure 4-135 on page 372 is displayed.

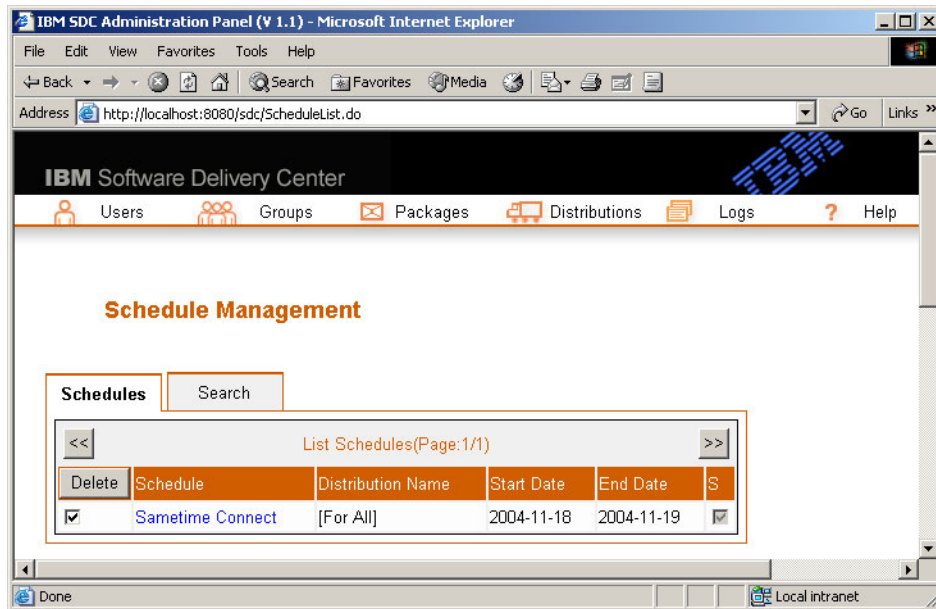


Figure 4-135 Software Delivery Center Schedule Management: Schedules

2. Select the schedule you want to delete.
3. Click **Delete**. The window shown in Figure 4-136 opens.

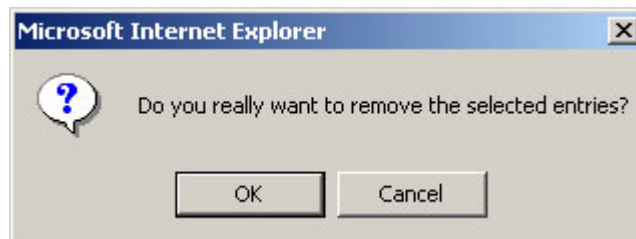


Figure 4-136 Software Delivery Center deletion confirmation window

4. Click **OK** to delete the schedule name or click **Cancel** for no action.

Searching for a specific schedule

To search for a specific schedule:

1. Select **Distributions** → **Schedules** → **All Schedules**. The List Schedules table shown in Figure 4-135 is displayed.
2. Click **Search**. The Search page shown in Figure 4-137 on page 373 opens.

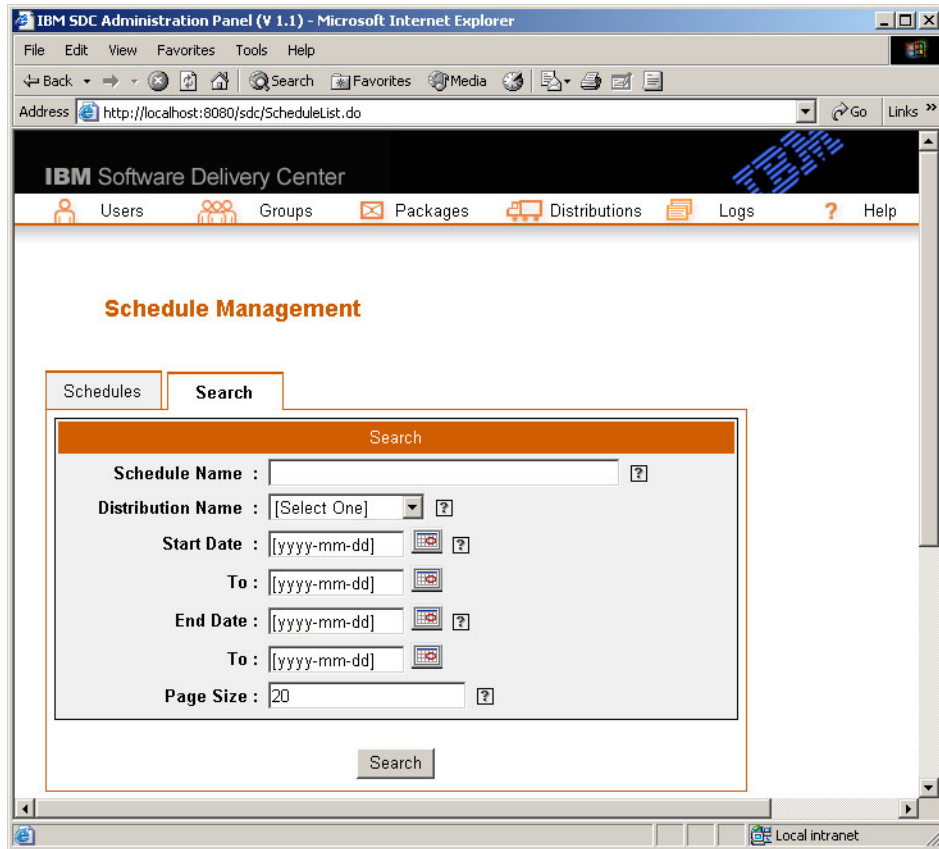


Figure 4-137 Software Delivery Center schedule search

3. You can search by schedule name, distribution name, start date, or end date. Do one or of any combination of the following:

- a. In the Schedule Name field, type the schedule name.

Note: The schedule name field is case sensitive. Type the name exactly as the name is listed in the schedule list you are searching. If you are not sure of the spelling, you can use the percent symbol (%) as a wild card in place of one or more characters.

- b. In the Distribution Name field, select the name of the distribution group to which the schedule belongs.
- c. In the Start Date field, select the schedule date and time designated to start a search for a schedule installation.

- d. In the End Date field, select the schedule date and time designated to end a search for a schedule installation.
4. In the Page Size field, type the maximum number of entries per page to display.

Figure 4-138 Software Delivery Center schedule search

5. Click **Search**. The selected schedule name displays in the schedule list.

Updating a schedule for a software package or a software bundle to be pushed

To update a schedule:

1. Select **Distributions** → **Schedules** → **All Schedules**. The List Schedules table shown in Figure 4-135 on page 372 is displayed.

2. Click the schedule name. The Update Schedule page shown in Figure 4-139 opens.

IBM SDC Administration Panel (V 1.1) - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://localhost:8080/sdc/ScheduleEdit.do?scheduleid=3>

IBM Software Delivery Center

Users Groups Packages Distributions Logs Help

Schedule Management Back

General Package

Update Schedule

Schedule : Sametime Connect ?

Description : Sametime Connect Deplo ?

Enable : ☒ ?

Distribution Name : [For All] ?

Daily Start Time : 18 : 0 ?

Daily End Time : 6 : 0 ?

Start Date : 2004-11-18 ?

End Date : 2004-11-19 ?

Update Next >> Reset

Done Local intranet

Figure 4-139 Software Delivery Center general schedule information

3. Make the changes to the schedule information fields.
4. Click **Update**. The List Schedules table shown in Figure 4-135 on page 372 is displayed.

4.7.11 Using the IBM Software Delivery Center logs

Software Delivery Center logs significant event information.

Viewing a log

To view a log:

1. Select **Logs** → **View Logs**. The List Logs table shown in Figure 4-140 opens.

TimeStamp	UserID	Client	HostName	Package	Status
2004-11-18 19:02:28.312	DEMO	AppletClient	itsot21a	Lotus Notes 6.5.2 (Download(Open))	-1
2004-11-18 19:02:23.562	DEMO	AppletClient	itsot21a	Lotus Notes 6.5.2 (Download(Open))	1
2004-11-18 19:02:10.453	DEMO	AppletClient	itsot21a	Lotus Sametime Client (Download(Secure))	0
2004-11-18 19:00:20.781	DEMO	AppletClient	itsot21a	Lotus Sametime Client (Download(Secure))	1
2004-11-18 18:59:34.109	DEMO	AppletClient	itsot21a	Adobe Acrobat Reader (Download(Open))	0
2004-11-18 18:58:34.375	DEMO	AppletClient	itsot21a	Adobe Acrobat Reader (Download(Open))	1
2004-11-18 18:58:27.938	DEMO	AppletClient	itsot21a	AdAware SE Personal Edition(Download(Open))	0
2004-11-18 18:58:14.188	DEMO	AppletClient	itsot21a	AdAware SE Personal Edition(Download(Open))	1

Figure 4-140 Software Delivery Center Log Management page

2. Click **TimeStamp**. The Log Details page shown in Figure 4-141 on page 377 opens.

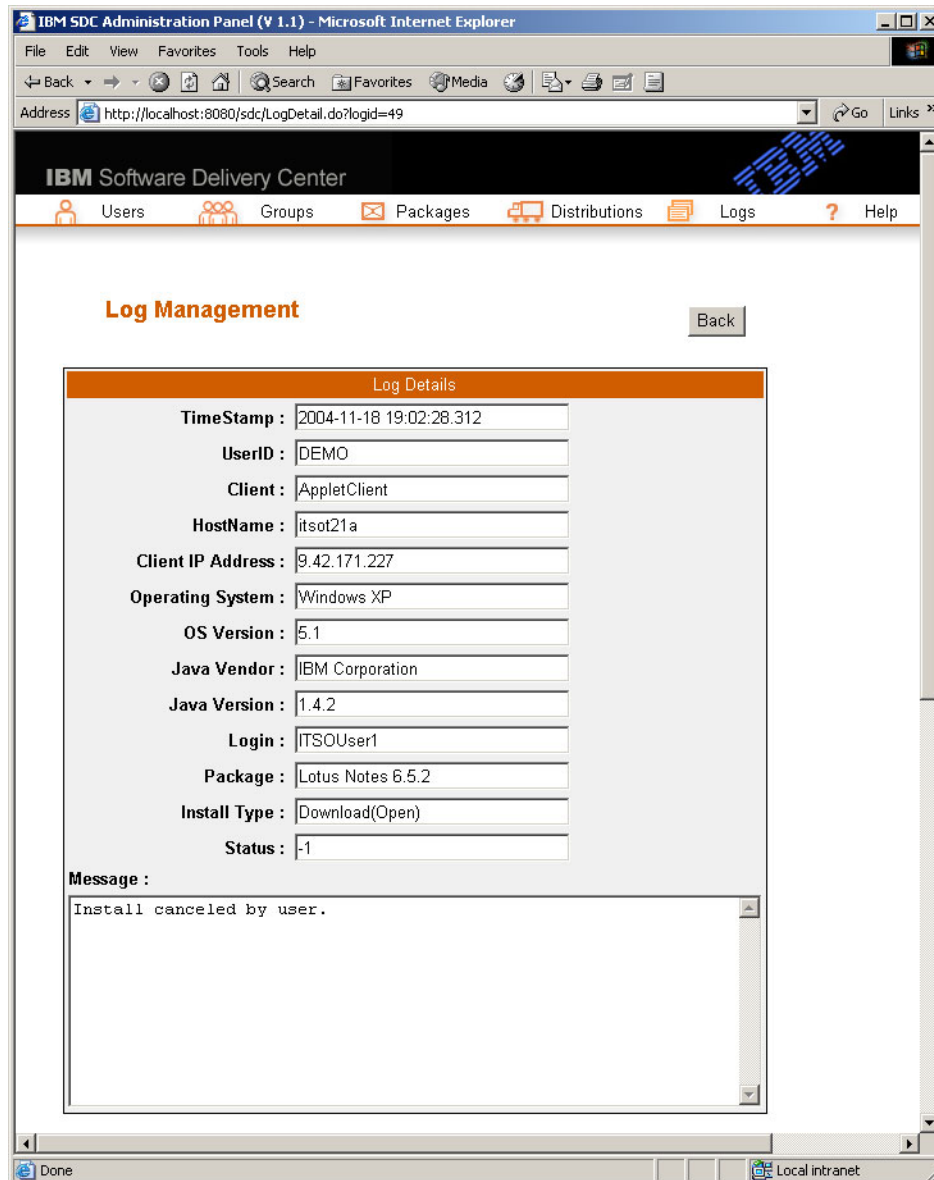


Figure 4-141 Software Delivery Center log information

3. View the details of each log entry. The following are the fields and descriptions displayed in the logs:
 - TimeStamp: The date and time of the log entry

- UserID: The Software Delivery Center user name used to access the catalog
- Client: The client type
- HostName: The host name of the client
- Client IP Address: The IP address of the host name that generated the log entry
- Operating System: The operating system of the client
- OS Version: The version number of the operating system of the client
- Java Vendor: The Java vendor of the JRE used by the client
- Java Version: The Java version of the JRE used by the client
- Login: The Windows user account used to log in to the Windows operating system on the client computer
- Package: The name of the software package involved
- Install Type: The software package installation type
- Status: 0 (Ended) or 1 (Started) or -1 (Failed)

Deleting a log

To delete the log:

1. Select **Logs** → **Delete**. The Delete Logs page shown in Figure 4-142 on page 379 opens.

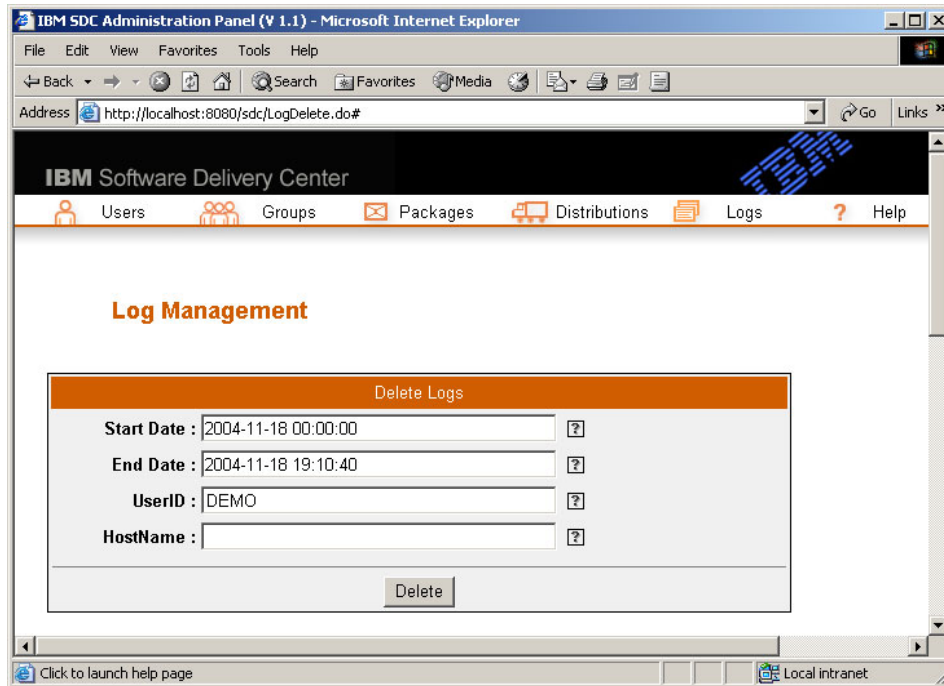


Figure 4-142 Software Delivery Center Delete Log page

2. Select the date range, host name, user name, or a combination for the logs you want to delete.
3. Click **Delete**.

Note: Logs will be deleted without a confirmation window.

Searching for a log

To search for a specific log:

1. Click **Logs** → **View Logs**. The List Logs table shown in Figure 4-140 on page 376 is displayed.
2. Click **Search**. The Search page shown in Figure 4-143 on page 380 opens.

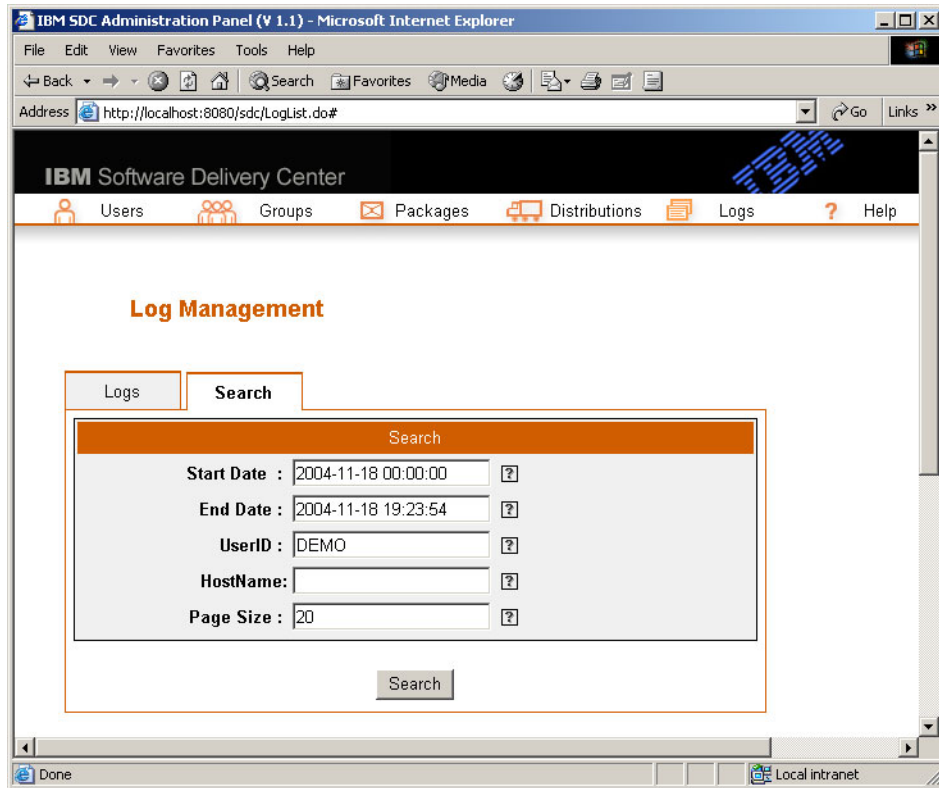


Figure 4-143 Software Delivery Center log search

3. You can search by start date, end date, user name, or host name. Do one of or any combination of the following:
 - a. In the Start Date field, select the schedule date and time designated to start a search for a schedule installation.
 - b. If the End Date field, select the schedule date and time designated to end a search for a schedule installation.
 - c. In the UserID field, type the user name.
 - d. In the HostName field, type the host name.

Note: The user name and host name fields are case sensitive. Type the name exactly as the name is listed in the log list you are searching. If you are not sure of the spelling, you can use the percent symbol (%) as a wild card in place of one or more characters.

4. In the Page Size field, type the maximum number of entries per page to display.
5. Click **Search**. The selected log entry displays in the log list page shown in Figure 4-140 on page 376.

4.7.12 Finding help

Help is available in two formats:

- ▶ Online help
- ▶ The *IBM Software Delivery Center Administrator's Guide*

Help is available from the administrator's console. To get help do one of the following:

- ▶ To access the *IBM Software Delivery Center Administrator's Guide*, click **Help** and then click **Administrator's Guide (PDF)**. The *IBM Software Delivery Center Administrator's Guide* PDF opens.
- ▶ To access the online help, click the question mark (?) beside the field to obtain an explanation of that field.

Note: Software Delivery Center uses Adobe Reader 6.0 or higher to view or print the file. Adobe Reader is available at no charge from:

<http://www.adobe.com/products/acrobat/readermain.html>

4.7.13 Logging out of the administrator's console

To log out, click **Logoff**. The Administration Login window opens.

4.8 Using the Software Delivery Center software catalog

This section describes how to launch the Software Delivery Center client applet and install software packages and bundles. The client applet allows users to select and install software packages and bundles from an online catalog. The Software Delivery Center client applet can be launched from any client computer that meets the following prerequisites:

- ▶ One of the following operating systems:
 - Windows 2000 Professional with Service Pack 4 or higher
 - Windows XP with Service Pack 1 or higher
- ▶ A Web browser (Internet Explorer 6.0 or higher)
- ▶ A network connection (for registration on the Software Delivery Center server)

Note: Support for additional operating systems and Web browsers is available from IBM Global Services. For more information send an e-mail to isdc@us.ibm.com.

This section includes the following topics:

- ▶ “Software Delivery Center client applet” on page 382
- ▶ “Accessing the Software Delivery Center server” on page 385
- ▶ “Launching the Software Delivery Center client applet” on page 386
- ▶ “Installing an application” on page 396
- ▶ “Installing a bundle” on page 398

4.8.1 Software Delivery Center client applet

The client applet runs either from the browser as a Java application or as a stand-alone Java Web Start application. Figure 4-144 shows functions of the Software Delivery Center client applet.

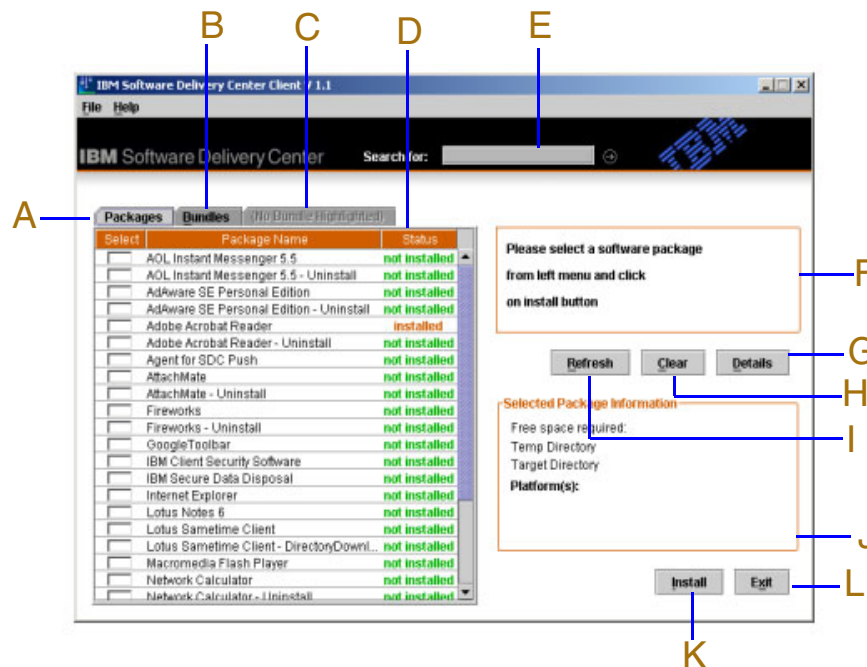


Figure 4-144 Software Delivery Center client applet

These functions are:

- ▶ **Packages (A):** This is a list of all the applications available for download. Highlighting a particular application will display size. Supported OS information is displayed in the Selected Package Information pane (J). Selecting an application and clicking **Install (K)** starts the installation process. Multiple selections are supported and will be installed sequentially.
- ▶ **Bundles (B):** This pane displays those applications that have been bundled or grouped together to facilitate installation. Selecting a bundle results in a list of the packages that will be installed in the next pane. Selecting a bundle and clicking **Install (K)** starts the install process.
- ▶ **Bundle Details (C):** This pane displays list of applications included in a bundle.
- ▶ **Status (D):** This pane displays whether an application is currently installed on the workstation.
- ▶ **Search (E):** In situations where there are a multitude of packages, you can perform a search to narrow the options. The search is based on package name. To display all the packages after a search, perform a search with an asterisk (*) as a wildcard character.
- ▶ **Install (F):** When an application is in the process of being installed, the pane shown in Figure 4-145 will be displayed.

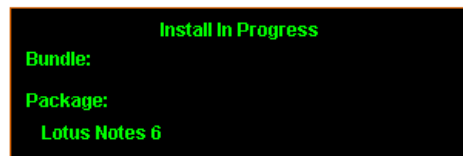


Figure 4-145 Software Delivery Center catalog installation progress

Once the installation is complete, the screen will return to the original state shown in Figure 4-146.

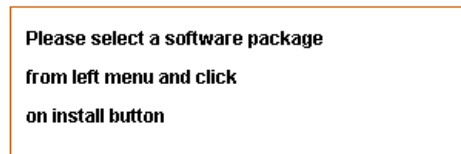


Figure 4-146 Software Delivery Center install status window

- ▶ **Details (D):** Displays the application-specific information or instructions window shown in Figure 4-147 on page 384.

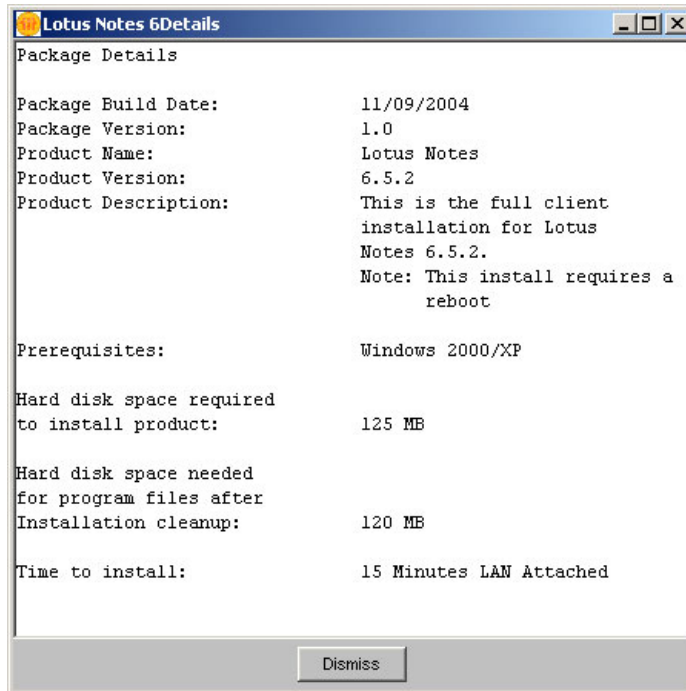


Figure 4-147 Software Delivery Center application details

Click **Dismiss** to close the window.

- ▶ Clear (H): This function clears all selected packages.
- ▶ Refresh (I): This function refreshes the catalog view with latest available applications.
- ▶ Selected Package Information (J): This pane displays information pertinent to the applications or a bundle selected as shown in shown in Figure 4-148.

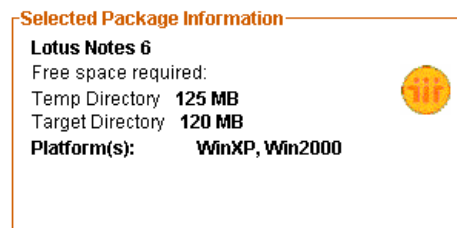


Figure 4-148 Software Delivery Center application information

- ▶ Install (K): This button starts the installation process for all of the selected packages or bundles.

- ▶ Exit (L): Closes the Software Delivery Center client applet

4.8.2 Accessing the Software Delivery Center server

To access Software Delivery Center server, follow this process from the client computer:

1. Open a Web browser.
2. In the Address bar, type one of the following:
 - `http://server_name` (where *server_name* is the name of the Software Delivery Center Server)
 - `http://server_IP_address` (where *server_IP_address* is the IP address of the Software Delivery Center Server)
3. Press **Enter**. The Software Delivery Center Welcome page shown in Figure 4-149 on page 386 opens.



Figure 4-149 Software Delivery Center Welcome message

4.8.3 Launching the Software Delivery Center client applet

The following procedure describes how to launch the Software Delivery Center client applet. To launch the client applet, follow this process from the client computer:

1. In the Access Software Catalog part of the page shown in Figure 4-149 on the Software Delivery Center Welcome page, click **Click here**. The File Download Security Warning window shown in Figure 4-150 on page 387 opens.

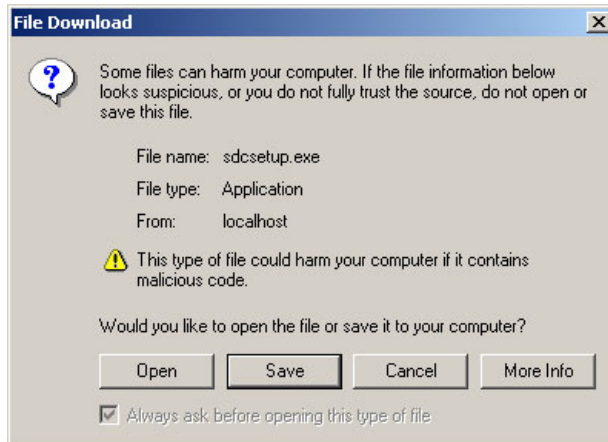


Figure 4-150 Software Delivery Center security warning

2. Click **Open**. The Software Delivery Center Installation wizard opens. The window shown in Figure 4-151 opens.

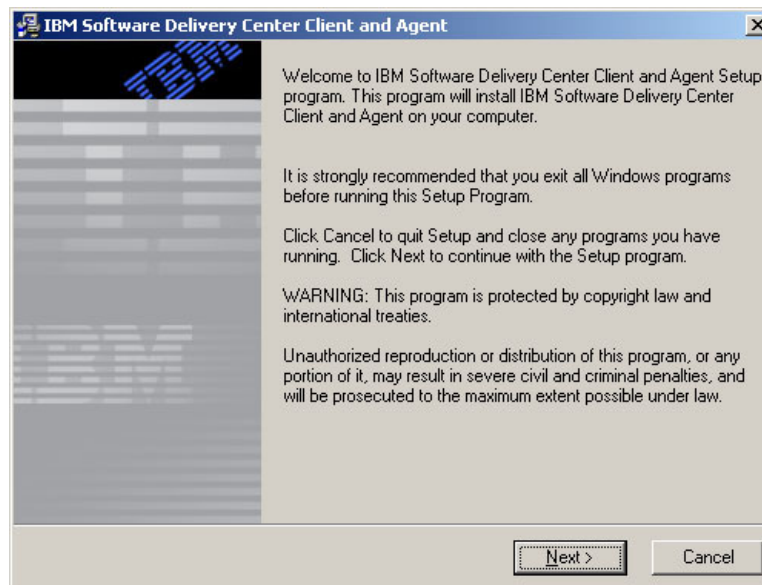


Figure 4-151 Software Delivery Center agent setup window

3. Click **Next**. The window shown in Figure 4-152 on page 388 opens.

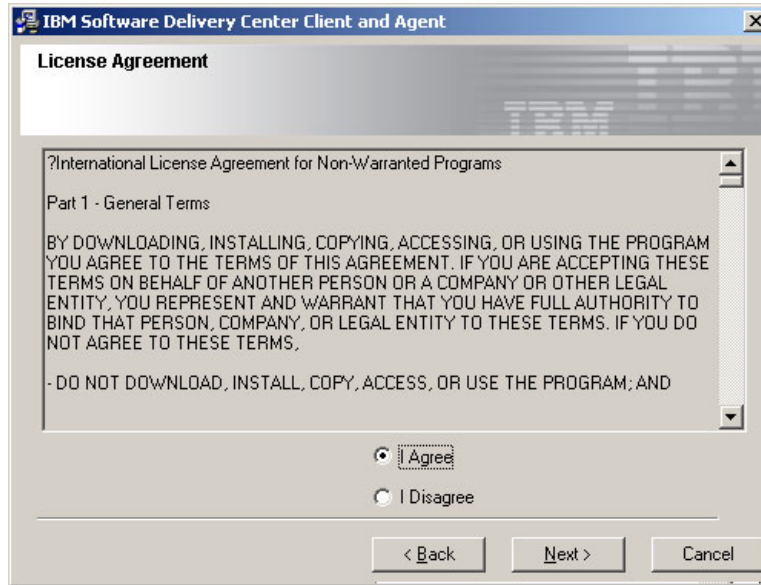


Figure 4-152 Software Delivery Center client license agreement

4. Read the license agreement and if you agree, select the **I Agree** option, and then click **Next**. The Destination Location window shown in Figure 4-153 on page 389 opens.

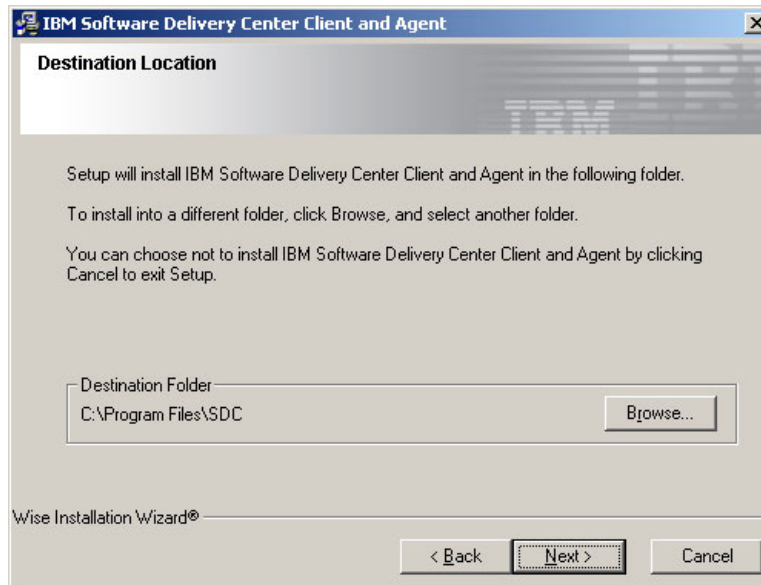


Figure 4-153 Software Delivery Center client installation location window

5. Either accept the default folder (c:\Program Files\SDC) or use the **Browse** button to select a different folder.
6. Click **Next**. The Server Name or IP Address window shown in Figure 4-154 on page 390 opens.

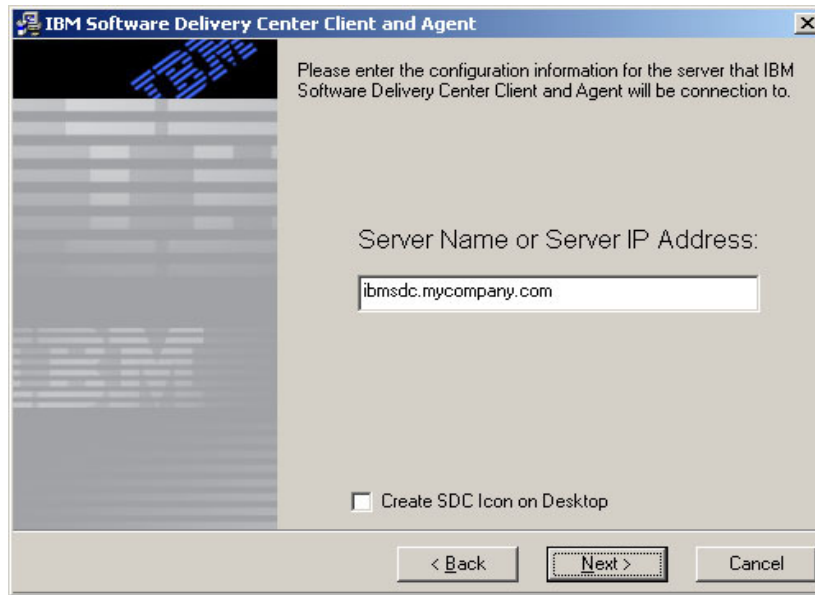


Figure 4-154 Software Delivery Center Server Name window

7. Type the fully qualified domain name of the Software Delivery Center server or the IP address that will be used to connect to Software Delivery Center server.
8. Select **Create SDC Icon on Desktop** and click **Next**.

Note: You may choose not to select the Create SDC Icon on Desktop option. If that is your choice, the user will be asked to create an SDC icon at the second launch of the Software Delivery Center client applet by Java Webstart application.

9. The Start Installation window shown in Figure 4-155 on page 391 opens.

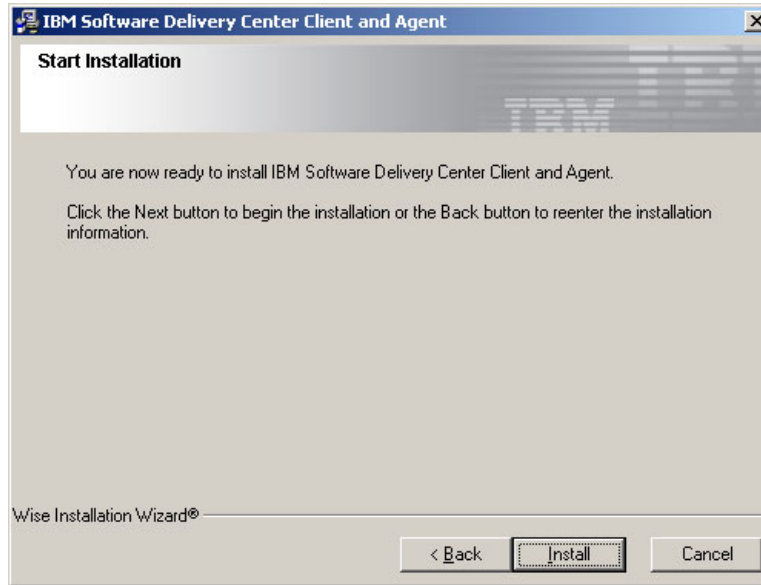


Figure 4-155 Software Delivery Center Start Installation window

10. Click **Install**. The Installing window shown in Figure 4-156 opens and the progress of the setup is shown by the indicator.

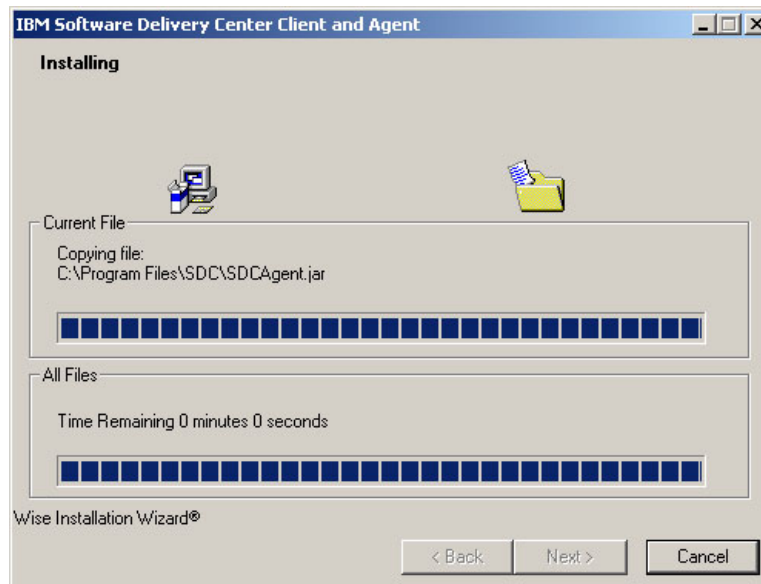


Figure 4-156 Software Delivery Center client installation

11. The window shown in Figure 4-157 opens when the installation is complete.

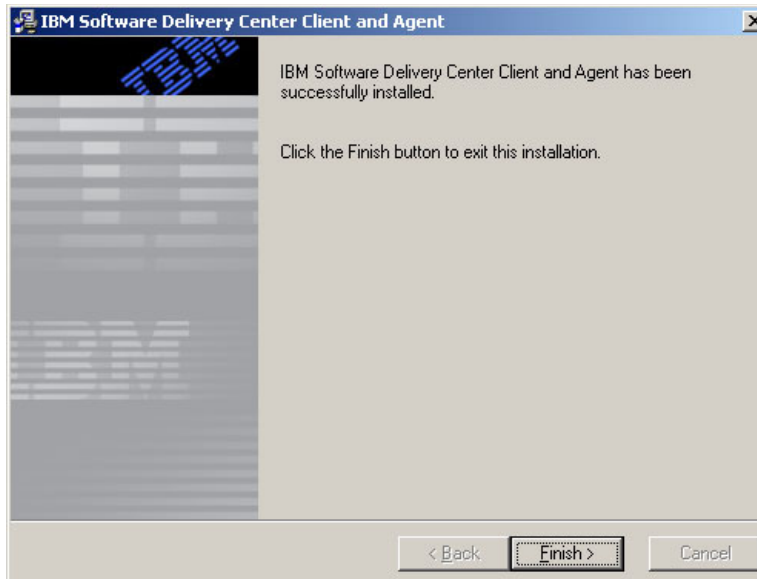


Figure 4-157 Software Delivery Center installation complete message

12. Click **Finish**.

13. Close all the windows and restart the machine.

Note: Software Delivery Center client setup includes IBM JRE and the Software Delivery Center client agent. This is a one-time setup only.

14. Open a Web browser.

15. In the Address bar, type one of the following:

- `http://server_name` (where *server_name* is the name of the Software Delivery Center Server)
- `http://server_IP_address` (where *server_IP_address* is the IP address of the Software Delivery Center Server)

16. Press **Enter**.

17. The Software Delivery Center home page shown in Figure 4-158 opens.

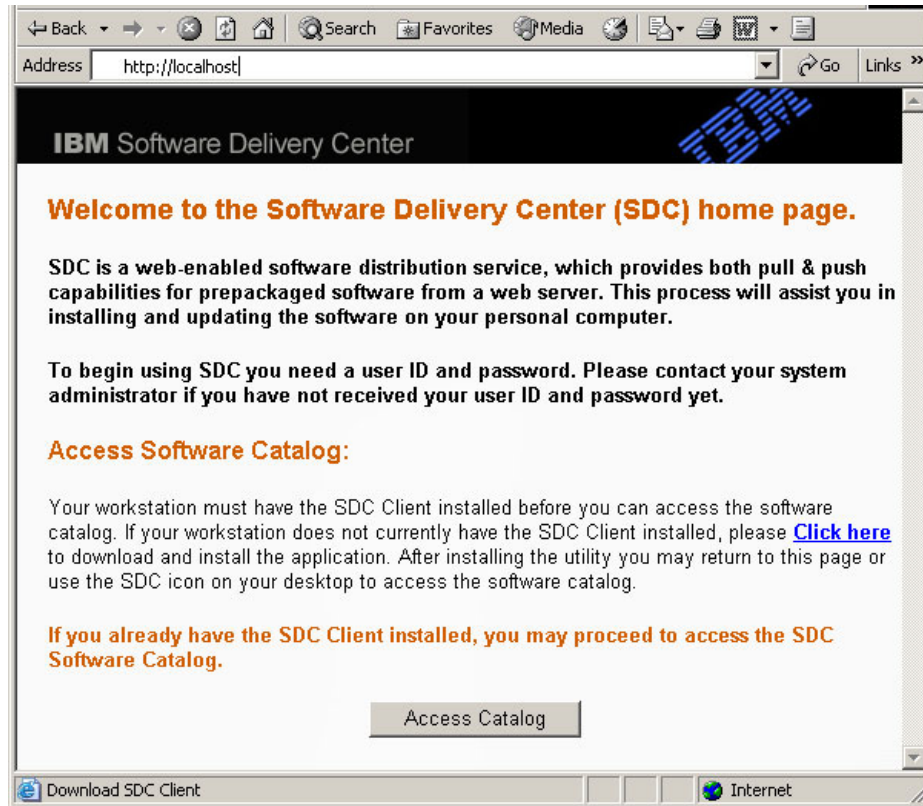


Figure 4-158 Software Delivery Center home page

18. Click **Access Catalog**. The Security Warning window shown in Figure 4-159 opens.

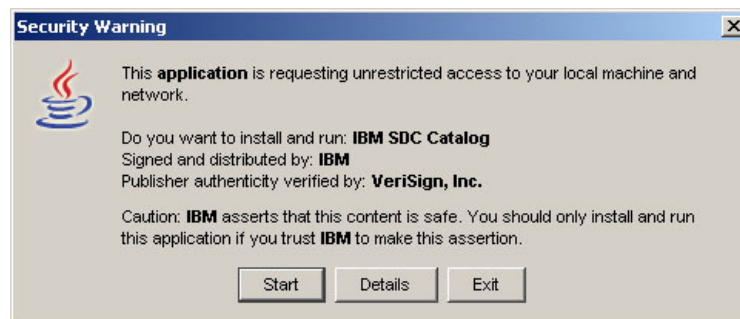


Figure 4-159 Software Delivery Center catalog security warning

Note: Verify that the security warning window displays IBM and that the publisher authenticity is verified by VeriSign, Inc. The security warning window will be displayed at first launch only.

19. Click **Start**. The Software Delivery Center Login window shown in Figure 4-160 opens.

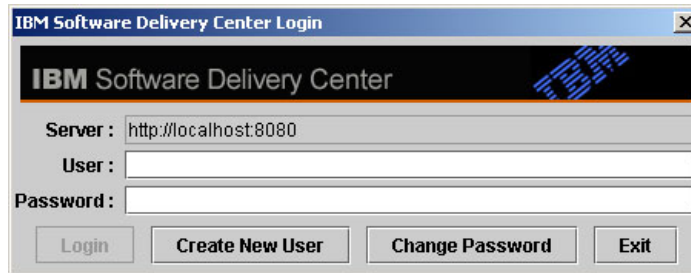


Figure 4-160 Software Delivery Center client login window

20. You may see IBM SDC Catalog - Desktop Integration window shown in Figure 4-161.

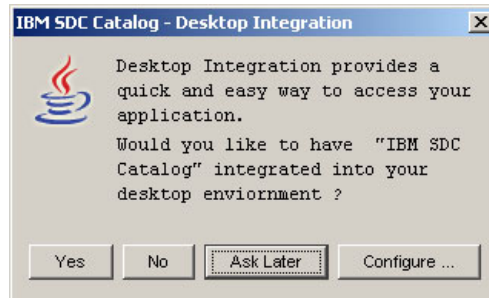


Figure 4-161 IBM SDC - Desktop Integration window

21. Click **Yes** to put a Software Delivery Center Catalog icon on the desktop for easier access if you chose not to create a desktop icon during client agent setup process. Click **No** if the icon is already present on your desktop. Click **Ask Later** to defer it to later time.

Note: Software Delivery Center uses Java Web Start technology to launch the Software Delivery Center client applet. The client applet can be launched either from an icon on the desktop or from Software Delivery Center welcome page by clicking **Access Catalog**.

22. If the administrator has provided you with a user name and password for a Software Delivery Center catalog, type the user name and password in the fields provided and then click **Login**. A software catalog like that shown in Figure 4-164 on page 396 opens.

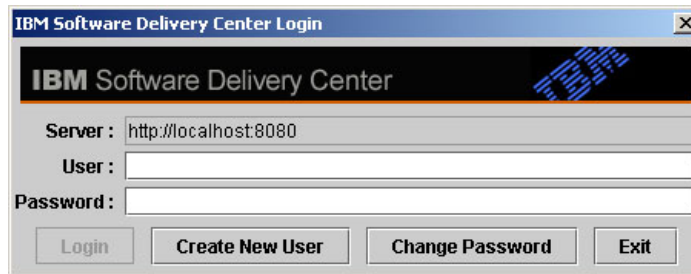
The image shows a window titled "IBM Software Delivery Center Login". It has a header bar with the IBM logo and the text "IBM Software Delivery Center". Below the header, there are three input fields: "Server:" with the value "http://localhost:8080", "User:" which is empty, and "Password:" which is empty. At the bottom, there are four buttons: "Login", "Create New User", "Change Password", and "Exit".

Figure 4-162 Software Delivery Center client login window

23. If the administrator has instructed you to create your own user name and password, do the following:
- Click **Create New User**. The window shown in Figure 4-163 on page 395 opens.

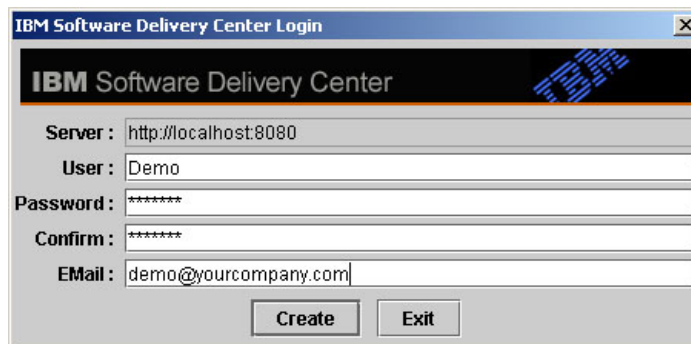
The image shows a window titled "IBM Software Delivery Center Login". It has a header bar with the IBM logo and the text "IBM Software Delivery Center". Below the header, there are five input fields: "Server:" with the value "http://localhost:8080", "User:" with the value "Demo", "Password:" with the value "*****", "Confirm:" with the value "*****", and "EMail:" with the value "demo@yourcompany.com". At the bottom, there are two buttons: "Create" and "Exit".

Figure 4-163 Software Delivery Center new user window

- In the User field, type the user name you want to use.
- In the Password field, type the password you want to use.
- In the Confirm Password field, type your password again. You must type the password exactly as you typed it in the Password field.
- In the EMail field, type your e-mail address.
- Click **Create**. A software catalog such as that shown in Figure 4-164 on page 396 opens.

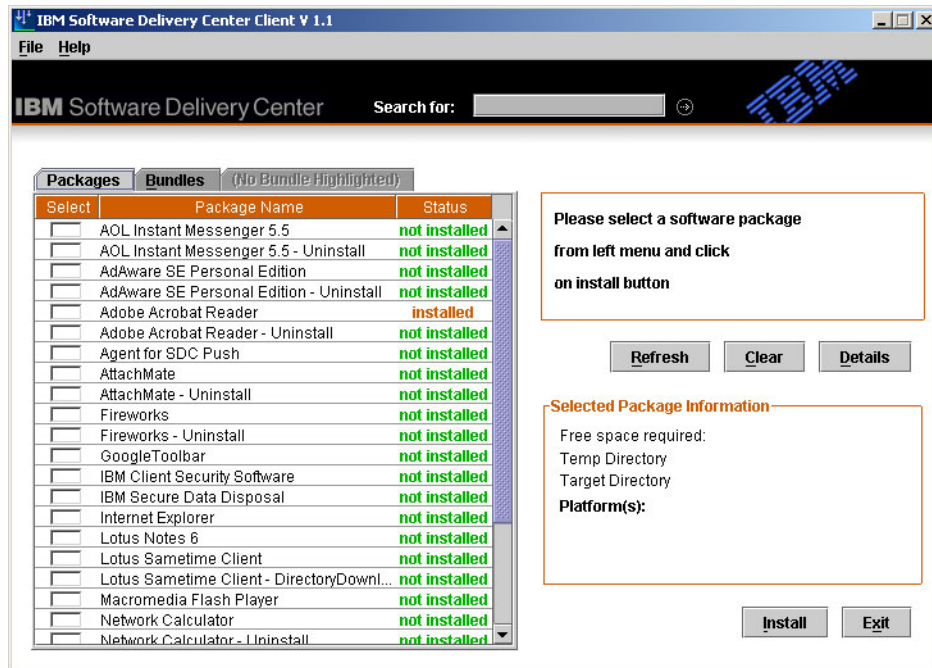


Figure 4-164 Software Delivery Center client applet

Note: Catalogs for new users might not have any software packages or bundles listed. In most cases, the administrator must assign a new user to a specific group before the user can install software from a catalog.

4.8.4 Installing an application

The client applet shows all software packages for which a particular user has access privileges. When the user selects a software package, the client applet shows detailed data about the software package. If the software package selected meets the user's needs, the user clicks the **Install** button. The install procedure starts automatically.

The following procedure describes how to install applications from the Software Delivery Center client applet.

1. Launch IBM Software Delivery Center client applet by following the steps described in 4.8.3, "Launching the Software Delivery Center client applet" on page 386.
2. Select an application as shown in Figure 4-165 on page 397.

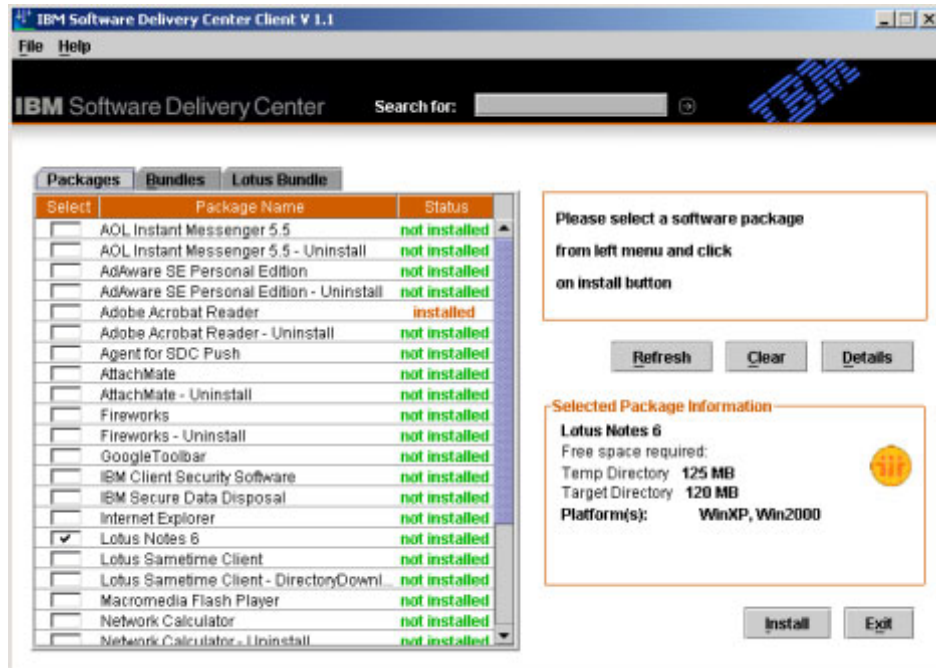


Figure 4-165 Selecting an application in the Software Delivery Center client applet

Note: Multiple applications can be selected using the check boxes provided. If one of the applications requires a restart, the install process for the subsequent package will not start.

3. Click **Details** to view the application-specific information or instructions.
4. Press **Install** to start the install process of the selected package. The install screen shown in Figure 4-166 will appear on client applet and it will show "install in progress".

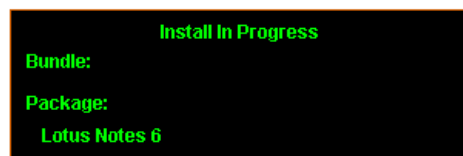


Figure 4-166 Software Delivery Center install in progress

5. The download window shown in Figure 4-167 on page 398 opens.

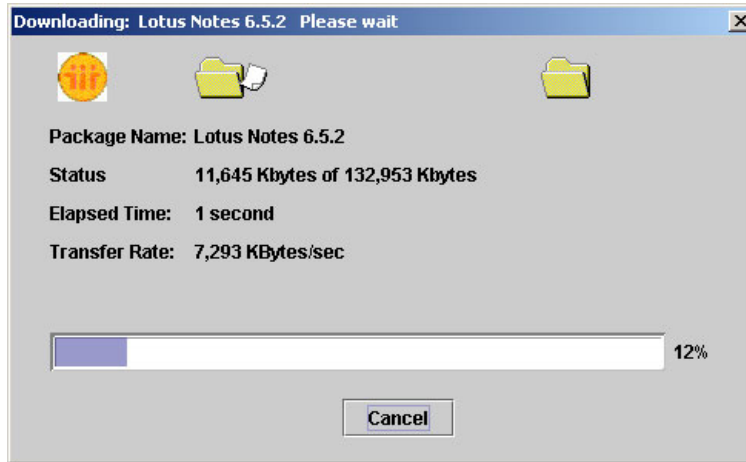


Figure 4-167 Software Delivery Center application download window

6. The application installation process starts after a successful download of an application.

Note: Some applications may require end user intervention to complete the installation.

7. Once the installation is complete, the Install in Progress panel shown in Figure 4-166 on page 397 returns to the original state shown in Figure 4-168 and the status changes to installed.

Please select a software package
from left menu and click
on install button

Figure 4-168 Software Delivery Center install status pane

8. Click **Exit** to close the Software Delivery Center client applet.

4.8.5 Installing a bundle

The client applet shows all bundles for which a particular user has access privileges. When the user selects a bundle, the client applet shows detailed data about it. If the bundle selected meets the user's needs, the user clicks the **Install** button. The install procedure starts automatically.

The following procedure describes how to install bundles from the Software Delivery Center client applet.

1. Launch the Software Delivery Center client applet from the IBM SDC Catalog icon or from the Software Delivery Center home page.
2. Click the **Bundles** tab. A list of available bundles such as that shown in Figure 4-169 appears.

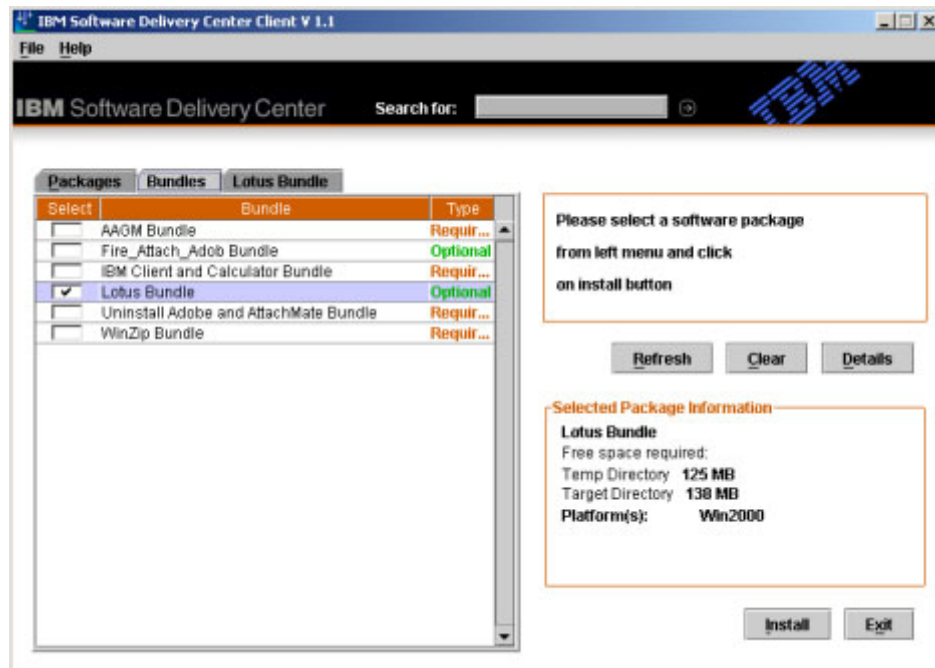


Figure 4-169 Software Delivery Center client applet bundle view

3. There are two types of bundle:
 - a. **Required:** This bundle has applications required for installation. All the applications in the required bundle are selected and must be installed.
 - b. **Optional:** This bundle has optional applications. An optional bundle allows individual packages to be selected for installation.
4. Select a bundle as shown in Figure 4-169. The bundle name appears on the third tab.
5. Click the tab with the bundle's name to view the list of applications included in a bundle (as shown in Figure 4-170 on page 400).

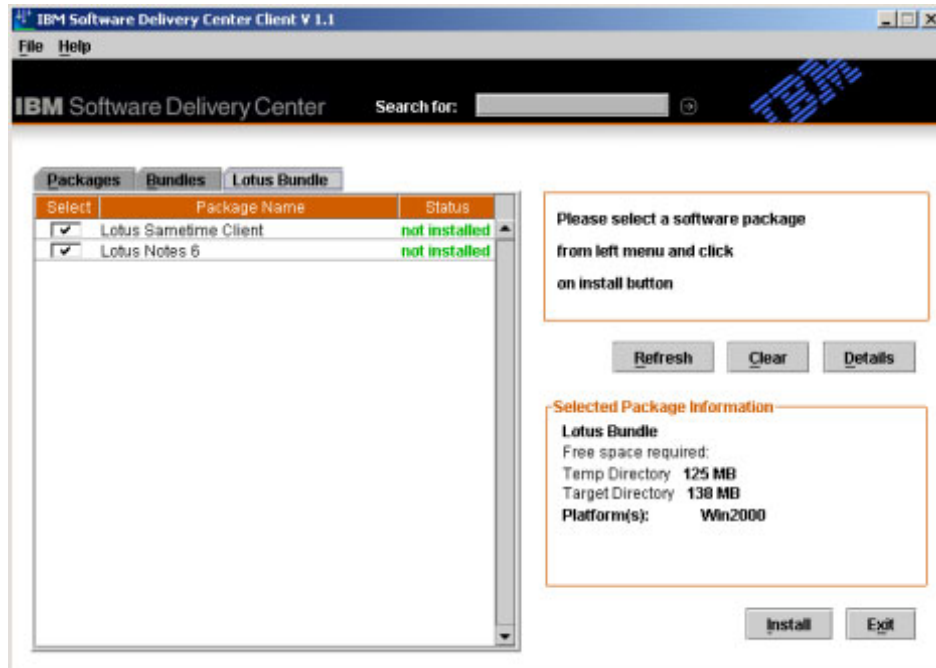


Figure 4-170 Software Delivery Center client applet list of applications in a bundle

Note: Multiple bundles can be selected using the check boxes provided.

6. To view application-specific information in a bundle, click the **Packages** tab, locate an application, and click **Details**.
7. Click **Install** to start the installation process for the selected bundle. The name of the bundle and application being installed appears (Figure 4-171).

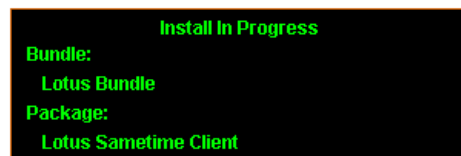


Figure 4-171 Software Delivery Center install in progress

8. The download window shown in Figure 4-172 on page 401 opens.
9. The application installation process begins after a successful download of the applications included in a bundle.

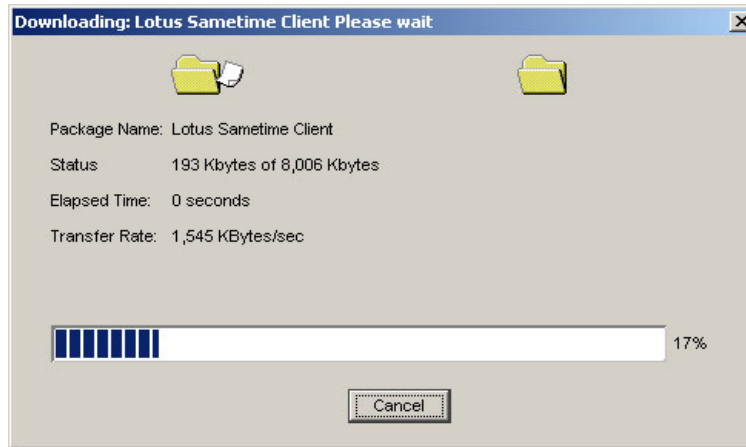


Figure 4-172 Software Delivery Center bundle download window

Note: End user intervention may be necessary to complete some installations.

10. Once the installation is complete, the Install In Progress panel shown in Figure 4-171 on page 400 returns to the original state shown in Figure 4-173.

Please select a software package
from left menu and click
on install button

Figure 4-173 Software Delivery Center installation status window

11. Click **Exit** to close the Software Delivery Center client applet.

4.9 Troubleshooting

This section describes troubleshooting methods for Software Delivery Center and includes the following topics:

- ▶ “IBM HTTP Server logs and manual” on page 402
- ▶ “Apache Tomcat logs and manual” on page 402
- ▶ “SDC Agent logs” on page 402
- ▶ “Controlling the Apache Tomcat service” on page 402

- ▶ “Enabling and disabling the client agent” on page 402
- ▶ “Setting up the Trusted Sites zone” on page 403

IBM HTTP Server logs and manual

IBM HTTP Server provides comprehensive and flexible logging capabilities that are very useful for troubleshooting Web site problems. These logs are located in the c:\IBM\SDC\IHS20\logs directory. In addition, you can view the IBM HTTP Server manual from the following Web site:

<http://www-306.ibm.com/software/webservers/httpservers/doc/v20/manual/>

Apache Tomcat logs and manual

The Apache Tomcat program also provides extensive logging capabilities that can be very useful for troubleshooting Web site problems. These logs are located in the C:\IBM\SDC\tomcat413\logs directory.

In addition, you can view the Apache Tomcat manual from the following Web site:

<http://jakarta.apache.org/tomcat/tomcat-4.1-doc/index.html>

SDC Agent logs

The Software Delivery Center agent logs events in the C:\Program Files\SDC\sdcagent.log file. If there are any errors related to the agent or the agent is not starting, review the contents of this file.

Controlling the Apache Tomcat service

To control the Apache Tomcat service, right-click **My Computer** and select **Manage**. Double-click **Services and Applications**, then double-click **Services**. Find Apache Tomcat in the list of services and select it. From the Actions menu, select the appropriate action.

Enabling and disabling the client agent

The Software Delivery Center client agent runs as a service. By default, it is set to start automatically when the operating system starts. You can change the start up type if needed as follows:

1. From your Windows desktop, click **Start**.
2. Click **Settings**.
3. Click **Control Panel**.
4. Double-click **Administrative Tools**.
5. Double-click **Services**.
6. Double-click **SDC agent**.
7. In the Startup Type field, select the startup type you want to use.
8. Click **OK**.

Setting up the Trusted Sites zone

If you encounter problems loading the Software Delivery Center administrator's console Web pages while running Windows XP with Service Pack 2, it may be necessary to add your Software Delivery Center server address to your Trusted Sites list as follows:

1. In Internet Explorer, select **Tools** → **Internet Options**.
2. Click the **Security** tab.
3. Click **Trusted sites**.
4. Click the **Sites...** button.
5. Clear the check box labeled Require server verification (https:) for all sites in this zone.
6. Type the server address in the Add this Web site to the zone: field.
7. Click **Add**.

Click **OK** and then load or reload the Software Delivery Center Administration Login panel.

4.10 Getting help and support

Software Delivery Center is supported by IBM. If you have a problem with Software Delivery Center or have questions about a specific feature, a variety of sources are available to help you. This section includes the following topics:

- ▶ “Using the documentation” on page 403
- ▶ “Using the help system” on page 404
- ▶ “Using the Web” on page 404
- ▶ “Contacting a IBM Software Delivery Center technical expert” on page 404
- ▶ “Obtaining support” on page 404

Using the documentation

Many problems can be solved without contacting IBM for assistance. If you experience a problem or have a question about the operation or functionality of Software Delivery Center, first review the *IBM Software Delivery Center Administrator's Guide*. You may access it as follows:

1. Click **Help** from the administrator's console
2. Click **Administrators Guide (PDF)**.

Using the help system

You can access the help system from the administrator's console. To access the help system, click the question mark (?) beside the field to obtain an explanation of that field.

Using the Web

The Software Delivery Center Web site provides the latest technical information and updates for download:

<http://www.ibm.com/pc/support/site.wss/document.do?Indocid=TVAN-SDC>

Contacting a IBM Software Delivery Center technical expert

Technical assistance for the IBM Software Delivery Center program is available from IBM. You can get support information from the following sources:

- ▶ From the Software Delivery Center Web site at:

<http://www.ibm.com/pc/support/site.wss/document.do?Indocid=TVAN-SDC>

- ▶ By telephone:

To get the telephone number for your country or region:

- a. Go to:

<http://www.ibm.com/pc/support>

- b. Click **Support phone list**.
- c. Click **ThinkVantage Technologies**.

Obtaining support

Charges for the IBM Software Delivery Center program apply as follows:

- ▶ Server code installed on IBM or non-IBM computers: All telephone support is provided on a fee-per-incident basis (regardless of the brand of computer on which the program is installed).
- ▶ Client code installed on IBM computers: During the first 30 days after the program has been installed, IBM provides free telephone support. After this period, telephone support is provided on a fee-per-incident basis.
- ▶ Client code installed on non-IBM computers: Telephone support is provided on a fee-per-incident basis.

The prices associated with fee-based support vary depending on your geographic location.



Access IBM

A major source of frustration for users of mobile and desktop computers is not having access to information, support, and utilities when needed. Information that is contained on the World Wide Web can be difficult to find and access, and hard copy information is frequently not carried by a mobile system. IBM is addressing this issue by equipping ThinkPad and ThinkCentre computers with a unique one-touch solution: Access IBM.

Access IBM can really be seen as a central location from where to access all tools, utilities and resources that IBM has to offer to help you learn about, set up, enhance, and protect your ThinkPad or ThinkCentre PC.

5.1 Overview

This chapter contains information and instructions about the new Access IBM experience: an updated help and support application for the Microsoft Windows operating system and Rescue and Recovery (a help, recovery, configuration, and diagnostic environment that can be opened even if Microsoft Windows cannot). In addition, with tools and instructions, various aspects of the applications (Access IBM, Access Help, Access IBM Message Center, and Rescue and Recovery) can be tailored to fit your in-house needs.

In this chapter we will discuss Access IBM V4.5. This version will be preloaded on all 2Q04 Thinkpads and ThinkCentres. Alternatively it can be downloaded from the web on:

<http://www.pc.ibm.com/us/think/thinkvantagetech/accessibm.html>

5.2 Access IBM

Access IBM is the window into IBM values provided with the system. Access IBM is displayed to the user when the blue **Access IBM** button is pressed, or the desktop icon is clicked. Access IBM makes available to the user information, services, and tools that are both local to the system (that is, available when the system is connected to the Internet or disconnected) and remote on IBM Internet sites.

When Access IBM is launched, the user is presented with a Welcome window to give a brief description of the five categories in the Access IBM user interface. See Figure 5-1.



Figure 5-1 Access IBM Welcome window

5.2.1 Access IBM user interface

In the tool bar header of Access IBM, there are five topics that categorize the information in the application. See Figure 5-2.



Figure 5-2 Access IBM topic toolbar

- **Learn**

This provides you with visual tour of your computer's hardware features.

- **Configure:**

You can use this to set up your system to run the way you want it and manage power, keyboard and pointing devices, connections, displays and other devices all from one place. It links you to operating system setup and configuration screens and gets you detailed system information including warranty and parts information.

- **Protect & Recover**

This option takes you through a series of windows that allow you to protect and backup your data with IBM Rescue and Recovery, secure your computer using passwords and antivirus software, diagnose problems and restore data.

- **Get Help & Support**

This option allows you to view on-system help and reference, find support information about the Web and update your computer with the latest device drivers.

- **Stay Current**

This provides solutions and options to keep your software and applications at the latest levels.

Access IBM provides the user an interface to the on-system user's guide, system tools, services, and to IBM Web sites on the Internet. The Access IBM interface also provides links to the Access Help, categorized to help the users find the information they are looking for more easily. At the top center is the Search field, which provides a keyword search into the Access Help Index. This Search capability provides a major advantage because a user can quickly find problem help or information.

5.2.2 Customizing Access IBM and Access Help

This section details the level of customization that can be achieved with both Access IBM and Access Help.

Advantages of customization

Access IBM and Access Help provide a powerful way for IBM customers to get help and information. Access IBM is started by pressing the blue Access IBM button that is prominently displayed on the ThinkPad keyboard, or by clicking the desktop icon, whenever the users need help or information about using their system. Access IBM then provides access to the Access Help, which contains information about using the IBM system, tools, and access to the IBM Internet Sites that provide updated information and help.

There are several different possibilities for customization of the Access IBM and Access Help products. Table 5-1 on page 410 shows the possibilities and advantages of each.

Table 5-1 Modification suggestion table

Option	Access IBM	Access Help	Advantage to the Business
Full Integration of Business information with IBM Help Information.	Modify topics of Access IBM to point to new or different information. Modify Web links of Access IBM to point to business specific Web sites.	Add new chapters and topics (HTML pages) to Access Help. Also some topics can be removed if they are not acceptable to business needs.	When a user presses the Access IBM button they will get information about there system as well as information about the business. The search field on the Access IBM interface will search system and business information. The Web links will point to business appropriate Web sites.
Access IBM integration with Access Help topic removal only.	Modify the sections of Access IBM to point to the remaining topics. Any unused categories can point to other programs or Web sites. Modify the Web links of Access IBM to point to business specific Web sites.	Remove topics that are not applicable or appropriate to the business environment.	When the user presses the Access IBM button they will get appropriate information about their system. The Search field on the Access IBM interface will search the remaining Access Help information. The Web links will point to business appropriate Web sites.
Access IBM integration with no Access Help changes.	Modify the Web link connections of the Access IBM interface to point to business specific Web sites.	No changes necessary.	The Web links will point to business specific Web sites, and the user will still have the power of the Access Help and the search capability

5.2.3 Customizing Access IBM

IBM provides many customization guides and tools that detail the process of customizing Access IBM and Access Help. The customization guide and tools can be downloaded from:

<http://www.ibm.com/pc/support/site.wss/AIBM-TOOLS.html>

These guides include the steps needed to customize the Access Help, and provide the Access IBM Customization tool that can be used to customize the Access IBM interface.

You can perform the following actions on elements of Access IBM using the Customization tool:

- ▶ Change the text in the Welcome window that opens when Access IBM is started
- ▶ Change the five category names at the top of the interface
- ▶ Change the Web links within Access IBM
- ▶ Change the text associated with the Web links
- ▶ Password protect the application so only an administrator can enable use of Access IBM
- ▶ Change user interface fonts and colors
- ▶ Change the color of the background for the Access IBM application
- ▶ Enable or disable application sounds and animations
- ▶ Change the “Alt-key” Quick launch keys for the five main topics
- ▶ Add and delete content in the interface at will so links to your company’s most important information and tools are easily accessed through the interface

5.2.4 Access IBM Customization Tool

The Access IBM Customization tool is offered by IBM to help in modifying Access IBM so as to better meet the customers’ company environment. This tool makes the task of modification easier for a system administrator to manage for the company systems. Changes can be made to one system and broadcast to other systems controlled by an administrator. Figure 5-3 on page 412 shows the Company tab of the Access IBM Customization Tool.

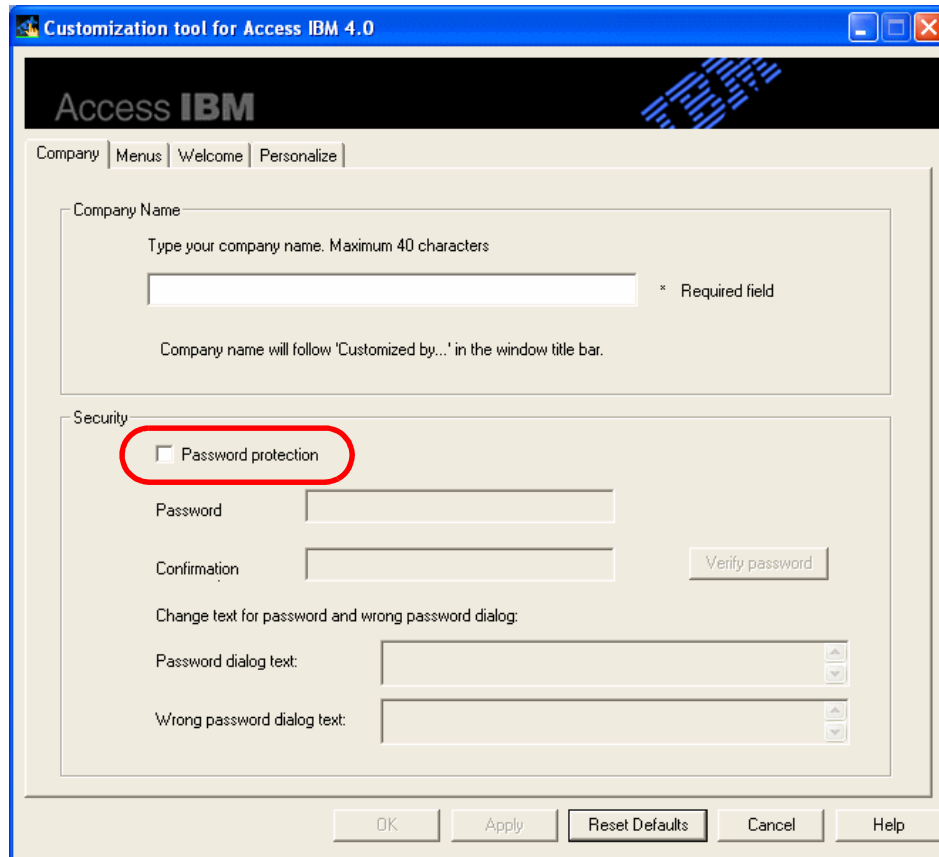


Figure 5-3 Access IBM Customization Tool - Company tab

In this tab, you can modify the name that will be displayed in the title bar of the Access IBM application. The title bar will display for example:

Access IBM Customized by ABC Company

If you would like to have the Access IBM application on the system, but not have the user access the application without a valid password, you can do this from the Access IBM Customization tool.

1. To password protect Access IBM, select **Password protection** and enter your chosen password in the Password field and the Confirmation field.
2. Click **Verify password** to set your password.

If password protection is enabled, the IT engineer can enter special instructions for the user in the Password dialog text field. This provides your message in a window when the user executes the Access IBM program. You can also

customize the Wrong password dialog text field by entering your custom message here. This will be included in a window if an invalid password is entered when prompted. Click **OK** when finished.

The **Menus** tab allows the editor to change which Access Help topics, Web links, and application links are displayed on the Access IBM user interface. This is very useful to modify existing links or adding company specific menu items.

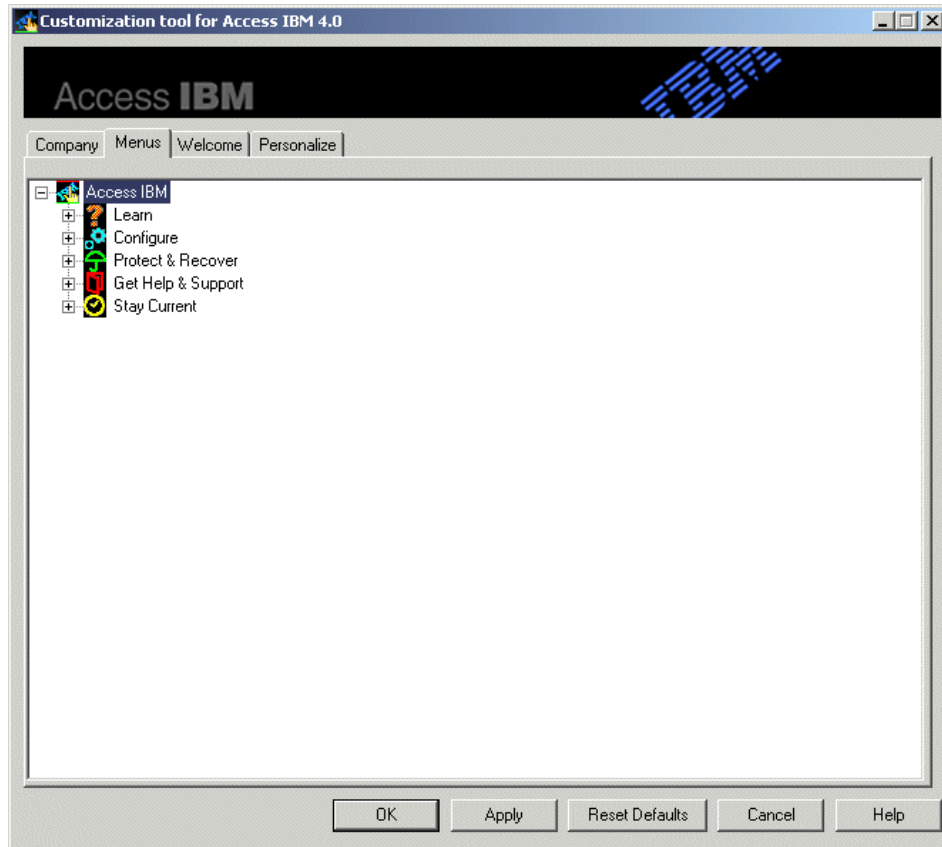


Figure 5-4 Menu window

To create new menu items:

1. Right-click the main title menu that you wish your item to appear under. For example the Learn section.
2. Select **New Submenu**.

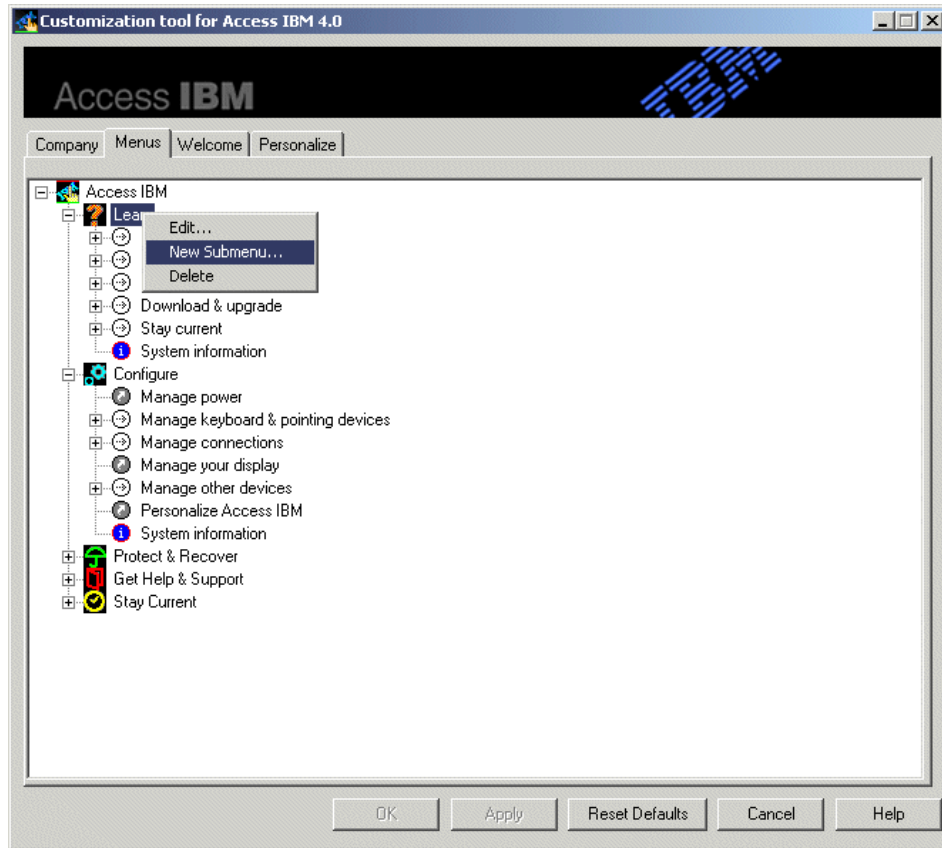


Figure 5-5 Adding new Submenu window

3. Enter your new Submenu's specific properties

- Select the Type of item you wish to create such as an application link, Help, or Internet Link.
- Enter the Title for your new menu item. This will be shown in the Access IBM application.
- Enter your launch link for your menu item. This can be the executable, an application menu item, a web address or a link to an existing help menu. A .chm file for example.
- Enter the Description of your new Menu item.

The example shown in Figure 5-6 on page 415 shows the information for creating a new submenu item for a fictitious company Web site.

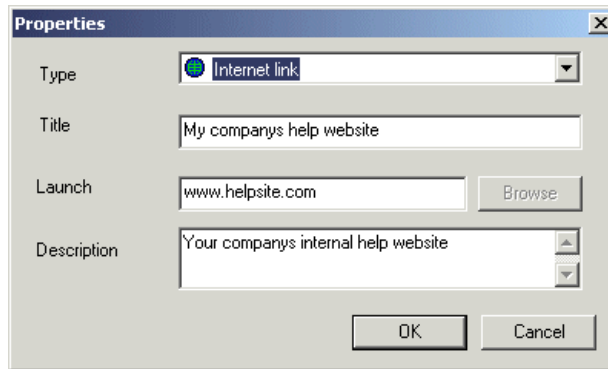


Figure 5-6 Submenu item properties

4. Click **OK** when you have entered all your information. This will add the new item to the Access IBM menu structure.

You can also Edit or Delete existing menu items using this same procedure.

1. To Edit an existing submenu item:
 - Right-click the item you wish to edit
 - Edit the properties window as required
2. To Delete an existing submenu item:
 - Right-click the item you wish to delete
 - Select **Delete**

This interface makes it easy for the IT engineer to modify the Access IBM configuration files that contain the user interface information. The output of the configuration data is stored in three files:

- ▶ machine-specifics.csv
- ▶ access-config.ini
- ▶ access-text.ini

These files can be edited manually. The machine-specifics.csv file can also be modified by using a spreadsheet program such as Microsoft Excel. However, the custom changes are more easily accomplished using the Customization tool. Once you have made your custom configuration settings, the three files can be copied to a target computer or group of computers for configuration settings distribution.

The Welcome tab shown in Figure 5-7 enables you to modify the content of the welcome page that is displayed to the user upon starting Access IBM. This would need to be done if you change the categories in the Access IBM user interface. The welcome page can be enabled or disabled from this window by selecting **Show welcome screen**.

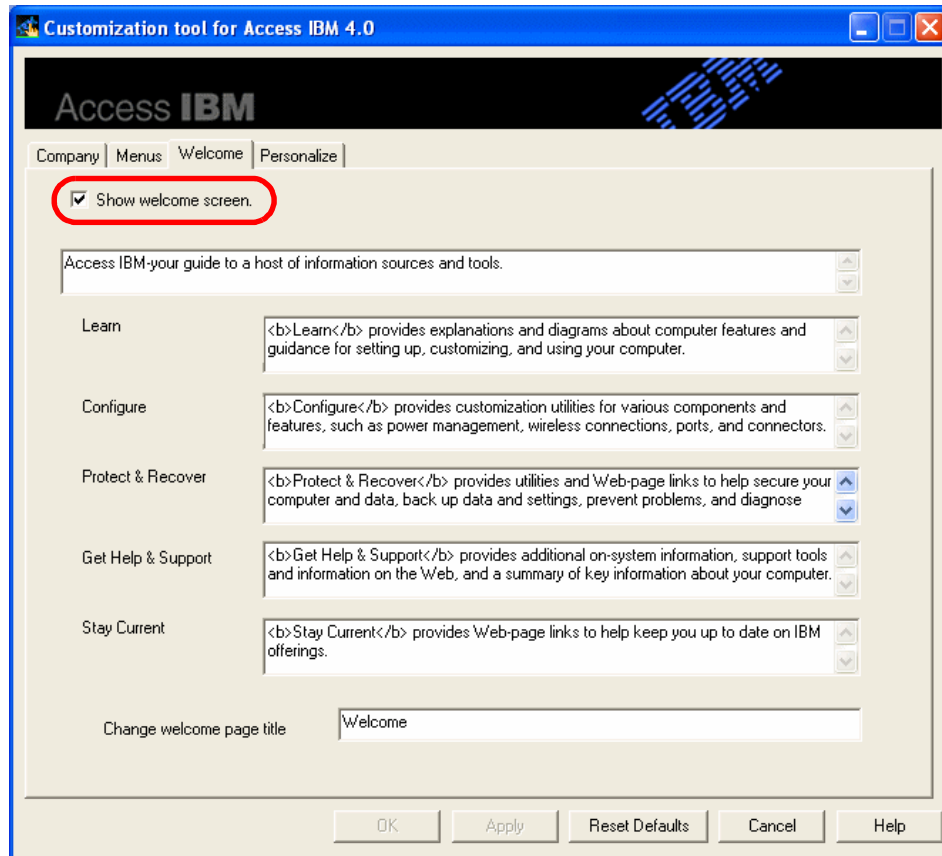


Figure 5-7 Access IBM Customization Tool - Welcome tab

The Personalization tab (see Figure 5-8) allows you to modify the default size of Access IBM when it is started. The size can be set to large for high-resolution screens, low for lower resolution screens, or automatic, which will let Access IBM choose depending on the system settings.

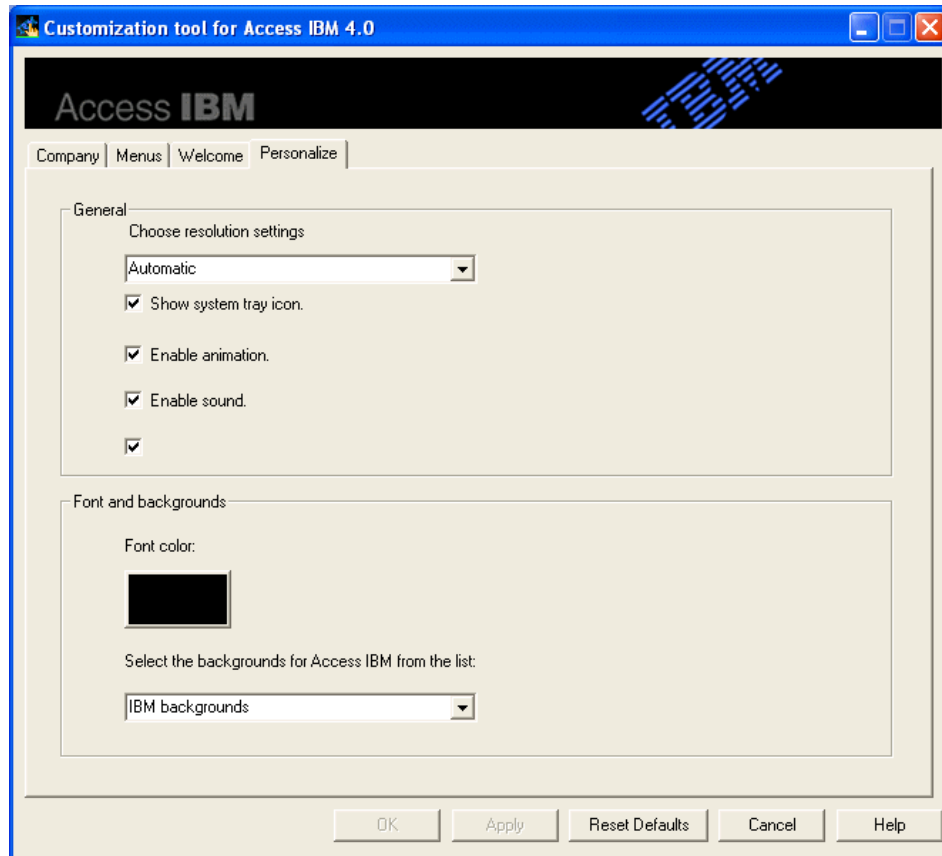


Figure 5-8 Access IBM Customization Tool - Personalization tab

You can choose whether to display the Access IBM Message Center icon in the task tray with the *Show system tray icon* option. When this box is unchecked, the user will not receive informative pop-up messages from Access IBM.

The next two check boxes enable the opening animation and startup sound for Access IBM. You may choose to disable these here or from the Access IBM personalization dialog.

Using the font color and background modification, you can make it easier for the user to read the information about the Access IBM user interface. Only the default pictures, a black or a white background are supported at this time.

5.3 Access Help

The Access Help is an online documentation system that provides hardware, software, and support information and help to the end user. Access Help is based on the Microsoft HTML Help engine included with Microsoft Windows, and therefore can use the power of the Internet browser to bring excellent content to the user, including:

- ▶ HTML-based content pages containing information about the hardware and software that is part of the ThinkPad product
- ▶ Hyperlinks to other topics included in the text
- ▶ Related topics links in topics
- ▶ Animations using Macromedia Flash and Shockwave technology to bring the user's understanding beyond what simple words and pictures can show
- ▶ Links to start software programs that are described as part of the content
- ▶ A visual map of the system to point out key features of the hardware

Note: See the *Access Help Customization Guide* for more information about modifying Access Help. The Access Help Customization Guide and tools are available at:

<http://www.ibm.com/pc/support/site.wss/MIGR-46027.html>

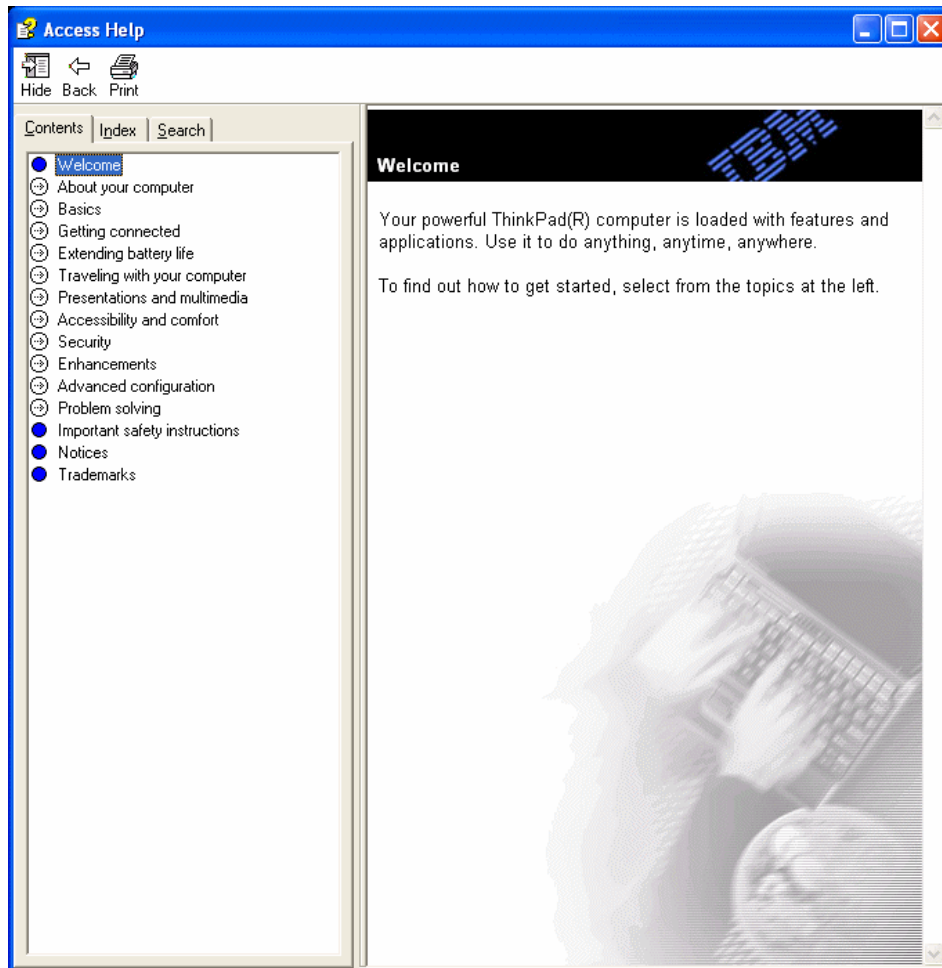


Figure 5-9 Access Help

Figure 5-9 shows an example of the Access Help interface. Shown in the figure is the main Welcome page. The entire online help document is broken up into topics; some major topics are shown in the above figure.

5.3.1 Customizing Access Help

The Access Help is compiled to run as an HTML Help System using the Macromedia RoboHelp HTML Edition product. More information about this product can be found at this Web site:

<http://www.macromedia.com/software/robohelp/>

You may also find information at the Microsoft HTML Help Workshop Web site:

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/htmlhelp/html/vsconwhtshw.asp>

Using these tools and an HTML editor, the Access Help can be readily customized. The Access Help customization guide will provide assistance and guidelines to help with editing.

5.4 Rescue and Recovery

Rescue and Recovery is a pre-OS environment. This means you can still access it, even if you are no longer able to boot into your Windows environment. It is an IBM developed environment based on industry-standard technology that supports both legacy and non-IBM platforms.

Rescue and Recovery is accessed by pressing the blue Access IBM button or by pressing the Enter key to interrupt the boot.

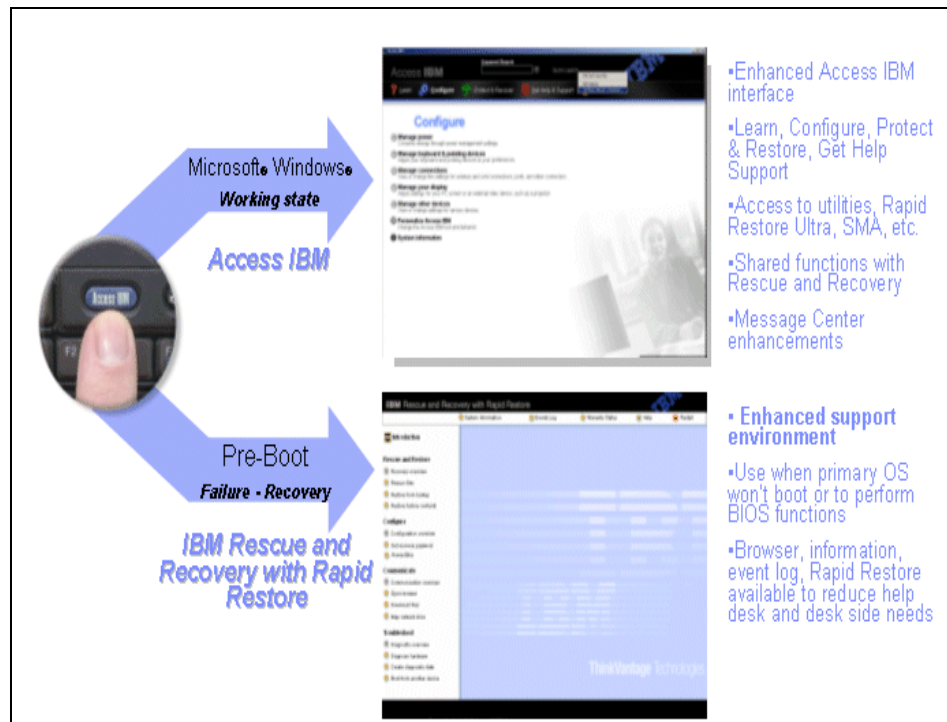


Figure 5-10 Accessing Rescue and Recovery

The Rescue and Recovery environment gives you access to a whole range of pre-boot tools:

- ▶ Rescue and Recovery
- ▶ Factory Recovery (Disk to Disk)
- ▶ PC Doctor
- ▶ F1/F12 (BIOS setup/Boot from alternative device)
- ▶ System Information
- ▶ Browser
- ▶ Comprehensive help system
- ▶ Events log
- ▶ Warranty/FRU info

The entire environment is customizable. Functions can be hidden, changed, and password protected.

Note: IBM Rescue and Recovery is covered extensively in Chapter 2, “Rescue and Recovery” on page 11.

5.5 Access IBM Message Center

The Access IBM Message Center is designed to deliver relevant, system-specific notifications to a user. These messages might be pre-installed on the computer by IBM (local messages), delivered through Access Support from IBM (Web messages), or added to the Message Center later by an IT department or system administrator. The Access IBM Message Center delivers important information about software installed on the computer and about device driver updates. Only messages that apply to the recipient’s computer model are displayed.

The Access IBM Message Center program icon resides in the system tray and, when a new message is broadcast, brings up a bubble display to get the attention of the user. Any program can deliver a message through the Message Center as long as the message adheres to the guidelines presented in this section. To open the Message Center, double-click the Message Center icon shown in Figure 5-11.

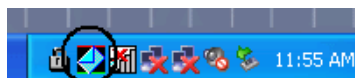


Figure 5-11 Access IBM Message Center icon

If there are any messages, they are displayed as shown in Figure 5-12 on page 422. Otherwise, the Message Center is blank.

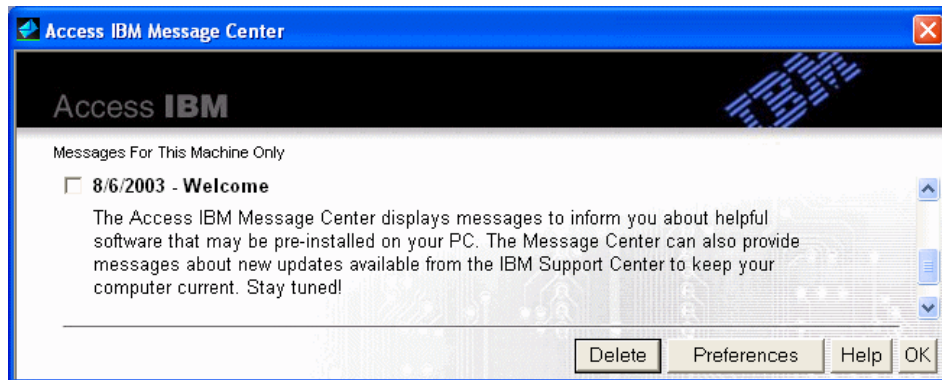


Figure 5-12 Message Center

When the icon in the system tray is clicked, a menu is displayed enabling the user to launch Access IBM programs, to view the Message Center, to hide the Access IBM bubble messages, or to exit the Message Center. When a message becomes available, the Message Center alerts the user with a pop-up bubble that displays the title of the new message. The icon in the system tray also changes color to indicate that a new message is available. On systems running Windows XP, the Message Center opens when the bubble is clicked. On systems running Windows 2000, the bubble message is minimized when the bubble is clicked.

5.5.1 Local messages versus Web messages

The Access IBM Message Center delivers two types of messages in the pre-installed environment:

- ▶ The first type is the local message. Local messages are pre-installed on the computer and programmed to display when certain events occur. For example, one message that might get delivered locally is a message reminding the user to use Access IBM. But this message is only delivered if Access IBM is installed on the computer, and it has not been opened two days after the computer is initially used. There are six local messages in the current implementation, but that could change at any time. Local messages do not require an Internet connection.
- ▶ Web messages are delivered through a program called Access Support. To get Web messages, Access Support must be enabled. To enable Access Support, simply click **Preferences** in the Message Center. Figure 5-13 on page 423 illustrates what the Preferences window will look like if Access Support is installed.

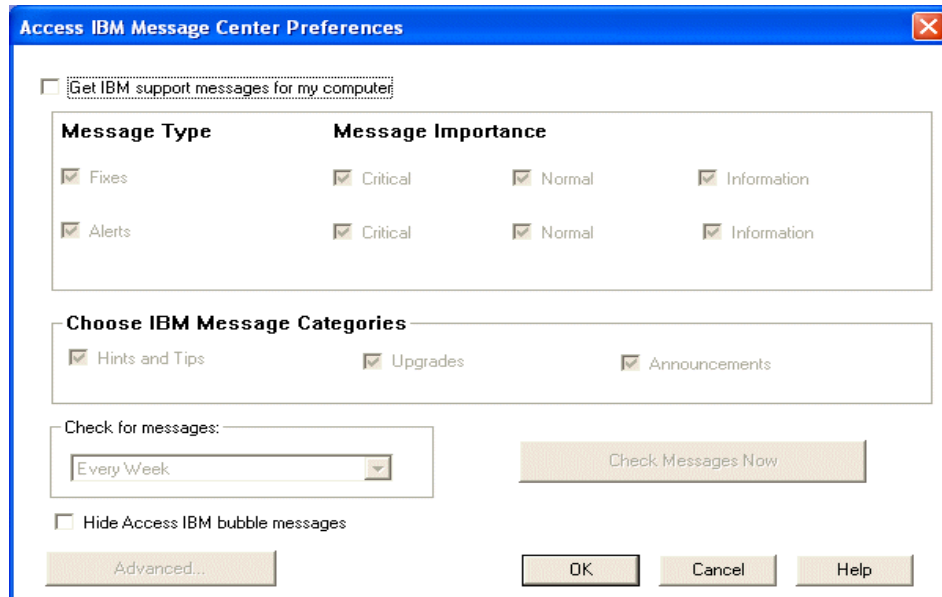


Figure 5-13 Preferences window

Select **Get IBM support messages for my computer** to get Web messages. Web messages enable IBM to inform users of useful information that is becoming available. The Message Center automatically filters these messages so that only those messages that apply to your particular machine type and operating system are displayed. For example, a Web message might inform the user that a new device driver is available for their particular machine type. This message will display automatically if Web messages are enabled.

Web messages can also be expanded to include messages about all IBM computers models and operating systems. When you select **Get IBM support messages for my computer**, the Advanced button is enabled. Click the **Advanced** button to get messages for other computer models and operating systems. The Advanced Messaging Preferences window is shown in Figure 5-14 on page 424.

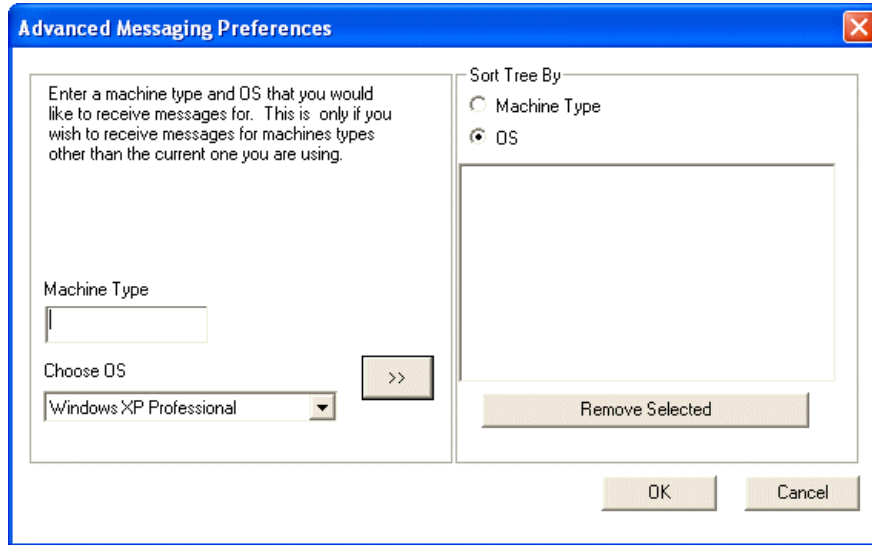


Figure 5-14 Advanced preferences

5.5.2 What a message file contains

The following is an example of what an XML message file might look like.

Example 5-1 Sample XML file

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<message id="aconn.xml">
<title>Manage all your connections simply!</title>
<body>Configure multiple network connections and easily switch between them.
Gain ultimate PC freedom with the latest in wireless networking.</body>
<category>Wireless</category>
<version>1.0</version>
<language>English</language>
<locale>AU</locale>
<machines>all</machines>
<launch1>
  <text>Start Now</text>
  <app>aibmrun.exe</app>
  <param1>'IBM Access Connections'</param1>
</launch1>
</message>
```

Table 5-2 on page 425 lists the elements that each Message Center message XML file might contain.

The `<?xml version="1.0" encoding="utf-8" standalone="yes"?>` line should always be at the top of the file. If other languages are used, then the encoding might need to change, but utf-8 should be used otherwise. Every message must be enclosed in the `< message id= "" >` element and have a unique ID, which is the same as the file name.

Table 5-2 XML message file elements

Element	Required	Contents	Example
version	No	Version of the Access IBM Message Centre	1.0
title	Yes	Title of the message	let Access IBM Simplify Your PC Experience
body	yes	Main text of the message	Learn Useful PC Tasks. Click Start now or press the Blue Access IBM Button anytime
date_received	No	Date of the message in MM/DD/YYYY format. If left blank, it will fill in with the current date.	08/06/2003
date_expired	No	Date the message expires in MM/DD/YYYY format. The message is deleted after this date.	09/06/2003
url	No	The URL of the Web site to present to the user	www.ibm.com
category	No	The message category	Driver Update
language	No	The message language	EN
locale	No	The message locale	AU
source	No	Program that generated the file	Access Support

Element	Required	Contents	Example
machines	Yes	This is the four-digit machine type number(s) that this message applies to. If there are multiple machine types, a comma separates the numbers. If every machine is involved, it can be all . The default should be all .	2653,2373
launch1	No	Inside of this element are the next three elements.	<pre><launch1> <app>c:\windows\n otepad.exe</app> <text>Notepad</tex t> <param1>c:\filetoo pen.txt</para,> </launch1></pre>
launch1 app	Yes, if a launch1	This is the path to the executable file that will be launched.	c:\windows\notepad.exe
launch1 text	Yes, if a launch1	Text to display to the user at launch, such as the application name	Notepad
launch1 param1	No	Parameter to pass to the application	c:\filetoopen.txt
launch2	No	Inside of this element are the next three elements.	<pre><launch2> <app>c:\windows\n otepad.exe</app> <text>Notepad</tex t> <param1>c:\filetoo pen.txt</para,> </launch2></pre>
launch2 app	Yes, if a launch2	This is the path to the executable file that will be launched.	c:\windows\notepad.exe
launch2 text	Yes, if a launch2	Text to display to the user at launch, such as the application name	Notepad

Element	Required	Contents	Example
launch2 param1	No	Parameter to pass to the application	c:\filetoopen.txt
launch3	No	Inside of this element are the next three elements.	<pre><launch3> <app>c:\windows\n otepad.exe</app> <text>Notepad</tex t> <param1>c:\filetoo pen.txt</para,> </launch3></pre>
launch3 app	Yes, if a launch3	This is the path to the executable file that will be launched.	c:\windows\notepad.exe
launch3 text	Yes, if a launch3	Text to display to the user at launch, such as the application name	Notepad
launch3 param1	No	Parameter to pass to the application	c:\filetoopen.txt

5.5.3 Delivering messages of your own

To use the Access IBM Message Center to deliver messages of your own, you must set up a client-server application so that every computer that will receive messages is linked as a client to the server application that will post the messages. This could be a simple client-server application where a client residing on the recipient system queries the server at given intervals for any available messages. You can use sockets or an HTTP protocol to accomplish this. The key is to deliver the message to the correct directory, and in the appropriate format.

To have a message display in the Access IBM Message Center, the message must be placed in the c:\documents and settings\all users\application data\ibm\messages\ directory. This directory changes for other languages and, in rare circumstances, for Microsoft Windows 2000 and XP. This folder is used because it is the *common application folder* and any user can write to it or read from it. This folder is stored in the path in the registry under the following key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\CommonAppData.

This key refers to the path c:\documents and settings\all users\application data only, but by simply appending the key with \ibm\messages\ the full path to the

message directory is provided. After a client-server application has been set up, the Access IBM Message Center will display local messages, Web messages, and customer messages, as illustrated in Figure 5-15.

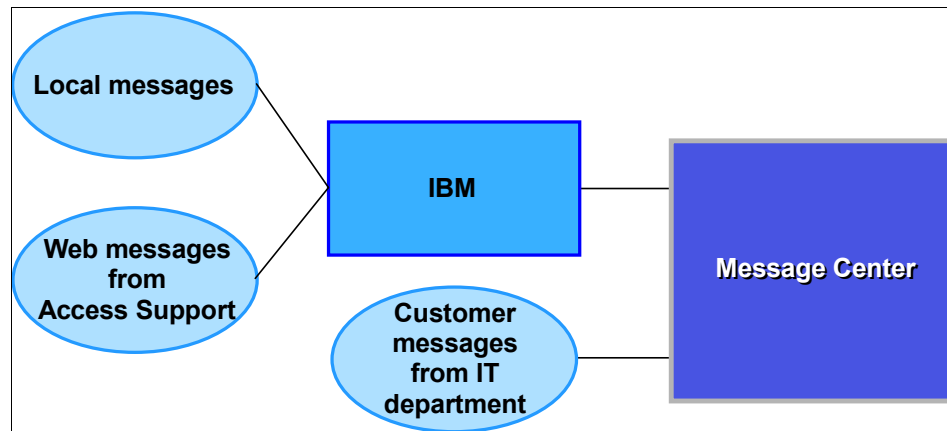


Figure 5-15 Customer message flow

After an XML message file is placed in the appropriate directory, it might take as many as 30 seconds for the Message Center to respond to it, if the Message Center is running. The typical response is a bubble message that pops up and that contains the title of the message. However, if a bubble has popped up in the past hour, the Message Center responds by changing the Message Center system tray icon and by adding flyover text to note that a new message is available. In this way, users are not distracted by too many pop-up messages.

If an XML message is placed in the appropriate directory and the Message Center does not respond at all, then either the XML file is incorrect or the message guidelines were not followed. To verify that the XML file is correct, open it with Microsoft Internet Explorer. The Message Center uses the same XML parser as Internet Explorer, so if the Internet Explorer can read the file, the Message Center can read it too. Figure 5-16 on page 429 illustrates how Microsoft Internet Explorer displays an XML file.

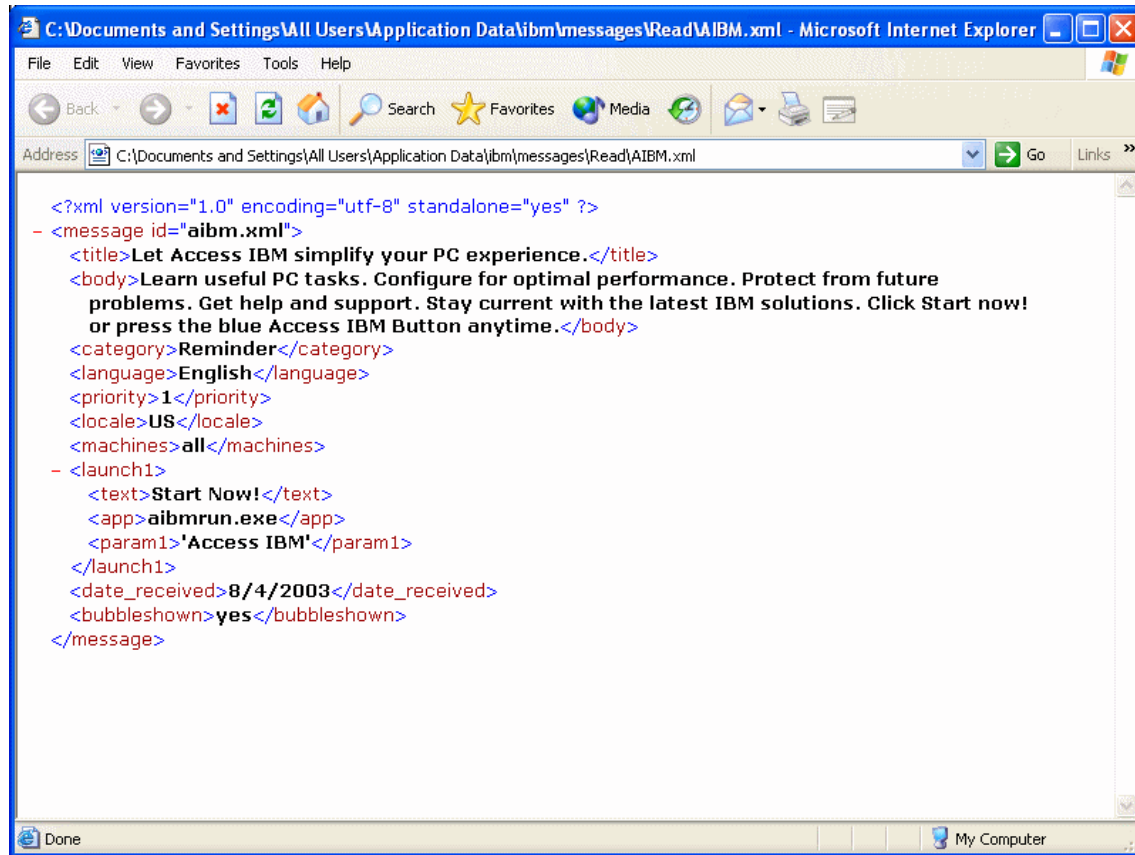


Figure 5-16 XML message in Explorer

After the Message Center has opened and new messages have been displayed, these messages are considered read. They are then moved to the Read directory in the c:\documents and settings\all users\IBM\messages\read path.

5.6 Update Connector

IBM Update Connector is an easy-to-use electronic delivery mechanism that allows you to conveniently download software programs and software updates over the Internet.

5.6.1 Overview

Update Connector is a software program that downloads device driver updates, BIOS updates, data updates, other software programs, and software updates from an IBM server directly from the Internet. The user does not require any specific knowledge of where updates are located or which updates are needed by the user's system.

The user only needs to start Update Connector on his or her system to be connected to the Update Connector database on IBM Universal Content Server. Once connected, Update Connector automatically determines whether the system needs available updates and, if so, downloads and installs them at the user's option. Update Connector automatically recognizes machine types and models as well as software versions and other criteria when figuring which updates to download.

This electronic delivery mechanism directs you to updates of interest without your having to first place a telephone call to IBM PC Help Center. If you know of an update that is due, suspect that some portion of your software is not functioning as designed or know a bug fix has been announced, a quick connection over the Internet using Update Connector to Universal Content Server will validate the condition and, if an update is available, the update can be automatically downloaded and installed on your system right then, preempting further diagnostic procedures.

Update Connector frees you from having to explain your problem to an intermediary, from having to locate where in the network a desired update is stored and from the intricacies of how to download and install selected updates. Update Connector automatically connects you to the appropriate server, figures out what is needed and proceeds to download and install updates on your system with minimal intervention required.

In addition to providing an easy way to find updates that are required by your specific system or set of systems, Update Connector provides a way for you to download updates for machines you specify, even if they do not currently need the update. You can do this using the Multiple File Download (MFD) capability built in to Update Connector 6. You can define a local repository and then use MFD to populate the local repository with the updates you would like to have available. Systems running Update Connector 6 can be told to use the local repository rather than the Universal Content Server to search for updates. This allows you to control which updates systems can find because you can decide which updates to place on the local repository.

5.6.2 Usage Scenarios

Usage scenarios can be broken into the following categories:

- ▶ Individual (self-managed) usage - Self-managed Mode
- ▶ Centrally managed usage - SMB LAN Mode

Customers can run Update Connector in self-managed mode or in centrally managed mode. In either mode they can obtain updates from a local repository or from the IBM server.

Individual (Self-managed) usage

In Self-managed Mode, users can manage their own systems with Update Connector. They can do this in several ways.

One way that the you can use Update Connector in Self-managed Mode is to set a periodic schedule for running Update Connector whenever a user logs on to the Windows operating system as an administrator. If you have set a periodic schedule for running Update Connector each time a log-on to Windows occurs a piece of stub code is executed to determine if the user logging on has administrator privileges. If they do have administrator privileges and if Update Connector needs to be run based on the periodic scheduler setting then the stub code will start Update Connector and Update Connector will run to check for updates. If there is no need to start Update Connector, the stub code will not start Update Connector and the stub code will cease execution. In this mode, no GUI is shown to the user unless updates are located that are needed by the user's machine. If appropriate updates are found a message will be displayed informing the user that updates are available. If the user decides to install the updates, a pick list of all updates is shown to the user. The user can then elect to download and install the updates desired.

Another way you can use Update Connector in Self-managed Mode is to start Update Connector directly. When the user starts Update Connector directly they can either use the MFD mode or they can obtain and install updates.

If the user is obtaining and installing updates they may elect to use the IBM server as the repository from which to obtain updates or they can select a local repository. The user is presented with a pick list of applicable updates and the user can chose which to download and install.

Using the MFD support, users can enter:

- ▶ A machine type and model number or set of machine types
- ▶ Operating system name for each machine type (or any if they want all operating systems)

- ▶ Operating system national language (such as English or French) for each machine type (or any if they want updates for all national languages for a specific machine type and operating system)
- ▶ Local repository to which they would like to have updates downloaded

The user is presented with a list of XML based updates they can download. They can select the ones they want to download and the selected updates are downloaded to the designated location. These updates can be used for image building. The user may want to use these updates for updating deployed systems. They can do this by using Update Connector to obtain and install updates from the updates downloaded by the MFD capability.

Centrally managed (SMB LAN Mode) usage

Update Connector can be run in centrally managed mode (SMB LAN mode). In this mode, an administrator manages all other participating systems. The administrator can go to any participating system and start the administrator console. Once in the administrator console the administrator can use either the MFD support or they can manage updates for various participating systems on the local LAN segment. Updates can be obtained from the IBM UCS or they can be obtained from a local repository. For an in-depth discussion of how centrally managed mode works see 5.6.3, “The network connection” on page 432.

Using the MFD support, users can enter:

- ▶ A machine type and model number or set of machine types
- ▶ Operating system name for each machine type (or any if they want all operating systems)
- ▶ Operating system national language (such as English or French) for each machine type (or any if they want updates for all national languages for a specific machine type and operating system)
- ▶ Local repository to which they would like to have updates downloaded

The user is presented with a list of XML based updates they can download. They can select the ones they want to download and the selected updates are downloaded to the designated location. These updates can be used for image building. The user may want to use these updates for updating deployed systems. They can do this by using Update Connector to obtain and install updates from the updates downloaded by the MFD capability.

5.6.3 The network connection

When you start Update Connector, the client portion of Update Connector attaches the client system over the Internet to the Universal Content Server. The

connection can be made using TCP/IP over a local area network (LAN), through a firewall with Proxy or Socks, through a TCP/IP broadband connection, or through a TCP/IP dial-up connection to an Internet service provider (ISP). Update Connector 6 supports Basic Authenticating Proxy and Microsoft® Challenge/Response (NTLM) Authenticating Proxy as well as autoproxy.

In Self-managed Mode, as soon as the client portion of Update Connector has established a connection to Universal Content Server, an application called the System Recognizer is downloaded to your computer. The System Recognizer collects various data, for example, BIOS level, hardware type, preload level, etc., and, with your approval, passes the data to IBM Universal Content Server. Universal Content Server uses this information to determine which updates might be needed for your computer. Next, for each candidate update, either a Java Update Recognizer or an XML descriptor file is downloaded to your machine. Java Update Recognizers are used by older updates. Newer updates use XML descriptor files. Update Connector determines whether the update is a Java Update Recognizer-based update or an XML-based update. If the update is a Java Update Recognizer-based update, the Java application is executed to determine if its specific update is required and, if so, the update is added to the list of updates to be downloaded. If the update is an XML-based update, Update Connector checks the rules defined in the XML against the data discovered by the system recognizer and determines if the conditions on the target system match the conditions specified in the XML descriptor file. If they do meet the applicability criteria the update is added to the list of updates to be downloaded.

The process of determining the system attributes and determining the appropriate updates is known as *Discovery*. When a list of applicable updates has been determined, it is presented to you so you can choose either a subset or the entire list of updates for FTP downloading at that time. Each update can provide readme information (in HTML) to describe the update and to help you select which updates to download and install. You can install updates as soon as they are downloaded or install them later. You can view a history of previous Update Connector activity from the main status window. An installed update can be uninstalled prior to running Update Connector again if the update was designed to be uninstallable.

In SMB LAN Mode, every time a system is started, that portion of the Discovery process that determines the system attributes is run and the discovered information is saved in a central file on the user's LAN that is accessible from the Administrator Console. The administrator can run Discovery manually or schedule it for a future time period. The administrator can also determine, either manually or scheduled for a future time, the updates that are applicable for a system or a set of systems. Having determined the updates that are applicable the administrator can decide which updates to download and install on a specific machine or set of machines and can either do that manually or schedule it for a

future time. Updates can be downloaded and installed or just downloaded and then later installed and either activity can be done manually or scheduled. Lastly, the administrator can determine to switch a machine from SMB LAN Mode back to Self-managed Mode if desired.

Regardless of which mode you are running in, you can use the MFD support to build a local repository and you can select which local repository to set active. You can have Update Connector search for updates on the local repository or on Universal Content Server.

In Self-managed Mode you can set a periodic scheduler to check for updates in the background whenever a user signs on to the Windows operating system as an administrator.

Update Connector technology thus consists of client code linked to a desktop icon or Windows Start Menu item, an FTP server that stores all current updates as well as their Update Recognizers and XML descriptors and a Universal Content Server that scans systems calling in for updating. Universal Content Server also contains databases that are used to determine eligibility for using Update Connector and information about each update.

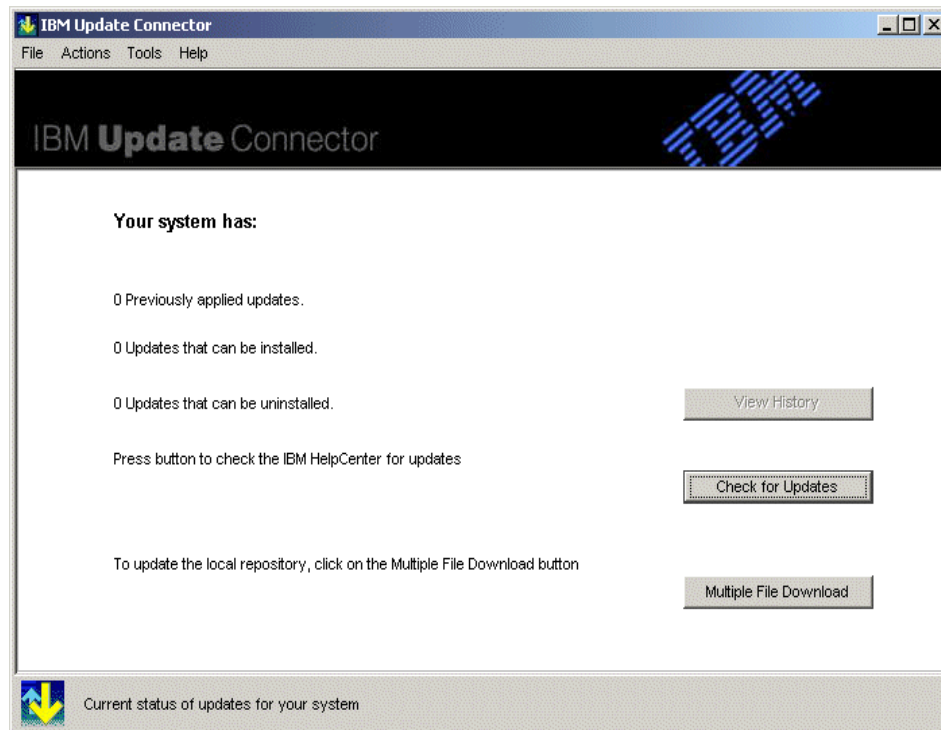


Figure 5-17 Update Connector main window

Update Connector can be run in either a **Self-managed Mode** or **SMB LAN Mode**. When you start Update Connector for the first time it starts in Self-managed Mode. You can switch Update Connector to SMB LAN Mode (Centrally-managed Mode).

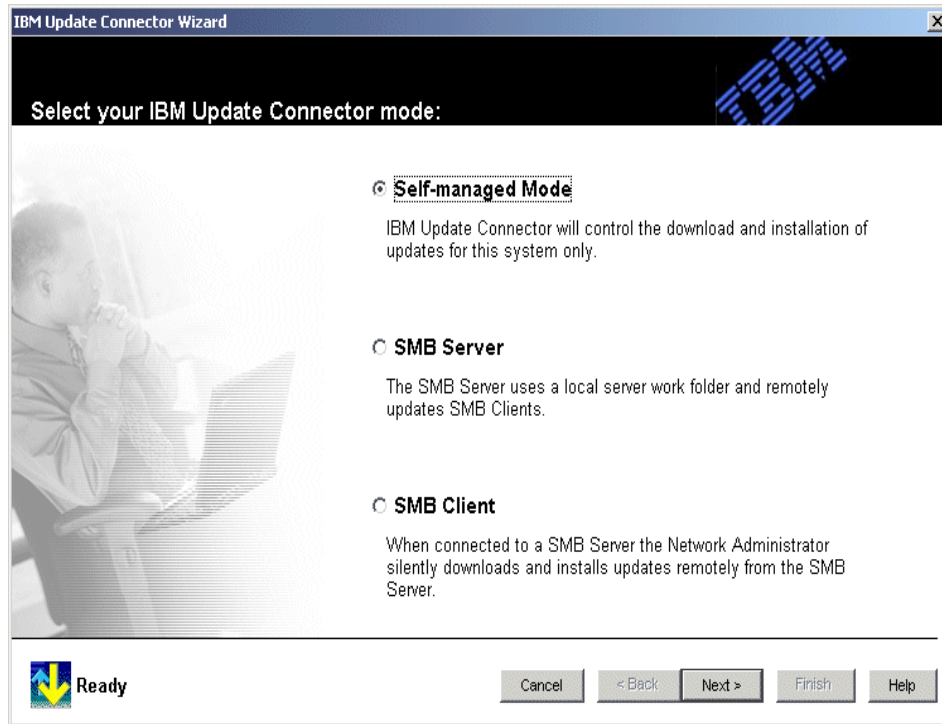


Figure 5-18 Update Connector mode selection

5.6.4 Self-managed Mode

Self-managed Mode (SM Mode) is where you control the download and installation of the updates for your own system. Update Connector installs in Self-managed Mode.

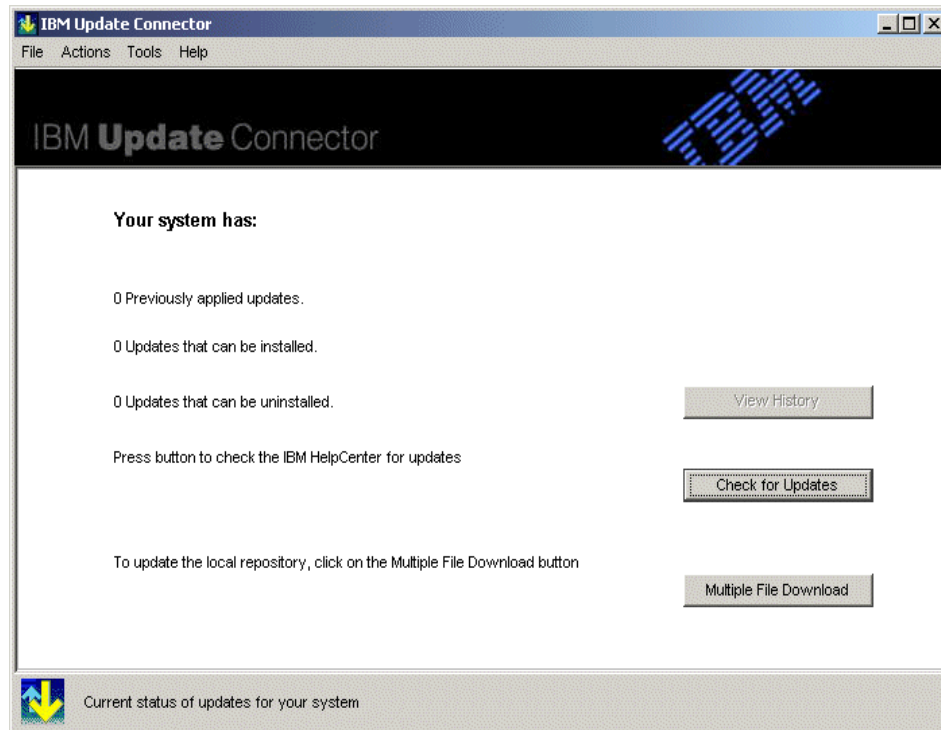


Figure 5-19 Update Connector self manage mode

5.6.5 SMB LAN Mode

This includes the following:

- ▶ **SMB Server**

The SMB Server uses a local server work folder and remotely updates SMB clients

- ▶ **SMB Client**

When connected to a SMB server the Network Administrator silently downloads and installs updates remotely from the SMB Server.

SMB LAN Mode is a centrally managed mode where an administrator manages the updates for a set of systems that are participating in SMB LAN Mode on the same LAN segment. You can have some systems on the LAN segment self-managed and others can be centrally-managed. To have a system participate in SMB LAN mode you must start Update Connector in Self-managed Mode on that system and then use the Mode Wizard under the Tools pull-down

on the Menu bar to set Update Connector to run as either a *SMB Server* or a *SMB Client*. The first system you set to participate should be the SMB Server.

Configuring an SMB Server

To set up a UC network, you should first set up an SMB Server. Use the Mode Wizard and select **SMB Server**.

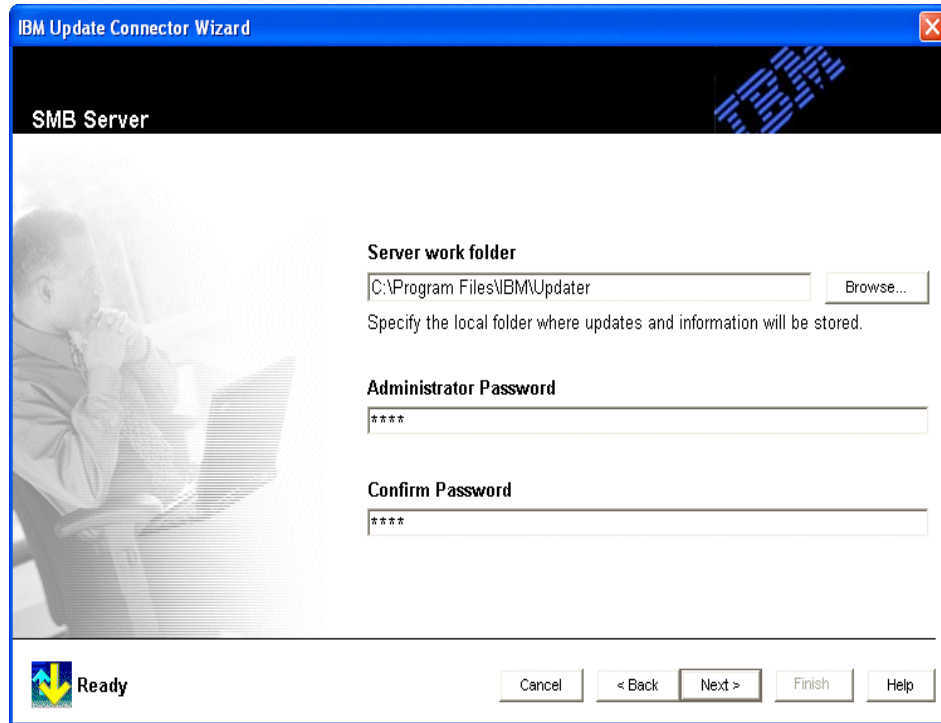


Figure 5-20 SMB server configuration

You need to provide some details:

- **Server workforce**

The path to the Server workforce, this is where the updates will be stored.

- **Administrator password**

Enter a password that the SMB Clients will use to connect to the SMB Server.

Configuring an SMB Client

Once you have an SMB Server on your network, you can then go on to configure the SMB Client systems. Use the Mode Wizard to select SMB Client.

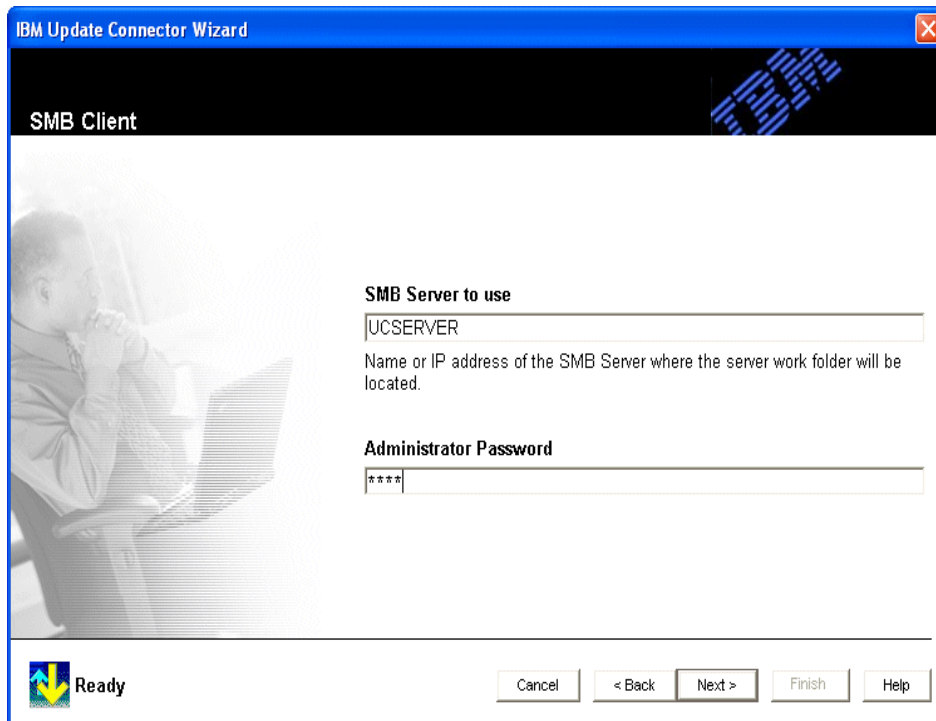


Figure 5-21 SMB Client configuration

To configure the SMB Client, you need to provide the following:

- ▶ SMB Server to use
Enter the Name or IP address of the (previously configured) SMB Server
- ▶ Administrator password
Enter the password that you have set up for the SMB Server

Administering the Update Connector SMB network

The administration of the UC SMB network is handled from the UC Administrator console. This console is usually run from the SMB Server system, but can be started from each client as well.

To access the Administrator console, right-click the Update Connector icon in the task bar and select Launch Administrator Console. You will have to provide the Administrator password.

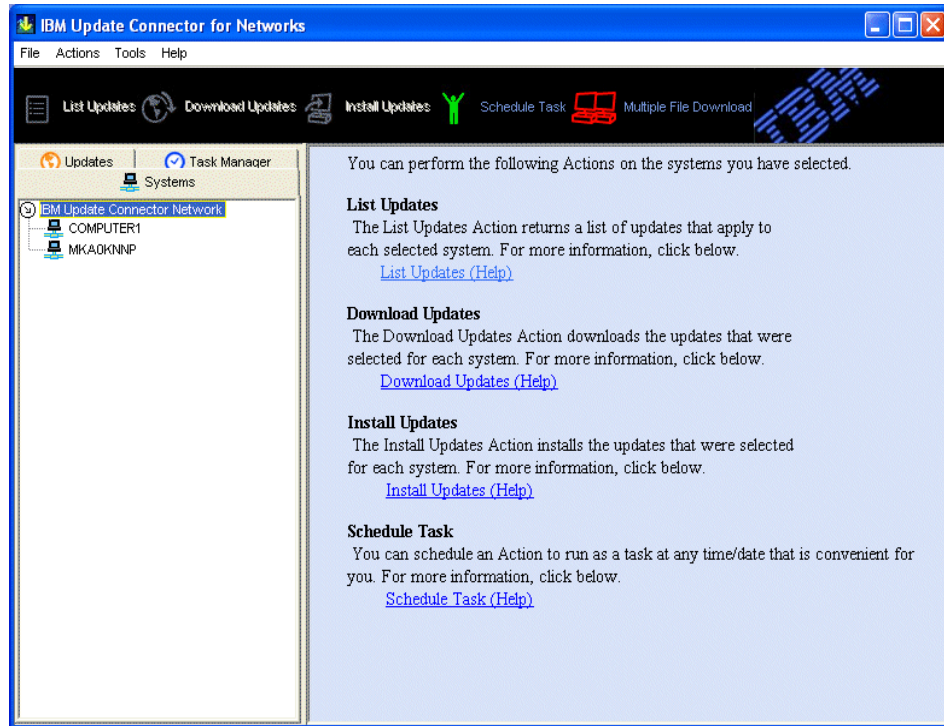


Figure 5-22 Update Connector Administrator console

From the Administrator console Menu bar, you can perform the following task.

► **File**

- Exit - exits IBM Update Connector (Ctrl + E).

► **Actions**

- Systems - This option lists the actions that can be performed on the systems selected in the Systems Tab.
 - List Updates - Goes over the Internet to the IBM Epicenter to check for new updates for the selected systems.
 - Download Updates - Downloads Updates from the IBM Epicenter for the selected systems.
 - Install Updates - Installs Updates on the selected systems.
 - Remove - Removes the selected off-line systems from the machine tree (note: a system must be off-line to be removed).
 - Schedule Task - Takes you to the SMB Scheduler to where you can schedule actions to be performed.

- Updates - This option lists the actions that can be performed on the updates selected in the Updates Tab.
 - Download Updates - Downloads the selected update.
 - Install updates - Installs the selected update on the selected systems if the system needs the update.
 - Unionist - Unionists the selected update from the selected systems where it is installed. The update must be designed as an un-insatiable update to be un-installed.
 - View Information - Shows the information about the selected update.
- Task Manager --This option allows you to schedule tasks, edit existing scheduled tasks, remove scheduled tasks, and cancel scheduled tasks. You can access these items under the Task Manager Tab.
 - Schedule task - This option takes you to the scheduler window where you can add new tasks to be performed on the selected systems (go to Schedule task section).
 - Edit Task - Allows you to Edit the selected scheduled task (go to Edit task section)
 - Remove Task - Removes the selected finished or failed task from the task list.
 - Cancel task - Cancels the selected running task. This action is only enabled if the selected task is running.

► **Tools**

- Server administration - These options allow the administrator to perform administrative functions on the SMB Server.
 - Change Password - Permits the administrator to change the administrator password.
- Connection - Displays a window allowing you to specify the kind of connection you make to the Internet (either direct or dial-up) and also displays a window which allows you to configure your system to use a Proxy server, a Socks server, or an auto-configuration script.
- Mode wizard - Shows the Mode wizard window, which lets you move between Update Connector Self-managed Mode and SMB LAN Mode.
- Search the IBM HelpCenter for updates - Allows you to look for updates at the IBM HelpCenter.
- Search for updates on a local repository - Allows you to look for updates that have been placed on the active local repository. You must have previously defined the repository and used the Multiple File Download

function to place updates in the local repository. The repository must be set to the active repository in order to use it.

- Local Repository Manager - Displays a window where you can define local repositories.
- Set a local repository as the active local repository - allows you to chose the repository that will be set as the active local repository. You can define any number of local repositories, but only one can be active at a time. You must have previously defined a local repository using the Local Repository Manager before you can set it as the active repository.

► **Help**

- Basics - Displays the Help Contents page.
- Context Help - Displays the Help page for the current displayed window.
- Program Information - Displays information (such as the version) about the IBM Update Connector program you are using.

Benefits of Update Connector SMB Network

There are several benefits to using Update Connector SMB mode:

- Gives the IT department a check that all clients are up to date. This includes clients that almost never connect to the network.
- Gives IT a possibility to test new functions and drivers before updating the hardware image.
- All clients will have the same hardware image over time. There can also be controlled differences.
- Cost of support will be reduced.
 - Help desk can quickly determine if user client is up to date.
 - IT can focus on handling problems with software.



Embedded Security Subsystem

As we become increasingly dependent on client systems (desktops and mobile PCs) for storage and transmission of important confidential information, security of data assets is becoming an increasingly important issue for businesses. Unwanted exposure of this information to the public, competitors or unauthorized users and hackers can prove very costly. Security requirements can vary from company to company and system to system. Due to the many configuration possibilities and usage scenarios, the hardware and software components in clients should complement each other to provide progressive, robust levels of security, both locally and across a network.

IBM addresses this issue by equipping selected ThinkPad, NetVista and ThinkCentre computers with built-in cryptographic technologies in both hardware and software that work together to provide a strong level of trust and security in the client PC platform.

The IBM solution supports key-management solutions such as Public Key Infrastructure (PKI), local file and folder encryption, and advanced authentication solutions, all of which combine to provide strong, secure transmission and storage of electronic information.

6.1 Overview

This chapter describes the installation, configuration and implementation of the IBM Embedded Security Subsystem. The IBM Embedded Security Subsystem consists of:

- ▶ IBM Embedded Security Chip discussed in 6.1.1, “IBM Embedded Security Chip” on page 444
- ▶ IBM Client Security Software (CSS) V5.21 discussed in Section 6.2.1, “IBM Client Security Software” on page 449

6.1.1 IBM Embedded Security Chip

The IBM Embedded Security Chip is a Trusted Computing Platform Alliance (TCPA) compliant, cryptographic microprocessor that is embedded in the mother board of the IBM client. The IBM Embedded Security Chip:

- ▶ Supports RSA (Rivest, Shamir, and Adelman) PKI (Public Key Infrastructure) operations such as encryption for privacy and digital signatures for authentication. The IBM Embedded Security Chip includes Electrically Erasable Programmable Read-Only Memory (EEPROM) where RSA key pairs are stored.
- ▶ Communicates with the main processor of the computer through the Low Pin count (LPC) bus.
- ▶ Performs RSA key generation.
- ▶ Contains a Pseudo Random Number Generator.
- ▶ Computes RSA operations in 200 milliseconds.
- ▶ Includes all TCPA (Trusted Computing Platform Alliance) functions defined in specification V1.1.

Note: In April 2003, the Trusted Computing Platform Alliance (TCPA) evolved into the Trusted Computing Group (TCG). The TCG has adopted existing trusted computing specifications from TCPA. For more information, visit <http://www.trustedcomputinggroup.org>.

6.1.2 Features

IBM has developed security software specially designed to be used with the IBM Embedded Security Chip. IBM Client Security Software consists of multiple software components that support cryptographic and identification services that strengthen the security of the personal computer.

These components are:

- ▶ Administrator Utility

This utility provides tools for the administration of the IBM Client Security Software and the IBM Embedded Security Chip, including initialization, configuration and archive and restore functions.

- ▶ Client Utility

This utility enables the end user to change individual and specific attributes such as the user's UVM passphrase and enrolled fingerprints.

- ▶ Microsoft Crypto API (MSCAPI)

This component supports the default cryptographic service for Microsoft operating systems and applications.

- ▶ Public-Key Cryptography Standard #11 (PKCS#11)

This component supports the cryptographic standard PKCS#11 as defined by RSA Data Security Inc., which is used by Netscape, Entrust and other products.

- ▶ File and Folder Protection:

- Right-Click File and Folder Protection

The end user right-clicks a file and selects **encrypt** or **decrypt**. Policies can be set to require authentication before encryption or decryption takes place.

- Transparent or On the Fly Encryption

The end user selects a particular folder to protect. All data saved or created in this directory is automatically encrypted with no additional end user requirements. When a file is selected by the end user to be opened by an application, the decryption happens on the fly, being passed unencrypted into the application. When the user saves the file in the protected folder, the contents are automatically encrypted. User authentication for on the fly encryption takes place after system logon as the client is starting services.

- ▶ UVM protection for Windows logon and the Client Security screen saver

User Verification Manager (UVM) protection for Windows logon and the Client Security screen saver ensure that only authorized users can gain access to the operating system. Multiple, configurable authentication methods supported.

- ▶ Lotus Notes

IBM Client Security Software provides User Verification Manager support for tasks performed in Notes that are password protected, such as logging on to Notes or changing the password for a User ID file and replacing the Lotus

Notes password prompt. Multiple, configurable authentication methods are supported.

► Entrust 6.0

IBM Client Security Software provides User Verification Manager-controlled embedded hardware protection and advanced authentication support for PKI operations performed by Entrust Desktop Solutions from this Web site

<http://www.entrust.com/partners/solutions/77.htm>

► RSA SecurID

IBM Client Security Software provides User Verification Manager-controlled embedded hardware protection and advanced authentication support for generation of software based RSA SecurID authentication passcodes from this Web site:

http://rsasecurity.agora.com/rsasecured/detail.asp?product_id=1082

► Tivoli

IBM Client Security Software was designed to interface with various components of IBM Tivoli Enterprise software, including:

– Tivoli Access Manager (TAM) plug-in

IBM Client Security Software policy can be set centrally and distributed to clients through a Tivoli Access Manager (TAM) plug-in available for download from the IBM Client Security Software download site. The client system is configured to pull the policy from TAM on a timed interval.

– Tivoli Global Sign-On and WebSeal Integration

WebSeal is a Web-based authentication method that allows a user to be authenticated through the Internet or intranet. This authentication can be based on certificates or username and password. In the case of the certificate, the private key operation can be carried out in the IBM Embedded Security Chip. In the case of a user name and password, the IBM Client Security Software Password Manager component can be used to store these values. In either case, the end user can be authenticated using the User Verification Manager multi-factor, policy-based capabilities. Once the end user is authenticated, the Tivoli Global Sign-On product can be used to determine the user's access privileges.

► Wireless

IBM Embedded Security Subsystem supports the latest industry standard 802.1x as well as Cisco Leap through IBM Access Connections. Learn more about IBM wireless offering at:

<http://www.pc.ibm.com/us/wireless/index.html>

- ▶ Checkpoint VPN-1

IBM Embedded Security Subsystem has been certified by Check Point Software Technologies to be an open platform for security (OPSEC). Private key operations for certificate-based operations are carried out in the IBM Embedded Security Chip with the capability to set configurable, multi-factor authentication.

- ▶ Verisign Personal Trust Agent (PTA)

The Personal Trust Agent (PTA) of Verisign, Inc. is used to manage user credentials. The Verisign PTA works well with the IBM Embedded Security Chip to perform all private key operations.

6.1.3 Client Security Password Manager

The IBM Client Security Password Manager enables you to manage the sensitive and easy-to-forget login information such as user IDs, passwords, and other personal information. The Password Manager stores all information through the IBM Embedded Security Chip so that the User Verification Manager can control access to your secure applications and Web sites based on an authentication policy.

This means that rather than having to remember and provide multiple individual passwords (all subject to different rules and expiration dates) you only have to remember one passphrase and provide any combination of identification elements, such as your fingerprint or proximity badge.

Client Security Password Manager software is available at:

<http://www.ibm.com/pc/support/site.wss/MIGR-46391.html>

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

- ▶ Encrypt your sensitive information onto the IBM Embedded Security Chip. This ensures that all your sensitive password information is secured by the IBM Client Security encryption keys.
- ▶ Transfer user IDs and passwords to other applications and Web browsers using a simple type-and-transfer interface. This helps minimize typing errors and enables you to save all of your information securely through the IBM Embedded Security Chip.
- ▶ Automatically logon to password secure Web sites. Use IBM Password Manager's autokey for User IDs and passwords to automate your login process when you access secure Web sites.

- ▶ Generate random passwords. IBM Password Manager enables you to generate random passwords for each Web site or application. This allows you to increase the security of your data because each application will have much more rigorous password protection enabled. Random passwords are far more secure than user-defined passwords because experience indicates that most users use easy-to-remember personal information for passwords that are often relatively easy to crack.
- ▶ Edit accounts and passwords. The IBM Password Manager enables you to edit all of your account entries and set up all optional password features in one easy-to-use interface. This makes managing your passwords and personal information quick and easy.
- ▶ Access Password Manager from the icon tray on your Windows desktop or with a simple keyboard shortcut. The IBM Password Manager icon enables you to have instant access to Password Manager if you want to quickly add another ID and password while using an application or surfing the Web. Each Password Manager function can also be easily accessed using a simple keyboard shortcut.

Note: The IBM Password Manager is only fully supported on Windows 2000 and Windows XP.

- ▶ Archive and retrieve your login information. Using IBM Client Security Software's archiving function and the IBM Password Manager you can restore your sensitive login information to protect against a hard drive or system failure. See the *Client Security Software User's Guide* for more information about how to archive information.

6.1.4 File and Folder Encryption (FFE) Utility

IBM File and Folder Encryption (FFE) Utility enables IBM Client Security Software users to protect sensitive files and folders using the right-click button of their mouse. How the utility protects a file and folder is dependent upon how the file or folder is initially encrypted.

Refer to 6.5.2, "File and Folder Encryption (FFE)" on page 487 to determine which encryption technique you should use to protect your data. IBM Client Security Software must be installed before you install the IBM File and Folder Encryption utility.

File and Folder Encryption software is available at:

<http://www.ibm.com/pc/support/site.wss/MIGR-46391.html>

Note: File and Folder Encryption is different from the right-click encryption that comes native in IBM Client Security Software install. You do not need to install File and Folder Encryption unless you are seeking the capability of protecting a folder on the fly.

The Check Disk utility might run when restarting the operating system after protecting or unprotecting folders. Wait for Check Disk to check your system before using your computer.

6.2 Installation considerations

IBM Embedded Security Chip is a cryptographic microprocessor that is embedded on the system board of select ThinkPad and ThinkCentre computers. The chip cannot be retro-fitted to existing hardware.

Note: If you try to install the software onto a computer that does not contain IBM Embedded Security Chip, the software will not install or run properly.

6.2.1 IBM Client Security Software

Supported IBM models

IBM Client Security Software is licensed for and supports numerous IBM desktop and notebook computers. For a complete list of supported models, refer to:

<http://www.pc.ibm.com/us/security/secdownload.html>

Operating systems supported

The supported operating systems are:

1. Microsoft Windows 2000
1. Microsoft Windows XP

User Verification Manager (UVM) aware products

IBM Client Security Software comes with User Verification Manager (UVM) software that enables you to customize authentication for your system. This first level of policy-based control increases asset protection and the efficiency of password management. User Verification Manager, which is compatible with enterprise-wide security policy programs, enables you to use UVM-aware products.

These UVM products include the following:

- ▶ Biometrics devices such as fingerprint readers
User Verification Manager provides a plug-and-play interface for biometrics devices.
- ▶ Tivoli Access Manager V3.8 or later
User Verification Manager software simplifies and improves policy management by smoothly integrating with a centralized, policy-based access control solution such as Tivoli Access Manager. User Verification Manager software enforces policy locally whether the system is in the network or stands alone, thus creating a single, unified policy model.
- ▶ Lotus Notes V4.5 or later
User Verification Manager works with Client Security Software to improve the security of your Lotus Notes login.
- ▶ Entrust Desktop Solutions V5.1, V6.0, or later
Entrust Desktop Solutions enhances Internet security capabilities so that critical enterprise processes can be moved to the Internet. Entrust Entelligence provides a single security layer that can encompass an enterprise's entire set of enhanced security needs including identification, privacy, verification, and security management.
- ▶ RSA SecurID Software Token
The RSA SecurID Software Token enables the same seed record that is used in traditional RSA hardware tokens to be embedded on existing user platforms. Consequently, users can authenticate to protected resources by accessing the embedded software instead of having to carry dedicated authentication devices.
- ▶ Targus fingerprint reader
The Targus fingerprint reader provides a simple easy interface that enables the security policy to include fingerprint authentication. This is discussed in detail in section 6.4.5, "Targus DEFCON Fingerprint Reader" on page 473.
- ▶ Gemplus GemPC400 smart card reader
The Gemplus GemPC400 smart card reader enables the security policy to include smart card authentication, adding an additional layer of security to the standard passphrase protection.

Web browsers supported

IBM Client Security Password Manager only supports Microsoft Internet Explorer. You must use Microsoft Internet Explorer Version 5.0 or higher to use the functions of IBM Password Manager.

Cryptographic services

IBM Client Security Software supports the following cryptographic services:

- ▶ Microsoft Crypto API

Crypto API is the default cryptographic service for Microsoft operating systems and applications. With built-in Crypto API support, IBM Client Security Software enables you to use the cryptographic operations of the IBM Embedded Security Chip when you create digital certificates for Microsoft applications.

- ▶ PKCS#11

PKCS#11 is the cryptographic standard for Netscape, Entrust, RSA and other products. After you install the IBM Embedded Security Chip PKCS#11 module, you can use the IBM Embedded Security Chip to generate digital certificates for Netscape, Entrust, RSA and other applications that use PKCS#11.

E-mail applications

IBM Client Security Software supports the following application types using secure e-mail:

- ▶ E-mail applications that use the Microsoft Crypto API for cryptographic operations, such as Outlook Express and Outlook (when used with a supported version of Internet Explorer)
- ▶ E-mail applications that use PKCS#11 for cryptographic operations, such as Netscape Messenger (when used with a supported version of Netscape)

6.2.2 File and Folder Encryption considerations

The following information might be useful when performing certain file and folder encryption functions:

- ▶ Drive-letter protection

The IBM File and Folder Encryption utility can be used to encrypt files and folders on the C drive only. This utility does not support encryption on any other hard-disk partition or physical drive.

- ▶ Deleting protected files and folders

To ensure that no sensitive files or folders are left unprotected in the Recycle Bin, you must press Shift+Del to delete protected folders and files. This performs an unconditional delete operation and does not attempt to put deleted files in the Recycle Bin.

- ▶ Before upgrading to a newer version of the IBM FFE

If you intend to upgrade from a previous version of the IBM FFE utility (V1.04 or earlier) and you have protected folders on drives other than the C drive, unprotect those folders before you install V2.00 of the IBM FFE utility. If you need to protect those folders after you install V2.00, move those folders to the C drive and then protect them.

- ▶ Before uninstalling the IBM FFE utility:

Before you uninstall the IBM FFE utility, use it to unprotect any files or folders that are currently protected.

6.2.3 Client Security Password Manager

The known limitations related to IBM Client Security Password Manager are:

- ▶ IBM Client Security Password Manager does not support Netscape Navigator. You must use Microsoft Internet Explorer to use the functions of IBM Password Manager.
- ▶ IBM Client Security Password Manager does not support icon tray functionality on computers running the Windows NT® operating system, nor does it support icon tray functionality on computers running Windows NT. If you use a Windows NT system, use the keyboard shortcuts.

6.3 Prerequisites

The following prerequisites may apply to your installation:

- ▶ Downloading the software

All files required for the installation of IBM Client Security Software, File and Folder Encryption, and Client Security Password Manager are available to download from the following IBM Web Site:

<http://www.pc.ibm.com/us/security/secdownload.html>

The Web site provides the specific information for your model number that helps you ensure that your system has the IBM Embedded Security Chip and to determine if your system is TCPA compliant. It will also inform you if you need to use the latest SMBus device driver.

Download the following items to a temporary directory (c:\temp):

- Atmel_TPM.msi - Atmel TPM Driver
- CCSmbusdriverpkg.exe - SMBus Support Package
- CSE521us_004b.exe - IBM Client Security Software for ESS 2.0 (TCPA)
- pwmgr130us_002c.exe - Client Security Password Manager (V1.3)
- ffe201us_010b.exe - File and Folder Encryption (V2.01)

You might want to consider downloading the associated reference documentation available at this site.

- ▶ Registration form

Before you download the software, you must complete a registration form and questionnaire, and agree to the license terms. Follow the instructions that are provided at the Web site to download the software.

The installation files for IBM Client Security Software are included within the self-extracting file. The version used in this Redbook was csec51.exe.

- ▶ Export regulations

IBM Client Security Software contains encryption code that can be downloaded within North America and internationally. If you live in a country where downloading encryption software from a Web site in the United States is prohibited, you cannot download IBM Client Security Software.

6.3.1 Before installing the software

The installation program installs IBM Client Security Software on the IBM client and enables the IBM Embedded Security Chip; however, installation specifics vary depending on a number of factors as follows:

- ▶ Installing on clients running Windows XP and Windows 2000

Windows XP and Windows 2000 users must log on with administrator rights to install IBM Client Security Software.

- ▶ Installing for use with Tivoli Access Manager

If you intend to use Tivoli Access Manager to control the authentication requirements for your computer, you must install some Tivoli Access Manager components before you install IBM Client Security Software. For details, see *Using Client Security with Tivoli Access Manager* listed in “*Related publications*” on page 637.

- ▶ Startup feature considerations

Two IBM startup features might affect the way that you enable the security subsystem (Embedded Security Chip) and generate hardware encryption keys. These features are the administrator password and supervisor passwords for enhanced security:

- Supervisor password (ThinkPad)

Supervisor passwords prevent unauthorized persons from changing the configuration settings of an IBM ThinkPad computer. These passwords are set up using the IBM BIOS Setup Utility program, which is accessed by pressing **F1** during the system startup sequence.

- Administrator password (NetVista and ThinkCentre)

Administrator passwords prevent unauthorized persons from changing the configuration settings of an IBM computer. These passwords are set up using the Configuration/Setup Utility program, which is accessed by pressing **F1** during the system startup sequence.

6.3.2 Setting up a supervisor password on a ThinkPad

Security settings available in the IBM BIOS Setup Utility enable administrators to perform the following tasks:

- ▶ Enable or disable the IBM Embedded Security Chip
- ▶ Clear the IBM Embedded Security Chip

When the IBM Embedded Security Chip is cleared, all encryption keys and certificates stored on the chip are lost. It is necessary to temporarily disable the supervisor password on some ThinkPad models before installing or upgrading IBM Client Security Software.

After setting up IBM Client Security Software, set up a supervisor password to deter unauthorized users from changing these settings. To set up a supervisor password, complete the following procedure:

1. Shut down and restart the computer.
2. When the IBM BIOS Setup Utility prompt appears, press F1 to open the main menu of the IBM BIOS Setup Utility.
3. Select **Password**.
4. Select **Supervisor Password**.
5. Type your password and press Enter.
6. Type your password again and press Enter.
7. Click **Continue**.
8. 8. Press F10 to save and exit.

After you set up a supervisor password, a prompt appears each time you attempt to access the IBM BIOS Setup Utility.

Important: Keep a record of your supervisor password in a secure place. If you lose or forget the supervisor password, you cannot access the IBM BIOS Setup Utility, and you cannot change or delete the password. See the hardware documentation that came with your computer for more information.

6.3.3 Setting up an administrator password for a ThinkCentre

Security settings available in the Configuration/Setup Utility enable administrators to do the following:

- ▶ Change the hardware password for the IBM Embedded Security Chip
- ▶ Enable or disable the IBM Embedded Security Chip
- ▶ Clear the IBM Embedded Security Chip

Because your security settings are accessible through the Configuration/Setup Utility of the computer, set up an administrator password to deter unauthorized users from changing these settings. To set up an administrator password:

1. Shut down and restart the computer.
2. When the Configuration/Setup Utility prompt appears on the screen, press F1. The main menu of the Configuration/Setup Utility opens.
3. Select **System Security**.
4. Select **Administrator password**.
5. Type your password and press the down arrow on your keyboard.
6. Type your password again and press the down arrow.
7. Select **Change Administrator password** and press Enter; then press Enter again.
8. 8. Press Esc to exit and save the settings.

After you set up an administrator password, a prompt appears each time you try to access the Configuration/Setup Utility.

Tip: You set a Security Chip password to enable IBM Embedded Security Chip for a client. After you set up a Security Chip password, access to the Administrator Utility is protected by this password. You should protect the Security Chip password to prohibit unauthorized users from changing settings in the Administrator Utility.

6.3.4 Clearing the IBM Embedded Security Chip on a ThinkPad

If you want to erase all user encryption keys and clear the hardware password from the IBM Embedded Security Chip on an IBM ThinkPad product, you must clear the chip using the procedure described in this section.

Important: Do not clear or disable the IBM Embedded Security Chip when User Verification Manager logon protection is enabled. If you do, you will be completely locked out of the system. To disable User Verification Manager protection, open the Administrator Utility, click **Configure Application Support and Policies**, and deselect the **Replace the standard Windows logon with UVM's secure logon** check box. You must restart the computer before User Verification Manager protection is disabled.

When the IBM Embedded Security Chip is cleared, all encryption keys and certificates stored on the chip are lost. To clear the IBM Embedded Security Chip on a ThinkPad, complete the following procedure:

1. Shut down and restart the computer. When prompted to interrupt the normal startup sequence, press the Access IBM button on the keyboard

Note: On some older ThinkPad models, you might need to press the F1 key at power on when prompted to access the IBM BIOS Setup Utility. Refer to the help facility for the IBM BIOS Setup Utility for details.

2. At the Access IBM predesktop area, double-click **Start setup utility**.
3. Select **Security**.
4. Select **IBM Security Chip**.
5. Select **Clear IBM Security Chip**.
6. When prompted to Clear encryption keys?, select **Yes**.
7. Press Enter to continue.
8. Press F10 to save and exit.
9. When prompted to Save configuration changes and exit now, select **Yes**.
10. Press Enter to continue.

6.3.5 Clearing the IBM Embedded Security Chip on a ThinkCentre

If you want to erase all user encryption keys and clear the hardware password from the IBM Embedded Security Chip on a ThinkCentre product, you must clear the chip using the procedure described in this section.

Important: Do not clear or disable the IBM Embedded Security Chip when User Verification Manager logon protection is enabled. If you do, you will be completely locked out of the system. To disable User Verification Manager protection, open the Administrator Utility, click **Configure Application Support and Policies**, and deselect the **Replace the standard Windows logon with UVM's secure logon** check box. You must restart the computer before User Verification Manager protection is disabled.

To clear the IBM Embedded Security Chip on a ThinkCentre, complete the following procedure:

1. Shut down and restart the computer.
2. When the Configuration/Setup Utility prompt appears on the screen, press F1 to open the main menu of the Configuration/Setup Utility.
3. Select **Security**.
4. Select **Clear IBM Security Chip**.
5. Press Enter.
6. Select Yes.
7. Press Enter.
8. Press Esc to continue.
9. Press F10 to exit and save the settings.
10. Click **Yes**.

6.4 Installation instructions

This section describes how to install and configure the IBM Client Security Software on IBM systems. This section also includes instructions for uninstalling the software. Be sure that you install IBM Client Security Software prior to installing any of the various utilities that enhance the Embedded Security Subsystem's functionality. More information including the user guide can be found on the IBM ThinkVantage Embedded Security Subsystem Web site:

<http://www.ibm.com/pc/support/site.wss/MIGR-46391.html>

6.4.1 Preparation

Before installing the IBM Client Security Software, you must perform the following steps to prepare the system.

Thinkpad preparation

For a Thinkpad, complete the following steps:

1. Turn off the system.
2. Press and hold the FN key.
3. Turn on the system.
4. When the IBM logo appears, press and release the F1 key.
5. Select **Security**.
6. Select **IBM Security Chip**.
7. Select **Clear IBM Security Chip**.
8. Select **Yes** when prompted to clear the encryption keys.
9. Press F10 to save the settings.
10. Restart the system.
11. Log in to Windows with an account that has local administrator rights.

Netvista or ThinkCentre preparation

For a Netvista or ThinkCentre, complete the following steps:

1. Turn off the system.
2. Turn on the system.
3. When the IBM logo appears; press and release the F1 key.
4. Select **Security**.
5. Select **Clear IBM Security Chip**.
6. Press Enter.
7. Select **Yes**.
8. Press Enter.
9. Press Esc to continue.
10. Press F10 to exit and save the settings.
11. Click **Yes**.
12. Restart the system.
13. Log in to Windows with an account that has local administrator rights.

Obtaining the required software

You can download necessary software from the following support Web site:

<http://www.pc.ibm.com/us/security/secdownload.html>

See 6.3, “Prerequisites” on page 452 for additional information and instructions.

6.4.2 Installing prerequisite device drivers

These device drivers must be installed before the IBM Client Security Software installation procedure:

- Atmel TPM Driver
- SMBus Driver

Install the Atmel TPM Driver as follows:

1. Run the hardware driver installation program, Atmel_TPM.msi
2. Click **Next**.
3. Click **Finish**.

Install the SMBus device driver as follows:

1. Run the SMBus device driver installation program, CCSmbusdriverpkg.exe
2. Click **Next**.
3. The Windows hardware installation wizard will display Found new hardware. Insure the install the software automatically (Recommended) option is selected.
4. Click **Next**.
5. IBM – SMBbus Device Hub, will be found.
6. Click **Finish**.
7. Wait for next device discovery to start.
8. The Windows hardware installation wizard will again display Found new hardware. Insure that install the software automatically (Recommended) is selected.
9. Click **Next**.
10. IBM – Generic SMBbus Device, will be found.
11. Click **Finish**.
12. Restart the system.

6.4.3 Installing IBM Client Security Software

Install IBM Client Security Software as follows:

1. Log into Windows with an account that has local administrator rights.
2. Run the IBM Client Security Software installation program, csec521us_004b.exe.
3. Click **Yes**.
4. Click **Next**.
5. Click **Next**.
6. Click **Finish**.
7. Restart the system.

Attention: The log in process will be slower than usual the first time a user tries to log in after installing the IBM Client Security Software.

6.4.4 Configuring the IBM Client Security Software for the first time

IBM Client Security Software must be configured before it is activated on the system as follows.

1. Log on to the system with an account that has local administrative rights.
2. If this is the first time you have logged on since installing the IBM Client Security Software, the Setup Wizard automatically opens. If you canceled this wizard the first time it opened, then you must start it again by selecting **Start → All Programs → Access IBM → IBM Client Security Software → Modify Your Security Settings.**

3. IBM Client Security Setup Wizard Welcome window will be displayed as shown in Figure 6-1.



Figure 6-1 IBM Client Security Setup Wizard - Welcome

4. In Figure 6-1 on page 461 click **Next** to continue. A window similar to Figure 6-2 will be displayed.

The screenshot shows the 'IBM Client Security Setup Wizard' window. The title bar is blue with the text 'IBM Client Security Setup Wizard'. Below the title bar is a black header with the 'IBM Client Security' logo. A navigation bar contains five icons: 'Password' (selected), 'Keys', 'Applications', 'Users', and 'Security Level'. The main content area is white and displays 'Step 1 of 5 - Set Security Administrator Password'. A text block explains that the Administrator Password is required for administrative tasks and must be exactly 8 characters long. Below this, there are two text input fields: 'Enter Administrator Password' and 'Confirm Administrator Password', both containing eight asterisks. At the bottom right, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

Figure 6-2 Set security administrator password

5. In Figure 6-2 enter the security administrator password. Re-enter the password to confirm it.

Important: It is critical that this password is never compromised nor lost. This password is used to configure the local IBM Client Security Software and can be used to recover the user's security keys if his or her passphrase is forgotten.

6. Click **Next** to continue. The window shown in Figure 6-3 on page 463 opens.

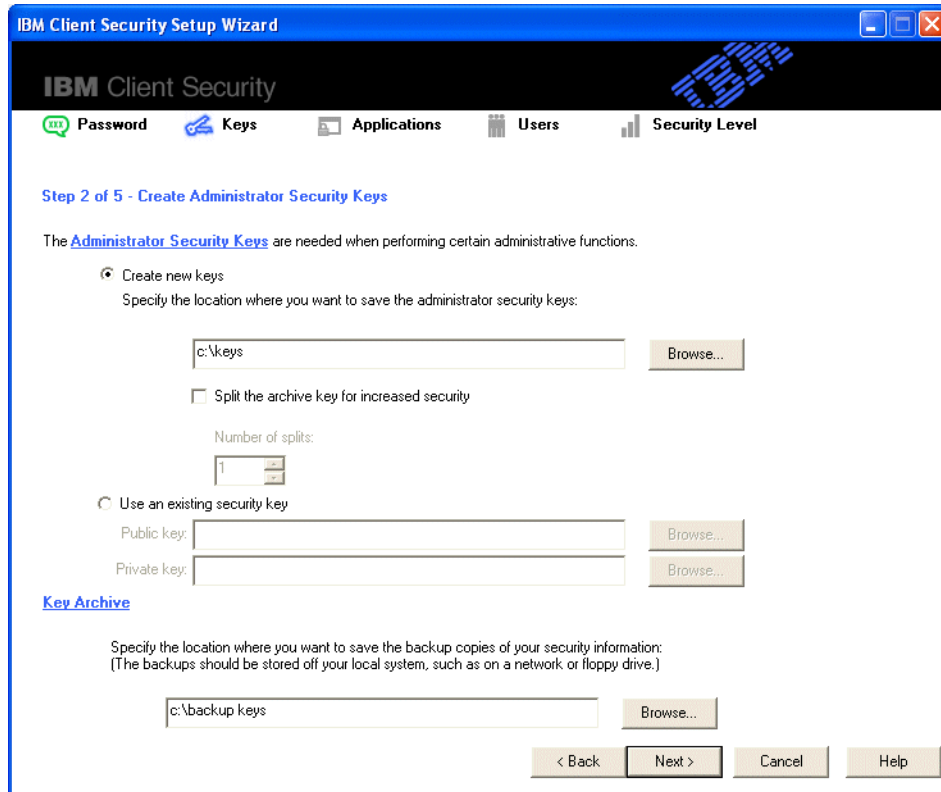


Figure 6-3 Create Administrator Security Keys

7. Click **Browse** or type in a location to store the administrator security keys. In this example, we use C:\keys.
8. Click **Browse** or type in a location to store the admin archive keys. In this example, we use C:\backup keys.
9. If you have existing keys, you can select **Use an existing key** and browse to the location for both the public and private keys.
10. Click **Next**. A window similar to the one in Figure 6-4 on page 464 opens.

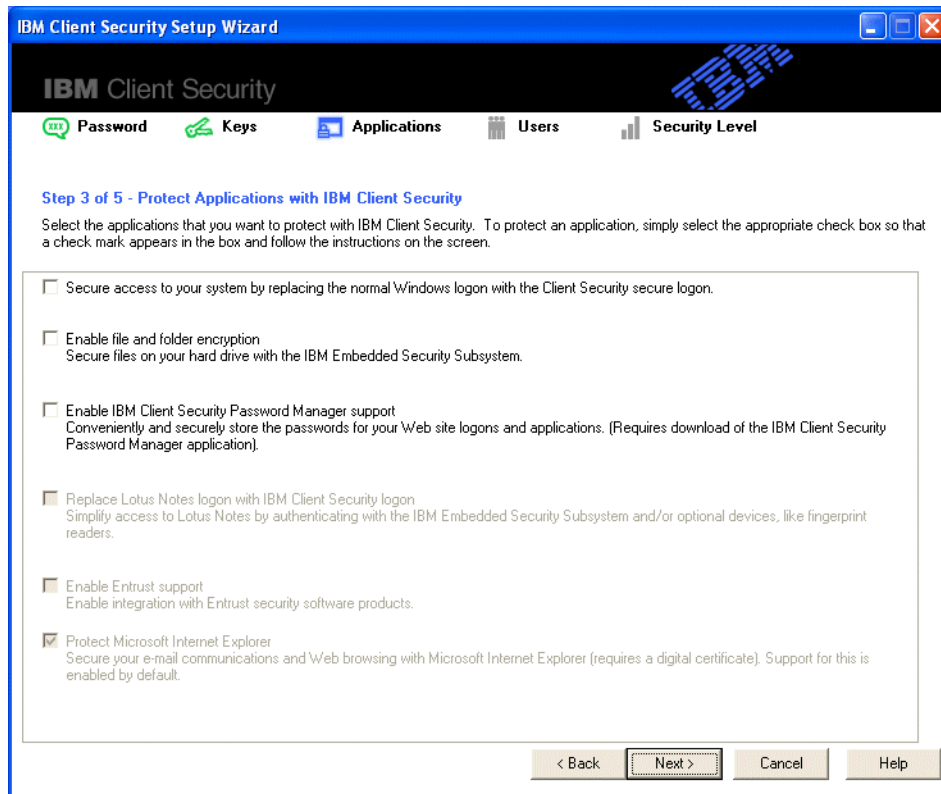


Figure 6-4 Protect Applications with IBM Client Security

11. Select any of the options that you wish to use or configure them later. By default, options 1 through 5 are disabled, and option 6 is enabled.
 - Option 1 replaces the standard Windows login window with an IBM Embedded Security System login.
 - Option 2 enables IBM File and Folder Encryption. This replaces the operating system's native file and folder encryption feature. Refer to 6.5.2, "File and Folder Encryption (FFE)" on page 487 for additional information.
 - Option 3 enables IBM Client Security Password Manager. This feature can be used to centrally manage passwords on a protected system. Refer to 6.5.1, "Client Security Password Manager" on page 483 for additional information.
 - Option 4 enables the use of the secured system login credentials to log into Lotus Notes. This is only available if Lotus Notes is installed on the system. Refer to 6.8, "Using User Verification Manager protection for Lotus Notes" on page 517 for additional information.

- Option 5 enables integration with Entrust security software products.
- Option 6 enables integrated support for Microsoft Internet Explorer using digital certificates.

12. Click **Next** to continue. The window shown in Figure 6-5 opens.

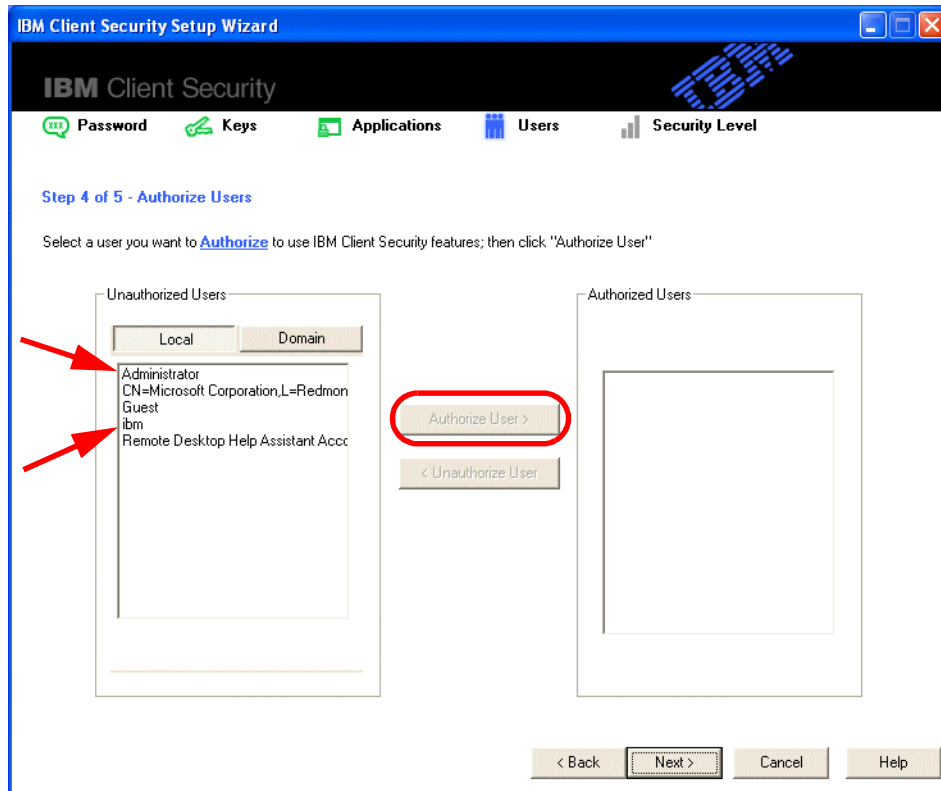
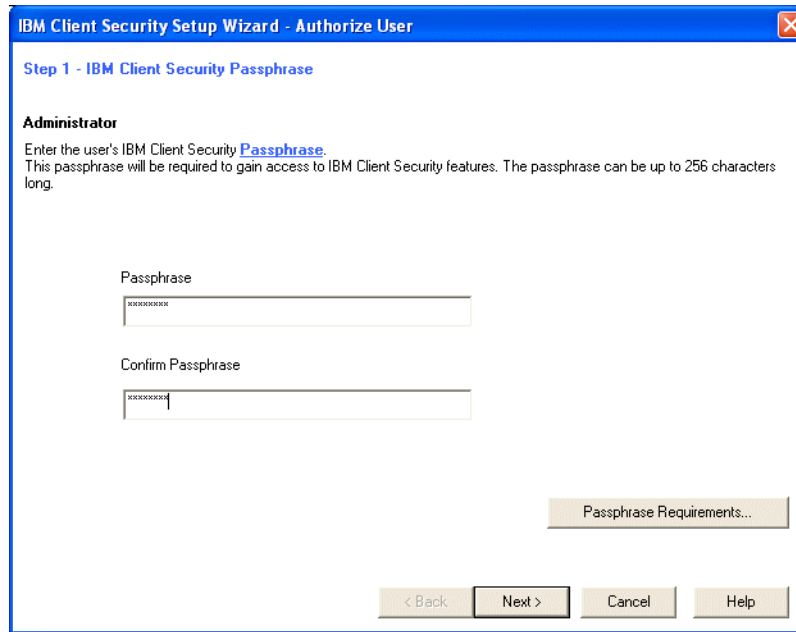


Figure 6-5 Authorize users

13. Select the user(s) you wish to authorize to use the IBM Client Security features. In this example, we authorize the local administrator and the user named IBM.
14. Select **Administrator**. You will either select a local or domain user by clicking one of the buttons in the Unauthorized Users pane.
15. Click **Authorize User**.

16. Click **Next** to open the window shown in Figure 6-6.



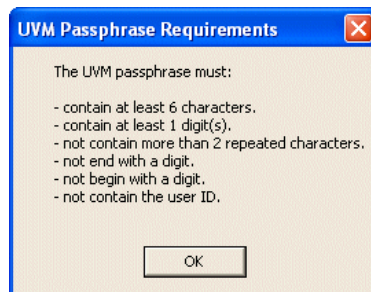
The image shows a window titled "IBM Client Security Setup Wizard - Authorize User". It is at "Step 1 - IBM Client Security Passphrase". Under the "Administrator" section, it says: "Enter the user's IBM Client Security [Passphrase](#). This passphrase will be required to gain access to IBM Client Security features. The passphrase can be up to 256 characters long." There are two text input fields: "Passphrase" and "Confirm Passphrase", both containing masked characters (asterisks). To the right of the "Confirm Passphrase" field is a button labeled "Passphrase Requirements...". At the bottom of the window are four buttons: "< Back", "Next >", "Cancel", and "Help".

Figure 6-6 IBM Client Security Passphrase

17. Enter a passphrase in the field for this user.

18. Confirm the passphrase in the field for this user.

Tip: You can display the passphrase requirements by clicking the passphrase requirements button. See Figure 6-7.



The image shows a dialog box titled "UVM Passphrase Requirements". It contains the text: "The UVM passphrase must:" followed by a bulleted list of requirements: "contain at least 6 characters.", "contain at least 1 digit(s).", "not contain more than 2 repeated characters.", "not end with a digit.", "not begin with a digit.", and "not contain the user ID." At the bottom of the dialog box is an "OK" button.

Figure 6-7 UVM Passphrase Requirements

Click **OK** to close the dialog box in Figure 6-7.

19. Click **Next** to display the window shown in Figure 6-8.

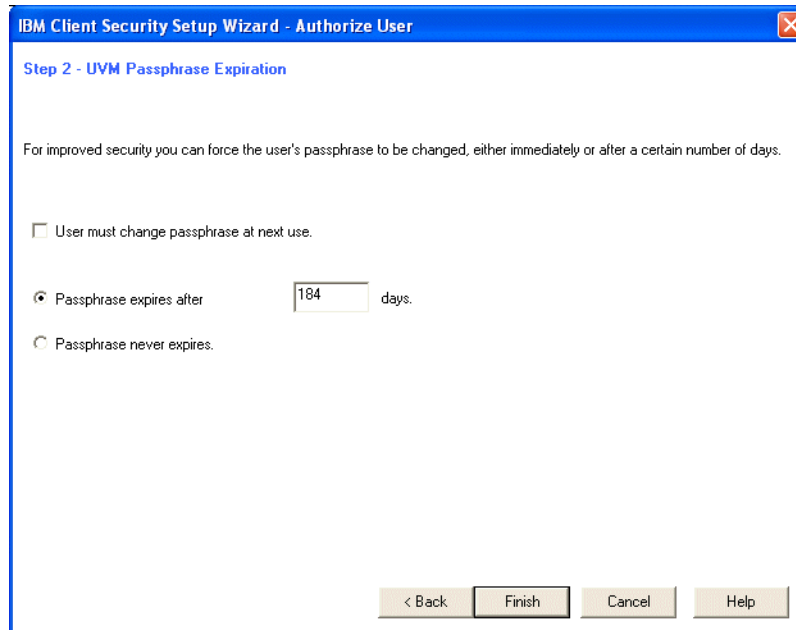


Figure 6-8 UVM Passphrase Expiration

20. Figure 6-8 allows you to configure the User Verification Manager (UVM) passphrase expiration.

21. Make the desired changes, then click **Next** to continue.

22. The Authorize Users window (shown in Figure 6-9) opens again so that you can continue to authorize additional users.

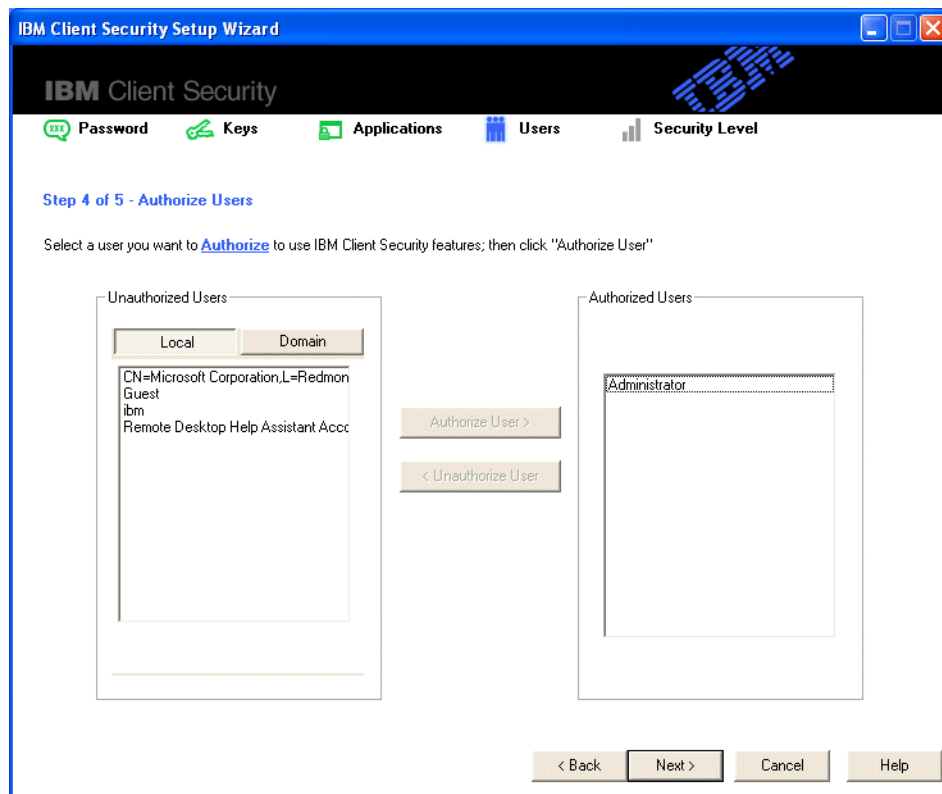


Figure 6-9 Authorize Users

23. Repeat steps 14 on page 465 through 21 on page 467 for all of the users that you wish to authorize.

24. If you select **Domain** on a system where no domain is available, as shown in Figure 6-10, the window shown in Figure 6-11 opens.

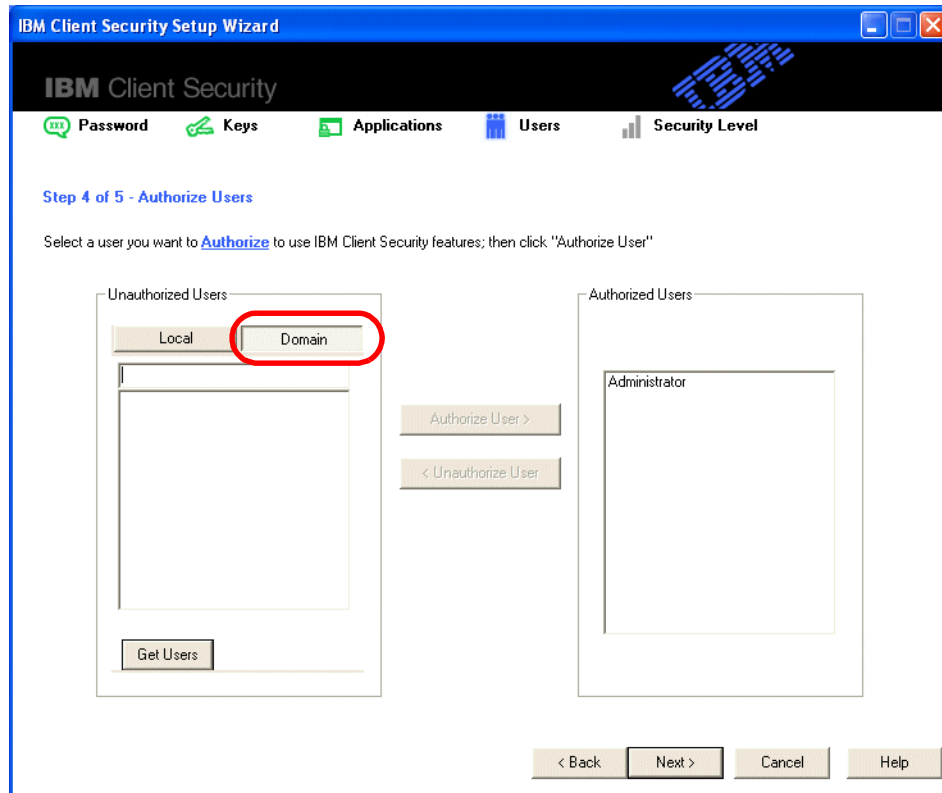


Figure 6-10 Authorize Users

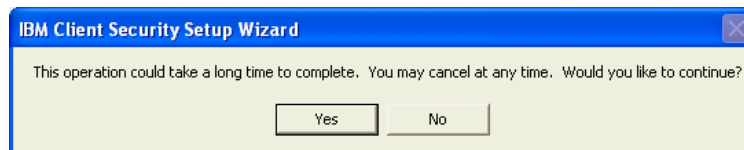


Figure 6-11 This operation could take a long time to complete.

Click **No** to exit or **Yes** to have IBM Client Security Software continue to search for a Windows domain. If no domain is found, a window as shown in Figure 6-12 on page 470 opens.



Figure 6-12 No domain was found

25. Click **OK** to return to the Authorize Users window shown in Figure 6-13.

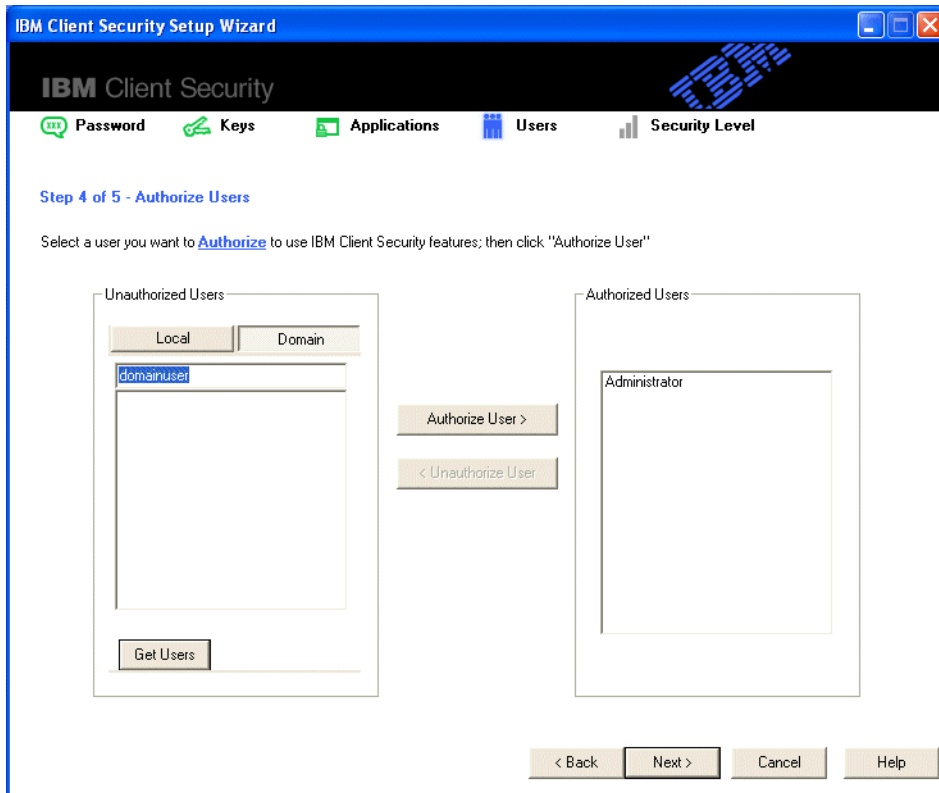


Figure 6-13 Authorize Users

26. When you are finished authorizing users, click **Next** to continue.

27.Next, the window shown in Figure 6-14 will display, allowing you to select the system security level.

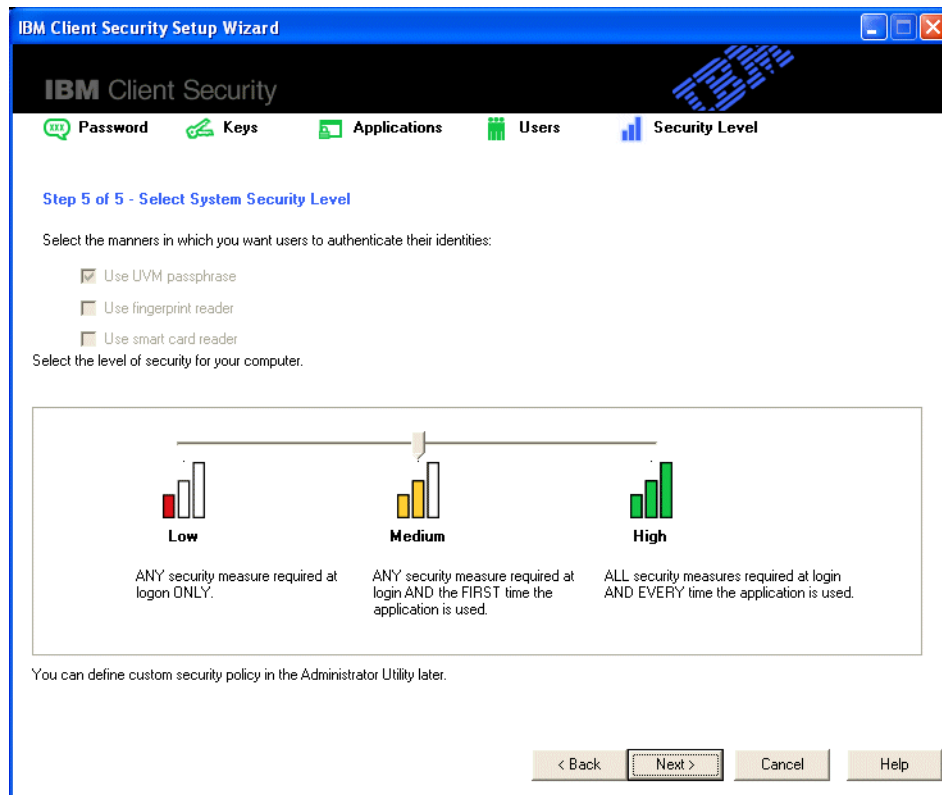


Figure 6-14 Select System Security Level

28.Slide the selection bar to the desired system security level (low, medium, high) then click **Next** to continue.

29. The window shown in Figure 6-15 opens, giving you the opportunity to review and verify your security settings.

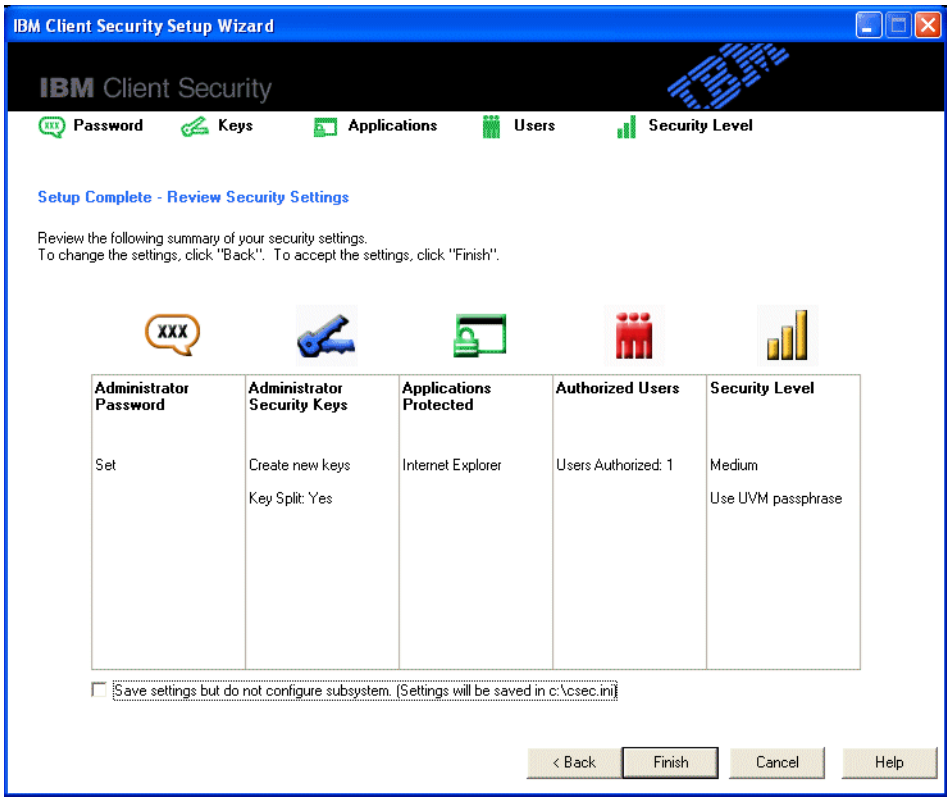


Figure 6-15 Setup Complete - Review Security Settings

30. Review the settings that you just made and click **Finish** to complete. The processing window shown in Figure 6-16 opens.

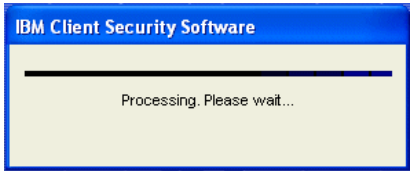


Figure 6-16 Processing Please Wait

Attention: This will take a long time as the system is generating the security keys.

31. When the system has finished processing, the success message shown in Figure 6-17 opens.



Figure 6-17 Your Computer is now protected

32. Click **OK** to close this window and restart your system.

Rebooting is recommended in order to initialize IBM Client Security Software protection features.

6.4.5 Targus DEFCON Fingerprint Reader

In this example, we install a Targus Defcon Authenticator PC Card Fingerprint Reader. The latest TARGUS software and driver can be downloaded from:

<http://www.targususa.com/downloads/download.asp>

The remaining steps to configure IBM Client Security Software using the Wizard are described in 6.4.4, "Configuring the IBM Client Security Software for the first time" on page 460. You may now install the BioMetric fingerprint reader.

Important: You must install IBM Client Security Software and restart your system before connecting the DEFCON Authenticator.

Install the Targus PC Card Fingerprint Reader as follows:

1. From the downloaded Targus installation files, run **install.exe**.

Note: It is important that you run the install.exe file and not setup.exe because the setup.exe file will skip the device type and orientation section of the install.

2. The DEFCON Authenticator windows opens. Click **Next**.
3. The sensor device selection windows open. Click the picture of the sensor device you are using.

If you select the PC Card device, you will be asked for the PC Card slot in which you wish to insert the device.
4. Click the green arrow indicating on which side of the ThinkPad the PC Card slot is located.
5. The Welcome to the InstallShield Wizard for the OmniPass window opens. Click **Next**.
6. At the InstallShield Wizard License Agreement window, click **YES**.
7. At the Choose Destination Location window, click **Browse** to select the Destination Folder you want, then click **Next**.
8. When the message box in Figure 6-18 displays, click **OK**.

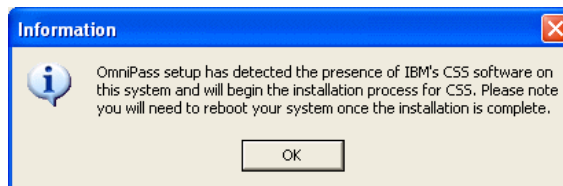


Figure 6-18 OmniPass installation for IBM Client Security Software

9. Click **OK** when the message Setup completed successfully displays.
10. You can now stop your system, insert your DEFCON Authenticator and restart. The Windows Found New Hardware Wizard pops up. Accept the recommended default. Click **Next**.
11. When the Windows Found New Hardware Wizard finishes installing, click **Finish**.

For information about how to register fingerprints, see 6.7, “Registering fingerprints” on page 515.

6.4.6 Performing an unattended installation

An unattended installation enables an administrator to install IBM Client Security Software on a remote IBM client without having to physically go to the client computer.

Before you begin an unattended installation, read 6.3.1, “Before installing the software” on page 453. No error messages are displayed during unattended

installations. If an unattended installation ends prematurely, you must perform an attended installation to view any error messages that might be displayed.

Note: Users must log on with administrator user rights to install IBM Client Security Software.

For complete information about how to perform an unattended installation, complete the following procedure. In addition, see the IBM Client Security Software Installation Guide available on the IBM Web site at:

<http://www.ibm.com/pc/support/site.wss/MIGR-46391.html>

Mass deployment

Mass deployment enables security administrators to initiate security policies on multiple computers simultaneously. This makes it easier to manage and deploy security measures and helps ensure that the correct security policies are implemented.

The SMBus device driver must be installed before completing the mass deployment procedure. See 6.4.2, “Installing prerequisite device drivers” on page 458.

Important: The drivers for the security chip are not signed by Microsoft. This means that you might get a message asking you to confirm the installation of the driver when you try to install it. If you would like to make an image of your system and perform a silent install of the IBM Embedded Security Subsystem afterwards, we recommend that you make a cloned image of it. With Windows XP, for example, you are able to change some settings in the `unattended.txt` file to make your machine accept these drivers should you need to do a scripted install of Windows.

There are two major steps to a mass deployment:

- ▶ Mass installation
- ▶ Mass configuration

The capability to perform a mass installation and mass configuration at two different times is supported. For example, some system administrators may prefer to perform the mass install at rollout time, but wait to configure or start using the Embedded Security Subsystem until a later date, perhaps when they have determined a full security policy or completed an installation of Tivoli Access Manager. In addition, it is likely that the system administrator will reconfigure these machines multiple times during the life cycle of these systems to adhere to changes in the company's security policies over time.

Mass installation

You must perform an unattended installation to install IBM Client Security Software on multiple clients simultaneously. You must use the unattended installation parameter \when initiating a mass deployment.

To initiate a mass installation, complete the following procedure:

1. Create the CSS.ini file.

The CSS.ini file is a response file used during mass configuration. This step is only required if you intend to perform a mass configuration. The CSS.ini file contains all the configuration options you would go through to set up the IBM Client Security Software software manually, for example, user names, location of the keys, and so on. The IBM Client Security Software.ini file must be created in the same directory as the install files. You can either create a csec.ini file on your own using the variables stated in this part of the section, or you can use the wizard that pops up during install to make a csec.ini file for you. To make a csec.ini file through the wizard, either run the file csecwiz.exe located in the c:\Program Files\IBM\Security folder or do a fresh install. On the last page (see figure Figure 6-15 on page 472), select **Save settings but do not configure subsystem**.

2. If you made a csec.ini file through the wizard, you will need to decrypt it before you can edit it. Look at 6.10.4, "Encrypt/Decrypt Setup Configuration File" on page 533 for more information.
3. Make the desired changes in the csec.ini file and copy it to a folder.
4. Extract the contents of the IBM Client Security Software installation package with WinZip (or similar application) to the same folder as described above. The directory structure needs to be the same as it was when the file was extracted.
5. Edit the szIniPath and szDir entries in the setup.iss file. The szDir entry is required for a mass installation and mass configuration. The szIniPath parameter is only required if you intend to perform a mass configuration. The full contents of this file is listed in Example 6-1 on page 477.
6. Before you are able to use the csec.ini file, you will have to encrypt it using the console. Refer to "Encrypt/Decrypt Setup Configuration File" on page 533 for more information.
7. Copy the files to the target system.
8. Create the \setup -s command prompt statement.

The -s parameter indicates an unattended installation. This command prompt statement should be run from the desktop of a user who has administrator rights. The StartUp program group or the Run key is a good place to do this.

9. Remove the command prompt statement on the next boot.

An example of the contents of the setup.iss file is listed below with a few descriptions:

Example 6-1 setup.iss file

```
[InstallShield Silent] Version=v6.00.000 File=Response File
szIniPath=d:\csssetup.ini
(The above parameter is the name and location of the .ini file, which is
required for mass configuration. If this is a network drive, it must be mapped.
When a mass configuration is not being used with a silent installation, remove
this entry.)
[FileTransfer] OverwrittenReadOnly=NoToAll
[{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-DlgOrder]
Dlg0={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdLicense- 0 Count=4
Dlg1={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdAskDestPath- 0
Dlg2={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdSelectFolder- 0
Dlg3={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdFinishReboot- 0
[{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdLicense-0] Result=1
[{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdAskDestPath-0] szDir=C:\Program
Files\IBM\Security
(The above parameter is the directory used to install Client Security. It must
be local to the computer.)
Result=1 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdSelectFolder-0] szFolder=IBM
Client Security Software
(The above parameter is the program group for Client Security.)
Result=1 [Application] Name=Client Security Version=5.00.002f Company=IBM
Lang=0009 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdFinishReboot- 0] Result=6
BootOption=
```

Mass configuration

The following file is also essential when initiating a mass configuration. The file can be given any name, as long as it has an .ini extension. This file can be created and distributed with the mass installation process. It can also be created and configured on any system and then distributed to all systems and then used just for a mass configuration.

Below is how the file should look. To the side is a brief description not to be included in the file. Each parameter must be on a separate line.

The following command runs this file from the command prompt when the mass configuration is not done along with a mass installation:

```
<CSS installation folder>\acamucli /ccf:c:\csec.ini
```

c:\csec.ini is the name of the mass configuration .ini file for our example.

Note: If any files or paths are on a network drive, the drive must be mapped to a letter.

[CSSSetup]	Section header for IBM Client Security Software setup.
suppw=bootup	Administrator/Supervisor password. Leave blank if not required.
hwpw=11111111	IBM Client Security Software hardware password. Must be eight characters. Always required. Must be correct if hardware password has already been set.
newkp=1	1 to generate a new admin key pair, 0 to use an existing admin key pair.
keysplit=1	When newkp equals 1, this determines the number of private key components. Note: If the existing keypair uses multiple private key parts, all private key parts must be stored in the same directory.
kpl=c:\jgk	Location of the admin key pair when newkp equals 1; if this is a network drive, it must be mapped.
kal=c:\jgk\archive	Location of the user key archive; if this is a network drive, it must be mapped.
pub=c:\jk\admin.key	Location of the admin public key when using an existing admin key pair; if this is a network drive, it must be mapped.
pri=c:\jk\private1.key	Location of the admin private key when using an existing admin key pair; if this is a network drive, it must be mapped.
clean=0	1 to delete the .ini file after initialization, 0 to leave the .ini file after initialization.
[UVMEnrollment]	Section header for user enrollment.
enrollall=0	1 to enroll all local user accounts in User Verification Manager, 0 to enroll specific user accounts in UVM.
defaultuvmpw=top	When enrollall equals 1, this will be the User Verification Manager passphrase for all users.
defaultwinpw=down	When enrollall equals 1, this will be the Windows password registered with User Verification Manager for all users.

enrollusers=2	When enrollall equals 0, this is the number of users that will be enrolled in User Verification Manager. Upgrading your version of IBM Client Security Software
user1=joseph	Enumerate number of users to be enrolled starting with 1, user names must be the account names. In order to get the actual account name on XP, do the following <ol style="list-style-type: none"> 1. Start Computer Management (Device Manager). 2. Expand the Local Users and Groups node. 3. Open the Users folder. The items listed in the Name column are the account names.
user1uvmpw=chrome	Enumerate the number of users to enroll with the User Verification Manager passphrase starting with 1.
user1winpw=spinning	Enumerate the number of users to enroll with a Windows passphrase registered with UVM starting with 1.
user1domain=0	0 to indicate that this account is local; 1 to indicate that this account is on the domain.
user2=hallie	
user2uvmpw=left	
user2winpw=right	
user2domain=0	
[UVMAAppConfig]	Section header for uvm-aware application setup and uvm-aware module setup.
uvmlogon=0	1 to use UVM logon protection, 0 to use Windows logon.
entrust=0	1 to use UVM for entrust authentication, 0 to use Entrust authentication.
notes=0	1 to use UVM protection for Lotus Notes, 0 to use Notes password protection.
passman=0	1 to use Password Manager; 0 to not use Password Manager
folderprotect=0	1 to use File and Folder Encryption; 0 to not use File and Folder Encryption.

6.4.7 Upgrading your version of IBM Client Security Software

Clients that have installed versions of Client Security prior to V5.0 should update their software to the latest level of IBM Client Security Software to take advantage of new Client Security features.

Important: Trusted Computing Platform Alliance systems that had IBM Client Security Software V4.0x installed must clear the chip before installing IBM Client Security Software V5.21 or later. Failure to do so might result in an installation failure or non-responsive software. Also, if you are upgrading from a version prior to IBM Client Security Software V5.0, you must decrypt all encrypted files before installing IBM Client Security Software V5.21 or later. IBM Client Security Software V5.21 or later cannot decrypt files that were encrypted using versions prior to IBM Client Security Software V5.0 because of changes in its file encryption implementation.

Upgrading with new security data

If you would like to completely remove IBM Client Security Software and start over, complete the following procedure:

1. Uninstall your previous version of IBM Client Security Software using the Control Panel Add/Remove Programs applet.
2. Restart the system.
3. Clear the IBM Embedded Security Chip in the BIOS utility.
4. Restart your system.
5. Install IBM Client Security Software V5.21 or later and configure it using the IBM Client Security Software Setup Wizard.

Upgrading using existing security data

If you would like to upgrade from a release of IBM Client Security Software prior to V5.0 using your existing security data, complete the following procedure:

1. Update your archive by completing the following steps:
 - a. Click the Windows **Start** button. Then select **Programs** → **Access IBM** → **IBM Client Security Software** → **Client Utility**.
 - b. Click the **Update Archive** button to ensure that your backup information is updated. Make note of the archive directory.
 - a. Exit the IBM Client Security Software Client Utility.

2. Remove the existing version of IBM Client Security Software by completing the following steps:
 - a. Locate the Administrator public and private keys that were created when you configured your previous version of IBM Client Security Software.
 - b. Select **Start** → **Settings** → **Control Panel** → **Add/Remove Programs** and choose to remove IBM Client Security Software.
 - c. Select **No** when prompted for a restart.
 - d. Shut down the system.
3. Clear the IBM Embedded Security Chip by completing the following steps:
 - a. Power on the system.
 - b. Press **F1** to enter the BIOS Setup utility.
 - c. Go to Security Chip settings, and clear the security chip.
 - d. Exit the BIOS Setup utility.

The system will continue its restart.
4. Run the IBM Client Security Software V5.21 or later installation program.
5. Restart when prompted.

Important: After restart, the IBM Client Security Software Setup Wizard will automatically launch. Do *not* run the Setup Wizard.

6. Click **Cancel** to exit the Setup Wizard.
7. Temporarily back up the default security policy by completing the following steps:
 - a. Using Windows Explorer, go to the IBM Client Security Software install directory (the default is c:\program files\ibm\security).
 - b. Right-click the **UVM_Policy** folder and select **Copy**.
 - c. Right-click the **Windows desktop** and click **Paste**.

This will create a temporary backup on the Windows desktop.

Note: Your existing security policy settings will be replaced with new defaults.

8. Restore settings from IBM Client Security Software V4.0x by completing the following steps:
 - a. Select **Start** → **Settings** → **Control Panel** → **IBM Client Security Subsystem** to open the IBM Client Security Software Administrator Utility main window.

- b. Click the **Key Configuration** button.
 - c. Select **Yes** to restore keys from the key archive.
9. Provide the location of the previous archive directory.
10. Provide the location of the Administrator public and private key files you created in the previous release. You will be notified that your archive will be updated for the new release.
11. Click **OK**.
12. Provide the location to create new Administrator keys. Be sure to create the keys in a location different from the location of your existing Administrator keys. If you have Administrator keys you already created for Release 5.21 on another system, you can select **Use an existing CSS Archive keypair** and provide the location of the existing keys.
13. Click **Next**. Your archive will be converted and restored.
14. Exit the application when finished.
15. Restore policy settings by completing the following steps:
 - a. Using Windows Explorer, go to the IBM Client Security Software install directory (the default is c:\program files\ibm\security).
 - b. Using the left-mouse button, drag the UVM_Policy folder from the desktop to the IBM Client Security Software install directory.
 - c. Click **Yes** to all warning messages.

Your security data has now been migrated to IBM Client Security Software V5.21 (or later).

Note: If you previously changed your security policy in IBM Client Security Software V4.0x, you might want to resubmit your security policy settings by completing the following steps:

1. Select **Start** → **Settings** → **Control Panel** → **IBM Client Security Subsystem**.
2. Click the **Configure Application Support and Policies** button.
3. Click **Application Policy**.
4. Click the **Edit Policy**.

Upgrading from Release 5.x using existing security data

If you would like to upgrade from IBM Client Security Software V5.0 to later versions of the software using your existing security data, complete the following procedure:

1. Update your archive by completing the following steps:
 - a. Select **Start → Programs → Access IBM → IBM Client Security Software → Modify Your Security Settings**.
 - b. Click the **Update Archive** button to ensure that your backup information is updated. Make note of the archive directory.
 - c. Exit the IBM Client Security Software User Configuration Utility.
2. Remove the existing version of IBM Client Security Software by completing the following steps:
 - a. Locate the Administrator public and private keys that were created when you configured your previous version of IBM Client Security Software.
 - b. Run csec51.exe.
 - c. Select **Upgrade**.
 - d. Restart the system.

6.5 Supplemental applications

Security applications and functions provided by the Embedded Security Subsystem include:

- ▶ Client Security Password Manager
- ▶ File and Folder Encryption (FFE)™

6.5.1 Client Security Password Manager

A component of IBM Client Security Software is the Client Security Password Manager. This utility, which incorporates encryption for peace of mind, is a convenient way to store and manage Internet and Microsoft Windows-based passwords, User IDs, and even common form entries. It can replace multiple passwords with a single password, passphrase or fingerprint.

Installing Client Security Password Manager

See 6.3, “Prerequisites” on page 452 for instructions on how to download the IBM Client Security Software Password Manager and its documentation.

Complete the following steps to install the Password Manager.

1. Run **pwmgr130us_002c.exe**.
2. The Welcome to the InstallShield Wizard for IBM Password Manager window opens. Click **Next**.
3. From the InstallShield Wizard License Agreement window, click **YES**.
4. From the Choose Destination Location window, click **Browse** to select the destination folder you want, then click **Next**.
5. From the InstallShield Wizard Complete window, click **Finish**.
6. Restart the system.

Configuring the Password Manager

The IBM Client Security Software Password Manager enables users to enter Web sites and applications using the Password Manager interface. The IBM Password Manager program encrypts and saves the information that is entered into the appropriate fields through the IBM Embedded Security Chip. Once the information is saved in Password Manager, these fields are automatically populated with this secure information whenever access to the Web site or application is granted according to the User Verification Manager user authentication policy.

Creating new entries

To enter password information into the Password Manager, complete the following procedure:

1. Open the application or Web site logon window.
2. Right-click the Password Manager icon in the Windows icon tray and select **Create**. You can also access the Password Manager Create function by pressing Ctrl+Shift+H.
3. Enter the information in the Password Manager - Create New Entry field.

Note: The information in this field must be less than 260 characters in length.

4. If you do not want the entered text to be displayed, select **Obscure typed text for privacy**.

Note: This check box only controls how the text is displayed within Password Manager. After the text is dropped into a Web site or application, its properties will be controlled by that application.

5. Using the Select Field target icon, drag the text from the Password Manager utility into the appropriate field on the Web site or application.

Note: This icon enables the text to be copied without using your computer clipboard or other non-secure locations.

6. Repeat step 3 through step 5 for each field, as necessary.
7. Click **Save New Entry**.
8. Select **Add Enter to automatically submit entry** if you want Password Manager to submit the login information after recalling.
9. Click **Save New Entry** to complete the procedure.

Managing entries

IBM Client Security Password Manager enables users to work with information stored in the Password Manager. The Password Manager- Manage window enables you to change your user ID, password, and other information entered into Password Manager that populate the fields on a Web site or application.

To change information stored in Password Manager, complete the following procedure:

1. Right-click the Password Manager icon in the Windows icon tray and click **Manage**. You can also access the Password Manager Manage function by pressing **Ctrl+Shift+B**.
2. Enter your User Verification Manager passphrase, or complete the access requirements specified by the User Verification Manager user authentication policy.
3. Edit your information. You have the following options:
 - a. To edit entry information, right-click the entry you want to edit. Select from the following actions:
 - i. **Add Enter**
Select **Add Enter** to automatically have your entry information entered into the Web site or application. A check icon will appear next to Add Enter when this function is activated.
 - ii. **Delete**
Select **Delete** to delete the entry entirely.
 - iii. Click **Save Changes**.
 - b. To edit entry field information, right-click the field you want to edit. Select from the following actions:

- i. Change entry field
Select **Change Entry Field** to change the information stored for this field. You can change an entry field in one of the following ways:
 - By creating a randomized entry
To create a randomized entry, select **Randomize**. Password Manager will create randomized entries that are 7, 14, or 127 characters in length.
 - By manually editing an entry field
To manually edit an entry field, select **Edit** and make the appropriate changes to the field.
 - ii. Delete entry field
Select **Delete** to delete the entry field entirely.
 - iii. Click **Save Changes**.
4. Click **Save Changes**.

Note: Changing a field in Password Manager will only update the login information within Password Manager. If you want to increase the security of your passwords by using the Password Manager randomize feature, you must synchronize the application or Web site with the new random password generated by this feature. Use the convenient Password Manager Transfer Field Tool to transfer the new randomized password into the application or Web site *Change Password* form. Verify that the new password is valid for the application or Web site and then use the Save Changes in the Password Manager - Manage window. There is no need to re-create the entry with the new password since all the necessary information has been retained.

Recalling entries

Recalling passwords using the Password Manager is simple and easy. To do this, complete the following procedure:

1. Open the application or Web site logon window for the information that you want to recall.
2. Double-click the **Password Manager** icon in the Windows icon tray. Password Manager will populate the fields on the logon window with the stored information. You can also access the Password Manager recall function by pressing **Ctrl+Shift+G**.

Note: The IBM Password Manager does not support icon tray functionality on computers running the Windows NT operating system. If you are using a Windows NT system, use the keyboard shortcut.

3. Enter your User Verification Manager passphrase, or complete the access requirements specified by the User Verification Manager user authentication policy.
4. If the *Add Enter to automatically submit entry* check box is not checked, click the **Submit** button on the application or the Web site.

If no entry is recalled, a prompt will ask you if you would like to create a new entry. Click **Yes** to launch the Password Manager - Create New Entry window.

6.5.2 File and Folder Encryption (FFE)

IBM Embedded Security Subsystem offers the user two types of encryption: on-the-fly and individual encryption. They give the client the ability to encrypt and decrypt files and folders located on a local hard disk drive. On-the-fly functionality means an administrator can specify that all files saved to a specific folder be automatically encrypted, so there are no extra steps for the user. Because the encryption and decryption processes are transparently managed by the Embedded Security Subsystem, no modification is required for applications to use on-the-fly encryption. For stronger encryption protection, an encryption policy can be written to require additional authentication. The user can be prompted for a pass phrase or fingerprint for the encryption/decryption to take place. Stronger encryption is not transparent when using applications; the user must decrypt files prior to use. This function helps protect valuable data from being viewed by an unauthorized user when the system is connected to a network, accessed while the owner is away (as in a lunchtime attack) or in the event of physical theft—a serious concern, especially with mobile computers. Both forms of encryption use the latest encryption standard, the Advanced Encryption Standard (AES). The Embedded Security Subsystem protects the key used during encryption.

Installing IBM File and Folder Encryption

Before beginning installation of File and Folder Encryption, review 6.2.2, “File and Folder Encryption considerations” on page 451.

See 6.3, “Prerequisites” on page 452 for instructions on how to download File and Folder Encryption software and documentation.

Complete the following steps to install File and Folder Encryption software.

1. Run `ffe201us_010b.exe`.
2. The Welcome to the InstallShield Wizard for IBM File and folder Encryption window opens. Click **Next** to unpack the installation file.
3. The Welcome to the InstallShield Wizard for IBM File and folder Encryption window opens. Click **Next** to begin the installation.

4. At the InstallShield Wizard License Agreement window, click **YES**.
5. At the Choose Destination Location window, click **Browse** to select the destination folder you want, then click **Next**.
6. From the Select Program Folder, choose the program folder into which you would like place the program icons. Click **Next**.
7. At the InstallShield Wizard Complete window, click **Finish**.
8. An information window will display telling you that you must enable FFE in the IBM ESS Administration Utility before FFE can be used. Click **OK** to close the window.
9. Restart the system.

Note: File and Folder Encryption is different from the right-click encryption that comes with the basic IBM Client Security Software. You do not need to install File and Folder Encryption unless you are seeking the on the fly capability to protect folders.

Configuring IBM File and Folder Encryption

Before using File and Folder Encryption, review 6.2.2, “File and Folder Encryption considerations” on page 451.

A folder can be in any one of the following states; each state is handled differently by the right-click protect folder option:

► An Unprotected Folder

Neither this folder, its subfolders, nor any of its parents has been designated as protected. The user is given the option to protect this folder.

► A Protected Folder

A protected folder can be in one of three states:

– Protected by the current user

The current user has designated this folder as protected. All files are encrypted, including files in all subfolders. The user is given the option to unprotect the folder.

– A subfolder of a folder protected by the current user

The current user has designated one of this folder’s parents as protected. All files are encrypted. The current user has no right-click options.

– Protected by a different user

A different user has designated this folder as protected. All files are encrypted, including files in all subfolders, and they are unavailable to the current user. The current user has no right-click options.

► A Parent of a Protected Folder

A parent of a protected folder can be in one of three states:

- It can contain one or more subfolders protected by the current user. In this state, the current user has designated one or more subfolders as protected. All files in the protected subfolders are encrypted. The user is given the option to protect the parent folder.
- It can contain one or more subfolders protected by one or more different users. In this state, a different user (or users) has designated one or more subfolders as protected. All files in the protected subfolders are encrypted and are unavailable to the current user. The current user has no right-click options.
- It can contain subfolders protected by the current user and one or more different users. Both the current user and one or more different users have designated subfolders as protected. The current user has no right-click options.

► A Critical Folder

A critical folder is a folder in a critical path; therefore, it cannot be protected. There are two critical paths: the Windows path and the IBM Client Security Software path.

Each state is handled differently by the right-click protect folder option.

Right-click file protection

Files can be encrypted and decrypted manually through the right-click menu. When files are encrypted in this manner, the encryption operation appends a `.enc` extension to the files. These encrypted files can then be securely stored on remote servers. They will remain encrypted and unavailable for use by applications until the right-click facility is used again to decrypt them.

Right-click file and folder protection

A user that has been verified through the User Verification Manager can select a folder to protect or unprotect using the right-click interface. This will encrypt all of the files contained in the folder or any of its subfolders. When files are protected in this manner, no extension is appended to the file name. When an application tries to access a file in an encrypted folder, the file will be decrypted into memory and will be re-encrypted before it is saved on the hard disk.

Any Windows operation that tries to access a file in a protected folder will be given access to the data in a decrypted form. This feature adds ease-of-use so that a file does not have to be decrypted before it is used, and then re-encrypted after a program is finished with it.

File and Folder Encryption utility limitations

The IBM FFE utility has the following limitations:

- ▶ The limitations when moving protected files and folders are:

- Moving files and folders within protected folders
- Moving files or folders between protected and unprotected folders

If you attempt to perform either of these unsupported Moves, the operating system will display an Access Denied message. This message is normal. It simply provides notification that this task is not supported. Instead of moving these files and folders, do the following:

- a. Copy the protected files or folders to the new location.
- b. Delete the original files or folders by using the **Shift+Del** key combination.

- ▶ The IBM FFE utility does not support running applications from a protected folder. For example, if you have an executable file named PROGRAM.EXE, you cannot run that application from a protected folder.
- ▶ There is a path name limitation. As you attempt to protect a folder using the IBM FFE utility or attempt to copy or move a file or folder from an unprotected folder to a protected folder, you might receive a One or more path names are too long message from the operating system. If you receive this message, you have one or more files or folders that have a path that exceeds the maximum allowable character length. To correct the problem, either rearrange the folder structure to shorten its depth or shorten some of the folder or file names.
- ▶ If you attempt to protect a folder and receive a message stating, The folder cannot be protected, one or more files may be in use. Check the following:
 - Verify that none of the files contained in the folder are currently in use.
 - If Windows Explorer is displaying one or more subfolders of a folder that you are attempting to protect, make sure that the folder you are attempting to protect is the one that is highlighted and active and not any of the subfolders.

File and Folder Encryption known issues

IBM File and Folder Encryption might encounter problems when using any application that re-partitions the hard drive.

You should disable File and Folder Encryption before using an application that re-partitions the computer hard drive because these types of applications might interfere with vital FFE operations. Applications that re-partition the hard drive include:

- ▶ PowerQuest PartitionMagic
- ▶ IBM Rescue and Recovery

To disable FFE, complete the following procedure:

1. From the Control Panel, select **IBM Client Security Software Subsystem**.
2. Click the **Configure Application Support and Policies** button.
3. Deselect the **Enable File and Folder protection** check box.
4. Restart the system.

For more known issues and limitations, see 6.15.3, “File and Folder Encryption utility known issues” on page 575.

6.6 Administrator Utility

The IBM Security Subsystem Administrator Utility is the heart of your IBM Embedded Security Subsystem. This is where you control all the different policies and settings for your machine. The IBM Security Subsystem Administrator Utility is a place that is controlled by the security administrator password. You should be careful about what users you want to allow into this utility.

Using the IBM Security Subsystem Administrator Utility, you can perform the following tasks:

- ▶ Add and remove users.
- ▶ Configure application support and policies.
- ▶ Configure the systems passphrase policy.
- ▶ Change the machines key settings.
- ▶ Change the machines chip settings.

6.6.1 Starting the Administrator Utility

Use this procedure to start the Administrator Utility:

1. Select **Start** → **Control Panel**. Navigate to the icon named IBM Embedded Security Subsystem
2. You will be prompted to enter your security administrator password. Enter your password in the field provided and click **OK**. This opens the main menu of the Administrator Utility, which resembles the window shown in Figure 6-19 on page 492.

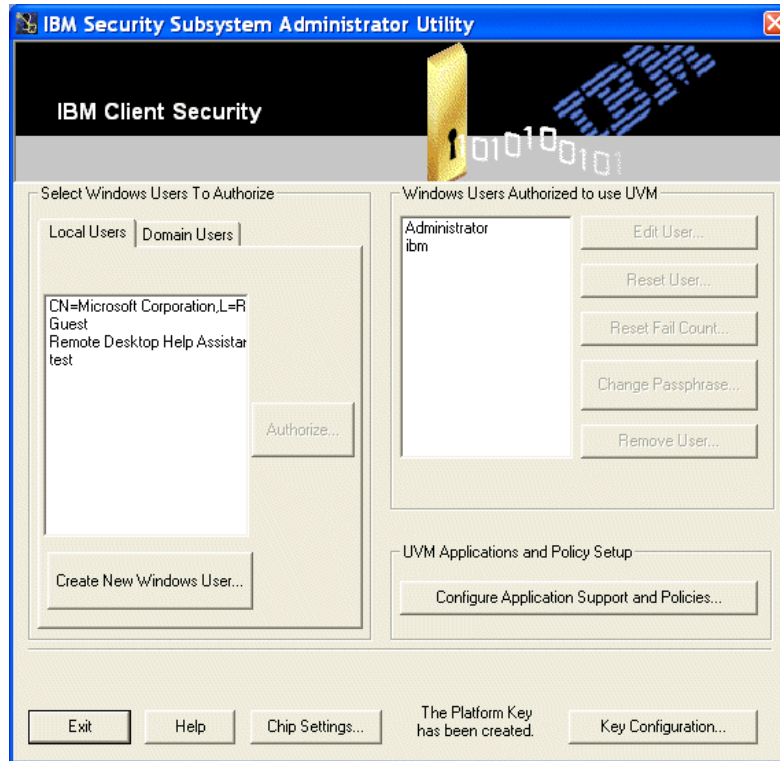


Figure 6-19 IBM Security Subsystem Administrator Utility

The Administrator Utility is divided into the following four main parts:

1. Enroll users (refer to 6.6.2, “User enrollment”).
2. Edit user settings (refer to 6.6.3, “Edit user settings” on page 494).
3. Application and policy setup (refer to 6.6.4, “Application and policy setup” on page 499).
4. Chip and key settings (refer to 6.6.5, “Chip and key settings” on page 508).

6.6.2 User enrollment

Before a user can use any of the IBM Embedded Security Subsystem features, you have to add the user to the system using the Administrator Utility.

There are two types of possible users:

- Local Users
- Domain Users

Local Users

If you would like to add a local user, see Figure 6-5 on page 465.

Domain Users

If you would like to add a Domain user, perform the following procedure (refer to Figure 6-5 on page 465):

1. Follow the steps in 6.6.1, “Starting the Administrator Utility” on page 491 to start the Administrator Utility.
2. In the area marked *Select Windows Users To Authorize*, click **Domain Users**. An empty list appears.
3. To retrieve a list of the domain users in your network, click **Refresh List**. A message tells you that it might take a long time to retrieve. If you have many users in your domain, it will.
4. Click **OK** to continue. After the domain controller processes your request, all your domain users will appear in the list.
5. Browse to your desired user and click it.
6. Click **Authorize**. A new window opens that asks you to type in the UVM Passphrase that you would like to use for this user. This is shown in Figure 6-6 on page 466. Please note that this passphrase is totally independent and does not have to be the same as the Windows password. You are free to use whatever you want as a password as long as you match the passphrase requirements.
7. Type in the passphrase twice and select the passphrase expiration option. When finished, click **Next**. A message confirms that the operation went well.
8. Click **OK** on that message.

A new window will appear asking you if you would like to store the Windows password in this user’s profile. This window will resemble the one shown in Figure 6-40 on page 533. You have two options:
 - Have the user store the Windows password later (at logon or with the User Configuration Utility)
 - Store user’s current Windows password now
9. Select what you want to do, enter any required information, then click **Next**. A new window tells you that the operation completed successfully.
10. Click **Finish**.

After the information is stored on the IBM Embedded Security Chip, your user should appear in the field marked Windows Users Authorized to use UVM.

Note: The machine must be a member of a domain to be able to import domain users. You can add domain users manually but the spelling of the user name has to be exact. To manually add a user, just type in the username in the input field on the Domain Users' pane and click **Authorize**. The rest of the procedure is as previously described.

Create New Windows User

Next, you may want to create new Windows Users by clicking the **Create New Windows User** under the heading labeled *Select Windows Users To Authorize*. If you do, the Windows User Account program will appear. You can add local users from this window.

6.6.3 Edit user settings

As soon as you have added your users to IBM Embedded Security Subsystem, you can modify the user settings in the Administrator Utility with the following tasks:

- ▶ Edit user.
 - Change UVM passphrase expiration (page 495).
 - Change windows password stored by UVM (page 496).
 - Register fingerprints and smart cards (page 496).
- ▶ Reset user ("Reset User" on page 497).
- ▶ Reset fail count ("Reset fail count" on page 498.)
- ▶ Change passphrase ("Change Passphrase" on page 498).
- ▶ Remove user ("Remove user" on page 498).

Edit User

This button allows you to change a user's authentication elements. To begin editing, use the following procedure:

1. Start the Administrator Utility as described in 6.6.1, "Starting the Administrator Utility" on page 491
2. Click the user you would like to change in the area marked *Windows Users Authorized to use UVM*.

3. Click **Edit User** to open the window shown in Figure 6-20.

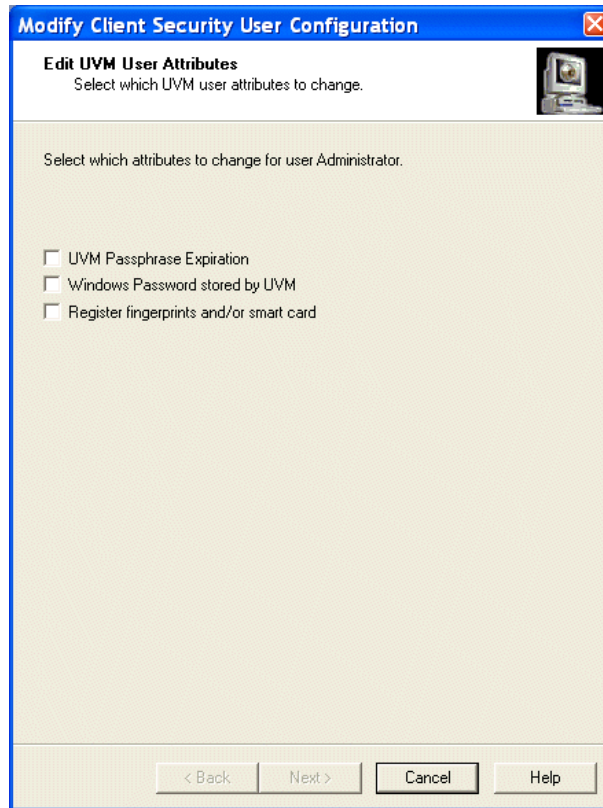


Figure 6-20 Modify Client Security User configuration

4. Depending on whether you have a fingerprint reader or a smart card reader installed on your machine, you may have either two or three options on this window. This is how you can use the three options:

Note: Please note that you will return to the main menu in the IBM Security Subsystem Administrator Utility if you make any changes in any of these menus. You might therefore have to click **Edit User** several times if you would like to perform multiple tasks on a user in this window.

- Change UVM passphrase expiration

This option allows you to change the expiration policy on a user's passphrase. Here is how to use it:

- i. Select the **UVM Passphrase Expiration** check box. Click **Next**.

A new window asks you to provide the path to your archive location and your private key.

- ii. Browse or type in the requested location. This location is not set up as a default and could be anywhere on your computer, depending on where you instructed the computer to put the keys during installation. After you have found your files, click **OK**. A new window that allows you to change the passphrase expiration for the selected user opens.
- iii. Change the user's password expiration policy as wanted and click **Next**. The information is saved to the IBM Embedded Security Subsystem and could take a while. Upon completion a confirmation page will display.
- iv. Click **Finish** on the confirmation page. Your machine will be returned to the main menu in the Administrator Utility.

– Windows Password stored by UVM

This function is used to change the Windows logon password that is stored through the IBM Embedded Security Subsystem. The user can also change this through the Modify Your Security Settings program as shown in Figure 6-29 on page 521. Here is how to use it:

- i. Select **Windows Password stored by UVM**.
- ii. Click **Next**. A new window opens that allows you to change your Windows logon password. Select from the following:
 - Store Windows password at logon or by the User Configuration Utility.
 - Store user's current Windows password now.
- iii. Enter the desired information and click **Next**. A confirmation page opens.
- i. Click **Finish** on the confirmation page. You will be returned to the main menu of the Administrator Utility.

– Register fingerprints and/or smart card

This option is only available if you have installed a fingerprint reader or a smart card reader/writer that is supported by the IBM Embedded Security Subsystem. This option allows you to enroll fingerprints for the selected user or to configure the user's smart card. The user can also change this him/herself through the Modify Your Security Settings program as shown in Figure 6-32 on page 524.

Here is how to use it:

- i. Select **Register fingerprints and/or smart card**. Click **Next**. A new window opens that asks you to select between enrolling fingerprints or a smart card.

- ii. Click the device type you would like to configure. You are only allowed to select supported devices that are already installed.
- iii. Follow the instructions on the monitor to complete your registration. For information about how to enroll fingerprints “Registering fingerprints” on page 515.

To ensure maximum security, you must provide to the system the user’s passphrase during the enrollment of these types of devices.

- iv. When asked for the user’s passphrase, type it into the input field and click **OK**.
- v. After you have configured your device for your user, a confirmation window opens. Click **OK**.
- vi. When you have configured all your options in the different device menus, click **Exit**. This will return you to the UVM Enabled Devices window.
- vii. Click **Next** on that menu when finished. A new confirmation page opens.
- viii. Click **Finish**. You will then be returned to the IBM Security Subsystem Administrator Utility main menu.

Reset User

This button can be used to reset all the data that is stored for that user. This means resetting keys, certificates, fingerprints and stored password. If there is something totally wrong with the user’s security profile, use this button. You should not use this button unless something is really wrong. It will reset all the data for the selected user.

Here is how to use it:

1. In the Windows Users Authorized to use UVM panel, click the users you want to change.
2. Click the **Reset User** button. A new window asks you to confirm that you really want to reset the selected user.
3. If this is your intention, click **Yes**.
4. After some processing, you will have to provide the IBM Embedded Security Subsystem with a passphrase, windows password, and fingerprint or smart card, if used. After you enter that information, a new window informs you that the operation was complete.
5. Click **Finish** and you will be returned to the main menu again.

Reset fail count

If a user has typed in too many wrong passphrases, the machine will lock up for a certain amount of time. See 6.15.2, “Fail counts on TCPA and non-TCPA systems” on page 574 for an explanation of the reason for this lockout. If you want to reset this so that the user does not have to wait anymore, you can use this button.

Here is how to use it:

1. In the Windows Users Authorized panel, click the users you wish to reset.
2. Click **Reset Fail Count**. A new asks you for the user's passphrase.
3. Type in the user's passphrase and click **OK**.
4. That users fail count will then be reset.

Note: You have to know the user's passphrase. This is to prevent unauthorized access to that users profile.

Change Passphrase

If you want to change a user's passphrase, you can do this by clicking **Change Passphrase**. The user can also do this by using the Modify Your Security Settings program as shown in Figure 6-29 on page 521:

The following procedure is what an administrator use to change the passphrase:

1. In the Windows Users Authorized to use UVM panel, click the user you would like to change.
2. Click **Change Passphrase**. A new window asks you to provide the IBM Embedded Security Subsystem with the path to the machine's security keys.
3. Browse to the location of your key files. This location is not set up as a default and could be anywhere on your computer, depending on where you instructed the computer to put the keys during installation. After you have found your files, click **OK**.

A new window asks you to type in the new passphrase and the expiration policy for this user. This window will resemble the one shown in Figure 6-39 on page 532.

4. Fill in the new passphrase for the selected user and click **Next**. A confirmation window opens.
5. Close the confirmation window by clicking **Finish**.

Remove user

If you no longer want a user to have access to the IBM Embedded Security Subsystem and its features, you can remove the user with the Remove User button. All information stored about that user will be lost if you use this function.

The user might be able to log on to windows after your remove him or her, but he or she will not be able to use any of the security functions.

Here is how to use it:

1. In the panel labeled *Windows Users Authorized to use UVM*, click the user you wish to remove.
2. Click **Remove User**. A new window asks you to confirm that you really want to remove the selected user.
3. If this is your intention, click **Yes**. A new window asks you if you would like to remove the user's archived information.
4. Click **Yes** or **No**, depending on the desired outcome. If you click **Yes**, all information about that user will be lost and you will not be able to restore any data for that user afterwards.
5. After a moment, the user will disappear from the list in the Windows Users Authorized to use UVM panel.

6.6.4 Application and policy setup

In the Application and policy setup part of the IBM Security Subsystem Administration Utility, you can configure the settings for certain applications or occurrences. This includes, for example, how your IBM Embedded Security Subsystem reacts when you would like to sign an e-mail. This part of the IBM Security Subsystem Administrator Utility is one of the most important functions you will have to deal with. With the settings on this menu, you can really set the strength of your security by adjusting your settings to exactly fit your needs or those of your company.

From the main menu in the IBM Security Subsystem Administrator Utility (refer to Figure 6-19 on page 492) click **Configure Application Support and Policies**. This will open the menu shown in Figure 6-21 on page 500.

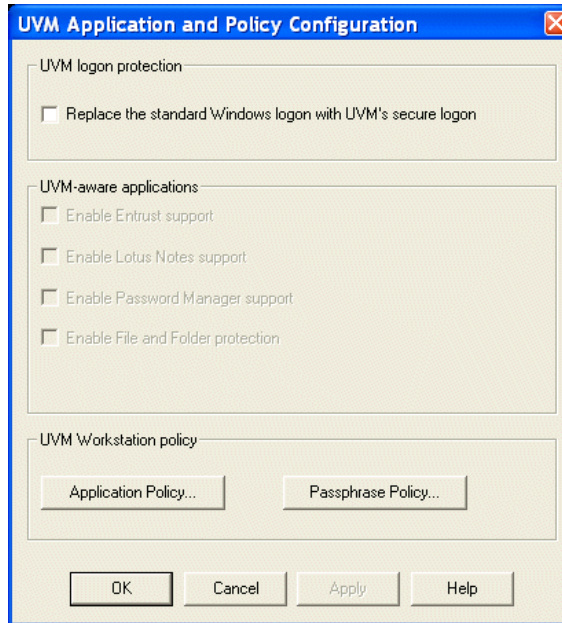


Figure 6-21 UVM Application and Policy Configuration

Supported applications

Depending on what applications you have installed on your computer, some items might be grayed out, and others might be available. Make the appropriate selection to enable support for one or more of these applications:

► Replace the standard Windows logon with UVM's secure logon

If you make this selection, the original Windows logon window is replaced by a new IBM secure logon window.

Important: Users that are not enrolled in the IBM Embedded Security Subsystem will not be able to log on to the machine if you replace their Windows logon with the IBM secure logon.

► Enable Entrust support

This selection enables support for solutions from Entrust.

► Enable Lotus Notes support

This option enables support for Lotus Notes and includes automatic logon to Notes.

► **Enable Password Manager support**

This option enables support for Password Manager. You will not be able to use Password Manager until you make this selection, even when it is installed.

► **Enable File and Folder Protection**

This option enables support for File and Folder Protection. You will not be able to use File and Folder protection before this box is checked even though it is installed.

After you have selected the applications you would like to enable, click either **OK** or **Apply** to save the changes.

As you can see from Figure 6-21 on page 500, there are also two buttons at the bottom of the window under the heading: UVM Workstation Policy. These buttons are Application Policy and Passphrase Policy.

Application Policy

The Application Policy menu is where you configure how the software is supposed to react to different security events on your machine. This is also where you configure the authentication requests that communicate with the IBM Embedded Security Subsystem.

Before you attempt to edit the UVM Application Policy for the local client, make sure that at least one user is authorized to use UVM. Otherwise, an error message appears when the policy editor attempts to open the local policy file. Then follow the steps below:

1. From the UVM Application and Policy Configuration window, click **Application Policy....** (see Figure 6-21 on page 500). The window shown in Figure 6-22 on page 502 opens.

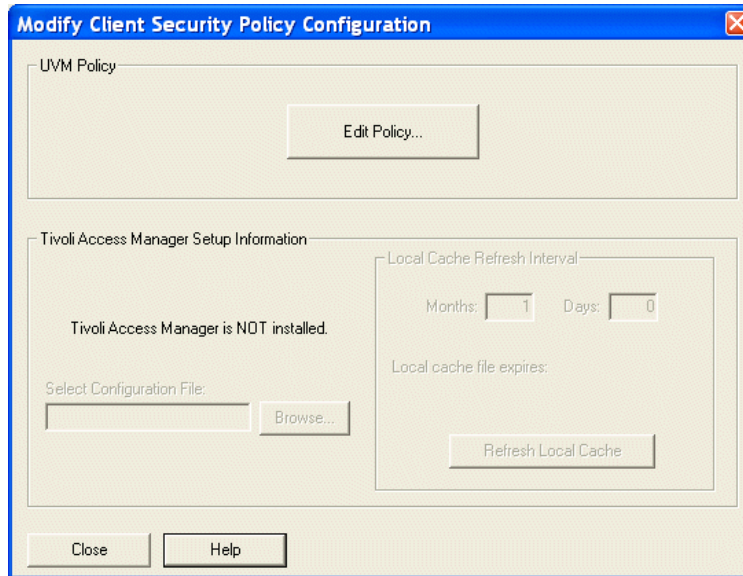


Figure 6-22 Modify Client Security Policy Configuration

If you have Tivoli Access Manager installed, you can configure IBM Client Security Software to communicate with Tivoli to manage and change your policies. For more information about how to combine Tivoli and the IBM Embedded Security Subsystem, see 6.15.11, “Tivoli Access Manager troubleshooting information” on page 587.

2. To change your policy without Tivoli, click **Edit Policy**. A new window asks for your security administrator password.
3. Enter the password and click **OK**. This password is the same password that you used to log into the IBM Security Subsystem Administration Utility. After you click **OK**, a new window (Figure 6-23 on page 503) opens.

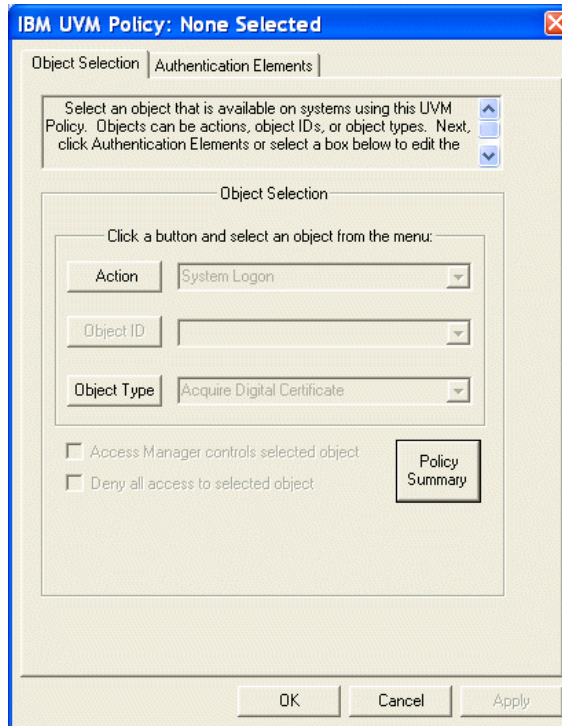


Figure 6-23 IBM UVM Policy

As you can see from Figure 6-23, you have several options. Since we are not using Tivoli Access Manager in this example, some options are grayed out. For more information about using Tivoli Access Manager, see 6.15.11, “Tivoli Access Manager troubleshooting information” on page 587.

On a machine without Tivoli Access Manager installed there are two main event types you can change:

- Action
- Objects type

Valid UVM actions include the following:

- System Logon

This object controls authentication requirements necessary to log onto the system.

- System Unlock

This object controls authentication requirements necessary to clear the Client Security screen saver.

- Lotus Notes Logon
This object controls authentication requirements necessary to log onto Lotus Notes.
- Lotus Notes Change Password
This object controls authentication requirements necessary to use UVM to generate a random Lotus Notes password.
- Digital Signature (e-mail)
This object controls authentication requirements necessary when you click the Sign button in Microsoft Outlook or Outlook Express.
- Decryption (e-mail)
This object controls authentication requirements necessary when you click the Decrypt button in Microsoft Outlook or Outlook Express.
- File and Folder Protection
This object controls authentication requirements necessary when right-click encryption and decryption has been selected.
- Password Manager
This object controls authentication requirements necessary when you use the IBM Password Manager, which is available from the IBM Web site. When activated, most users should leave this setting as *No passphrase required after 1st used this way*.
- Netscape - PKCS#11 Logon
This object controls authentication requirements necessary when a PKCS#11 C_OpenSession call is received by the PKCS#11 module. Most users should leave this setting as *No passphrase required after 1st used this way*.
- Entrust Logon
This object controls authentication requirements necessary when Entrust issues a PKCS#11 C_OpenSession call to be received by the PKCS#11 module. Most users should leave this setting as *No passphrase required after 1st used this way*.
- Change Entrust Logon Password
This object controls authentication requirements necessary to change the Entrust logon password. Entrust does this by issuing a PKCS#11 C_OpenSession call to be received by the PKCS#11 module. Most users should leave this setting as “No passphrase required after 1st used this way.”

Valid UVM object types include: Acquire Digital Certificate

This object controls authentication requirements necessary when you acquire a digital certificate.

4. The procedure for changing the policy for one or more of these objects is described below:
 - a. Click either **Action** or **Object Type**.
 - b. Select the object you would like to change from the menu.
 - c. On the top of the IBM UVM Policy menu (refer to Figure 6-23 on page 503), click **Authentication Elements** to open the window shown in Figure 6-24.

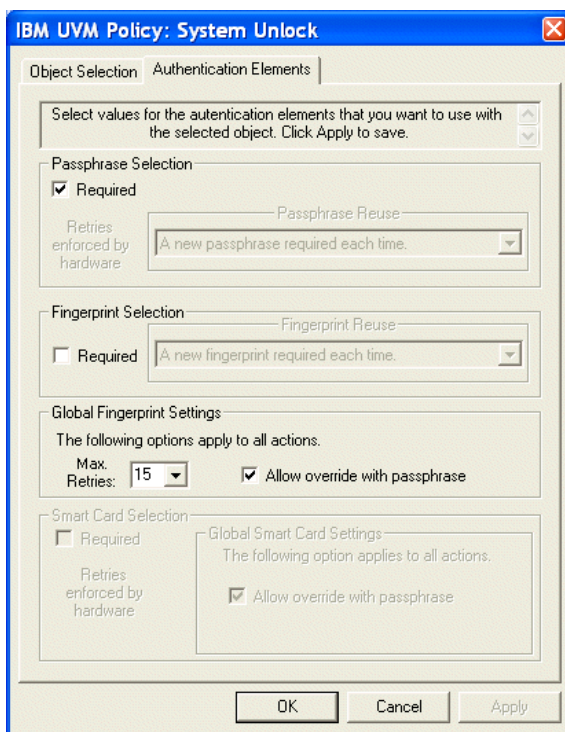


Figure 6-24 IBM UVM Policy

- d. Make your desired changes to the policy. Some alternatives are grayed out. This is because you do not have the device installed. Install the device first to make this option available.

You have many possibilities on how to set policy. You can require no, one, or several types of authentications. It is just a matter of your preferences.

Select from the following options:

- Passphrase Selection

This selection enables an administrator to establish that the UVM passphrase be used to authenticate a user in any of the following three ways:

- A new passphrase required each time.
- No passphrase required after 1st used this way.
- No passphrase required if given at system logon.

- Fingerprint Selection

This selection enables an administrator to establish that a fingerprint scan be used to authenticate a user in any of the following three ways:

- A new fingerprint required each time.
- No fingerprint required after 1st used this way.
- No fingerprint required if given at system logon.

- Global Fingerprint Settings

This selection enables an administrator to establish a maximum number of authentication retries before the system will lock out a user. This area also enables the administrator to allow fingerprint authentication protection to be overridden with the UVM passphrase.

- Smart Card Selection

This selection enables an administrator to require that a smart card be provided as an additional authentication device.

- Global Smart Card Settings

This selection enables an administrator to set the policy to allow overrides when the UVM passphrase is provided and can also be set to lock the computer whenever the smart card is removed. This option is only available if the UVM-secure logon is enabled.

5. If there are more policies you would like to change at the same time, click the **Object Selection** tab on the top of the menu in the UVM Policy window. Select another object and make the policy changes again as described previously. When you are finished with setting up your policies, click **OK**.
6. You will be prompted for the location of your private key. Navigate to the place where the private1.key is located and select it.
7. When you have selected it, click **OK**. Your policy changes are saved to your IBM Embedded Security System.

Editing a UVM policy on remote clients

To use UVM policy across multiple IBM clients, edit and save UVM policy for a remote client, and then copy the UVM policy file to other IBM clients. If you install Client Security in its default location, the UVM policy file will be stored as \Program Files\IBM\Security\UVM_Policy\remote\globalpolicy.gvm.

Copy the following files to other remote IBM clients that will use this UVM policy:

- ▶ \IBM\Security\UVM_Policy\remote\globalpolicy.gvm
- ▶ \IBM\Security\UVM_Policy\remote\globalpolicy.gvm.sig

If you installed IBM Client Security Software in its default location, the root directory for the preceding paths is \Program Files. Copy both files to the \IBM\Security\UVM_Policy\ directory path on the remote clients.

Passphrase Policy

The second button that is available in the UVM Application and Policy Configuration window (see Figure 6-21 on page 500) is the Passphrase Policy button. This button allows you to change the way the passphrase of any user on the machine must be used.

1. From the UVM Application and Policy Configuration window, click the **Passphrase Policy...** button.
2. A new window opens that resembles the one in Figure 6-25 on page 508.

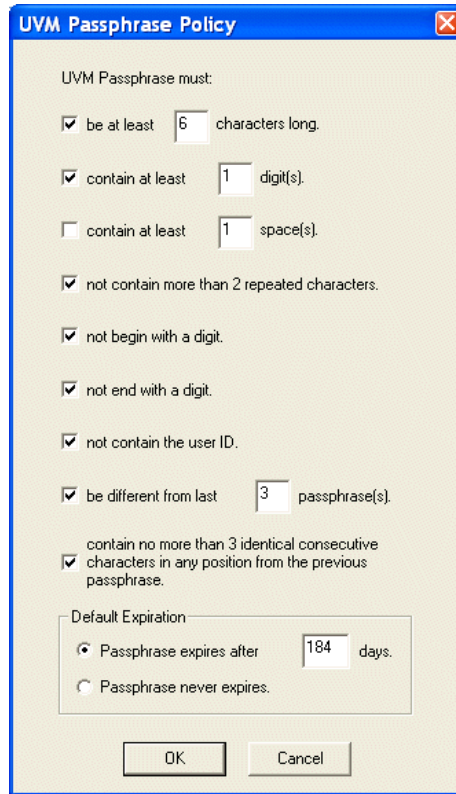


Figure 6-25 UVM Passphrase Policy

3. Change the items that you would like to change.
4. Click **OK**. A new window asks you for the location of the private1.key file.
5. Navigate to the place where the private1.key is located and select it.
6. Click **OK**. Your passphrase policy changes will then be saved to your IBM Embedded Security System.

6.6.5 Chip and key settings

The two last buttons on the main menu of the IBM Security Subsystem Administrator Utility (see Figure 6-19 on page 492) are Chip Settings and Key Configuration. These two buttons are very seldom used; however, they provide a more advanced way of managing the IBM Embedded Security Subsystem.

Chip Settings

This option allows you to access some information about the built-in security chip on the machine. From the main menu of the Administrator Utility, click the **Chip Settings...** button. This opens a window that resembles the one in Figure 6-26.

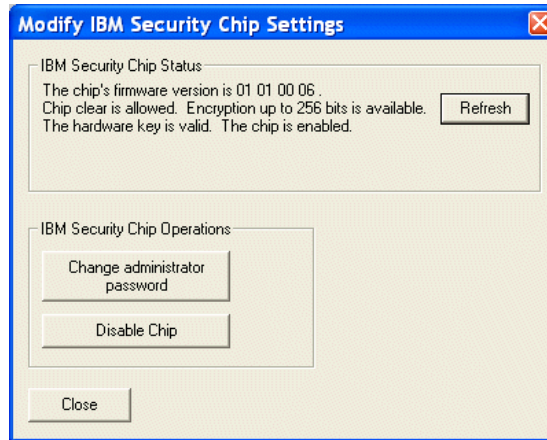


Figure 6-26 *Modify IBM Security Chip Settings*

There are three areas in this window:

- ▶ IBM Security Chip Status
- ▶ Change administrator password
- ▶ Disable chip

IBM Security Chip Status

The following information about the IBM Embedded Security Chip and IBM Client Security Software is available by clicking **Chip Settings** button:

- ▶ The version number of the firmware used with IBM Client Security Software
- ▶ The encryption status of the IBM Embedded Security Chip
- ▶ The validity of the hardware encryption keys
- ▶ The status of the IBM Embedded Security Chip

Change administrator password

This option allows you to change the security chip administrator password on the machine (not the windows administrator password). To do this, follow these steps:

1. Click the **Change administrator password** button in the Modify IBM Security Chip Settings window. A new window asks you to type in the new IBM Embedded Security Subsystem administrator password.

2. Type in the new password twice and click **OK**. After processing, you will receive a confirmation message.
3. Click **OK** on the confirmation message. You now have a new administrator password for your security system.

Disable chip

The IBM Security Administrator Utility provides a way to disable the IBM Embedded Security Chip. To prevent unauthorized users from disabling the chip, the Administrator Utility requires someone with administrator authority to disable the chip.

Important: Do not disable the chip if UVM protection is enabled for the system logon. If you do, you will be completely locked out of the system. To clear UVM protection, open the Administrator Utility and click the **Replace the standard Windows logon with UVM's secure logon** check box to remove the check mark. You must restart the computer before UVM protection for the system logon is disabled.

To disable the IBM Embedded Security Chip, follow this procedure:

1. In the Modify IBM Security Chip Settings window, click the **Disable Chip** button.
2. Follow the on-screen instructions.
3. If your computer has Enhanced Security enabled, you might have to type the administrator password that was set in the Configuration/Setup Utility to disable the chip.
4. To use the IBM Embedded Security Chip and hardware encryption keys after the chip is disabled, the chip must be re-enabled.

Key Configuration

As the name implies, the key configuration window is the place where you can make changes to your keys. This is a part of the IBM Security Subsystem Administrator Utility that is very seldom used.

From the IBM Security Subsystem Administrator Utility window (see Figure 6-19 on page 492), click **Key Configuration**. A window such as the one in Figure 6-27 on page 511 opens.

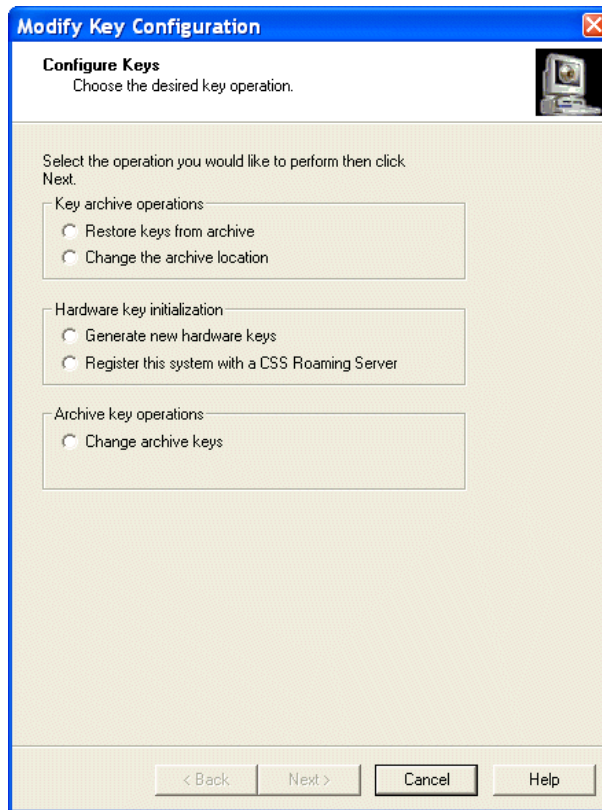


Figure 6-27 *Modify Key Configuration*

As you can see in Figure 6-27, there are five options on this window:

- ▶ Restore keys from archive, discussed on page 511
- ▶ Change the archive location, discussed on page 512
- ▶ Generate new hardware keys, discussed on page 513
- ▶ Register this system with a IBM Client Security Software Roaming Server, discussed on page 513
- ▶ Change archive keys, discussed on page 514

Restore keys from archive

You might need to restore keys if you have replaced a system board or a failed hard disk drive. When you restore keys, you are copying the most recent user key files from the key archive and storing them on the IBM Embedded Security Chip. These copied user key files appear in the directory where they were previously stored on the computer, such as on a network directory or diskette.

If a hard disk drive failure in the computer compromises the integrity of the user keys, you can restore the keys from the key archive. Restoring the keys will overwrite any keys that have been stored.

If you replace the system board in your computer with a system board that contains the IBM Embedded Security Chip, and the encryption keys are still valid on your hard disk drive, you can restore the encryption keys that were previously associated with the computer by re-encrypting them with the IBM Embedded Security Chip on the new system board.

To restore encryption keys from a key archive, complete the tasks in the Administrator Utility:

1. Start the Modify Key Configuration window as described above.
2. Select **Restore Keys from archive** and click **Next**.
The Modify Client Key Configuration - Restore All IBM Security Subsystem Keys window opens.
3. In the Archive Directory (Path) field, type the file path of the archive directory, or click **Browse** to search for the directory.
4. In the CSS Archive Public Key File field, type the path and file name of the admin public key, or click **Browse** to search for the file.
5. In the CSS Archive Private Key File field, type the path and file name of the admin private key, or click **Browse** to search for the file.
6. Click **Next**. A message indicates that the operation completed successfully.

Note: If the admin private key was split into multiple files, a message is displayed that asks you to type in the location and name of each file. Click **Read Next** after you type each file in the Key File field.

7. Click **OK**.
8. Click **Finish**.

Note: If you change the admin key pair after you restore the archive, an error message displays. If this occurs, you must add the users to UVM and then request new certificates.

Change the archive location

When the key archive is first created, copies of all encryption keys are created and saved to the location specified at installation. The client user can also change the key archive location using the User Configuration Utility. To change the key archive location, follow the Administrator Utility procedure:

1. Start the Modify Key Configuration window as described previously.
2. Select **Change the archive location** and click **Next**. The Modify Client Key Configuration - New Key Archive Location window opens.
3. Type the new path, or click **Browse** to select the path.
4. Click **OK**.
5. Click **Finish**.

Generate new hardware keys

If you need to regenerate your hardware keys inside your IBM Embedded Security Chip, follow this procedure:

1. Start the Modify Key Configuration window as described previously.
2. Click the **Generate new hardware keys** radio button and click **Next**. A new window asks you to select where you would like to put your keys.
3. Enter your new location and the amount of times you would like to split your keys. Click **Next**. After a moment, you receive a confirmation message.
4. Click **OK** to that message. A new window asks you where you would like to put your archive keys.
5. Type in the designated location and click **Next**. The machine processes for a few seconds before a new confirmation message appears.
6. Click **OK** to that message. A new window asks you to type in the new passphrase for the current user.
7. Type in the new passphrase and expiration. Click **Next**. The machine writes the information to the security chip. This will take at least 30 seconds. When it is finished, a new confirmation message will appear.
8. Click **OK**. A new window asks for the Windows logon password for the user.
9. Enter the requested information and click **Next**. If you have installed a fingerprint reader or a smart card reader (writer) you will get a new window that asks you to enroll the fingerprints or smart card again.
10. Type the appropriate information for the desired devices. Click **Next**.
A new confirmation message window will appear.
11. Click **Finish**.

Register this system with an IBM Client Security Software Roaming Server

This option allows you to register your system as a part of a roaming profiles network. See 6.11, "Roaming profiles" on page 534 for more information.

Change archive keys

When the archive key pair is first created, it is usually stored on a diskette or shared directory that can be accessed by multiple users. If the archive key pair becomes damaged, you can change to a different archive key pair.

Note: Be sure to update the archive before changing the archive key pair.

To change the archive key pair, complete the following procedure using the Administrator Utility:

1. Start the Modify Key Configuration window as described above.
2. Select the **Change Archive key** radio button and click **Next**. The Modify Client Security Key Configuration - New UVM Administrator Public Key File window opens.
3. In the New CSS Archive Key area of the window, type the file name for the new archive public key in the Public Key File field. You can also click **Browse** to search for the new file, or click **Create** to generate a new archive public key.

Note: Make sure you create the new public key in a location other than the one that contains the old archive key files.

4. In the New CSS Archive Key area, type the file name for the new archive private key in the Private Key File field. You can also click **Browse** to search for the new file, or click **Create** to generate a new archive key private pair.

Note: Make sure you create the new public key in a location other than that which contains the old archive key files.

5. In the Old CSS Archive Key area, type the file name for the old archive public key in the Public Key File field, or click **Browse** to search for the file.
6. In the Old CSS Archive Key area, type the file name for the old archive private key in the Private Key File field, or click **Browse** to search for the file.
7. In the Archive Location area, type the file path where the key archive is stored, or click Browse to select the path.
8. Click **Next**.

Note: If the archive key pair was split into multiple files, a message is displayed that asks you to type in the location and name of each file. Click Read Next after you type each file name in the Key File field.

9. Click **OK**. A message displays that the operation is complete.
10. Click **Finish**.

6.7 Registering fingerprints

When UVM policy has been edited to include fingerprint authentication, fingerprints must be registered with User Verification Manager. There are two ways to register fingerprints: as an Administrator or as a User.

Registering a fingerprint as an administrator

An administrator can register a fingerprint as follows:

1. From the Windows Control Panel, double-click the **IBM Client Security Subsystem** icon.
2. Enter the Security Administrator Password that you set up in 6.4.4, “Configuring the IBM Client Security Software for the first time” on page 460.
3. In the Windows Users Authorized to use User Verification Manager area, select a user name from the list. Click **Edit User**.
4. The Modify Client Security Key Configuration - Edit UVM User Attributes window opens. Select **Register fingerprint and/or smart card** and click **Next**.
5. The UVM Enabled Devices window opens. Click **Enroll user fingerprints**.

6. The Fingerprint Registration window shown opens. In the Select a hand area, click **Left** or **Right**.

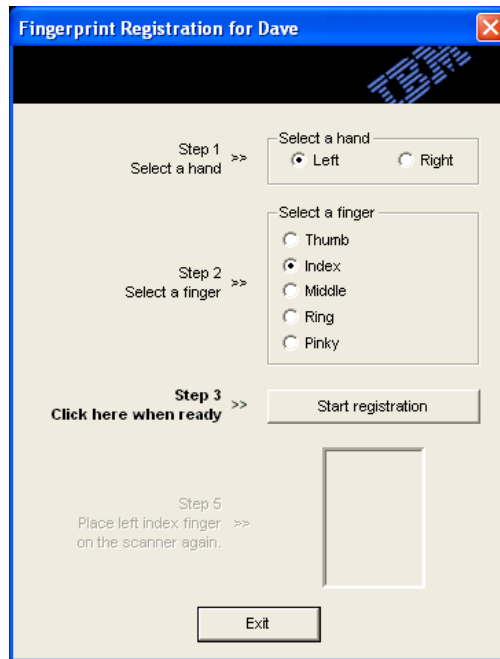


Figure 6-28 Fingerprint Registration window

7. In the Select a finger area, select the finger you will scan for prints, and click **Start registration**.
8. Place your finger on the fingerprint sensor and follow the instructions.
9. Click **OK** once you have registered your fingerprint.
10. Specify another finger to register or click **Exit** to finish.

Registering a fingerprint as a user

A user can register a fingerprint as follows:

1. Click the Windows **Start** button. Then select **All Programs** → **Access IBM** → **IBM Client Security Software** → **Modify Your Security Settings**.
2. Select the **Fingerprint/Smart Card Registration** tab.
3. Click the Click to launch fingerprint registration tab.
4. Enter your passphrase, click **OK**.
5. The Fingerprint Registration window, shown in Figure 6-28, opens. In the Select a hand area, click **Left** or **Right**.

6. In the Select a finger area, click the check box next to the finger you will scan for prints and click **Start registration**.
7. Place your finger on the fingerprint sensor and follow the on-screen instructions.
8. Click **OK** once you have registered your fingerprint.
9. Specify another finger to register, or click **Exit** to finish.

6.8 Using User Verification Manager protection for Lotus Notes

User Verification Manager provides enhanced security protection for Lotus Notes users. The following section explains the process of setting this up.

Note: If there is a planar failure while using User Verification Manager protection for Lotus Notes, an administrator will be required to recover the keys to enable Lotus Notes use again. It is also possible to use IBM Password Manager to gain the same level of protection without this issue.

Configuring UVM protection for a Lotus Notes User ID

The prerequisites for enabling User Verification Manager protection for Lotus Notes are:

- ▶ Lotus Notes must be installed on the IBM client.
- ▶ A Lotus Notes User ID and password must be established for the user.
- ▶ The Lotus Notes user must be authorized to use User Verification Manager.

To set up User Verification Manager protection for Lotus Notes, complete the following procedure:

1. From the Windows desktop of the IBM client, click the Windows **Start** button. Then select **Settings** → **Control Panel** → **IBM Client Security Subsystem**.
2. The Administrator Utility main window opens. Click **Configure Application Support and Policies**.
3. The UVM Application and Policy Configuration window opens. Select **Enable Lotus Notes support**.

User Verification Manager protection for the Lotus Notes User ID is now enabled.

Refer to Figure 6-4 on page 464 to learn how to configure Lotus Notes support during the IBM Client Security Software installation.

If necessary, continue with the following optional steps to configure a policy for the Lotus Notes Logon:

1. Click **Application Policy**. The Modify Client Security Policy Configuration window opens. See Figure 6-22 on page 502.
2. Click **Edit Policy**.
3. Enter the administrator password and click **OK**. The IBM UVM Policy: Lotus Notes Logon window displays.
4. On the Object Selection tab, select **Lotus Notes Logon** from the Action menu.
5. On the Authentication Elements tab, select the authentication elements that you want to require for Lotus Notes Logon.
6. Click **Apply** to save the selections. The Admin Private Key Required window opens.
7. Specify the location of the Private Key either by typing the path name in the provided field or by clicking **Browse** and selecting the appropriate folder.
8. Click **OK**.

The IBM User Verification Manager: Summary of Policy window displays a summary of objects controlled by the local client policy.

9. Start Lotus Notes.

The User Verification Manager Password registration is complete when Lotus Notes is started.

Using User Verification Manager protection within Lotus Notes

Before you can use User Verification Manager protection for Lotus Notes, you must follow the steps in 6.8, “Using User Verification Manager protection for Lotus Notes” on page 517.

Setting up UVM protection within Lotus Notes

To set up UVM protection within Lotus Notes, do the following:

1. Log into Lotus Notes. The IBM User Verification Manager window displays.
2. Enter and verify your Lotus Notes password in the available fields.

Your Lotus Notes password is now registered with UVM.

Resetting your Lotus Notes password

To reset your Lotus Notes password, do the following:

1. Log in to Lotus Notes.

2. From the Lotus Notes menu bar, click **File** → **Tools** → **User ID**. The IBM User Verification Manager window opens.
3. Enter your User Verification Manager passphrase and click **OK**. The User ID window opens.
4. Click **Set Password**. The IBM User Verification Manager window opens.
5. Select **Create your own password**.
6. Enter and verify your new Lotus Notes password in the available fields, then click **OK**.

Important: When you change your password within Lotus Notes to a value that you have used before, Notes rejects the password change, but does not inform the IBM Client Security Software. Consequently, User Verification Manager stores the password that Notes rejected.

If you receive a message indicating that the password has been used previously when changing your password within Lotus Notes, you will need to exit Lotus Notes, start the User Configuration Utility, and restore the Lotus Notes password to the value it was before.

If your Lotus Notes password was randomly generated and you get this error, you have no way of knowing what the password was, and therefore you cannot reset it manually. You must request a new ID file from your administrator or restore a previously-saved copy of your ID file.

Disabling UVM protection for a Lotus Notes User ID

If you want to disable User Verification Manager protection for a Lotus Notes User ID, do the following:

1. From the Windows desktop of the IBM client, click the Windows **Start** button. Then select **Settings** → **Control Panel** → **IBM Client Security Subsystem**. After you enter your password, the Administrator Utility main window displays.
2. Click **Configure Application Support and Policies**. The User Verification Manager Application and Policy Configuration window opens.
3. Clear **Enable Lotus Notes support**.
4. Click **OK**. The Application Support Actions window opens with a message indicating that Lotus Notes support is disabled.

Setting up UVM protection for a switched Lotus Notes User ID

To switch from a User ID that has User Verification Manager protection enabled to another User ID, do the following:

1. Exit Lotus Notes.
2. Disable User Verification Manager protection for the current User ID.
3. Enter Lotus Notes and switch User IDs. See your Lotus Notes documentation for information about how to switch User IDs.
4. Enter the Lotus Notes Configuration tool (provided by IBM Client Security Software) and set up UVM protection for the User ID that you switched to. Refer to 6.8, “Using User Verification Manager protection for Lotus Notes” on page 517.

6.9 User Configuration Utility

The User Configuration Utility is used to modify the security settings on the system. This interface provides a simple windows environment in which you can make these changes.

6.9.1 Modify Your Security Settings

To open the User Configuration Utility do the following:

1. Click the Windows **Start** button. Then select **All Programs → Access IBM → IBM Client Security Software → Modify Your Security Settings**. A window resembling the one in Figure 6-29 on page 521 opens.

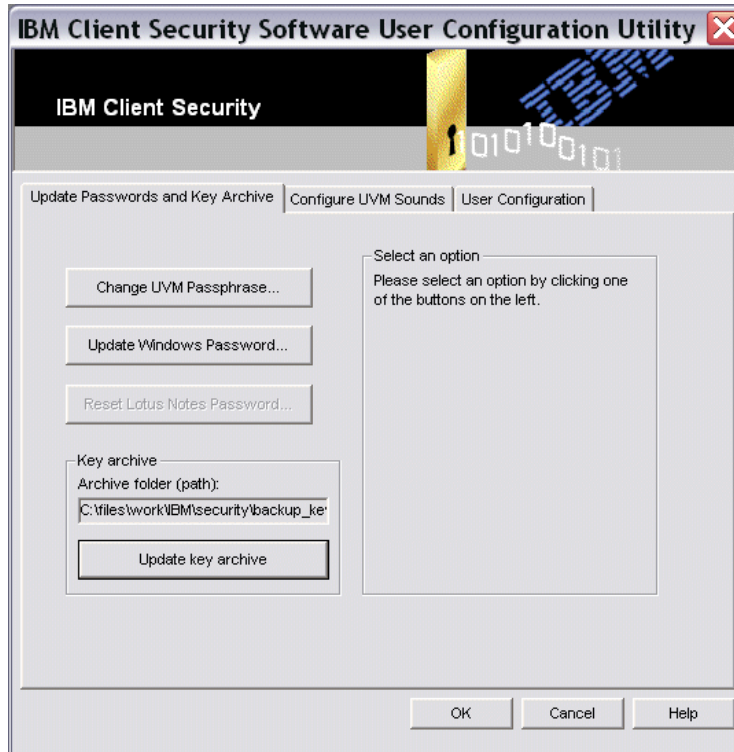


Figure 6-29 User Configuration Utility - Update Passwords and Key Archive

2. From this window, select the appropriate task from the options below:
 - Tabs
 - Update Passwords and Key Archive tab shown in Figure 6-29
 - Configure UVM Sounds tab shown in Figure 6-30 on page 522
 - User Configuration tab shown in Figure 6-31 on page 523
 - Buttons available from the Update Passwords and Key Archive tab:
 - Change UVM Passphrase
This is used to change the UVM passphrase on this system.
 - Update Windows Password
This is used to change the Windows logon password.
 - Reset Lotus Notes Password
This option is only available if Lotus Notes is installed on this system.
This button enables you to change the Lotus Notes password.

- Update key archive
This is used to update the key archive.
- Options available from the Configure UVM Sounds tab (see Figure 6-30):
 - Authentication success
Select **Enable authentication event sounds** and enter the path to the success message in the Authentication success field. You can click the Browse button to locate this file, and you can test the sound by clicking the Test button.
 - Authentication failure
Select **Enable authentication event sounds** and enter the path to the failure message in the Authentication failure field. You can click the **Browse** button to locate this file, and you can test the sound by clicking **Test**.



Figure 6-30 User Configuration Utility - Configure UVM Sounds

- Buttons available from the User Configuration tab (see Figure 6-31):
 - **Reset User...**

This button enables you to reset the security configuration.
 - **Restore user configuration from archive**

This is used if your files have been corrupted or if you want to return to a previous configuration.
 - **Register with a CSS Roaming Server...**

This is used to register with an IBM Client Security Software roaming server. For more detailed information about roaming servers, see 6.11, “Roaming profiles” on page 534.

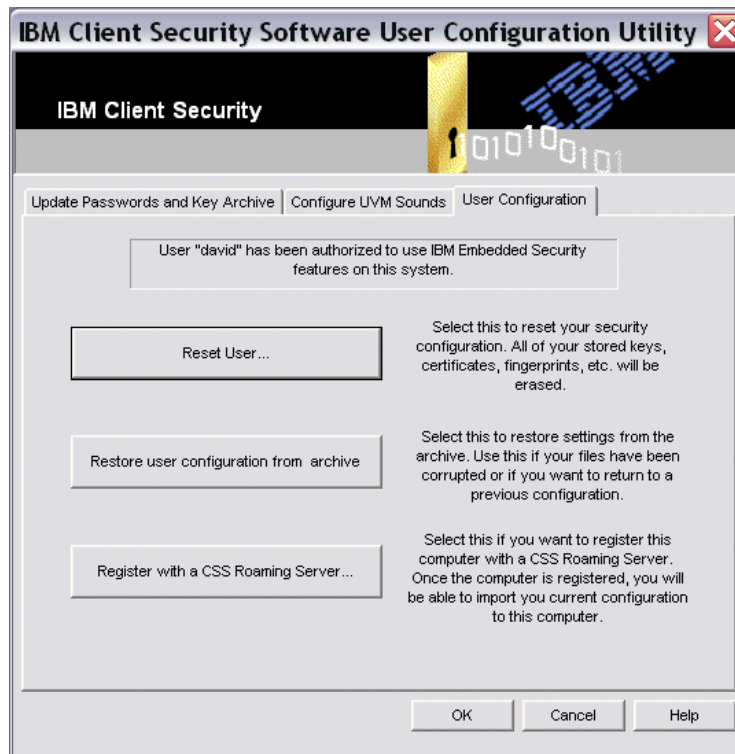


Figure 6-31 User Configuration Utility - User Configuration

Note: If you have installed a fingerprint reader or smartcard reader, you will see an additional tab in this User Configuration Utility as shown in Figure 6-32 on page 524.

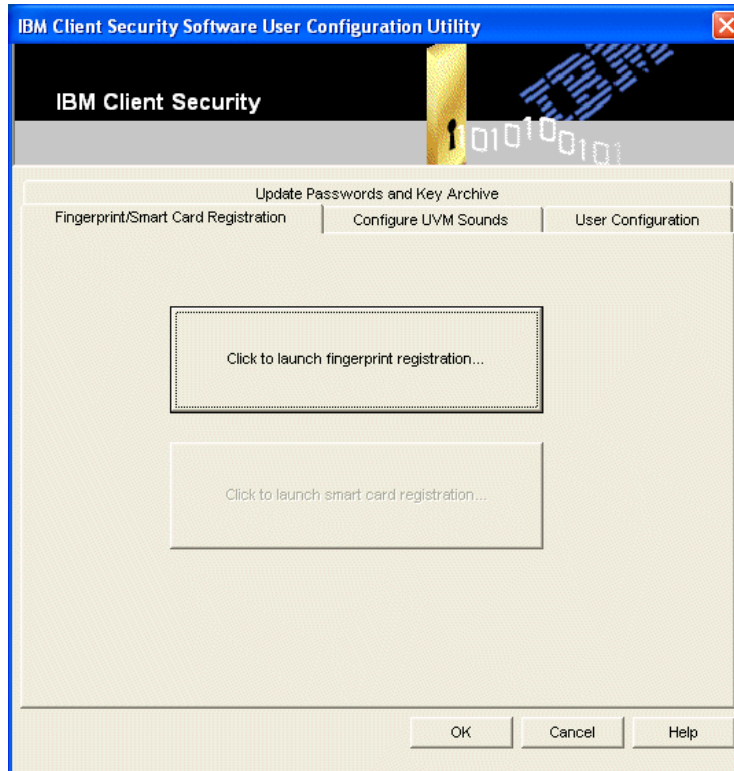


Figure 6-32 User Configuration Utility -Fingerprint/SmartCard Registration

- Buttons on this tab include:
 - The fingerprint reader registration button used to register a user's fingerprints for authentication (see 6.7, "Registering fingerprints" on page 515 and 6.4.5, "Targus DEFCON Fingerprint Reader" on page 473).
 - The smartcard reader registration button used to register a user for smartcard authentication.
- 3. After making the appropriate changes on the User Configuration Utility window, click **OK** to save your changes.

6.10 Administrator Console

The IBM Client Security Software Administrator Console enables a Security Administrator to perform administrator-specific tasks remotely from the system.

The console program is where you perform most of the administrative tasks in your security system. It is especially useful if you have your system set up as a roaming profile system, but it can also be used in a stand alone system.

1. To start it, click the Windows **Start** button. Then select **Run**
2. Enter `C:\Program Files\IBM\Security\console.exe` (the location might differ on your system if you installed it to another location) to start the application. You are then prompted to enter your IBM Embedded Security Chip administrator password.
3. Type the password. A window resembling the one in Figure 6-33 opens.

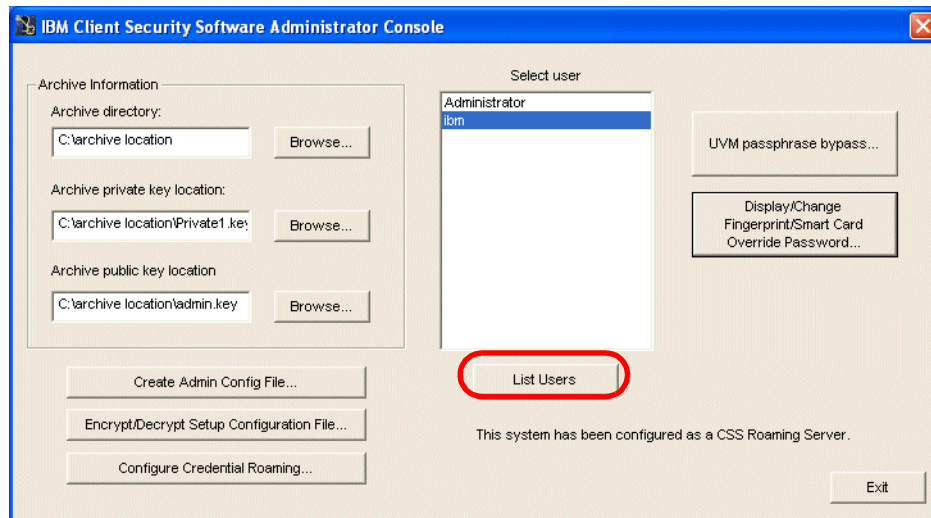


Figure 6-33 IBM Client Security Software Administrator Console

To use the console, you will have to tell the console where your keys are located. It usually edits the Archive directory for you. Depending on whether you use the system as a stand alone system or as a part of a roaming profile system, your keys might be located anywhere on the computer. It also depends on where you instructed the system to put them during your installation. In a roaming profile system, you will find them in your archive folder. In a stand alone system, you will probably find them where you put the administrator security keys. In worst case you can do a search for them. The archive private key is named *private1.key* and the archive public key is named *admin.key*.

4. Use the **Browse** buttons to find the path to the keys:
 - Archive directory
 - Archive private key location
 - Archive public key location

5. When you have filled in all the correct information, click the **List Users** button.

The enrolled users on your system will then show up in the Select user box.

The following sections detail the different functions you can perform from the Administrator Console and how to use them. Use the appropriate procedure for the task you want to perform.

6.10.1 UVM passphrase bypass

If a user forgets his or her passphrase, the UVM passphrase bypass button on the Administrator Console allows you to generate a file and a passphrase for him or her for a one time use. After that, the user can use this information to generate a new password. Typically, this problem appears when the user is about to log on to the machine. If the user does not remember the password and he or she has the IBM UVM logon instead of the ordinary Windows logon, you will have a check box on the logon page that says "I Forgot My Passphrase." If the user selects this box, a new window will appear that instructs the user to provide the machine with a temporary password and a file. It is this information we are creating through the console.

To generate a new passphrase for the user, use the following procedure:

1. Start the console as stated above.
2. Select the user that requires a new passphrase.
3. Click the **UVM passphrase bypass...** button to open the window shown in Figure 6-34 on page 527.

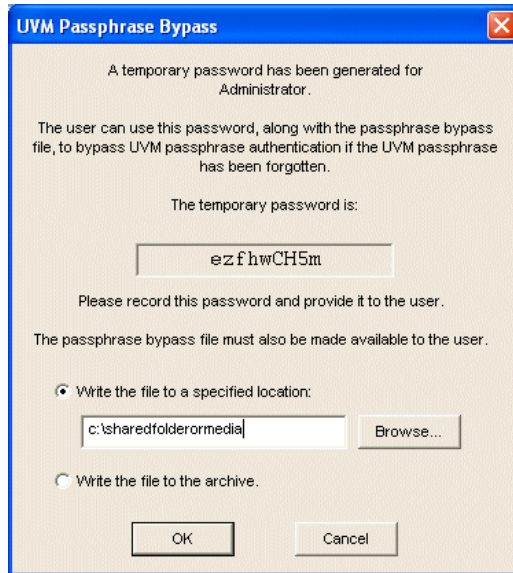


Figure 6-34 UVM Passphrase Bypass

4. Note the temporary password. This is the password that you have to give to the user together with a file.
5. Select a location where you would like to put the temporary file. It is important that you put it in a place where the user can access it. You can either enter it manually or browse for a location. You may also save the file in your archive location. Saving it in your archive location is a very good solution if you use roaming profiles.
6. Click **OK**.
7. A message stating the location of your temporary file opens. Confirm that the file is stored in the correct place and click **OK**.

6.10.2 Display/Change fingerprint/smart card override password

This function enables the administrator to override the security policy even if it is set to not allow passphrase override for fingerprint or smart card. This might be necessary if a user's fingerprint reader is broken or his or her smart card is not available. The administrator can read or e-mail the override password to the user. If you use roaming profiles, the administrator can generate this password through the security files that are located on the roaming profiles server. If you use a stand alone system, you will have to generate this password from the local files in some way. Follow these steps below:

1. Start the console as stated above.
2. Select the user you would like to override (the one that is currently logged on to the machine).
3. Click **Display/Change Fingerprint/Smart Card Override Password...** See Figure 6-33 on page 525. The window shown in Figure 6-35 opens.



Figure 6-35 Override password

4. On the client that is locked up, you will now have a window that asks you for your fingerprint or your smart card. That window should be named IBM User Verification Manager. At the bottom of that window, select **Device is not available or is not functioning**, and click **OK**.
5. A new window asks you to provide the bypass password to the machine. In the input field on the client, enter the current override password that was previously displayed in the window depicted in Figure 6-35 and click **OK**.
When you type the password, the client now continues as though the external unit worked properly.
6. Check the system and correct the error that disabled the client.

6.10.3 Create administrator configuration file

If you use the IBM Embedded Security Subsystem in a stand-alone environment, this gives users the possibility to enroll the client by themselves. If you have a machine that is already configured to use the IBM Embedded Security Subsystem for a user, you can easily add another user by completing the procedure to join the security system. It is not possible to do this procedure if you have configured your system to use the IBM UVM logon instead of the ordinary Windows logon.

Follow the procedure below to complete this task:

1. Start the console as stated above.
2. Click the **Create Admin Config File...** button (refer to Figure 6-33 on page 525). The window shown in Figure 6-36 will appear.

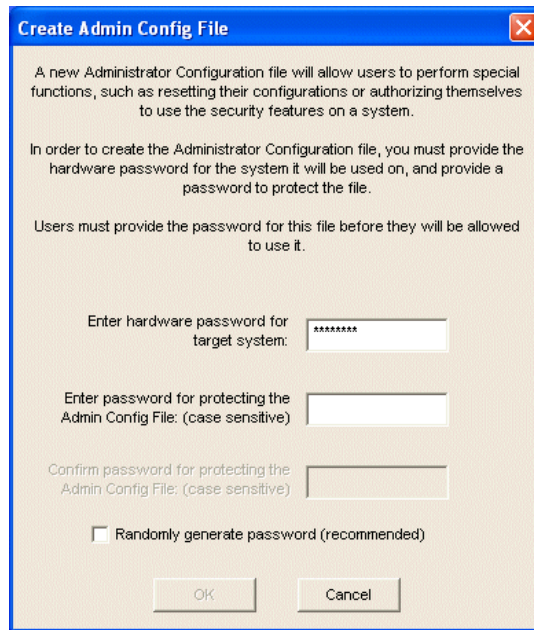


Figure 6-36 Create Admin Config File

3. In the field marked *Enter hardware password for target system*, type in your security administrator password. It is very important that this password be the same as the actual password on the machine you are about to add a user to. If the password is wrong the file will not work.
4. In the field marked *Enter password for protecting the Admin Config File*, type in your desired password. You will also have to confirm the password. This is the password the user will have to give to the IBM Embedded Security Subsystem when he or she is enrolling. If you want, you can randomly generate a password.
5. Click **OK**. A new window asks you where you would like to put the configuration file. You should put it in a location where the user can access it.

6. After the user has received the file, he or she should click the Windows **Start** button. Then select **Programs** → **Access IBM** → **IBM Client Security Software** → **Modify Your Security Settings**.

The window shown in Figure 6-37 opens. Please note that this is done on the client on which you want to enroll the user.

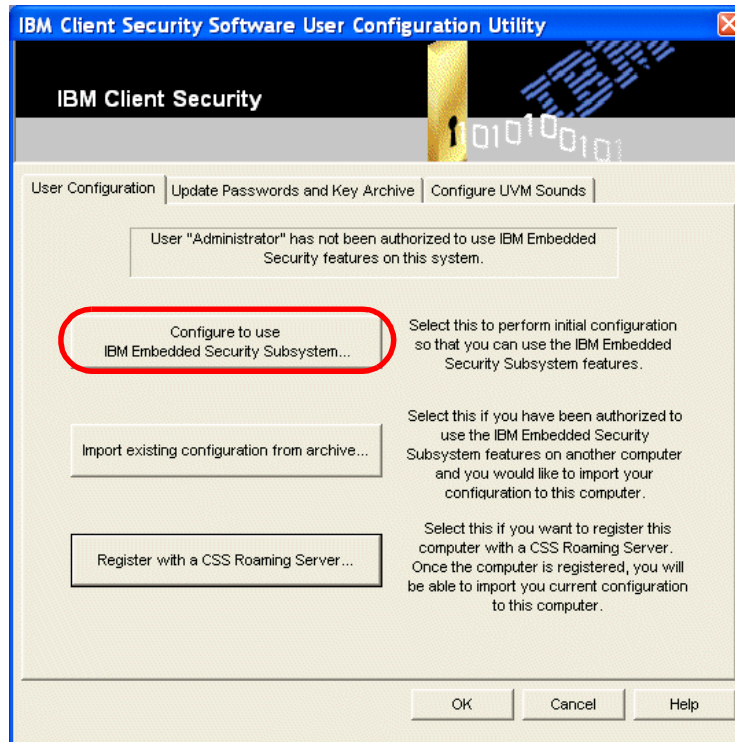


Figure 6-37 IBM Client Security Software User Configuration Utility

7. Click **Configure to use IBM Embedded Security Subsystem**. The window shown in Figure 6-38 on page 531 opens.
8. Enter the path to the configuration file and the password as shown in Figure 6-38 on page 531.

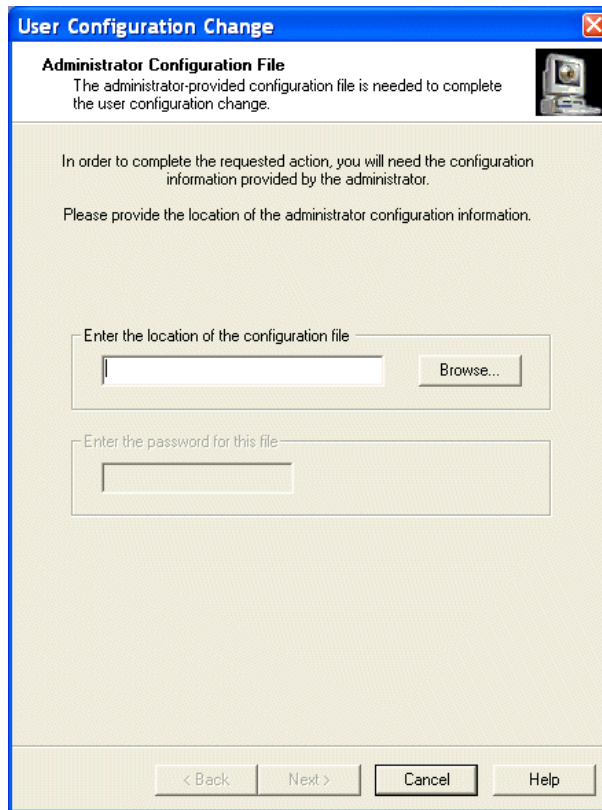


Figure 6-38 User Configuration Change

9. Click **Next** when you have finished. The window shown in Figure 6-39 on page 532 opens.
10. The user must type in his or her desired password twice. The password must match the passphrase policy.
11. When finished, click **Next**.

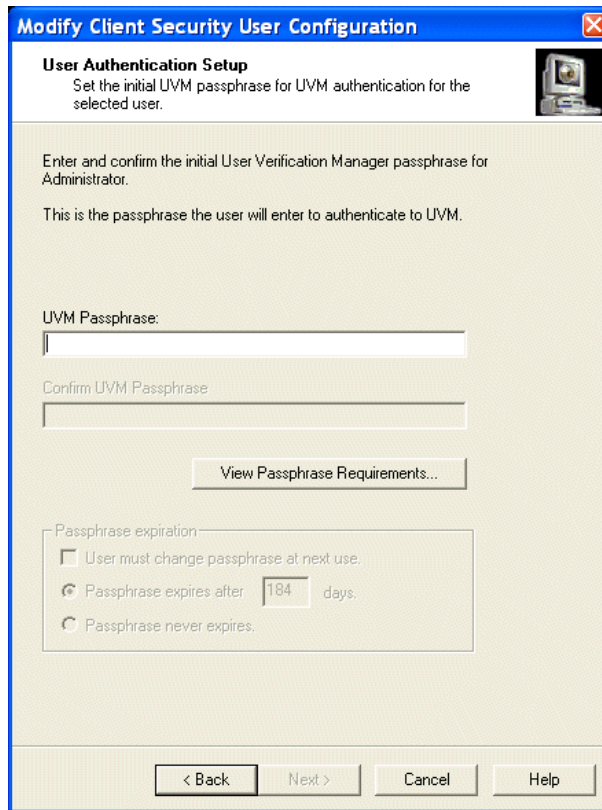


Figure 6-39 Modify Client Security User Configuration

12. Some reading and writing through the security chip will occur. A new window that looks like that in Figure 6-40 on page 533 opens.
13. If a confirmation message between these two windows appears, the user should click **OK**.

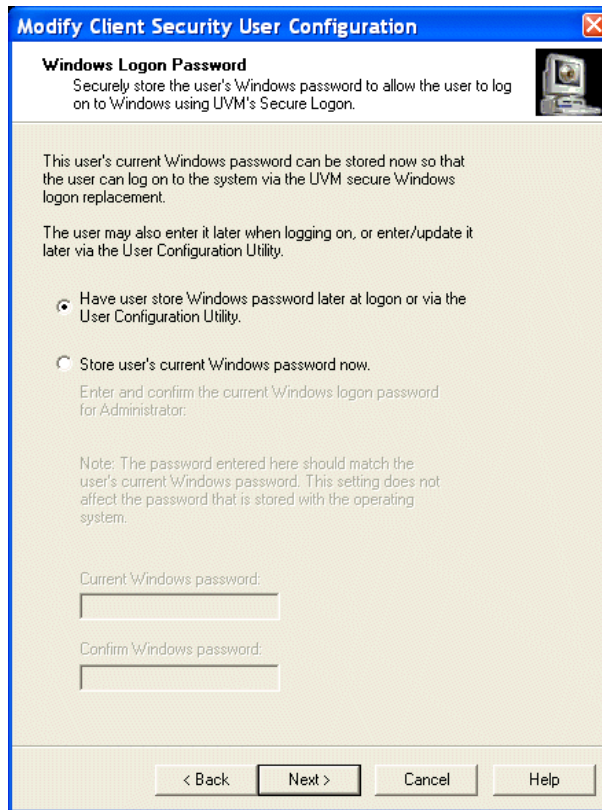


Figure 6-40 Modify Client Security User Configuration

14. The user may insert his or her ordinary Windows password. Fill in the desired information and click **Next**.
15. The user will now get a confirmation message about the installation.

6.10.4 Encrypt/Decrypt Setup Configuration File

This Encrypt/Decrypt Setup Configuration File button, shown in Figure 6-33 on page 525, allows you to manually edit a configuration file. You can create a configuration file using the csecwiz.exe program located in your security folder (typically c:\Program Files\IBM\Security) or through the wizard you see the first time you install the IBM Embedded Security Subsystem. You will have to remember to select **Save settings but do not configure subsystem** on the final page of those wizards. When you have a configuration file you can decrypt it, change whatever variables you would like to change and then encrypt it again. This will prevent other users from being able to read the passphrases or other

confidential information in the configuration file. For more information about this, see “Performing an unattended installation” on page 474.

Here is how to use it:

1. Start the console as stated above.
2. Click the **Encrypt/Decrypt Setup Configuration File...** button. A new window opens that allows you to browse to your configuration file.
3. Locate your configuration file and click **Open**.

The configuration file will be either decrypted or encrypted, depending on what state it was in when you clicked the **Encrypt/Decrypt Setup Configuration File...** button.

6.10.5 Configure Credential Roaming

This Configure Credential Roaming button, shown in Figure 6-33 on page 525, allows you to configure your system for roaming security profiles. This is described in detail in the following section.

6.11 Roaming profiles

The IBM Embedded Security Subsystem is a very advanced system supporting many security settings and policies, including designating one system as a roaming server. Roaming profiles contain user configurations and settings that allow the user to roam from system to system within the network, be recognized as a valid user, and have access privileges to the applications to which the user is entitled, provided the server is available. By setting up a roaming server using IBM Embedded Security Subsystem, the users will be able to log on to any machine in the network with their security passphrase and be able to use all of the tools for which they have user privileges.

One example of how to use roaming profiles is that a user can encrypt a file on one machine using the IBM File and Folder protection tool. The user can then copy this file over to a server, log on to another machine with the same credentials, copy the file to the second machine, and decrypt it with the File and Folder protection system.

Note: It is important that you have some experience with the security chip before you start setting up the roaming server. The solution is easy to use, but a bit complex to set up the first time.

In this section we show you how to set up a roaming server and connect clients to it. However, we will not describe all the different functions and possibilities. Think of this section as merely an introduction to roaming profiles.

6.11.1 Prerequisites

To set up a security system with roaming profiles, you will need to have a machine that has a TCPA 1.1 chip to use as your server.

Note: At the time this redbook was written, the only machines that had this chip were the IBM Netvista, ThinkCentre, and ThinkPad models. We therefore recommend that you use a Netvista or a ThinkCentre machine as your server. This machine requires that a Windows operating system be installed. We have tested it on both Windows XP and Windows 2000 Server. Since your roaming profiles server will send and receive a lot of requests, we recommend that you use Windows 2000 Server or similar as your operating system. Windows 2000 is also better at having multiple concurrent connections.

You will need to have two shared folders on your server. Depending on the number of clients that you want to connect to it, and the load that the server will experience, you will need to decide whether to run anything else on it. If you have a machine to spare, we recommend that you not use your roaming profiles server for anything else other than a roaming server.

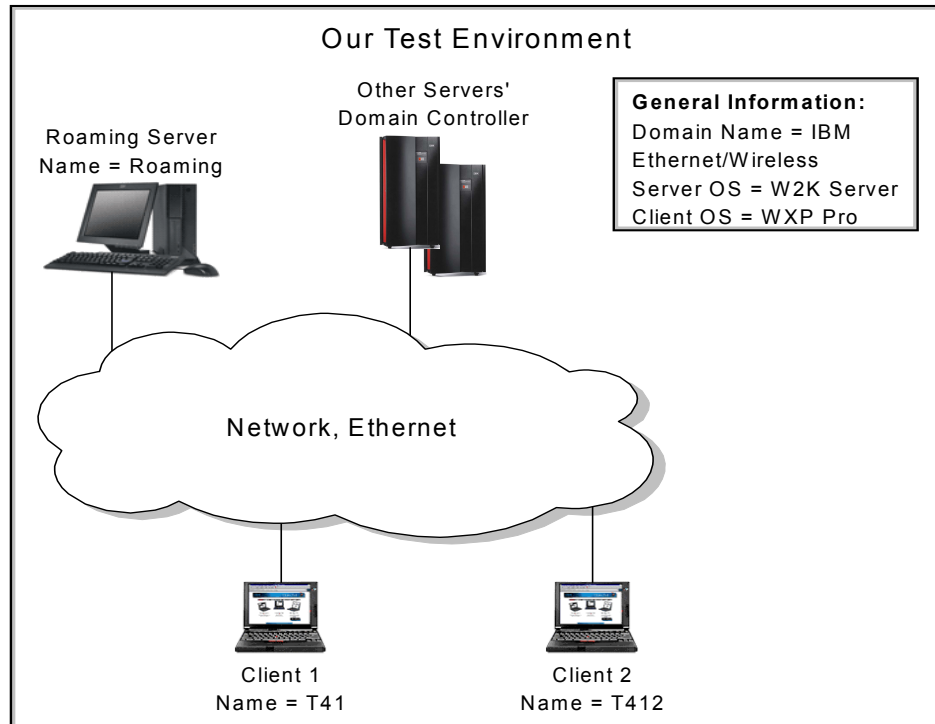


Figure 6-41 Our test environment

Restriction: We experienced some challenges using Windows 2000 terminal services during test. Therefore, we recommend that you not use terminal services on your roaming server.

6.11.2 Setup

In the example we tested, we first installed the machines as ordinary clients using the procedure mentioned in Figure 6.4 on page 457. There is also a way to set up the clients automatically. This is explained later in this section. Most of the functions on the server are controlled from a program called console.exe in the IBM Embedded Security Subsystem control panel and Windows' Control Panel. The console.exe program is used to configure the system, while the Windows Control Panel is used to configure the users.

Configuration of server

Before proceeding with configuration setup, verify that you installed the IBM Embedded Security Subsystem as an ordinary stand-alone installation.

In our example we created the following key structure:

- ▶ All the Administrator Security Keys are stored in c:\admin keypair.
- ▶ All the Key Archive files are stored in c:\archive location.
- ▶ All the configuration files are stored in c:\config.

You will need to share the following folders:

- ▶ C:\archive location (we shared it as archive)
- ▶ C:\config (we shared it as config)

Make note of these locations. We refer to them many times during this procedure. These locations may be renamed, if you like, as long as you use the same structure throughout.

Note: We gave the shares on our server full read and write privileges for all users. You should test what is best for your environment after you understand the basics of roaming profiles. Make sure that you configure the proper privileges when you are deploying the roaming profile system in your network. This will ensure that you do not loose data or settings.

Changing security system to a roaming profile server

This is the procedure for setting up the server as a roaming profile server:

1. Click the Windows **Start** button. Then select **Run**.
2. Type c:\Program Files\ibm\Security\console.exe and press **Enter**. This is the default location; your file might be in a different location, depending on where you placed it during installation.

3. Type the Administrator password to log into the console. No other Security Subsystem windows should be open. After you enter the password, the window shown in Figure 6-42 opens.

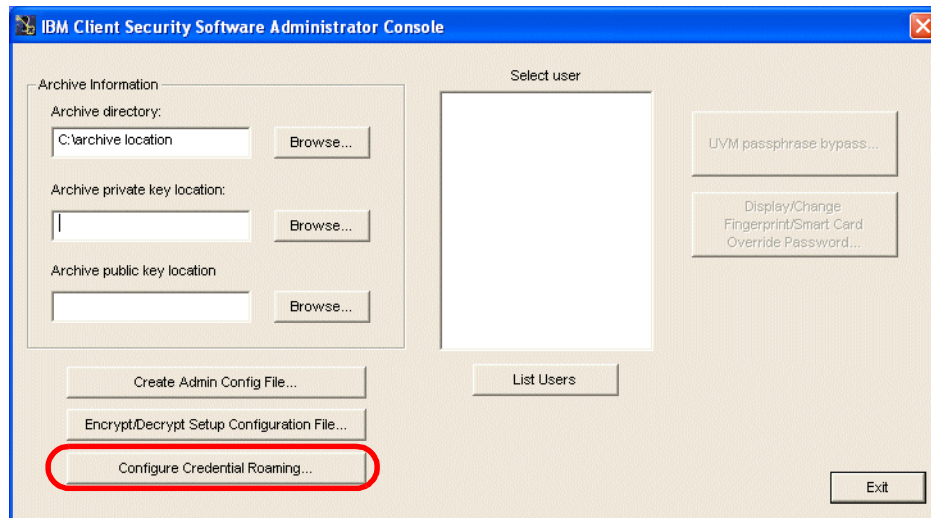


Figure 6-42 IBM Client Security Subsystem Administrator Console

4. Click **Configure Credential Roaming**.

The window shown in Figure 6-43 on page 539 opens.

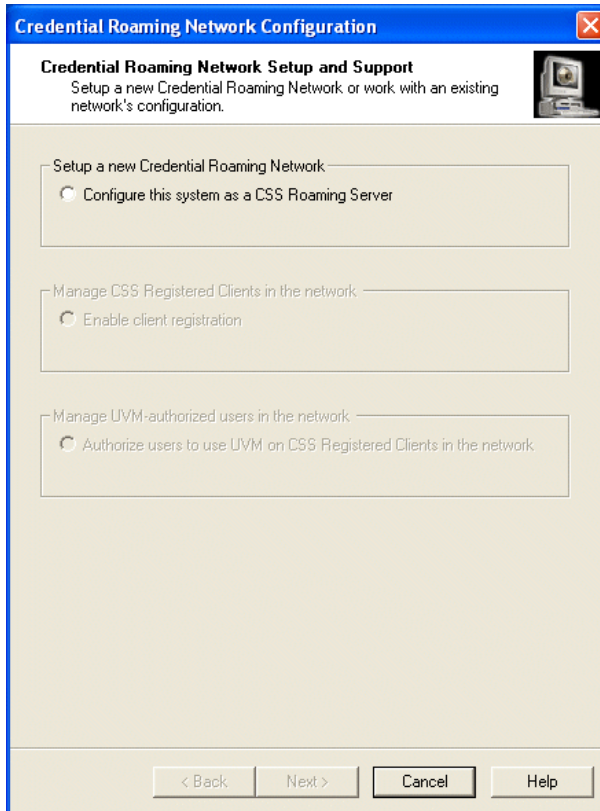


Figure 6-43 Credential Roaming Network Configuration

5. Click **Configure this system as a CSS Roaming Server** and click **Next**. After a few moments of processing, the window shown in Figure 6-44 opens.

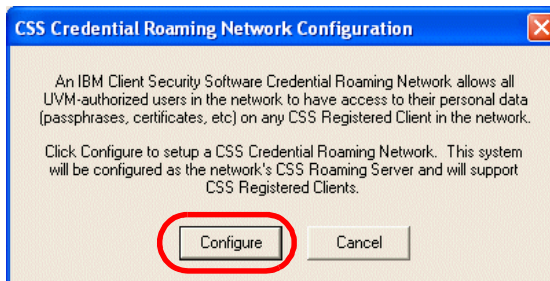


Figure 6-44 Configure Credential Roaming

6. Click the **Configure** button, and the window shown in Figure 6-45 on page 540 opens.

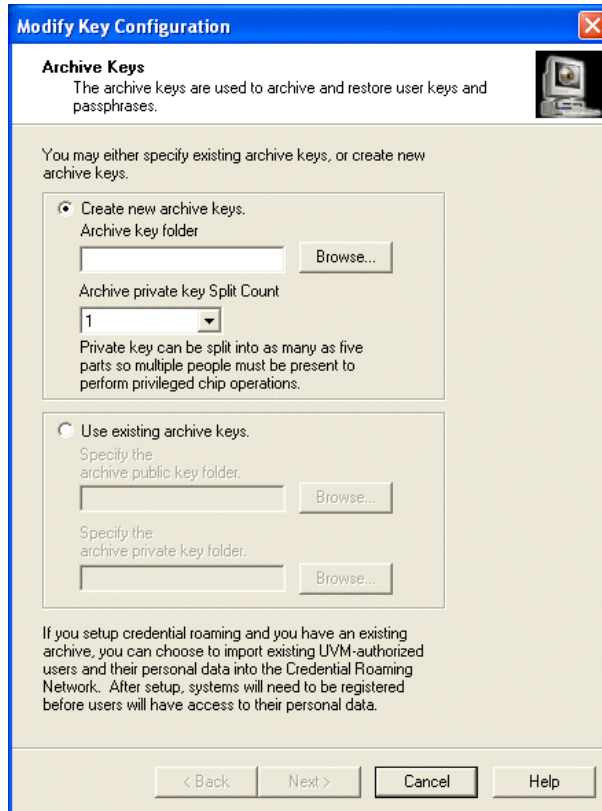


Figure 6-45 Modify Key Configuration

7. In our lab, we decided to make archive keys for our system so that we could be assured that the keys would be fresh and clean. You can use your existing keys if you want, but in our example we are using new ones. In the field under Create new archive keys; Archive key folder, enter C:\archive location and click **Next**.
8. After a few seconds of processing, a message displays stating that the operation was successful. See Figure 6-46.

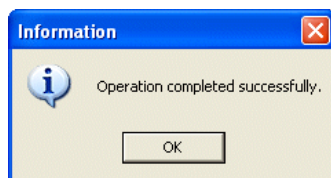


Figure 6-46 Operation completed successfully

9. Click **OK**. A new window opens like that shown in Figure 6-47.

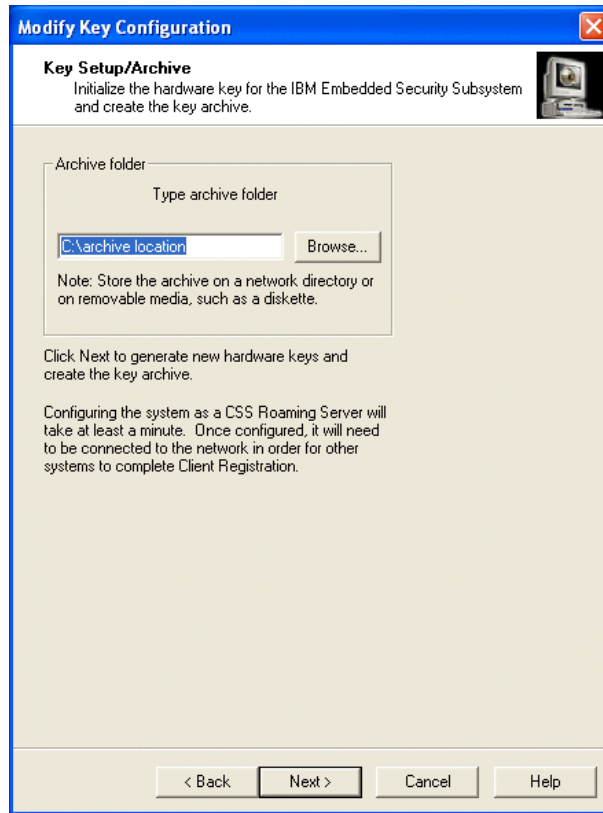


Figure 6-47 *Key Setup/Archive*

10. Confirm the location of the archive folder. This field should already be filled in. After you have confirmed that this is the correct folder, click **Next**. Since we have chosen to make new keys, a new window opens (Figure 6-48 on page 542).

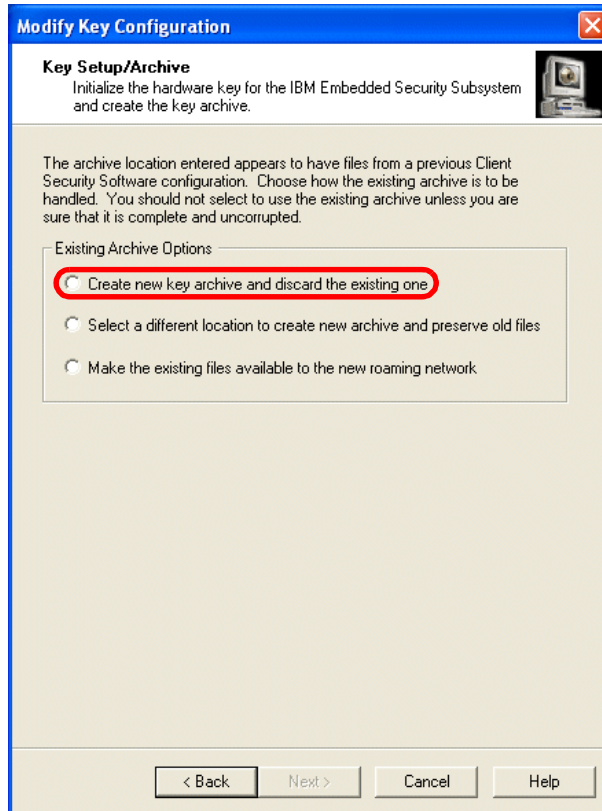


Figure 6-48 Generate new keys

11. Select **Create new key archive and discard the existing one** and click **Next**. A warning message such as the one in Figure 6-49 appears.

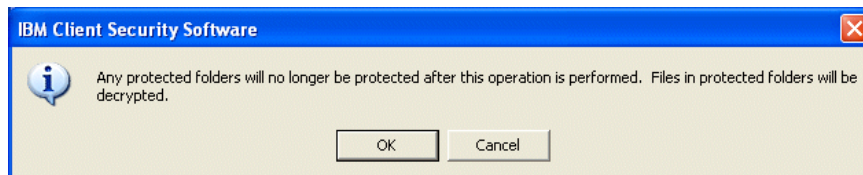


Figure 6-49 Warning file and folder protection

12. Click **OK** to remove the message. Your machine is now writing to the security chip. This will take some time: at least one minute. When it is finished processing, the message shown in Figure 6-50 appears.

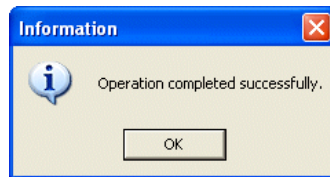


Figure 6-50 Completed successfully

13. Click **OK**. A second confirmation window such as the one in Figure 6-51 appears. Your server is now reconfigured to be a roaming profiles server.

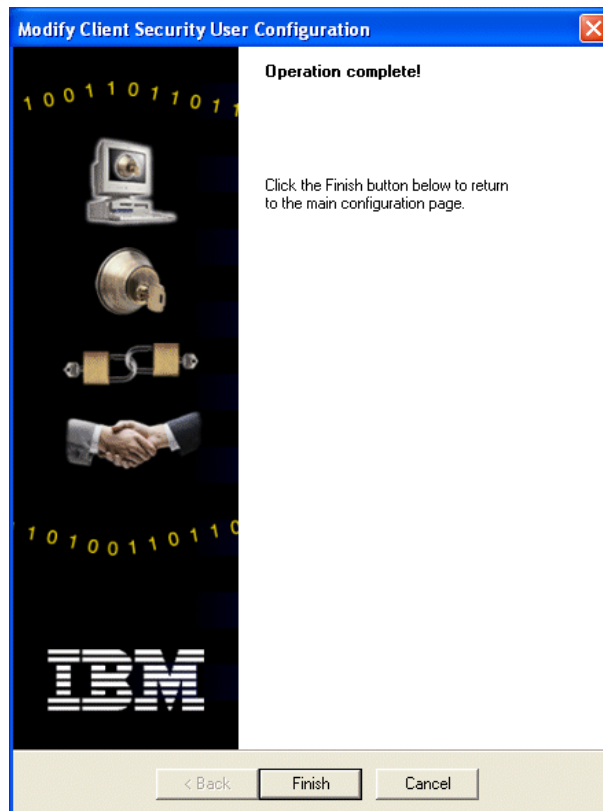


Figure 6-51 Operation completed

Tip: If during this configuration, you get an error message, try to delete all your old keys and to clear the security chip. Remember that you must not do this if you have replaced your Windows logon with the IBM Embedded Security Subsystem logon. You are not required to use the IBM logon to make a machine a server.

Client registration

As soon as you have made your machine a roaming profiles server, it is time to configure a way to let the clients join your roaming profile system. To do this, you will need to create some files that contain configuration settings. You should still be on the same window as you were when you configured your server as the roaming profile server (see Figure 6-43 on page 539).

This is the procedure for giving clients access to the roaming server:

1. Select **Enable client registration** if it is not selected for you already. Click **Next**. This opens the window shown in Figure 6-52 on page 545.

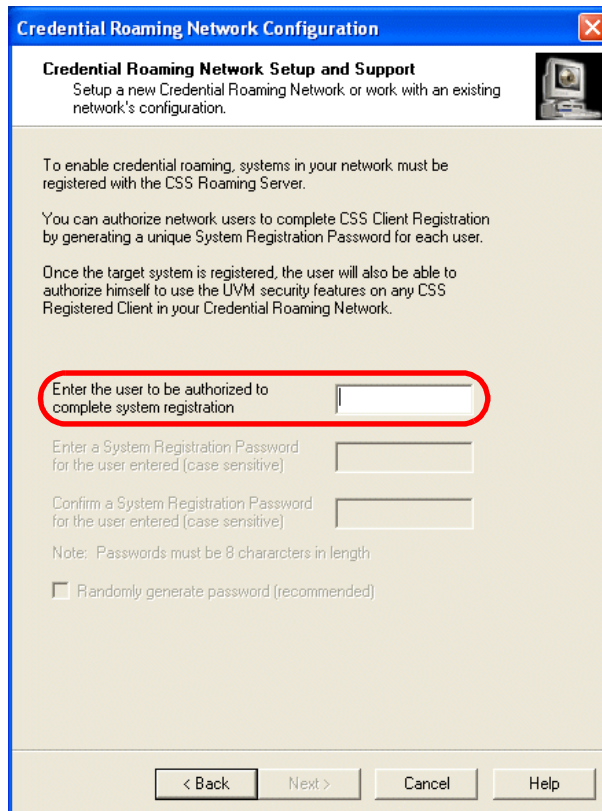


Figure 6-52 Credential Roaming Network Setup and Support

2. In the *Enter the user to be authorized to complete system registration* field, type in the username of the person you will be authorizing to give his or her machine access to the roaming profile system. In our example we have a domain user named administrator. We therefore type administrator in this field. You can change this username to whatever you want as long as you keep track of what user you selected, and that the user has windows administrator rights. After you have typed in this username, you will be able to fill in information in the password fields as well. This is a password that the person who will perform the configuration on the client must know. In this example, we used the word password as the password. You might also wish to generate a unique password through the chip by selecting the **Randomly generate password** check box.

3. When you have filled in all the required information, click **Next**. A new window opens (Figure 6-53).

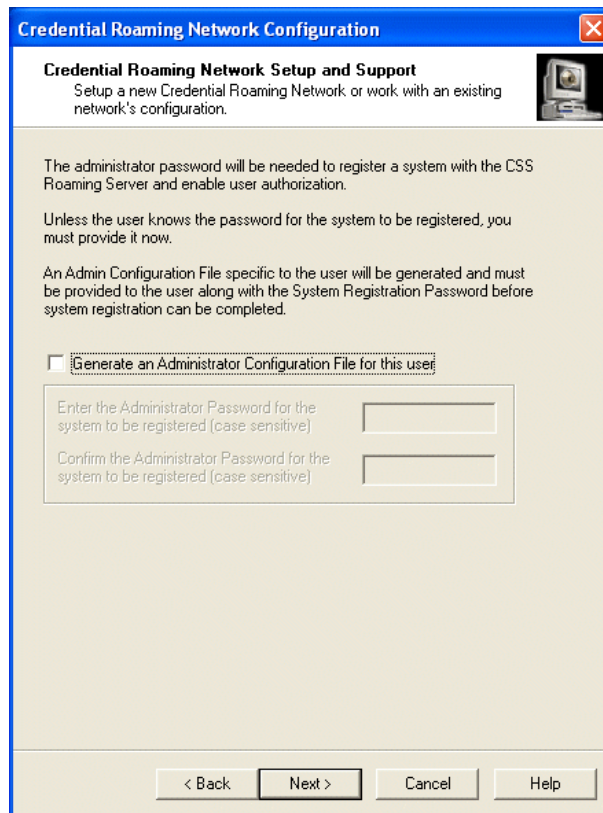


Figure 6-53 Administrator password

4. If the person to whom you are granting access to join the roaming server does not know the administrator password (chip administrator), you enter this information on this page. This password must be the same as the administrator password on the security chip that you are migrating into your roaming profile system. This is not the password for the user administrator in Windows, but the password you typed in when you installed the security chip. Refer back to Figure 6-2 on page 462. Type in the current administrator password in both fields and click **Next**.

A new window opens that resembles the one shown in Figure 6-54 on page 547 opens and shows the configuration file.

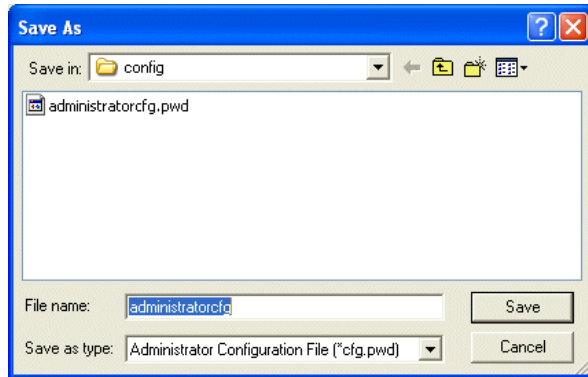


Figure 6-54 Save as

It is very important that you do not change the name of this file. As described previously, we are using the c:\config folder as a place where we store all the configuration files.

5. Select the appropriate folder for your system and click **Save**.

A new window with a confirmation message will appear as shown in Figure 6-55.

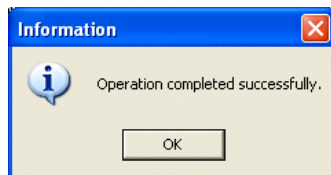


Figure 6-55 Completed successfully

6. After you have clicked **OK** on this message, you will be returned to the same window you were on when you started your client registration (see Figure 6-52 on page 545). If you would like to give more people access to enroll clients, repeat the steps above. If not, click **Back** and you will return to the roaming profile main menu.

If everything is performed as described above, you should now have successfully created a configuration file to include clients into your roaming profile network.

Authorize users to use UVM on IBM Client Security Software registered clients

After you have reconfigured your server to be a roaming profiles server and made a configuration file that allows you to include clients into the roaming profiles system, it is time to add users to your system.

Note: This is the radio button: Authorize users to use UVM on CSS Registered Clients in the network radio button. It is the third option (grayed out) listed on the window in Figure 6-43 on page 539.

Follow the procedure below to use this method:

1. Select **Authorize users to use UVM on CSS Registered Clients in the network**.
2. Click **Next**.

This opens a menu as though you were starting the IBM Embedded Security Subsystem program from your Control Panel. It works exactly the same way as Figure 6-4 on page 464. The only difference is that now your list will be empty and you may decide policies for your entire network and select the users that should be allowed to log on to your roaming profile network.

3. Add the desired users from the list as shown in Figure 6-5 on page 465. It is also important that you select the user that you created a configuration file for as described in “Client registration” on page 544, otherwise you might experience some complications when you try to register a client afterwards.

After you have finished adding all of your desired users, you are ready to begin configuring the clients.

Configuring the clients

After you have finished setting up your server as a roaming profile server, there are still some things you will have to do with your clients. You will need to perform some configuration that binds the client to the server. In our test, we had already installed the IBM Embedded Security Subsystem on the client. You can join a roaming profile server automatically during an unattended install, but you will have to change some switches in your csec.ini file to make it happen. See 6.4.6, “Performing an unattended installation” on page 474 for more information about unattended install and the possibility of joining a roaming server at the same time. In our example, we will do it manually. We have installed the IBM Embedded Security Subsystem the same way as we did on the server.

Important: Be sure to use the same security administrator password on all machines including the server.

First configuration of your client

This section describes how to configure your client to communicate with the roaming profiles server. Please note that this description is made on a machine that already has the IBM Embedded Security Subsystem installed. Follow the steps below:

1. Click the Windows **Start** button. Then select **Programs → Access IBM → IBM Client Security Software → Modify your Security Settings**. This opens a window that allows you to bind your machine to the roaming profiles server.
2. Click **User Configuration** in the upper right corner of this window. After this, a window such as the one shown Figure 6-56 opens.

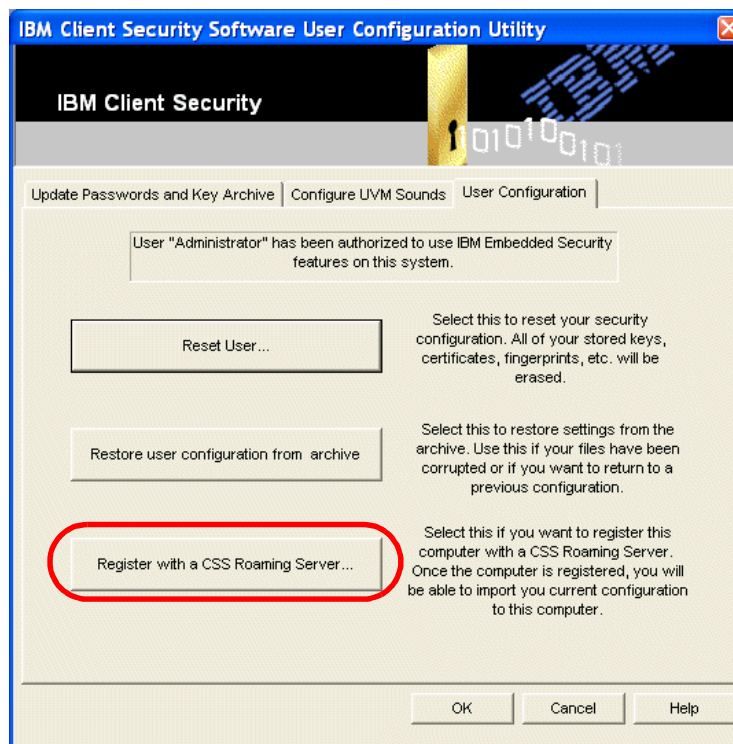


Figure 6-56 IBM Client Security Software User Configuration Utility

3. Click the **Register with a CSS Roaming Server** button. The window shown in Figure 6-57 opens

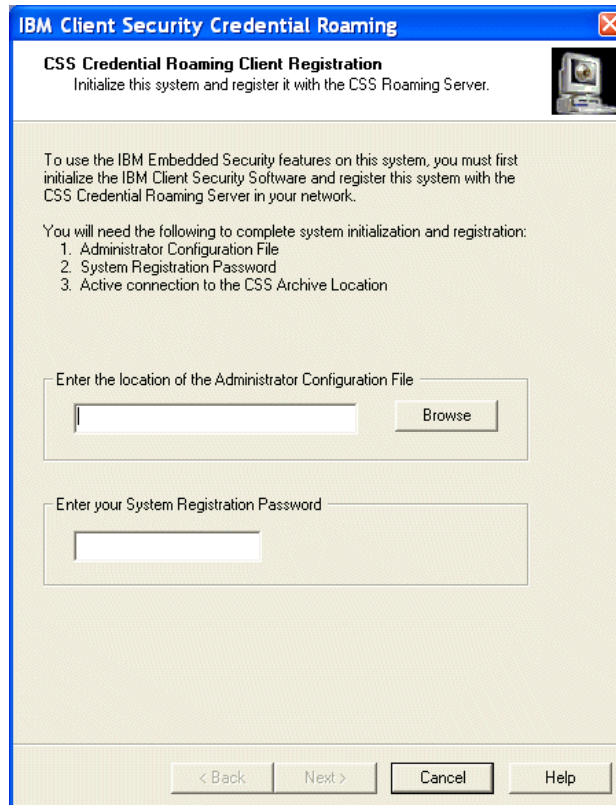


Figure 6-57 IBM Client Security Credential Roaming

As mentioned earlier in this section, our roaming server is called `roaming`. We created a share named `config` that contains the configuration files for our clients. This is the server we are connecting to.

4. In the Enter the location of the Administrator Configuration File field, type `\\roaming\\config\\administratorcfg.pwd`. (You can use the Browse button to locate this file). This location might be different on your server. You must point to the share that contains the `*cfg.pwd` file (in our example, the `administratorcfg.pwd` file) and select it.
5. In the Enter your System Registration Password field, you must use the same password you used when you set up the configuration file in Step 2 on page 545 (see Figure 6-52 on page 545).

After the IBM Client Security Software reads and writes this information, the window shown in Figure 6-58 opens.

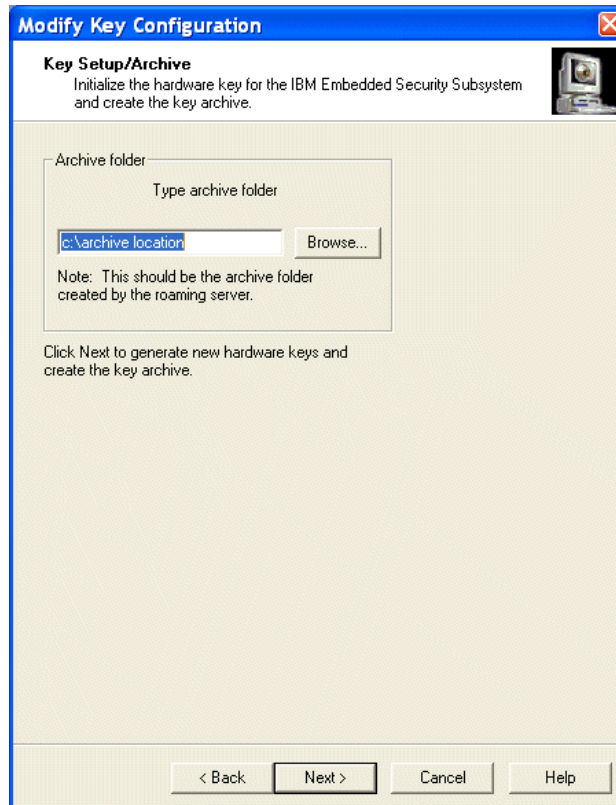


Figure 6-58 Modify Key Configuration

6. In this window, it is very important that you enter a new location. In the Type archive folder field, enter the network location of your archive files. That should be the share you have on your roaming server that contains your archive profiles. On our server, we stored our archive keys in the c:\archive. folder (see Figure 6-45 on page 540). We then shared that folder as \\roaming\archive. This is the share you must put into the field on this window. It is very important that you change this field manually, as the default is the original location that is on your local hard drive. Your local hard drive is the wrong location for roaming profiles.
7. After you have typed in the correct network location, click **Next**.

After processing the information, the message shown in Figure 6-59 appears

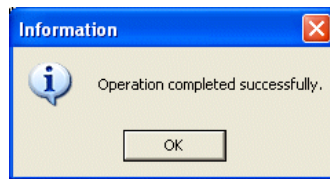


Figure 6-59 Operation completed successfully

8. After more processing, the window shown in Figure 6-60 opens.

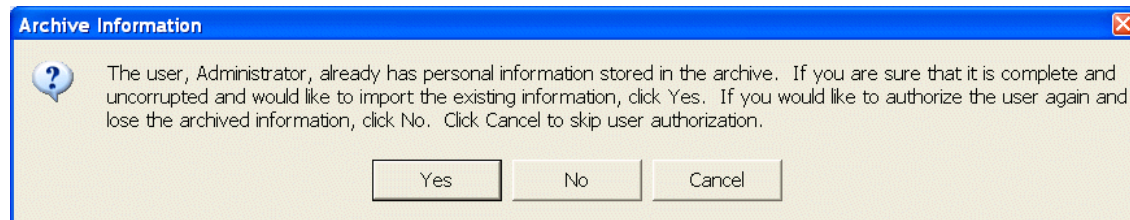


Figure 6-60 Archive Information

9. This window allows you to use the previously stored personal information or create new information. Since we just created the profile for this user on the roaming profile server, we are pretty sure that there is nothing wrong with our files; therefore, we click **Yes**.

Note: If you are setting up several machines at the same time, you do not want to write new information all the time either. If you select authorize the user again, all previous information will be overwritten.

After about 10-20 seconds of processing, you receive a message that looks like Figure 6-61 on page 553.

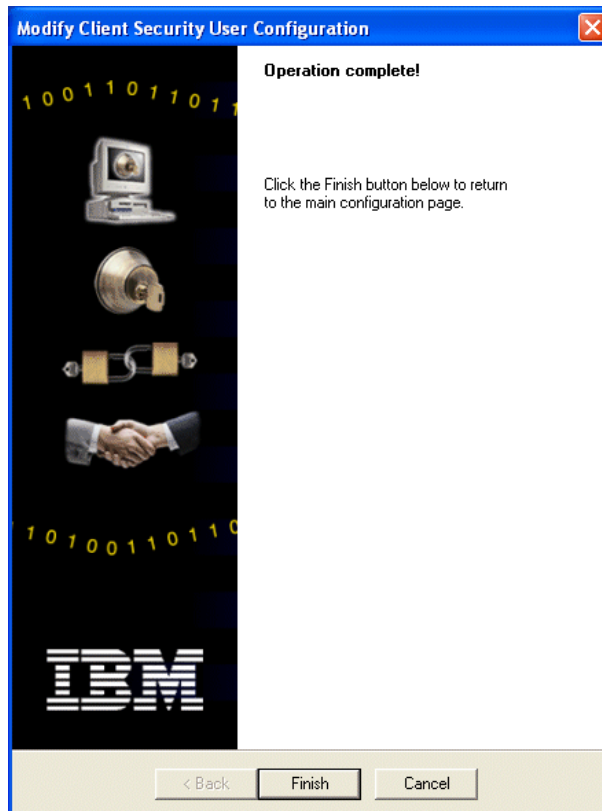


Figure 6-61 Operation completed

10. Click the **Finish** button to complete the user configuration.

Important: After you have configured your client, it is very important that you restart your computer or that you log off and back on. This will ensure that the security chip receives the keys from the roaming profiles server.

Testing the roaming profiles configuration

The procedure that we just described is what you should use to bind all the clients that you would like to be a part of your roaming profiles system. You should be able to test your roaming capability. Try the following test to see if your roaming profile system is configured in the right way:

1. Log on to the machine.
2. Right-click a text document and select **Encrypt this file**.
3. Copy this file to a shared area on your network.

4. Go to a second machine.
5. Copy the same encrypted file from your shared area to your local machine.
6. Right click the file and select **Decrypt this file**.
7. You should receive a message that states that the file was successfully decrypted.

Note: Depending on how your local policy is configured, you might have to type in your user password when performing this test. The password is the password you inserted in that user's account when you configured the user in the security control panel.

Now that you have configured and tested one user in your roaming profiles server configuration, it is easy to add more users. This is discussed in the next section.

6.11.3 Utilization of roaming clients

When your machines are configured for the roaming profiles system, you can use whatever machine you would like in your network in combination with the IBM Embedded Security Chip and the IBM Client Security Software to make managing your security policies for your organization easier.

Here are some examples of how to utilize the roaming capability:

- ▶ Fingerprint reader or smartcard readers can be used on any machine. Information about them can be stored on the roaming server.
- ▶ All passwords in Password Manager can be stored on the server
- ▶ You can encrypt files, put them on the server, and decrypt them on another machine.

6.11.4 Adding users to a roaming profiles system

If you are on a domain (which is highly recommended), you first must add your new user as an ordinary user in your domain. If the user already exists, this user name will be in the list in the window on the left (see Figure 6-62 on page 555). These existing users can be authorized by selecting them and then clicking **Authorize**. The only difference from the original procedure is the possibility to control it all from the console.exe program.

From the menu you see in Figure 6-43 on page 539 select **Authorize users to use UVM on CSS Registered Clients in the network** and then click **Next**.

This will take you to the user authorization window as shown in Figure 6-62. It is important that you add users from a domain so that the credentials are exactly the same.

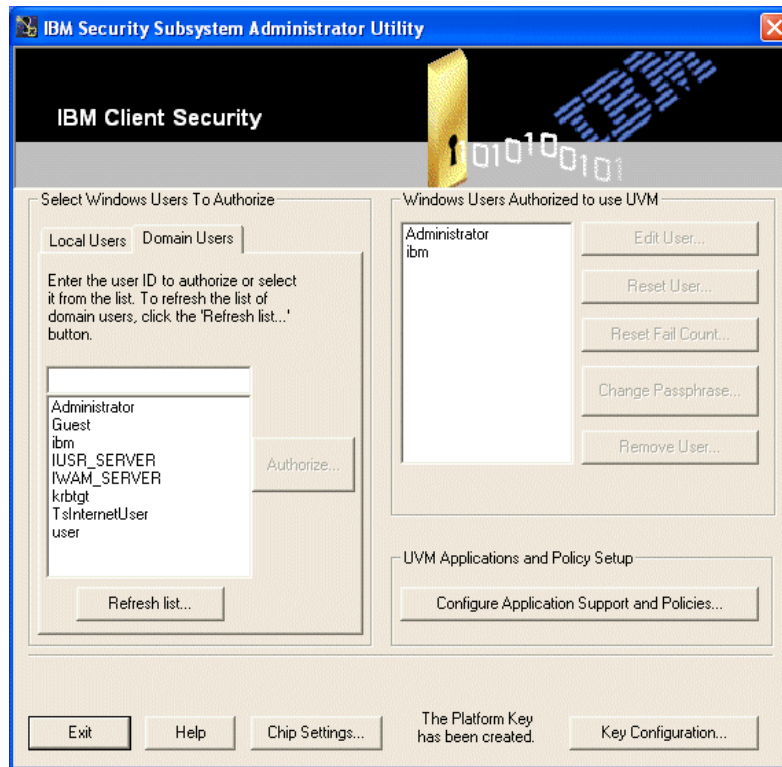


Figure 6-62 Adding users

The procedure to add users is described earlier in this chapter in 6.4, “Installation instructions” on page 457. After you have added your users, log on to a machine in your network that is configured to use roaming with your ordinary domain user name and password as usual. When you are logged on to Windows as the new user, perform the following procedure:

1. Click the Windows **Start** button. Then select **Programs** → **Access IBM** → **IBM Client security software** → **Modify your security settings**.

The window shown in Figure 6-63 will display.

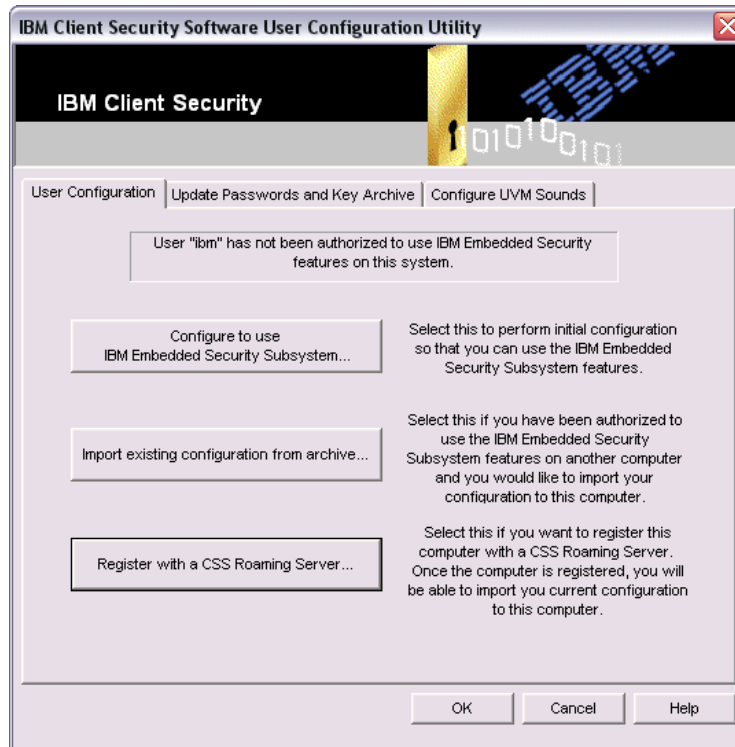


Figure 6-63 Import existing information from archive

2. Click **Import existing information from archive**. After some seconds of processing, your machine can use your security software together with the selected machine.

Important: You will have to do this with all the users that have not been enrolled in your roaming server network previously, and on all machines in your roaming network that will be used by that user.

6.11.5 Unattended install with roaming profiles

As described in 6.4.6, "Performing an unattended installation" on page 474, you can install the IBM Embedded Security Subsystem without any user interaction. To install IBM Embedded Security Subsystem unattended while enabling roaming profiles at the same time is almost identical to the procedure described in 6.4.6, "Performing an unattended installation" on page 474, with the exception

of a few extra steps that you will need to take to make the roaming profiles system install properly.

These are the key actions you must do for proper unattended installation with roaming profiles:

- ▶ You must share the archive folder on your server.
- ▶ You must map the archive folder, for example `z:\`, on your client before the installation procedure is executed. This drive must be available at all times. You cannot delete it after you install it.
- ▶ You must have installed all the required drivers for the security chip before the installation. These drivers are currently not signed by Microsoft so you will have to figure out a good solution for installing them, perhaps a cloning tool.
- ▶ Even though it looks a bit illogical, you must use the `newkp` variable in your `csec.ini` file and it must equal 1. Even though `newkp=1`, it will not create new keys on your server.

Here are some facts about our test system:

- ▶ Our roaming profiles server is named `Roaming`.
- ▶ We have two shares on that server, `Archive` and `Config`. In the unattended install, we only use the `Archive` share.
- ▶ We have mapped the archive share on the roaming profile server as `y:\` on the client.
- ▶ The drivers for the IBM Embedded Security Subsystem are installed.

Important: Make sure that you follow the steps as described in “Client registration” on page 544. You do not have to create the config file, but you do need to authorize a user so that you are able to enroll the machine into your system.

You must configure your roaming server to accept enrollment to the roaming profile system from the user that is logged onto the client before you can proceed.

You must perform the steps described in 6.4.6, “Performing an unattended installation” on page 474. Create the `csec.ini` file and edit the other file for silent install. You will have to modify it a bit to be able to automatically enroll the machine into your roaming profile system.

The `csec.ini` file in Example 6-2 on page 558 is the one we tested. This file worked fine on our system.

Example 6-2 csec.ini file

```
[CSSSetup]
suppw=
hwpw=passw0rd
newkp=1
keysplit=1
kpl=y:\
kal=y:\
enableroaming=1
username=[current]
sysregpwd=password
clean=0

[UVMErollment]
enrollall=0
enrollusers=1
user1=administrator
user1uvmwpw=passw0rd
user1winpw=
user1ppchange=0
user1ppexppolicy=0
user1domain=0

[UVMAppConfig]
uvmlogon=0
entrust=0
notes=0
netscape=0
passman=1
folderprotect=0
autoprotect=0
```

Note: Make sure that the following items are set up correctly for your unattended install of roaming files. Otherwise, your unattended install will not work.

Verify that these items are correct in your configuration file:

- ▶ **hwpw=passw0rd:** You must use the same security administrator password as you used on your roaming profiles server. Otherwise, you might have some problems with communication.
- ▶ **newkp=1:** Even though it does not generate new keys on the server, this variable must be set to 1.
- ▶ **kpl=y:\:** You must map your archive folder to the roaming profile archive share. It is not possible to use for example \\roaming\archive. This mapping

must be permanent. `y:\` is a good example of a mapped version of the archive location folder on the roaming profiles server.

- ▶ **kal=y:**: Same as above.
- ▶ **enableroaming=1**: This variable must be set to 1 to let the IBM Embedded Security Subsystem know that this is a roaming client.
- ▶ **username=[current]**: This variable tells the system that it should use the current logged on username to enroll the client to the system. You can also type in the desired username in this field.
- ▶ **sysregpwd=password**: This is the password you made for the user in the client registration part of the installation, as described in “Client registration” on page 544.

These are the most important items you will need to configure to automatically make the client a part of a roaming system. You will also need to fill in the rest of the information but that can be set to almost whatever you want. You should also add at least one user and give that user access to the IBM Embedded Security Subsystem. Otherwise, it can cause some problems with the policies on the client.

After everything is configured as stated in this part, you are ready to install. Just use the `setup.exe -s` command to start the install. After you reboot, your client should be connected to the roaming profile server.

6.12 Using Adobe Acrobat 6.0 Professional

In this section, we demonstrate how to use the IBM Embedded Security Subsystem with Adobe Acrobat Version 6.0 Professional software from Adobe Systems Incorporated.

6.12.1 Introduction

Adobe Acrobat V6.0 allows you to encrypt or sign documents. It is these Acrobat operations that are better secured if you use them in conjunction with the IBM Embedded Security Subsystem. Using IBM Embedded Security System, you will be able to better verify the user. An example of this is to require a fingerprint every time a user signs a document.

Please note that Adobe Acrobat Professional is licensed software from Adobe Systems Incorporated. The instructions mentioned in this text are only a guide for how to use their software together with the IBM Embedded Security Subsystem.

The procedure described in this chapter requires experience or knowledge of Public Key Infrastructure (PKI) encryption and authentication. Not all steps are described in detail. You can configure each system as a stand-alone system; however, in a professional environment, we recommend that you designate one system to control your public keys. This can include an external trusted third party or an internal system. If you do not have a system that can control your public keys, you must configure each system so that it trusts other self made public keys (self-signed certificates). In the example and text that follows, we create and use a self-signed ID file. You must decide if this is secure enough for your system. The procedures mentioned in this text should be almost identical if you use a trusted third party certificate authority system.

6.12.2 Prerequisites

You must have your IBM Embedded Security Subsystem installed. The ESS must also be configured so that it is in working order. The prerequisites for Adobe Acrobat software can be found on their Web site at:

<http://www.adobe.com/>

In this example we are using Version 6.0.0 of Adobe Acrobat 6.0 Professional.

6.12.3 Installation and configuration

Setting up Adobe Acrobat 6.0 Professional

Follow these steps to configure Adobe Acrobat 6.0 Professional to enable digital IDs:

1. Install Adobe Acrobat 6.0 Professional as described in the user guide for the application. Perform a normal installation.
2. After installation, start Adobe Acrobat 6.0 Professional (from now on called Acrobat) from the Start menu.

You should then see the main Acrobat menu shown in Figure 6-64, which also shows the selections we have made.

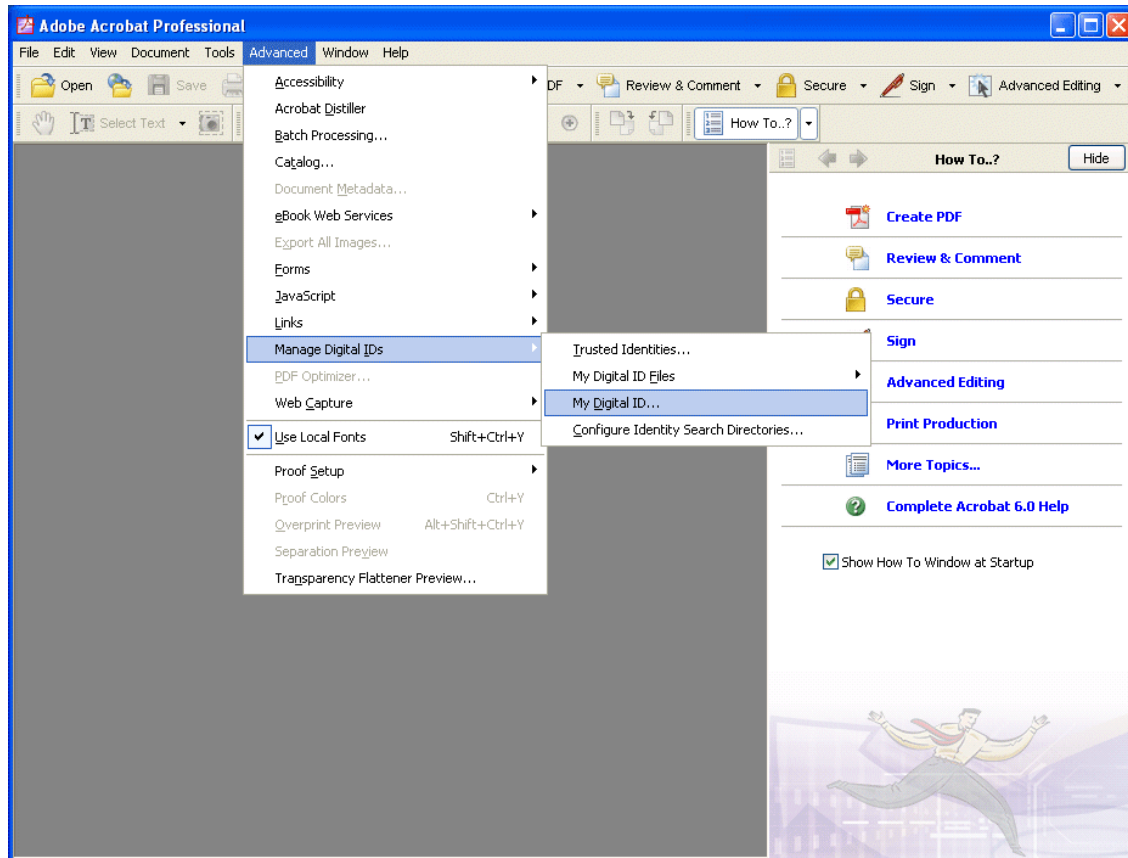


Figure 6-64 Adobe Acrobat 6.0 Professional main menu

3. As shown on Figure 6-64, select **Tools** → **Manage Digital IDs** → **My Digital ID...**

A new window (Figure 6-65) opens.

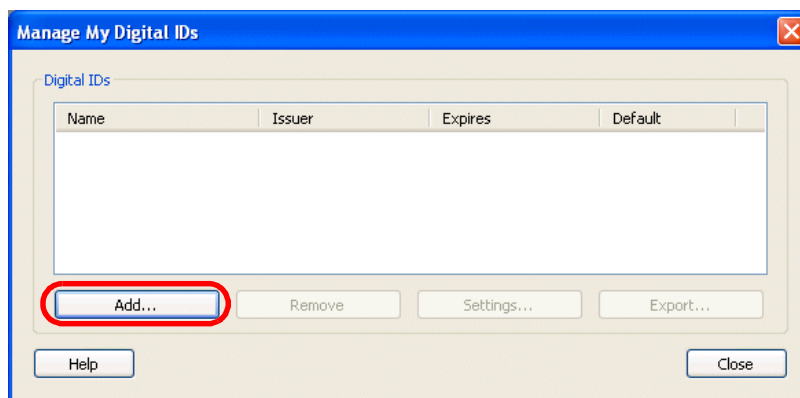


Figure 6-65 Manage My Digital IDs ¹

4. Click **Add...**

The window shown in Figure 6-66 will display.

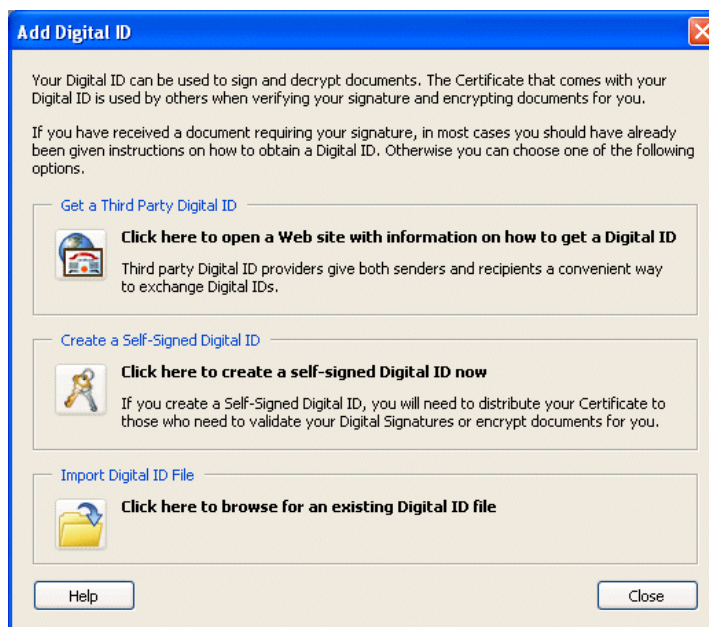


Figure 6-66 Add Digital ID

¹ Adobe Systems Incorporated, Reprinted by Permission

5. As stated in the introduction to this section, you can connect to a third party to authenticate users or create a self-signed Digital ID. Click the icon next to the text Click here to create a self-signed Digital ID now.

A new window such as the one shown in Figure 6-67 opens.



Figure 6-67 Self-Signed Digital ID Disclaimer²

6. Read the disclaimer and click **Continue**.

² Adobe Systems Incorporated, Reprinted by Permission

7. Enter your user information as shown in Figure 6-68. It is important that you select **Add as a “Windows Trusted Root” Digital ID** if it is not already selected. This allows you to use Adobe Acrobat together with the IBM Embedded Security Subsystem.

Create Self-Signed Digital ID

The following options are used to generate a Digital ID and an accompanying Certificate.

Digital ID Details

Name (e.g. John Smith): Haakon Fosshaug

Organizational Unit: PCD

Organization Name: IBM

Email Address: haakon.fosshaug@no.ibm

Country/Region: NO - NORWAY

☐ Enable Unicode Support

Key Algorithm: 1024-bit RSA

Use Digital ID for: Digital Signatures and Data Encryption

Windows Certificate Security

☒ Add as a "Windows Trusted Root" Digital ID

If this option is chosen, the Digital ID will be available for use by non-Acrobat applications.

Access to this Digital ID will be protected by your Windows login

Create Cancel

Figure 6-68 Create Self-Signed Digital ID³

8. Click **Create** when you have filled in all the fields.

³ Adobe Systems Incorporated, Reprinted by Permission

The window shown in Figure 6-69 opens.

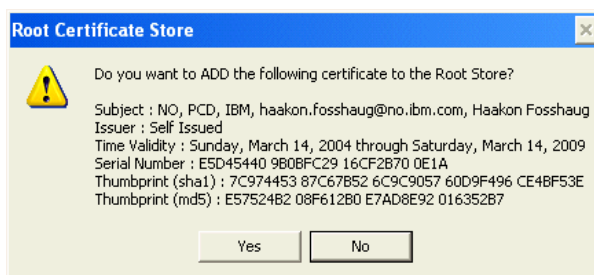


Figure 6-69 Root Certificate Store

9. Click **Yes** to add your root certificate to Windows.

You are returned to the Manage My Digital IDs menu. Your new Digital ID is in the list. See Figure 6-70.

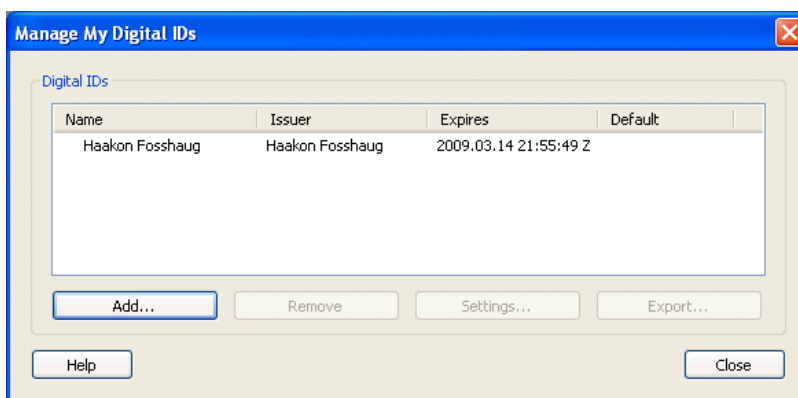


Figure 6-70 Manage My Digital IDs ⁴

10. Click **Close**.

This concludes the tasks you must perform in Adobe Acrobat. You now must configure the IBM Embedded Security Subsystem so that it controls your certificate.

Configuring the IBM ESS to control your Digital ID

If you create a Digital ID as mentioned in the text above, your certificate is stored on your hard drive. This ID might be reachable by hackers or trojan-style hacking applications. To ensure that it is properly secured, you would therefore encrypt it

⁴ Adobe Systems Incorporated, Reprinted by Permission

with the IBM Embedded Security Subsystem. The procedure mentioned below can also be used for any other Microsoft-based certificates.

This is how you add your certificate to the IBM Embedded Security Subsystem:

1. Click the Windows **Start** button. Then select **Run**.
2. Type `C:\Program Files\IBM\Security\xfercert.exe` (this is the default location, but you might have changed it during installation) and click **Enter**.

This opens the IBM Client Security Certificate Transfer Tool. The window should look like Figure 6-71.

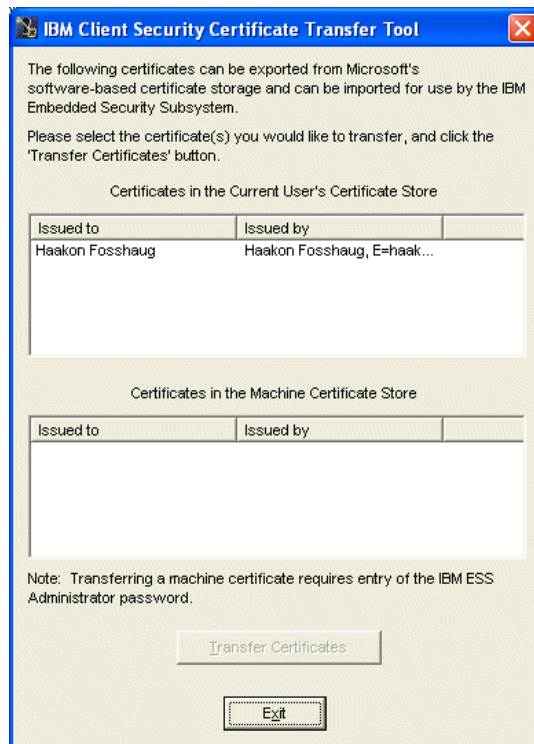


Figure 6-71 IBM Client Security Certificate Transfer Tool

3. Select the certificate(s) you would like to transfer, and click the **Transfer Certificates** button.

After processing, a message as shown in Figure 6-72 opens.



Figure 6-72 Certificates transferred

4. Confirm that the number of certificates transferred is correct and click **OK**.

This concludes the certificate transfer. You can now exit the IBM Client Security Certificate Transfer Tool. Your certificate is safely stored through the IBM Embedded Security Subsystem.

Tip: This procedure can be used for any Microsoft-based certificates, not only for Adobe Acrobat Professional V6.0. It is, for example, a part of the procedure to secure an 802.1x network.

6.12.4 Hints and tips

The use of Adobe Acrobat 6.0 Professional for digital signatures or encryption is a easy way to make sure that your documents do not fall into the wrong hands. In addition, it can ensure that a person has actually viewed and confirmed the contents of a document.

By using this function in conjunction with IBM Embedded Security Subsystem, you will take it one step further. If you have a company network where you use digital signatures as a company policy, you can easily setup a system that mandates use, for example, of your fingerprint to sign documents. In that way, you can be secure in the fact that a particular person wrote a specific document. By storing the certificates through the security chip, you will also have a potential of 2048 bit encryption on your certificates. It will be very unlikely for a trojan application or a hacker to get access to the keys due to the hardware encryption through the built in chip.

If you decide at a later date to change the way users must authenticate to give them permission to sign, encrypt or decrypt PDF files, you must change your policy in the IBM Embedded Security Subsystem control panel. The policy you would have to change is the policy for Digital Signature (e-mail) and Decryption (e-mail). See "Application Policy" on page 501 for more information about how to change your policies.

6.13 Usage scenarios

Administrators can use the multiple components provided by IBM Client Security Software to set up the security features that IBM client users require. You can use the following examples to guide you in your planning and execution of your client security policy.

6.13.1 Windows 2000 and Windows XP clients and Outlook Express

This example involves two client systems:

- ▶ Client 1
 - Windows 2000 and Outlook Express are installed.
 - Three users with authentication setup using User Verification Manager.
- ▶ Client 2
 - Windows XP and Outlook Express are installed.
 - One user with authentication setup using User Verification Manager.

All client users must register their fingerprints so that they can be used for authentication. A Targus DEFCON fingerprint sensor will be installed during this example. It has also been established that both clients will require User Verification Manager protection for the Windows logon. The administrator has decided that the local UVM policy will be edited and used at the client level.

To set up client security, complete the following procedure:

1. Install the software on client 1 and client 2. Refer to 6.4, “Installation instructions” on page 457 for details.
2. Install the Targus fingerprint reader and its associated software on each client. Refer to “Install the Targus PC Card Fingerprint Reader as follows:” on page 473 for details.
3. Set up user authentication using User Verification Manager for each client. Do the following:
 - a. Add users to User Verification Manager by assigning them a User Verification Manager passphrase. Because client 1 has three users, you must repeat the process for adding users to User Verification Manager until all users have been added.
 - b. Set up User Verification Manager protection for the Windows logon for each client.
 - c. Register user fingerprints. Because the policy allows three users to use client 1, all three users must register their fingerprints.

Note: If you designate that a fingerprint is required for authentication as part of User Verification Manager policy for a client, each user must register his or her fingerprint.

4. Edit and save a local User Verification Manager policy for each client that requires authentication for the following:
 - Logging on to the operating system
 - Acquiring a digital certificate
 - Using a digital signature for e-mail messages
5. Restart each client to enable User Verification Manager protection for the Windows logon.
6. Inform the users of the User Verification Manager passphrases that you have set for them and of the authentication requirements that you set up in the UVM policy for the IBM client.

Client users can now perform the following tasks:

- ▶ Use User Verification Manager protection to lock and unlock the operating system.
- ▶ Apply for a digital certificate and choose the IBM Embedded Security Chip as the cryptographic service provider associated with the certificate.
- ▶ Use the digital certificate to encrypt e-mail messages created with Outlook Express.

6.13.2 Windows 2000 clients using Lotus Notes

This example involves two client systems:

- ▶ Client 1
 - Windows 2000 and Lotus Notes are installed.
 - Two users with authentication setup using User Verification Manager.
- ▶ Client 2
 - Windows 2000 and Lotus Notes are installed.
 - One user with authentication setup using User Verification Manager.

Both clients require User Verification Manager protection for the system logon, and must use the IBM Client Security Software screen saver and User Verification Manager protection for Lotus Notes. In this example, the administrator decided that a User Verification Manager policy for remote clients will be edited on client 1, and then copied to client 2.

To set up client security, complete the following procedure:

1. Install the software on client 1 and client 2. Because a UVM policy for remote clients will be used, you must use the same admin public key when you install the software on both client 1 and client 2. Refer to 6.4, “Installation instructions” on page 457 for details about the software installation.
2. Set up user authentication with User Verification Manager for each client. Then, do the following:
 - a. Add users to User Verification Manager by assigning them a User Verification Manager passphrase. Because client 1 has two users, you must repeat the process for adding users to User Verification Manager until both users have been added.
 - b. Set up User Verification Manager protection for Windows logon on each client.
3. Enable User Verification Manager protection for Lotus Notes on both clients. Refer to 6.8, “Using User Verification Manager protection for Lotus Notes” on page 517.
4. Edit and save a User Verification Manager policy for remote clients on client 1, and then copy it to client 2. The User Verification Manager policy would require user authentication for clearing the screen saver, logging on to Lotus Notes, and logging on to the operating system. Refer to “Editing a UVM policy on remote clients” on page 507 for details.
5. Restart each client to enable the User Verification Manager protection for the system logon.
6. Inform the client users of the User Verification Manager passphrases and the policy that has been set for each client.

The users can now read the IBM Client Security Software User’s Guide to learn how to perform the following tasks:

- ▶ Enable the Client Security screen saver
- ▶ Use User Verification Manager protection for Windows 2000

6.13.3 Windows 2000 clients managed by Tivoli Access Manager

The intended audience for the following example is an enterprise administrator who plans to use Tivoli Access Manager to manage the authentication objects set up in the UVM policy. In this example, multiple IBM clients have both Windows 2000 and Netscape (for e-mail) installed. All clients have NetSEAT client, a component of Tivoli Access Manager, installed. All clients using a Lightweight Directory Access Protocol (LDAP) server have the LDAP client installed. UVM policy for remote clients will be installed on all clients. The UVM

policy will enable Tivoli Access Manager to control selected authentication objects for the clients.

In this example, one user will require authentication setup with User Verification Manager on each client. All users will register their fingerprints so that they can be used for authentication. In this example, a Targus DEFCON fingerprint sensor will be installed and all clients will require User Verification Manager protection for Windows logon.

To set up client security, complete the following procedure:

1. Install the IBM Client Security Software on the Tivoli Access Manager server. For details, see *Using Client Security with Tivoli Access Manager*:
<http://www.ibm.com/pc/support/site.wss/document.do?ln docid=MIGR-4639>
2. Install IBM Client Security Software on all clients. Because a User Verification Manager policy for remote clients will be used, you must use the same admin public key when you install the software on all clients. Refer to 6.4.2, "Installing prerequisite device drivers" on page 458 for details about the software installation.
3. Install the User Verification Manager-aware fingerprint sensors and any associated software on each client. For information about available User Verification Manager-aware products, access this Web site:
<http://www.pc.ibm.com/us/security/secdownload.html>
4. Set up user authentication with User Verification Manager on each client. Then, do the following:
 - a. Add users to User Verification Manager by assigning them a User Verification Manager passphrase.
 - b. Set up User Verification Manager protection for the Windows logon on each client.
 - c. Register the fingerprints for each client user. If fingerprint authentication is required on an IBM client, all users of that client must register their fingerprints.
5. Configure the Tivoli Access Manager setup information for each client. For details, see *Using Client Security with Tivoli Access Manager*:
<http://www.ibm.com/pc/support/site.wss/document.do?ln docid=MIGR-4639>
6. Edit and save a UVM policy for remote clients on one of the clients, and then copy it to the other clients. Set the UVM policy so that Tivoli Access Manager will control the following authentication objects:
 - Logging on the operating system
 - Acquiring a digital certificate
 - Using a digital signature for e-mail messages

For details, refer to “Editing a UVM policy on remote clients” on page 507.

7. Restart each client to enable User Verification Manager protection for the Windows logon.

Install the IBM Embedded Security Chip PKCS#11 module onto each client. This module provides cryptographic support on clients that use Netscape for sending and receiving e-mail messages and use the IBM Embedded Security Chip for acquiring digital certificates. For more information, see the *Client Security Software Installation Guide*, available at this Web site:

<http://www.ibm.com/pc/support/site.wss/document.do?ln docid=MIGR-4639>

8. Enable Tivoli Access Manager to control the IBM Client Security Software objects that appear in the Tivoli Access Manager's Management Console.
9. Inform client users of the User Verification Manager passphrases and the policy that has been set up for each client.
10. Advise client users to read the *IBM Client Security Software User's Guide* available at the following Web site:

<http://www.ibm.com/pc/support/site.wss/document.do?ln docid=MIGR-4639>

Users can learn how to:

- Use User Verification Manager protection to lock and unlock the operating system.
- Use the User Configuration Utility.
- Apply for a digital certificate that uses the IBM Embedded Security Chip as the cryptographic service provider associated with the certificate.
- Use the digital certificate to encrypt e-mail messages created with Netscape.

6.14 Uninstalling

Before you uninstall IBM Client Security Software, be sure that you uninstall the various utilities that enhance its functionality. Users must log on with administrator privileges to uninstall IBM Client Security Software.

Note: You must uninstall all IBM Client Security Software utilities and all User Verification Manager-aware software before you uninstall IBM Client Security Software.

To uninstall IBM Client Security Software, complete the following procedure:

1. Close all Windows programs.
2. From the Windows desktop, select **Start** → **Settings** → **Control Panel**.
3. Click the **Add/Remove Programs** icon.
4. In the list of software that can be automatically removed, select **IBM Client Security**.
5. Click **Add/Remove**.
6. Select **Remove**.
7. Click **Yes** to uninstall the software.
8. Do one of the following:
 - If you installed the IBM Embedded Security Chip PKCS#11 module for Netscape, a message is displayed asking you to start the process to disable it. Click **Yes** to proceed.

A series of messages will be displayed. Click **OK** for each message until the IBM Embedded Security Chip PKCS#11 module is removed.
 - If you did not install the IBM Embedded Security Chip PKCS#11 module for Netscape, a message is displayed asking whether you want to delete shared DLL files that were installed with IBM Client Security Software.

Click **Yes** to uninstall these files, or click **No** to leave the files installed. Leaving these files installed has no effect on the normal operation of your computer.
9. Click **OK** after the software is removed.

You must restart the computer after uninstalling IBM Client Security Software for the changes to take effect.

Note: When you uninstall IBM Client Security Software, make sure that you remove all installed IBM Client Security Software components along with all user keys, digital certificates, registered fingerprints and stored passwords. However, the key archive is not affected when IBM Client Security Software is uninstalled.

6.15 Troubleshooting

This section contains information that an administrator might find helpful when identifying and correcting problems that might arise as you use IBM Client Security Software.

6.15.1 Error messages

Error messages related to IBM Client Security Software are generated in the event log. IBM Client Security Software uses a device driver that might generate error messages in the event log. The errors associated with these messages do not affect the normal operation of your computer.

UVM invokes error messages that are generated by the associated program if access is denied for an authentication object. If the UVM policy is set to deny access for an authentication object, for example e-mail decryption, the message stating that access has been denied will vary, depending on what software is being used. For example, an error message from Outlook Express stating that access is denied to an authentication object will differ from an error message from Netscape stating that access was denied.

6.15.2 Fail counts on TCPA and non-TCPA systems

Anti-hammering refers to a technique used to block out users for a certain period of time if they fail to login after a certain amount of attempts. This is needed to prevent rogue password cracking software from guessing account passwords and hacking into the computer. Systems manufactured according to the guidelines set forth by the TCPA (Trusted Computing Platform Alliance) as well as non-compliant systems have built-in, anti-hammering locking features. IBM is a member of the TCPA.

Table 4-1 shows the anti-hammering delay settings for a TCPA system.

Table 6-1 Fail counts

Attempts	Delay on next failure
15	1.1 minutes
31	2.2 minutes
47	4.4 minutes
63	8.8 minutes
79	17.6 minutes
95	35.2 minutes
111	1.2 hours
127	2.3 hours
143	4.7 hours

The advantages of the anti-hammering scheme for TCPA systems are:

- ▶ It is graduated; the more failed logins attempted, the longer period of time the user is locked out. This is good because it is more likely that the real user will make only a few attempts to login if he or she forgets the password. The hackers are more likely to make many brut force attempts. Therefore, this graduated scheme is designed to lock out hackers for a long enough period of time to discourage them, while bonafide users who have forgotten their passwords should be able to get back on the system quickly for the sake of productivity.
- ▶ There is no distinction between user passphrases and the administrator password. That means hackers will be subject to the same lock-out policy whether they're feigning to be a legitimate user or the administrator. Any authentication using the IBM Embedded Security Chip adheres to the same policy.
- ▶ There is a maximum lockout period of 4.7 hours so that the maximum amount of time that the user or administrator would have to be without the system is kept to a reasonable level.

The anti-hammering policy for non-TCPA systems is more generalized. Non-TCPA systems distinguish between the administrator password and user passphrases. On non-TCPA systems, failed login attempts using the administrator password cause longer delays (77-minutes after ten failed attempts) than the user passwords (a one-minute delay after 32 failed attempts) and then the lock-out time doubles after every 32 failed attempts.

6.15.3 File and Folder Encryption utility known issues

The IBM File and Folder Encryption Utility might encounter a blue screen error when using an application that repartitions the hard drive. If you encounter a blue screen error, you must disable IBM File and Folder Encryption. Complete the following procedure to recover from the error state:

1. Restart and log onto the system.
2. Disable FFE using the Administrator Utility procedure described in "File and Folder Encryption known issues" on page 490.

If the procedure does not work because your system continues in a blue screen loop, complete the following procedure:

1. Stop the system from the blue screen.
2. Start the system in Safe Mode by pressing F8 while the BIOS IBM logo screen is displayed during startup.
3. Select **Safe Mode** from the Windows menu.

4. Log on to Windows.
5. Rename the device driver from ibmfilter.sys to ibmfilter.xxx in the \system32\drivers folder of the Windows installation directory.
6. Restart the system and log on to the system.
7. Disable FFE using the Administrator Utility procedure described above.

Recovering from a blue screen STOP condition (BSOD) while installing Norton Anti-Virus 2003 application software with IBM Client Security Software

With IBM Client Security Software and FFE installed on a system, a Norton Anti-Virus 2003 software installation will terminate with a STOP 0x7A condition. To recover from this condition, complete the following procedure:

1. Restart your computer from the blue screen.
2. When the system has restarted, log on to the system and authenticate with FFE. The Norton Anti-virus software has only been partially installed. Norton AntiVirus 2003 will display the error message shown in Figure 6-73.

Note: Do not click the **OK** button shown in Figure 6-73. This will restart the system.

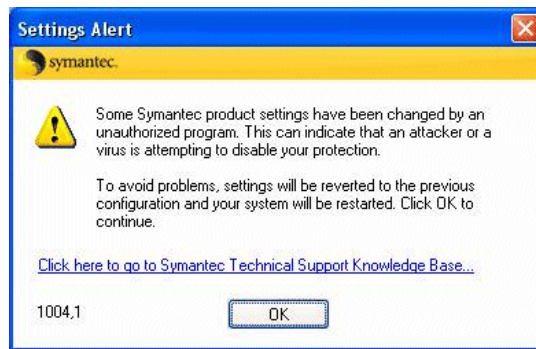


Figure 6-73 NAV error message

3. Click the hyperlink within the message box to go to the Symantec Technical Support Knowledge Base.
4. In the middle of the page, find the section labelled: NAV installed as a stand-alone product. Follow the instructions to download and run the Rnav2003.exe removal utility, as follows:
 - a. Click the **Rnav2003.exe** icon to start the download process.

- b. Click **Save this program to disk**, and then click **OK**.
 - c. Change the location in the Save in field to Desktop, and then click **Save**.
 - d. Click **Close** when the download is complete.
 - e. Double-click the **Rnav2003.exe** icon on the Desktop to launch the application.
5. On the RNAV Question window, click **No** to continue.
6. Select the appropriate version of Norton AntiVirus, and then click **OK**.
7. Click **Yes** to start the uninstall procedure.
A progress indicator appears while the Rnav2003.exe utility removes Norton AntiVirus files and registry keys.
8. Click **No** to stop the computer from restarting when the uninstallation is completed.
9. Disable the FFE component through the IBM Client Security Software Administrator Utility using the following procedure:
 - a. Start the Administrator Utility.
 - b. Click the **Configure Application Support and Policies** button.
 - c. Clear the **Enable File and Folder protection** check box.
 - d. Click **OK**.
10. Restart the computer.
11. Reinstall the Norton AntiVirus 2003 utility.
12. Enable the FFE component through the Administrator Utility. The computer will restart.

6.15.4 Installation troubleshooting information

The following troubleshooting information might be helpful if you experience problems when installing IBM Client Security Software.

Table 6-2 Installation troubleshooting information

Problem Symptom	Possible Solution
An error message is displayed during software installation. A message is displayed when you install the software that asks if you want to remove the selected application and all of its components.	Click OK to exit the window. Begin the installation process again to install the new version of IBM Client Security Software.

Problem Symptom	Possible Solution
A message is displayed during installation stating that a previous version of IBM Client Security Software is already installed.	Click OK to exit from the window. Do the following: 1. Uninstall the software. 2. Reinstall the software. Note: If you plan to use the same hardware password to secure the IBM Embedded Security Chip, you do not have to clear the chip and reset the password.
Installation access is denied due to an unknown hardware password. When installing the software on an IBM client with an enabled IBM Embedded Security Chip, the hardware password for the IBM Embedded Security Chip is unknown.	Clear the chip to continue with the installation.
The setup.exe file does not respond properly (IBM Client Security Software V4.0x). If you extract all files from the csec4_0.exe file into a common directory, the setup.exe file will not work properly.	Run the smbush.exe file to install the SMBus device driver, and then run the csec4_0.exe file to install the IBM Client Security Software code.

6.15.5 Administrator Utility troubleshooting information

The troubleshooting information in Table 6-3 might be helpful if you experience problems when using the Administrator Utility.

Table 6-3 Administrator Utility troubleshooting information

Problem Symptom	Possible Solution
UVM passphrase policy is not enforced. The not contain more than 2 repeated characters check box does not work in IBM Client Security Software V5.0	This is a known limitation with IBM Client Security Software V5.0.
The Next button is unavailable after entering and confirming your UVM passphrase in the Administrator Utility. When you add users to UVM, the Next button might not be available after you enter and confirm your UVM passphrase in the Administrator Utility.	Click the Information item on the Windows Task Bar and continue the procedure.

Problem Symptom	Possible Solution
<p>An error message displays when you attempt to edit local UVM policy. When you edit the local UVM policy, an error message might display if no users are enrolled in UVM.</p>	<p>Add a user to UVM before attempting to edit the policy file.</p>
<p>An error message displays when you change the admin public key. When you clear the Embedded Security Chip and then restore the key archive, an error message might display if you change the admin public key.</p>	<p>Add the users to UVM and request new certificates, if applicable.</p>
<p>An error message displays when you attempt to recover a UVM passphrase. When you change the admin public key and then attempt to recover a UVM passphrase for a user, an error message might display.</p>	<p>Do one of the following:</p> <ul style="list-style-type: none"> ▶ If the UVM passphrase for the user is not needed, no action is required. ▶ If the UVM passphrase for the user is needed, you must add the user to UVM, and request new certificates, if applicable.
<p>An error message displays when you try to save the UVM-policy file. When you attempt to save a UVM-policy file (globalpolicy.gvm) by clicking Apply or Save, an error message is displayed.</p>	<p>Exit the error message, edit the UVM-policy file again to make your changes, and then save the file.</p>
<p>An error message displays when you try to open the UVM-policy editor. When the current user (logged on to the operating system) has not been added to UVM, the UVM-policy editor will not open.</p>	<p>Add the user to UVM and open the UVM-policy editor.</p>
<p>An error message displays when you are using the Administrator Utility. When you are using the Administrator Utility, the following error message might display:</p> <p>A buffer I/O error occurred while trying to access the Client Security chip. This might be corrected by a restart.</p>	<p>Exit the error message and restart your computer.</p>

Problem Symptom	Possible Solution
<p>A disable chip message is displayed when changing the Security Chip password.</p> <p>When you attempt to change the Security Chip password, and you press Enter or Tab →Enter after you type the confirmation password, the Disable chip button will be enabled and a disable chip confirmation message is displayed.</p>	<p>Do the following:</p> <ol style="list-style-type: none"> 1. Exit from the disable chip confirmation window. 2. To change the Security Chip password, type the new password, type the confirmation password, and then click Change. Do not press Enter or Tab →Enter after you type the confirmation password.

6.15.6 User Configuration Utility troubleshooting information

The following troubleshooting information might be helpful if you experience problems when using the User Configuration Utility.

Table 6-4 User Configuration Utility troubleshooting information

Problem Symptom	Possible Solution
<p>Limited Users are unable to perform certain User Configuration Utility functions in Windows XP Professional.</p> <p>Windows XP Professional Limited Users might not be able to perform the following User Configuration Utility tasks:</p> <ul style="list-style-type: none"> ► Change their UVM passphrases ► Update the Windows password registered with UVM ► Update the key archive 	<p>These limitations are cleared after an administrator starts and exits the Administrator Utility.</p>
<p>Limited Users are unable to use the User Configuration Utility in Windows XP Home.</p> <p>Windows XP Home Limited Users will not be able to use the User Configuration Utility in any of the following situations:</p> <ul style="list-style-type: none"> ► IBM Client Security Software is installed on an NTFS formatted partition ► The Windows folder is on an NTFS formatted partition ► The archive folder is on an NTFS formatted partition 	<p>This is a known limitation with Windows XP Home. There is no solution to this problem.</p>

6.15.7 ThinkPad-specific troubleshooting information

The following troubleshooting information might be helpful if you experience problems when using IBM Client Security Software on ThinkPad computers.

Table 6-5 ThinkPad specific troubleshooting

Problem Symptom	Possible Solution
An error message is displayed when attempting an IBM Client Security Software administrator function. The following error message is displayed after trying to perform an administrator function: ERROR 0197: Invalid Remote change requested. Press F1 to Setup	The ThinkPad supervisor password must be disabled to perform certain IBM Client Security Software administrator functions. To disable the supervisor password, complete the following procedure: <ol style="list-style-type: none">1. Press F1 to access the IBM BIOS Setup Utility.2. Enter the current supervisor password.3. Enter a blank new supervisor password, and confirm a blank password.4. Press Enter.5. Press F10 to save and exit.
Different UVM-aware fingerprint sensors do not work properly. The IBM ThinkPad computer does not support the interchanging of multiple UVM-aware fingerprint sensors.	Do not switch fingerprint sensor models. Use the same model when working remotely as when working from a docking station.

6.15.8 Microsoft troubleshooting information

The following troubleshooting charts contain information that might be helpful if you experience problems using IBM Client Security Software with Microsoft applications or operating systems.

Restriction: In Windows XP, users enrolled in UVM that previously had their Windows user name changed will not be recognized by UVM. This limitation applies even if the Windows user name was changed prior to installing IBM Client Security Software.

Table 6-6 Microsoft troubleshooting information

Problem Symptom	Possible Solution
<p>Screen saver only displays on the local screen.</p> <p>When using the Windows extended desktop function, the IBM Client Security Software screen saver will only be displayed on the local screen even though access to your system and its keyboard will be protected.</p>	<p>If any sensitive information is being displayed, minimize the windows on your extended desktop before you invoke the IBM Client Security Software screen saver.</p>
<p>Windows Media Player files are encrypted rather than being played in Windows XP.</p> <p>In Windows XP, when you open a folder and click Play all, the contents of the file will be encrypted rather than played by the Windows Media Player.</p>	<p>To enable the Windows Media Player to play the files, complete the following procedure:</p> <ol style="list-style-type: none"> 1. Start Windows Media Player. 2. Select all the files in the appropriate folder. 3. Drag the files to the Windows Media Player playlist area.
<p>Client Security does not work properly for a user enrolled in UVM.</p> <p>The enrolled client user might have changed his Windows user name. If that occurs, all IBM Client Security Software functionality is lost.</p>	<p>Re-enroll the new user name in UVM and request all new credentials.</p>
<p>Problems reading encrypted e-mail using Outlook Express.</p> <p>Encrypted e-mail cannot be decrypted because of the differences in encryption strengths of the Web browsers used by the sender and recipient.</p>	<p>Verify the following:</p> <ol style="list-style-type: none"> 1. The encryption strength for the Web browser that the sender uses is compatible with the encryption strength of the Web browser that the recipient uses. 2. The encryption strength for the Web browser is compatible with the encryption strength provided by the firmware of IBM Client Security Software.

Problem Symptom	Possible Solution
<p>Problems arise when using a certificate from an address that has multiple certificates associated with it.</p> <p>Outlook Express can list multiple certificates associated with a single e-mail address and some of those certificates can become invalid. A certificate can become invalid if the private key associated with the certificate no longer exists on the IBM Embedded Security Chip of the sender's computer where the certificate was generated.</p>	<p>Ask the recipient to resend his digital certificate; then select that certificate in the address book for Outlook Express.</p>
<p>Failure message when trying to digitally sign an e-mail message.</p> <p>If the composer of an e-mail message tries to digitally sign it when the composer does not yet have a certificate associated with his or her e-mail account, an error message displays.</p>	<p>Use the security settings in Outlook Express to specify a certificate to be associated with the user account. See the documentation provided for Outlook Express for more information.</p>
<p>Outlook Express (128 bit) only encrypts e-mail messages with the 3DES algorithm.</p> <p>When sending encrypted e-mail between clients that use Outlook Express with the 128-bit version of Internet Explorer 4.0 or 5.0, only the 3DES algorithm can be used.</p>	<p>To use 128-bit browsers with IBM Client Security Software, the IBM Embedded Security Chip must support 256-bit encryption. If the IBM Embedded Security Chip supports 56-bit encryption, you must use a 40-bit Web browser. You can obtain the encryption strength provided by IBM Client Security Software in the Administrator Utility. See Microsoft for current information about the encryption algorithms used with your version of Outlook Express.</p>
<p>Outlook Express clients return e-mail messages with a different algorithm.</p> <p>An e-mail message encrypted with the RC2(40), RC2(64), or RC2(128) algorithm is sent from a client using Netscape Messenger to a client using Outlook Express (128-bit). A returned e-mail message from the Outlook Express client is encrypted with the RC2(40) algorithm.</p>	<p>No action is required. An RC2(40), RC2(64), or RC2(128) encryption request from a Netscape client to an Outlook Express (128-bit) client is always returned to the Netscape client with the RC2(40) algorithm. See Microsoft for current information about the encryption algorithms used with your version of Outlook Express.</p>

Problem Symptom	Possible Solution
<p>Error message occurs when using a certificate in Outlook Express after a hard disk drive failure.</p> <p>Certificates can be restored by using the key restoration feature in the Administrator Utility. Some certificates, such as the free certificates provided by VeriSign, might not be restored after a key restoration.</p>	<p>After restoring the keys, do one of the following:</p> <ul style="list-style-type: none"> ▶ Obtain new certificates ▶ Register the certificate authority again in Outlook Express
<p>Outlook Express does not update the encryption strength associated with a certificate.</p> <p>When a sender selects the encryption strength in Netscape and sends a signed e-mail message to a client using Outlook Express with Internet Explorer 4.0 (128-bit), the encryption strength of the returned e-mail might not match.</p>	<p>Delete the associated certificate from the address book in Outlook Express. Open the signed e-mail again and add the certificate to the address book in Outlook Express.</p>
<p>An error decryption message displays in Outlook Express.</p> <p>You can open a message in Outlook Express by double-clicking it. In some instances, when you double-click an encrypted message too quickly, a decryption error message appears. Also, a decryption error message might display in the preview pane when you select an encrypted message.</p>	<p>Close the message, and open the encrypted e-mail message again. If an error message appears in the preview pane, no action is required.</p>
<p>An error message displays when you click the Send button twice on encrypted e-mails.</p> <p>When using Outlook Express, if you click the send button twice to send an encrypted e-mail message, an error message displays stating that the message could not be sent.</p>	<p>Close the error message and click the Send button once.</p>
<p>An error message displays when you requesting a certificate.</p> <p>When using Internet Explorer, you might receive an error message if you request a certificate that uses the IBM Embedded Security Chip CSP.</p>	<p>Request the digital certificate again.</p>

6.15.9 Netscape application troubleshooting information

Table 6-7 contains information that might be helpful if you experience problems using IBM Client Security Software with Netscape applications.

Note: To use 128-bit browsers with IBM Client Security Software, the IBM Embedded Security Chip must support 256-bit encryption. If the IBM Embedded Security Chip does not supports 256-bit encryption, you must use a 40-bit Web browser. You can obtain the encryption strength provided by IBM Client Security Software in the Administrator Utility.

Table 6-7 Netscape application troubleshooting information

Problem Symptom	Possible Solution
Problems reading encrypted e-mail. Encrypted e-mail cannot be decrypted because of the differences in encryption strengths of the Web browsers used by the sender and recipient.	Verify the following: <ol style="list-style-type: none">1. That the encryption strength for the Web browser that the sender uses is compatible with the encryption strength of the Web browser that the recipient uses.2. That the encryption strength for the Web browser is compatible with the encryption strength provided by the firmware of IBM Client Security Software.
Failure message when trying to digitally sign an e-mail message. When the IBM Embedded Security Chip certificate has not been selected in Netscape Messenger, and the writer of an e-mail message tries to sign the message with the certificate, an error message displays.	Use the security settings in Netscape Messenger to select the certificate. When Netscape Messenger is open, click the security icon on the toolbar. The Security Info window opens. Click Messenger in the left panel and then select the IBM Embedded Security Chip certificate . See the documentation provided by Netscape for more information.
An e-mail message is returned to the client with a different algorithm. An e-mail message encrypted with the RC2(40), RC2(64), or RC2(128) algorithm is sent from a client using Netscape Messenger to a client using Outlook Express (128-bit). A returned e-mail message from the Outlook Express client is encrypted with the RC2(40) algorithm.	No action is required. An RC2(40), RC2(64), or RC2(128) encryption request from a Netscape client to an Outlook Express (128-bit) client is always returned to the Netscape client with the RC2(40) algorithm. See Microsoft for current information about the encryption algorithms used with your version of Outlook Express.

Problem Symptom	Possible Solution
<p>Unable to use a digital certificate generated by the IBM Embedded Security Chip. The digital certificate generated by the IBM Embedded Security Chip is not available for use.</p>	<p>Verify that the correct UVM passphrase was typed when Netscape was opened. If you type the incorrect UVM passphrase, an error message displays stating an authentication failure. If you click OK, Netscape opens, but you will not be able to use the certificate generated by the IBM Embedded Security Chip. You must exit and re-open Netscape, and then type the correct UVM passphrase.</p>
<p>New digital certificates from the same sender are not replaced within Netscape. When a digitally signed e-mail is received more than once by the same sender, the first digital certificate associated with the e-mail is not overwritten.</p>	<p>If you receive multiple e-mail certificates, only one certificate is the default certificate. Use the security features in Netscape to delete the first certificate, and then re-open the second certificate or ask the sender to send another signed e-mail.</p>
<p>Cannot export the IBM Embedded Security Chip certificate. The IBM Embedded Security Chip certificate cannot be exported in Netscape. The export feature in Netscape can be used to back up certificates.</p>	<p>Go to the Administrator Utility or User Configuration Utility to update the key archive. When you update the key archive, copies of all the certificates associated with the IBM Embedded Security Chip are created.</p>
<p>Error message when trying to use a restored certificate after a hard disk drive failure. Certificates can be restored by using the key restoration feature in the Administrator Utility. Some certificates, such as the free certificates provided by VeriSign, might not be restored after a key restoration.</p>	<p>After restoring the keys, obtain a new certificate.</p>
<p>Netscape agent opens and causes Netscape to fail. Netscape agent opens and closes Netscape.</p>	<p>Turn off the Netscape agent.</p>
<p>Netscape delays if you try to open it. If you add the IBM Embedded Security Chip PKCS#11 module and then open Netscape, a short delay will occur before Netscape opens.</p>	<p>No action is required. This is for informational purposes only.</p>

6.15.10 Digital certificate troubleshooting information

The troubleshooting information in Table 6-8 might be helpful if you experience problems obtaining a digital certificate.

Table 6-8 Digital certificate troubleshooting

Problem Symptom	Possible Solution
UVM passphrase window or fingerprint authentication window displays multiple times during a digital certificate request. The UVM security policy dictates that a user provide the UVM passphrase or fingerprint authentication before a digital certificate can be acquired. If the user tries to acquire a certificate, the authentication window that asks for the UVM passphrase or fingerprint scan displays more than once.	Type your UVM passphrase or scan your fingerprint each time the authentication window opens.
A VBScript or JavaScript error message displays. When you request a digital certificate, an error message related to VBScript or JavaScript might display.	Restart the computer, and obtain the certificate again

6.15.11 Tivoli Access Manager troubleshooting information

The troubleshooting information in Table 6-9 might be helpful if you experience problems when using Tivoli Access Manager with IBM Client Security Software.

Table 6-9 Tivoli Access manager

Problem Symptom	Possible Solution
Local policy settings do not correspond to those on the server. Tivoli Access Manager allows certain bit configurations that are not supported by UVM. Consequently, local policy requirements can override settings made by an administrator when configuring the PD server.	This is a known limitation.

Problem Symptom	Possible Solution
Tivoli Access Manager setup settings are not accessible Tivoli Access Manager setup and local cache setup settings are not accessible on the Policy Setup page in the Administrator Utility.	Install the Tivoli Access Manager runtime Environment. If the Runtime Environment is not installed on the IBM client, the Tivoli Access Manager settings on the Policy Setup page will not be available.
A user's control is valid for both the user and the group. When configuring the Tivoli Access Manager server, if you define a user to a group, the user's control is valid for both the user and the group if Traverse bit is on.	No action is required.

6.15.12 Lotus Notes troubleshooting information

The troubleshooting information in Table 6-10 might be helpful if you experience problems using Lotus Notes with IBM Client Security Software.

Table 6-10 Lotus Notes troubleshooting

Problem Symptom	Possible Solution
After enabling UVM protection for Lotus Notes, Notes is not able to finish its setup. Lotus Notes is not able to finish setup after UVM protection is enabled using the Administrator Utility.	This is a known limitation. Lotus Notes must be configured and running before Lotus Notes support is enabled in the Administrator Utility.
An error message displays when you try to change the Notes password. Changing the Notes password when using IBM Client Security Software might display an error message.	Retry the password change. If this does not work, restart the client.
An error message opens after you randomly generate a password. This may happen when you do the following: <ul style="list-style-type: none"> ► Use Lotus Notes Configuration tool to set UVM protection for a Notes ID. ► Open Notes and use the function provided by Notes to change the password for Notes ID file. ► Close Notes immediately after you change the password. 	Click OK to close the message. No other action is required. Contrary to the error message, the password has changed. The new password is a randomly-generated password created by IBM Client Security Software. The Notes ID file is now encrypted with the randomly-generated password, and the user does not need a new User ID file. If the end user changes the password again, UVM will generate a new random password for the Notes ID.

6.15.13 Encryption troubleshooting information

The troubleshooting information in Table 6-11 might be helpful if you experience problems when encrypting files using IBM Client Security Software 3.0 or later.

Table 6-11 Encryption troubleshooting

Problem Symptom	Possible Solution
Previously encrypted files will not decrypt. Files encrypted with previous versions of IBM Client Security Software do not decrypt after upgrading to IBM Client Security Software 3.0 or later.	This is a known limitation. You must decrypt all files that were encrypted using prior versions of IBM Client Security Software before installing IBM Client Security Software 3.0 or later. IBM Client Security Software 3.0 cannot decrypt files that were encrypted using prior versions because of changes in its file encryption implementation.

6.15.14 UVM-aware device troubleshooting information

The troubleshooting information in Table 6-12 might be helpful if you experience problems when using UVM-aware devices.

Table 6-12 UVM-aware device troubleshooting

Problem Symptom	Possible Solution
A UVM-aware device stops working properly. When you disconnect a UVM-aware device from a Universal Serial Bus (USB) port, and then reconnect the device to the USB port, the device might not work properly.	Restart the computer after the device has been reconnected to the USB port.



Rescue and Recovery additional information

Values and settings of TVT.TXT

The TVT.TXT file is the main control file for Rescue and Recovery.

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

Table A-1 TVT.TXT settings and values

Setting	Values
EncryptBackupData	0 = do not encrypt backup 1 = encrypt backup (default)

Setting	Values
LocalBackup2Location	<p>x:\foldername (where x = drive letter \foldername = any fully qualified folder name. The default is this: <1st partition letter on the second drive>:\IBMBackupData.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Because the drive letter can change over time, IBM Rescue and Recovery will associate the drive letter to a partition at the time of install, and then use the partition information rather than the drive letter. 2. This is the location filed of TaskParameters entry.
NetworkUNCPath	<p>network share using the format \\<computername> \<share folder> (no default)</p> <p>Note: This location will not be protected by the File Filter Driver.</p>
MaxNumberOfBaseBackups	default 1, min=1, max=32
MaxNumberOfIncrementalBackups	default 5, min=2, max=32
CPU Priority	n where n=1 to 5; 1 is the lowest priority and 5 is highest priority. The default is 3.
Yield	<p>n where n=0 to 8; 0 means that IBM Rescue and Recovery does not yield and 8 means that IBM Rescue and Recovery produces the maximum yield value.</p> <p>Note: A higher yield will incrementally slow down backup performance and provide better interactive performance. The default is 0.</p>
HideGUI	<p>0 = show the GUI to authorized users</p> <p>1 = hide the GUI from all users</p>
DisableArchive	<p>0 = enable archive</p> <p>1 = hide archive</p> <p>The default is 0.</p>
DisableRestore	<p>0 = enable restore</p> <p>1 = hide restore</p> <p>The default is 0.</p>
DisablePreferences	<p>0 = enable set preferences</p> <p>1 = hide set preferences</p> <p>The default is 0</p>
DisableSFR	<p>0 = enable single file restore</p> <p>1 = single file restore</p> <p>The default is 0</p>

Setting	Values
MaxBackupSize	x, where x is the size in GB. This value will not prevent a backup from exceeding this threshold. If the threshold is exceeded, however, the user will be warned about the file size the next time an .On Demand. backup is taken.
RunBaseBackup	0 = don't perform the base backup 1 = perform base backup The default is 0.
GUIGroup (see AccessFile)	<group>, where <group> is a Windows local group (not a domain group) that is permitted to perform IBM Rescue and Recovery operations. The list of privileged groups is stored in a file that is defined by the AccessFile entry.
AccessFile (see GUIGroup)	<filename>, where <filename> is the fully qualified path to a file that holds the names of Windows local groups (not domain groups) that are permitted to perform IBM Rescue and Recovery operations. If blank or missing, all users who can log onto the computer can launch the GUI and perform command prompt operations. By default the file is blank.
ScheduleFrequency	0 = not scheduled 1 = daily 2 = weekly 3 = monthly The default is 2 (weekly).
ScheduleDayOfTheMonth	x, where x = 1 to 28 or 35 for monthly backups only. 35 = the last day of the month
ScheduleDayOfTheWeek	For weekly backups only 0 = Sunday 1 = Monday 2 = Tuesday 3 = Wednesday 4 = Thursday 5 = Friday 6 = Saturday The default is 0 (Sunday).
ScheduleHour	x, where x = 0 to 23 and 0 is 12:00 AM, 12 is noon, and 23 is 11:00 PM. The default is 0.
ScheduleMinute	x, where x = 0 to 59, which increments represent the minute within the hour to start the incremental backup. The default is 0.
ScheduleWakeForBackup	0 = do not wake the computer for scheduled backups 1 = wake the computer, if it is a desktop for scheduled backups, but do not wake notebook computers 2 = wake the computer regardless of whether it is a desktop or notebook The default is 2. Note: If a notebook wakes for a backup, but ac power is not detected, it will return to suspend/hibernate before a backup operation starts.
Pre (see PreParameters)	cmd, where cmd is a fully qualified path to an executable file to run prior to the primary task.

Setting	Values
PreParameters (see Pre)	parms, where parms are parameters to be used in the pre-task
PreShow	0 = hide pre-task 1 = show pre-task The default is 0.
Post (see PostParameters)	cmd, where cmd is a fully qualified path to an executable file to run after to the primary task.
PostParameters (see Post)	parms, where parms are parameters to be used in the post-task
PostShow	0 = hide post-task 1 = show post-task The default is 0.
Task	cmd (fully qualified path to the program to run as the primary task)
TaskParameter	parms (parameters to be used in the task)
TaskShow	x (0 - hide task, 1 - show task (default is 1))
PasswordRequired	0 = no password required to open the IBM Rescue and Recovery environment 1 - password required to open the IBM Rescue and Recovery environment
UUIDMatchRequired	0 = Computer UUID match is not required 1 = Computer UUID match is required Note: Backups that have been captured when the UUIDMatchRequired was set to 1 will continue to require a UUID match, even if this setting is changed later.
Exclude (see Include)	0 = do not apply GULexcl.d.txt 1 = apply GULexcl.d.txt Notes: 1. Exclude and select files can be defined prior to installation and be applied during the installation process. 2. Exclude and Include cannot both be 1
Include (see Exclude)	0 = do not apply GULincl.d.txt 1 = apply GULincl.d.txt and display the option to set include files & folders Notes: 1. Exclude and select files can be defined prior to installation and be applied during the installation process. 2. Exclude and Include cannot both be 1.

Setting	Values
HideAdminBackups	0 = Show administrator backups in list 1 = Hide administrator backups The default is 0.
HidePasswordProtect	0 = Show password protect check box 1 = Hide password protect check box The default is 0.
NetworkUNCPath	<server share name>, for example, \\myserver\share\folder
BackupPartition	0 = First partition on a specified drive 1 = Second partition on a specified drive 2 = Third partition on a specified drive 3 = Fourth partition on a specified drive. Drives are specified in the following sections: [BackupDisk] = local hard disk drive [SecondDisk] = second local hard disk drive [USBDrive] = USB hard disk drive Note: Partitions must already exist. If not set, the user will be prompted to establish the partition (if there is more than one partition on the destination drive when the destination drive is selected in the user interface).

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

- ▶ Encrypt backup dataBackup data targets
- ▶ Max Number of base backups: No base backups will be removed if this number is reduced below the current number of existing base backups.
- ▶ Max Number of incremental backups: MaxNumberOfIncrementalBackups=n (Note: This number should not be reduced to a value less than the current number of incremental backups)
- ▶ CPU Priority
- ▶ Disk I/O Priority
- ▶ Suppress GUI
- ▶ Suppress Archive GUI
- ▶ Suppress Restore GUI
- ▶ Suppress Set Preference GUI
- ▶ Suppress Single File Restore GUI
- ▶ Maximum disk space to be used for backups

- ▶ Prompt for creating backup prior to restore operation
- ▶ List of Windows local groups
- ▶ Incremental backup schedule
- ▶ Use Pre-desktop Password to protect the backup (applies to future backups)
- ▶ UUID of the computer must match to restore the backup
- ▶ Exclude
- ▶ Include
- ▶ HideAdminBackups
- ▶ HidePasswordProtect
- ▶ NetworkUNCPath
- ▶ BackupPartition

Scheduling backups and associated tasks

The scheduler is not designed to be specific to IBM Rescue and Recovery. However, the configuration is stored in the same TVT.txt file. When IBM Rescue and Recovery is installed, it will populate the scheduler with the appropriate settings. The configuration settings for the scheduler are shaded in the settings table. Here is a description of the structure for the scheduler:

- ▶ Location: Install folder
- ▶ Entry for each scheduled “job”:
 - Script to run
 - Named pipe to be used for progress notifications (optional)
 - Schedule information - monthly, weekly, daily, (weekday, weekend) - multiple schedules (e.g. Tuesdays and Fridays) can be supported by creating two schedules.
 - Variables to pass to functions

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

Example: A-1 Scheduler example

```
[SCHEDULER]
Task1=RapidRestoreUltra
[RapidRestoreUltra]
Task="c:\program files\ibm\rapid restore ultra\rrucmd.exebackup.bat"
TaskParameters=BACKUP location=L name="Scheduled"
ScheduleFrequency=2
```

```
ScheduleDayOfTheMonth=31
ScheduleDayOfTheWeek=2
ScheduleHour=20
ScheduleMinute=0
ScheduleWakeForBackup=0
Pre="c:\program files\antivirus\scan.exe"
Post="c:\program
files\logger\log.bat"
```

Making changes to TVT.txt via cfgmod command

The **cfgmod** command provides a method of updating the TVT.txt file via a script. If you modify the backup schedule, this command must be followed by **reloadsched**. This utility must be run with administrator privileges.

Syntax: `chgmod <tv.txt> <mod file>`

The format of the <mod file> requires one line per entry. Each entry includes a section number (delimited by [and]), followed by a parameter name, followed by equal sign, followed by the value.

For example, if you want to modify the TVT.txt so the GUI is only available for Administrators and a backup schedule is set weekly starting at 8 o'clock also waking the system if in suspend or hibernation mode, you could write the following modification file (named change.txt):

Example: A-2 change.txt file

```
[RapidRestoreUltra]HideGUI=0
[RapidRestoreUltra]GUIGroup=Administrators
[RapidRestoreUltra]ScheduleFrequency=2
[RapidRestoreUltra]ScheduleHour=8
[RapidRestoreUltra]ScheduleMinue=0
[RapidRestoreUltra]ScheduleWakeForBackup=2
```

The command, **reloadsched**, applies schedule changes made to the tv.txt file.

Example: A-3 cfgmod and reloadsched example

```
cd %RRU%
cfgmode tvt.txt change.txt
reloadsched
```

Note: In this example the modification file <mod file> is called change.txt and is also located in the c:\program files\IBM\IBM Rapid Restore Ultra directory. The system variable %RRU% directs you to the location of the directory where IBM Rapid Restore is installed and makes for easier script writing.

RRU command prompt interface RRUcmd

The primary Rescue and Recovery command prompt interface is RRUcmd. Refer to Table A-2 to use the command prompt interface for Rescue and Recovery.

Syntax: RRUcmd <command> <location=<x>>[Name=<abc> or level=<x>]

Table A-2 RRUcmd

Command	Result
backup	To initiate a normal backup operation (must include location & name parameters)
restore	To initiate a normal restore operation (must include location & level)
list	To list files that are included in the backup level (must include location & level)
basebackup	To initiate an alternative base backup (not to be used as a basis for incremental backups) (must include location, name, & level) (level must be > 99) (if another base backup with the same level already exists, it will be overwritten)
copy	Copy backups from one location to another (also known as archive) (must include location)
delete	Delete backups (must include location)
Location=<X> (one or more of the following can be selected)	Result
L	for primary local hard drive
U	for USB HDD
S	for secondary hard drive
N	network
name=<abc>	where abc is the name of the backup

Command	Result
level=<x>	where x is a number from 0 (for the base) to max number of incremental backups (only used with the restore option)

Other command prompt tools for IBM Rescue and Recovery

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

Rescue and Recovery—Boot Manager Control (BMGR32)

The boot manager interface command prompt interface is bmgr32. It resides in the directory c:\IBMTTOOLS\UTILS. Table A-3 describes Boot manager commands.

Table A-3 Boot manager commands

BGR32 switch	Result
/B0	Boot to partition 0 (based on the order in the partition table)
/B1	Boot to partition 1
/B2	Boot to partition 2
/B3	Boot to patition3
/BS	Boot to IBM Service Partition
/BW	Boot to Rescue and Recovery protected partition
/CFG<file>	Apply the configuration file parameters. (See the following section for details regarding the configuration file.)
/D<n>	apply changes to disk n, where n is 0-based (default: n=0)
/H0	Hide partition 0
/H1	Hide partition 1
/H2	Hide partition 2
/H3	Hide partition 3
/HS	Hide the IBM Service Partition
/P12	Hide the IBM Service Partition by setting partition type to 12

BGR32 switch	Result
/IBM	System is an IBM computer
/INFO	Display HDD information
/M0	Rescue and Recovery environment is located in the Service Partition
/M1	Rescue and Recovery environment is located in the C:\ partition (dual boot Windows and Windows PE)
/M2	Rescue and Recovery environment is located in the Service Partition with DOS (dual boot Windows PE and DOS; IBM Preload Only)
/OEM	Computer is not an IBM computer. This forces a second check for the F11 (default) key press after POST. This may be required for older IBM systems. This is also the default setting for the OEM version of Rescue and Recovery.
/Q	silent
/V	verbose
/R	Reboot computer
/U0	Unhide partition 0
/U1	Unhide partition 1
/U2	Unhide partition 2
/U3	Unhide partition 3
/US	Unhide IBM service partition
/F<mbr>	Load RRE master boot record program
/U	Unload RRE master boot record program
/>	List command prompt options

Boot Manager Control File

The format of the boot manager configuration file is backwardly compatible with the previous version of boot manager. Any switch not shown below is not supported. Each entry is on one line. The entries are listed in Table A-4 on page 601.

Table A-4 Boot manager control file

Entries	Notes
<PROMPT1=This is the text that will appear on F11 prompt>	PROMPT1 is limited to 78 bytes.
<KEY1=F11>	KEY1 can have the value F1 to F12, or a scan code (decimal form or can use hex if in the format 0xFF).
<WAIT=40>	The value of WAIT measured in units of 0.25 seconds.

FTR

Syntax: FTR [/h /b /u/v /sr]

Table A-5

Switch	Result
/sr	Launches to the Single File Restore view, to get individual files from backups.
/h	Displays list of command prompt options
/b	Launches and sets “backup” as the source
/u	Launches and sets “unbacked up files” as the source
/v	Turns on verbose debugging

IBMmigrate

The Rescue and Recovery migration program will migrate the primary hard drive to a second hard drive. The contents of the second hard drive will be deleted and the contents of the primary drive will be copied to the second hard drive. The partitions on the target hard drive will scale based on the comparison to the first hard drive. The command prompt interface is as follows:

Syntax: IBMmigrate [switches]

Table A-6 lists the switch.

Table A-6 Migrate switches

Switch	Result
silent	User prompts are suppressed.

mapdrv

The map network drive interface supports the switches listed in Table A-7.

Syntax: mapdrv [switches]

Table A-7 Migrate switches

Switch	Result
/rru	Reads and saves, UNC, encrypted UserID and encrypted Password in C:\IBMTTOOLS\Utils\mnd\mapdrv.ini file, prompts user if connection cannot be made (unless /s is also specified)
/nodrive	Make network connection without assigning driver letter to the connection
/s	silent. Do not prompt the user regardless of whether connection is made - only effective if used in conjunction with /rru Return codes: 0 = success, > 0 = failed

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

You must uninstall all previous IBM Rapid Restore applications. If an older version of Rapid Restore is detected during the Install, you will be prompted to uninstall the older application. To uninstall earlier versions of Rapid Restore do the following:

1. Click the Windows **Start** button. Then select **Settings** → **Control Panel**.
2. Double-click **Add/Remove Programs**.
3. Select **IBM Rapid Restore PC** or **IBM Rapid Restore Ultra**, and then click **Change/Remove**.
4. Follow the on-screen instructions to complete the software removal. If IBM Rapid Restore Ultra is not in this list of programs, continue to step 5.
5. In the **Add/Remove Programs** applet, select **Access IBM Tools**. This will open an Access IBM uninstall program that lists multiple IBM applications. If IBM is not in this list of programs, continue to step 6.
6. Run the following command from a command prompt:

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

Including and excluding files in backups

IBM Rescue and Recovery has extensive include and exclude capabilities. It can include and exclude an individual file or folder or an entire partition. The files that control the include and exclude functions, listed in order of precedence are as follows:

- ▶ `ibmexcl`
- ▶ `guiexcl`
- ▶ `ibmincl`

Note: `ibmincl` always supersedes `ibmexcl` and `guiexcl`.

All are located in the directory `c:\Program Files\IBM\IBM Rapid Restore Ultra`.

By design, IBM Rescue and Recovery takes a conservative approach to the files that it must include in the backup process. The primary goal of the default backup process is to ensure that in the event you must restore your system from the RRU backup, Windows will start. To do this, we identify the several files, file types, and paths that must be backed up no matter what the end user selects in the user interface. These components are identified in the file **`ibmincl`**. This file can be viewed with any text editing program. The Administrator can modify the contents of this file as part of the customization process.

The default files and folders listed in `ibmincl` are as follows:

`*.ocx,*.dll,*.exe,*.ini v *.drv,*.com,*.sys,*.cpl,*.icm,*.lnk,*.hlp,*.cat,*.xml,*.jre
.cab,.sdb,*.bat,*\ntldr,*\peldr,*\bootlog.prv,*\bootlog.txt,*\bootsect.dos,
*winnt,*windows,*minint,*preboot,*application data,*documents and settings,
*ibmtools,*program files,*msapps`

To further protect the user and computer, we have prevented the user from excluding certain files in the Rescue and Recovery user interface.

Files that are prevented from being excluded from a backup are listed in the file `c:\Program Files\IBM\IBM Rapid Restore Ultra\excldmk.txt`. The default entries in this file match the values in the file `ibmincl`. Similar to `ibmincl`, the contents of this file may be modified by an Administrator.

It is important to note that after a folder has been placed into an include list, all files and sub-folders in that folder will automatically be included regardless of the setting in an exclude file (`ibmexcl` or `guiexcl`). The user, by default, can select individual files and folders to be excluded from the backup. These files and folders are stored in the file `guiexcl`. If an administrator wants to ensure that a particular file or folder is always backed up, he or she can include the file names or types the `ibmincl` file.

Any entry in this file will always be included in a backup regardless of an entry in the other lists. Administrators also have the ability to always exclude a file, folder, or partition from a backup.

The following files and folder are always excluded from any backup:

- ▶ pagefile.sys
- ▶ hiberfile.sys
- ▶ c:\System Volume Information

When restored, both pagefile.sys and hiberfile.sys will be regenerated automatically by Windows. In addition, the Windows System Restore data will be regenerated with a new restore point by Windows after a backup has been restored. The format for each of these files (ibmincld, ibmexcl, and guiexcl) is standard DOS style for commands and wildcards.

▶ Example with Lotus Notes and IBM Client Security Software

Assuming your enterprise is using Lotus Notes® for your mail client and IBM Client Security Software with FFE to protect critical files that reside locally on your systems. Because many Notes deployments leverage a local replica of a server based mail file, it would be appropriate to exclude *.NSF files from the backups. If the computer did need to be restored from the backups, the local copy of the NSF file (often quite large and backed up elsewhere) could be replicated after the system restore.

To facilitate this exclusion, the administrator would simply add the entry *.nsf to ibmexcl. The entry in ibmexcl would look like this: *.nsf You must use great caution in excluding every file with a given extension. If you blindly exclude all *.NSF files, for example, you will not backup several files that are critical for Lotus® Notes to function correctly.

One key file that would not be backed up is NAMES.NSF. Because NAMES.NSF is the core control file for Notes as well as the personal address book, it would be very important to ensure it is backed up. To do this, place the entry *names.nsf in the file ibmincl.

By combining inclusion and exclusion, you can backup reliably critical files and exclude files that can be obtained from other sources. Consider adding JOURNAL.NSF to the inclusion list and any database files that are strictly local.

In this example, you will also notice that we include IBM Client Security Software with FFE. The database that FFE uses to keep track of what folders are protected by FFE also has an .NSF extension.

To ensure that these files are always backed up, include the entry c:\Program Files\IBM\Security*flt.nsf in the ibmincl file. If this database file is not backed up and an IBM Rescue and Recovery backup is restored, the *flt.nsf files will not be restored (because *.nsf is listed in the libmexcl list).

After the restore, you will be unable access your File and Folder Encryption-protected files and folders.

The entries in the ibmincl file for this example would appear as:

- *names.nsf
- *journal.nsf
- c:\Program Files\IBM\Security*flt.nsf



B

Alternate SQL database for System Information Center

IBM System Information Center ships with the Java-based Cloudscape database. A default installation of the product will install, configure, and use Cloudscape as the asset repository. However, System Information Center uses standard SQL calls to store and retrieve asset information in the repository database. Therefore, a System Information Center installation can be modified to work with databases that support standard SQL calls.

In this appendix, we document a procedure that can be used to reconfigure a default System Information Center installation that is using IBM Cloudscape database to use IBM DB2 or Microsoft SQL 2000 database. These procedures are based on the following conditions:

1. A default installation of System Information Center for all path locations.
2. Tomcat 4.1.30
3. A local Windows user account with administrator rights named `admin`.

How to use IBM DB2 with System Information Center

The version of IBM DB2 we tested was V8.2. The System Information Center version we used was prerelease version 1.0.0.

The following procedure describes how to install and use these versions:

1. Install System Information Center and Tomcat 4 as described in 3.2, “System Information Center server installation” on page 96.
2. Install IBM DB2 version 8.1.4 as follows:
 - a. Use all default settings for the installation and make sure that Java Database Connectivity (JDBC) support is also installed.
 - b. Install Web update 8.1.7 for DB2. This will change the version of DB2 from 8.1.4 to 8.2.
3. Set the DB2 services to automatic and to run as local accounts (admin in our testing) as shown in Figure B-1.

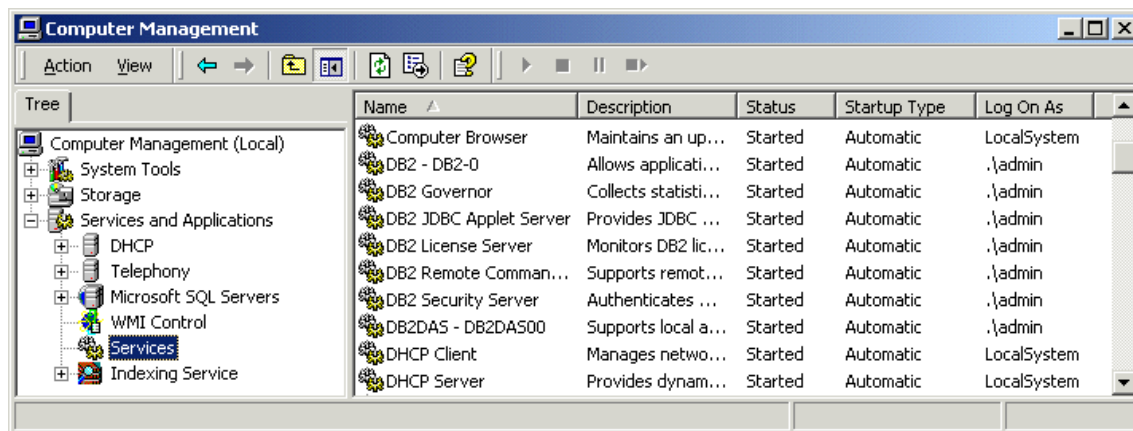
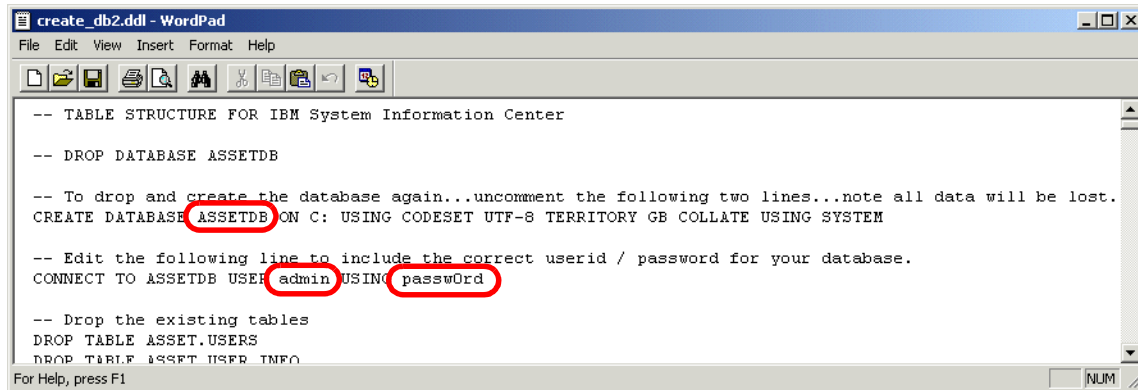


Figure B-1 DB2 services

4. Copy db2java.zip (located in C:\Program Files\IBM\SQLLIB\java\ by default) into C:\ISIC\tomcat\jakarta-tomcat-4.1.30\common\lib\.
5. Rename db2java.zip to db2java.jar.
6. Stop and restart Windows.
7. Stop the System Information Center Tomcat4 service.
8. Open the C:\ISIC\web\database\db2\create_db2.ddl file (see Figure B-2 on page 609.) This file is used to create the DB2 database used by System Information Center.



```
-- TABLE STRUCTURE FOR IBM System Information Center

-- DROP DATABASE ASSETDB

-- To drop and create the database again...uncomment the following two lines...note all data will be lost.
CREATE DATABASE ASSETDB ON C: USING CODESET UTF-8 TERRITORY GB COLLATE USING SYSTEM

-- Edit the following line to include the correct userid / password for your database.
CONNECT TO ASSETDB USER admin USING passw0rd

-- Drop the existing tables
DROP TABLE ASSET.USERS
DROP TABLE ASSET.USER_INFO

For Help, press F1
```

Figure B-2 create_db2.ddl file

Figure B-2 illustrates the contents of this file, which has the following parameters:

- The name that appears after CREATE DATABASE is the name of the System Information Center DB2 database. In the example shown, it is called ASSETDB. The name is not important as long as it is unique within the system.
- The database administrator user ID is admin. Ensure this name is a valid DB2 user ID. It will be used later to configure the System Information Center connectivity to the database.
- The database administrator password for our example is passw0rd. It will be used later to configure the System Information Center connectivity to the database.

9. Modify the three parameters as desired and then save the file.

10. Open the C:\ISIC\web\database\db2\populate_db2.ddl file (see Figure B-3 on page 610). This file is used to initialize the databases created using the create_db2.ddl file.

```

CONNECT TO ASSETDB USER admin USING passwd

-- Uncomment the following line if you are creating a new instance and require a default admin userid.
INSERT INTO ASSET.USERS (USERKEY,USERID,EMAIL,FORENAME,SURNAME,AUTHORITY,PASSWORD,EXPIRED) VALUES
(1,'ADMIN','admin@isic.com','Default','Administrator','A','password','Y')

INSERT INTO ASSET.TABLE_INFO VALUES('ASSET','USERS','PASSWORD','','','A','N')

INSERT INTO ASSET.QUERY (QUERYKEY,NAME,DESCRIPTION,SQL_DATA,AUTHORITY,DISPLAY,CREATOR,FSIZE) VALUES
(0,'All Reports','List all reports which the user has the correct authority to run','Select DISTINCT
A.QUERYKEY,B.GROUP_NAME,A.NAME,A.DESCRPTION,A.DISPLAY,A.CREATOR,A.CREATED FROM $#SCHEMA.QUERY A,
$#SCHEMA.QUERY B WHERE A.QUERYKEY = B.QUERYKEY AND A.AUTHORITY IN ($#AUTHLIST) ORDER BY

```

Figure B-3 populate_db2.ddl file

Figure B-3 is an example of the populate_db2.ddl file. The parameters of interest are:

- The name that comes after CONNECT TO is the name of the DB2 database created in the previous step. In our example, it is called ASSETDB.
- The database administrator user name for this example is admin.
- The database administrator password for this example is passwd.

11. Modify these three parameters as desired and then save the file.

12. Open a DB2 command interface window by selecting

Start → Programs → IBM DB2 → Command Line Tools → Command Window

13. Change directories to the directory containing the DB2 create command (C:\ISIC\web\database\db2\) and execute the following command in the DB2 command window (see Figure B-4):

```
db2 -f create_db2.ddl
```

```

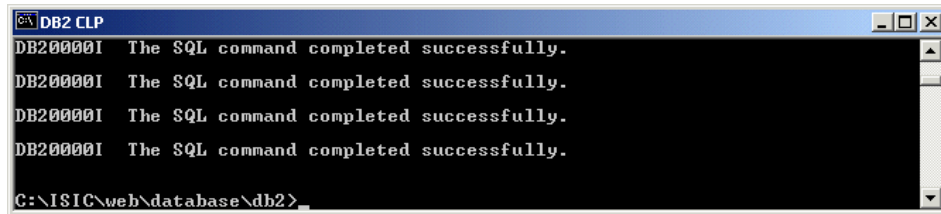
C:\Program Files\IBM\SQLLIB\BIN>cd c:\ISIC\web\database\db2
C:\ISIC\web\database\db2>db2 -f create_db2.ddl
DB20000I The CREATE DATABASE command completed successfully.

Database Connection Information
Database server      = DB2/NT 8.2.0
SQL authorization ID = ADMIN
Local database alias = ASSETDB

DB21034E The command was processed as an SQL statement because it was not a
valid Command Line Processor command. During SQL processing it returned:

```

Figure B-4 System Information Center DB2 database create

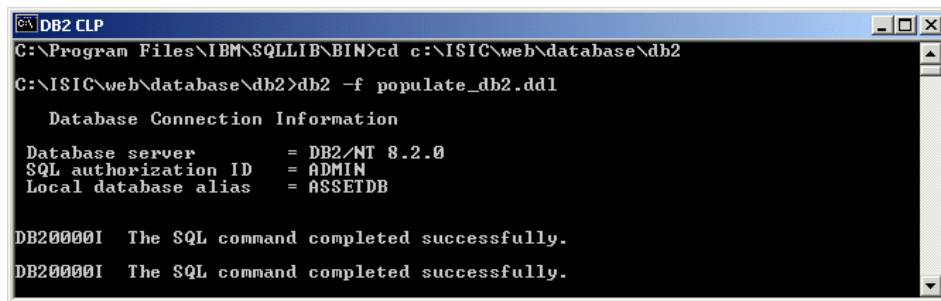


```
C:\ DB2 CLP
DB20000I The SQL command completed successfully.
DB20000I The SQL command completed successfully.
DB20000I The SQL command completed successfully.
DB20000I The SQL command completed successfully.
C:\ISIC\web\database\db2>_
```

Figure B-5 System Information Center DB2 database create results

14. When the database creation is complete, as shown in Figure B-5, make sure you are still in the C:\ISIC\web\database\db2\ directory, and execute the following command in the DB2 command window (see Figure B-6):

```
db2 -f populate_db2.ddl
```



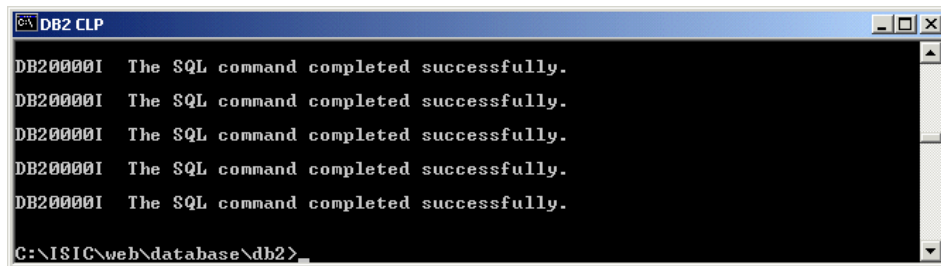
```
C:\Program Files\IBM\SQLLIB\BIN>cd c:\ISIC\web\database\db2
C:\ISIC\web\database\db2>db2 -f populate_db2.ddl

Database Connection Information

Database server      = DB2/NT 8.2.0
SQL authorization ID = ADMIN
Local database alias = ASSETDB

DB20000I The SQL command completed successfully.
DB20000I The SQL command completed successfully.
```

Figure B-6 System Information Center DB2 database populate



```
C:\ DB2 CLP
DB20000I The SQL command completed successfully.
DB20000I The SQL command completed successfully.
DB20000I The SQL command completed successfully.
DB20000I The SQL command completed successfully.
DB20000I The SQL command completed successfully.
C:\ISIC\web\database\db2>_
```

Figure B-7 System Information Center DB2 database populate results

15. When the database population process is complete, as shown in Figure B-7, close the DB2 command window and restart Windows.
16. When Windows is running again, stop the System Information Center Tomcat 4 service.

Attention: When you are editing XML files in the following steps, note that command statements beginning with `<!--` and ending with `-->` are comments used to clarify the meaning of the section of code that follows. These comments are not executed and may be edited or removed as desired.

17. Edit both of the following files using WordPad:

`c:\ISIC\tomcat\jakarta-tomcat-4.1.30\webapps\isic.xml`

and

`c:\ISIC\isic.xml`

Replace the text in both files with the text shown in Example B-1.

Example: B-1 isic.xml file

```
<Context
  path="/isic"
  docBase="C:/ISIC/web"
  debug="0" privileged="true">

  <ResourceLink
    global="jdbc/assetdb"
    name="jdbc/assetdb"
    type="javax.sql.DataSource"/>
</Context>
```

Restriction: Text editors like Notepad do not support the editing of XML files. Saving XML files edited with Notepad can corrupt these files. Use WordPad or a similar editor that correctly handles XML files.

18. Save the changes made to `isic.xml` and close the files. Ignore any warnings similar to the one shown in Figure B-8.

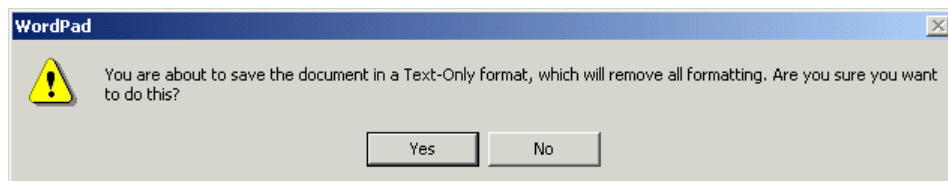


Figure B-8 WordPad warning

Important: Do not leave copies of the original .xml files in the original locations. Tomcat will read and utilize all .xml files located in the Tomcat structure.

19. Edit the \ISIC\web\database\db2\tomcat4.1\server.xml.db2 file using WordPad and copy the highlighted lines shown in Example B-2.

Example: B-2 Server.xml.db2

```
.  
.  
</parameter>  
  </ResourceParams>  
  
  <Resource auth="Container" description="Database connection pool"  
name="jdbc/assetdb" type="javax.sql.DataSource"/>  
  <ResourceParams name="jdbc/assetdb">  
    <parameter>  
      <name>factory</name>  
      <value>org.apache.commons.dbcp.BasicDataSourceFactory</value>  
    </parameter>  
    <parameter>  
      <name>maxWait</name>  
      <value>5000</value>  
    </parameter>  
    <parameter>  
      <name>maxActive</name>  
      <value>100</value>  
    </parameter>  
    <parameter>  
      <name>maxIdle</name>  
      <value>20</value>  
    </parameter>  
    <parameter>  
      <name>removeAbandoned</name>  
      <value>true</value>  
    </parameter>  
    <parameter>  
      <name>removeAbandonedTimeout</name>  
      <value>60</value>  
    </parameter>  
    <parameter>  
      <name>url</name>  
      <value>jdbc:db2:ASSETDB</value>  
    </parameter>  
    <parameter>  
      <name>driverClassName</name>
```

```

        <value>COM.ibm.db2.jdbc.app.DB2Driver</value>
    </parameter>
    <parameter>
        <name>username</name>
        <value>db2admin</value>
    </parameter>
    <parameter>
        <name>password</name>
        <value>db2admin</value>
    </parameter>
</ResourceParams>

<!-- Test entry for demonstration purposes -->
<Environment name="simpleValue" type="java.lang.Integer" value="30"/>
.
.

```

20. In the \SIC\tomcat\jakarta-tomcat-4.1.30\conf\server.xml file, replace the lines highlighted in Example B-3 by pasting the lines you copied from the server.xml.db2 file.

Example: B-3 Paste and replace the highlighted lines in server.xml

```

.
.
<!-- Global JNDI resources -->
<GlobalNamingResources>
    <Resource auth="Container"
        description="Database connection pool"
        name="jdbc/assetdb"
        type="javax.sql.DataSource">
    </Resource>
    <ResourceParams name="jdbc/assetdb">
        <parameter>
            <name>factory</name>
            <value>org.apache.commons.dbcp.BasicDataSourceFactory</value>
        </parameter>
        <parameter>
            <name>maxWait</name>
            <value>5000</value>
        </parameter>
        <parameter>
            <name>maxActive</name>
            <value>100</value>
        </parameter>
        <parameter>
            <name>maxIdle</name>
            <value>20</value>
        </parameter>
    </ResourceParams>

```



```

    <parameter>
      <name>removeAbandoned</name>
      <value>true</value>
    </parameter>
    <parameter>
      <name>removeAbandonedTimeout</name>
      <value>60</value>
    </parameter>
    <parameter>
      <name>url</name>
      <value>jdbc:db2j:C:/ISIC/db/assetdb</value>
    </parameter>
    <parameter>
      <name>driverClassName</name>
      <!-- <value>com.ibm.db2.jdbc.app.DB2Driver</value> -->
      <value>com.ibm.db2j.jdbc.DB2jDriver</value>
    </parameter>
  </ResourceParams>

  <!-- Test entry for demonstration purposes -->
  <Environment name="simpleValue" type="java.lang.Integer" value="30"/>
  .
  .

```

21. After pasting the replacement lines into server.xml, make the following changes to the file (refer to Example B-4):
- Change the DB administrator user name (db2admin in Example B-4) to your DB administrator user ID (admin in our example).
 - Change the DB administrator password (db2admin in Example B-4) to the correct password (passw0rd in our example).
 - Save the server.xml file.

Example: B-4 Changes to server.xml

```

.
.
    <parameter>
      <name>username</name>
      <value>db2admin</value>
    </parameter>
    <parameter>
      <name>password</name>
      <value>db2admin</value>
    </parameter>
  .
  .

```

22. Add the highlighted text shown in Example B-5 into the c:\isic\tomcat\jakarta-tomcat-4.1.30\conf\web.xml file (near the bottom of the file). This text must be inserted after the `</welcome-file-list>` command and before the `</web-app>` command.

Example: B-5 Add the highlighted lines to web.xml

```
</welcome-file-list>
<resource-ref>
  <description>Resource reference to a factory for java.sql.Connection
instances that may be used for talking to a particular database that is
configured in the server.xml file.</description>
  <res-ref-name>jdbc/assetdb</res-ref-name>
  <res-type>javax.sql.DataSource</res-type>
  <res-auth>Container</res-auth>
</resource-ref>
</web-app>
```

23. Delete the c:\isic.log file.

24. Restart Windows.

Testing System Information Center with DB2

To test System Information Center to ensure that it is using the DB2 database, perform the following steps:

1. Open Internet Explorer and go to:

http://localhost/isic

This opens a window similar to the one shown in Figure B-9 on page 617.

Attention: The System Information Center administration Web interface is fully supported only with Microsoft Internet Explorer 6.0.

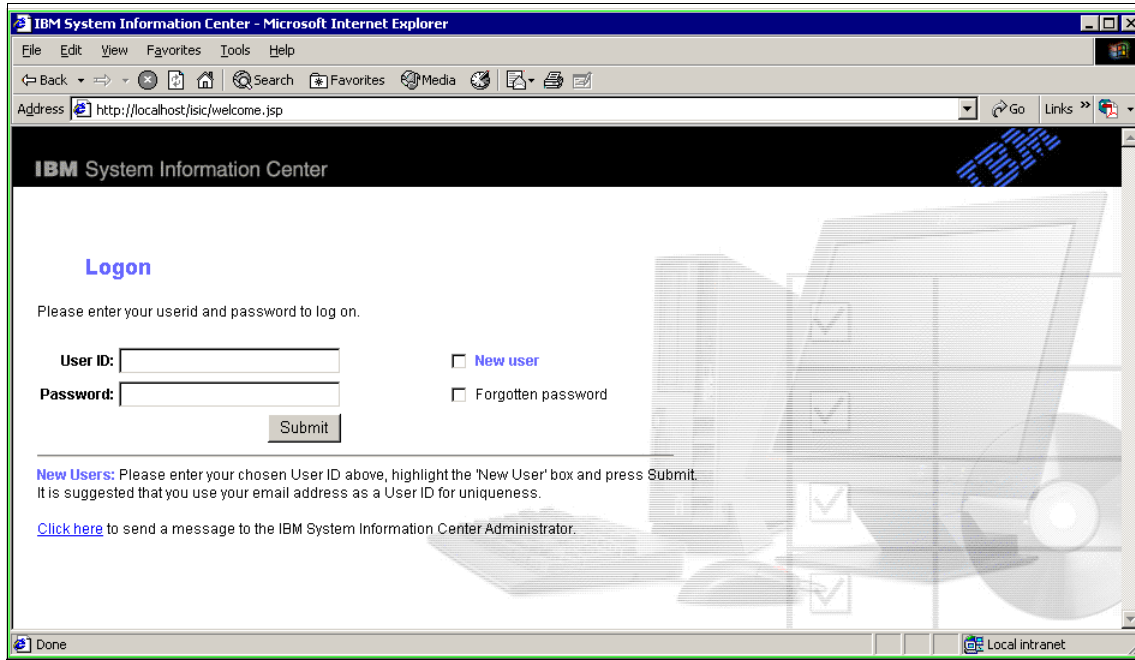


Figure B-9 System Information Center Home page

2. Log on to System Information Center.
3. Add an asset.
4. Log out of System Information Center.
5. Open c:\isis.log file using a text editor.
6. Look for the following entry:
Got Database MetaData for DB DB2/NT....
7. System Information Center is now using the DB2 SQL database.

Tip: If you experience database connectivity issues with DB2, check the following:

```
CLASSPATH=.;C:\Program Files\IBM\SQLLIB\java\db2java.zip;C:\Program
Files\IBM\SQLLIB\java\db2jcc.jar;C:\Program
Files\IBM\SQLLIB\java\sqlj.zip;C:\Program Files\IBM\SQLLIB\bin;C:\Program
Files\IBM\SQLLIB\java\common.jar
```

Remove Cloudscape database

After you have verified that System Information Center is correctly using DB2, you can use the Delete `c:\isic\db\command` to remove the Cloudscape database if desired.

Using SQL Server 2000 with System Information Center

To use SQL Server 2000 with System Information Center, perform the following actions:

1. Install System Information Center and Tomcat 4 as described in 3.2, "System Information Center server installation" on page 96.
2. Install Microsoft SQL 2000 Server as follows:
 - a. Select **mixed mode** as the authentication mode.
 - b. Set the SA account password. This will be used by System Information Center. In our example, we entered `asset` as the password.
 - c. Use the defaults for all other settings.
3. Install Service Pack 3 (SP3) for Microsoft SQL 2000 Server. Use the SA account and password.
4. Install Service Pack 3 (SP3) for Microsoft SQL 2000 Server JDBC.
5. Copy the following files (located in `C:\Program Files\Microsoft SQL Server 2000 Driver for JDBC\lib\` by default) into the `C:\ISIC\tomcat\jakarta-tomcat-4.1.30\common\lib\` file.
 - `msbase.jar`
 - `mssqlserver.jar`
 - `msutil.jar`
6. Stop and restart Windows.
7. Stop the System Information Center Tomcat4 service.
8. Open the `C:\ISIC\web\database\ms2k\readme.txt` file. This file has a series of Microsoft SQL commands used to create and populate the SQL databases required for IBM System Information Center as shown in Example B-6.

Example: B-6 readme.txt file containing SQL commands

Instructions

1 - Install Microsoft Server 2000. When choosing an authentication mode, 'select mixed mode' and enter 'asset' as the password.

2 - Install the JDBC driver service pack 3. Add the 3 jar files in the lib folder to the tomcat common/lib

3 - open a command prompt and enter the following commands:

```
osql -U sa -P asset -Q"CREATE DATABASE ASSETDB"<return>
osql -U sa -P asset -Q"sp_addlogin 'asset','asset','assetdb' "<return>
osql -U sa -P asset -Q"sp_addsrvrolemember 'asset','sysadmin' "<return>
osql -U sa -P asset -d assetdb -Q"sp_grantdbaccess 'asset' "<return>
osql -U asset -P asset -d assetdb -i C:\ISIC\database\ms2k\create_ms2k.ddl<return>
osql -U asset -P asset -d assetdb -i C:\ISIC\database\ms2k\populate_ms2k.ddl<return>
```

9. Open a command prompt. In the command window, complete the following steps:
 - a. `cd \`
 - b. Copy the first command from the readme.txt file shown in Example B-6 on page 618 into the command window. Do not copy the `<return>` command. See Figure B-10.

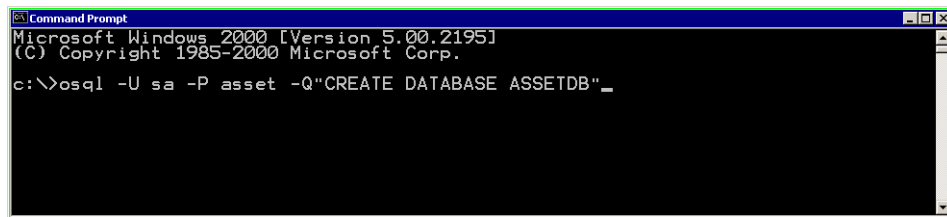


Figure B-10 SQL command copied from readme.txt

- c. Change the administrator user name and password to match the SA account and password set during Microsoft SQL 2000 installation.
 - d. Execute the command.
 - e. Repeat these steps for each command in the readme.txt file. When you execute the last two commands, make sure you modify the command to point to the location of the create_ms2k.ddl and populate_ms2k.ddl files.
10. After completing all the commands, close the command window and restart Windows.
11. When Windows is running again, stop the System Information Center Tomcat 4 service.

Attention: When you are editing the XML files in the following steps, note that command statements beginning with `<!--` and ending with `-->` are comments used to clarify the meaning of the section of code that follows. These comments are not executed and may be edited or removed as desired.

12. Edit the `C:\ISIC\tomcat\jakarta-tomcat-4.1.30\webapps\isic.xml` file using WordPad. Delete the text in the file starting from `<Resource` `auth="Container"` and ending with `</ResourceParams>` as shown in Example B-7.

Example: B-7 isic.xml file

```
<Context
  path="/isic"
<!-- ## AUTOEDIT1 ## -->
  docBase="C:/ISIC"
  debug="0"
  privileged="true">
  <Logger className="org.apache.catalina.logger.FileLogger"
prefix="lynx_log." suffix=".txt" level="1" timestamp="true" />
  <Resource auth="Container"
    description="Database connection pool"
    name="jdbc/assetdb"
    type="javax.sql.DataSource" />
  <ResourceParams name="jdbc/assetdb">
    <parameter>
      <name>factory</name>
      <value>org.apache.commons.dbcp.BasicDataSourceFactory</value>
    </parameter>
    <parameter>
      <name>maxWait</name>
      <value>5000</value>
    </parameter>
    <parameter>
      <name>maxActive</name>
      <value>100</value>
    </parameter>
    <parameter>
      <name>maxIdle</name>
      <value>20</value>
    </parameter>
    <parameter>
      <name>removeAbandoned</name>
      <value>true</value>
    </parameter>
    <parameter>
      <name>removeAbandonedTimeout</name>
```

```

        <value>60</value>
    </parameter>
    <parameter>
        <name>url</name>
    <!-- ## AUTOEDIT2 ## -->
        <value>jdbc:db2j:C:/ISIC/db/assetdb</value>
    </parameter>
    <parameter>
        <name>driverClassName</name>
        <!-- <value>com.ibm.db2.jdbc.app.DB2Driver</value> -->
        <value>com.ibm.db2j.jdbc.DB2jDriver</value>
    </parameter>
</ResourceParams>
</Context>

```

Restriction: Text editors like Notepad do not support the editing of XML files. Saving XML files edited with Notepad can corrupt these files. Use WordPad or any other editor that fully supports XML edits.

13. Save the changes made to isic.xml and close the file. Ignore any warnings similar to the one shown in Figure B-11.

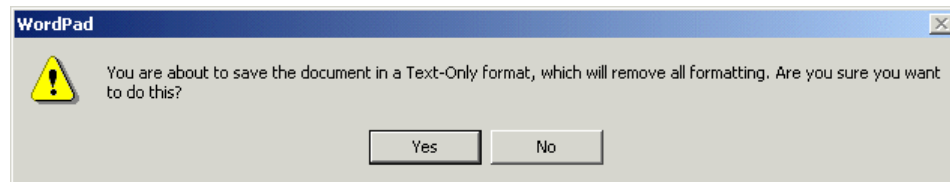


Figure B-11 WordPad warning

Important: Do not leave copies of the original .xml files in the original locations. Tomcat will read and utilize all .xml files located in the Tomcat structure.

14. Edit the C:\ISIC\web\database\ms2k\tomcat4.1\server.xml.ms2k file using WordPad by copying the section that begins with <!-- Global JNDI resources --> and ends with </GlobalNamingResources> as shown in Example B-8.

Example: B-8 server.xml.ms2k

.

.

```

<Listener
className="org.apache.catalina.mbeans.GlobalResourcesLifecycleListener"
debug="0"/>

<!-- Global JNDI resources -->
<GlobalNamingResources>

    <!-- Test entry for demonstration purposes -->
    <Environment name="simpleValue" type="java.lang.Integer" value="30"/>

    <!-- Editable user database that can also be used by
         UserDatabaseRealm to authenticate users -->
    <Resource name="UserDatabase" auth="Container"
              type="org.apache.catalina.UserDatabase"
              description="User database that can be updated and saved">
    </Resource>
    <ResourceParams name="UserDatabase">
        <parameter>
            <name>factory</name>
            <value>org.apache.catalina.users.MemoryUserDatabaseFactory</value>
        </parameter>
        <parameter>
            <name>pathname</name>
            <value>conf/tomcat-users.xml</value>
        </parameter>
    </ResourceParams>

    <Resource auth="Container" description="Database connection pool"
name="jdbc/assetdb" type="javax.sql.DataSource"/>
    <ResourceParams name="jdbc/assetdb">
        <parameter>
            <name>factory</name>
            <value>org.apache.commons.dbcp.BasicDataSourceFactory</value>
        </parameter>
        <parameter>
            <name>maxWait</name>
            <value>5000</value>
        </parameter>
        <parameter>
            <name>maxActive</name>
            <value>100</value>
        </parameter>
        <parameter>
            <name>maxIdle</name>
            <value>20</value>
        </parameter>
        <parameter>
            <name>removeAbandoned</name>
            <value>true</value>

```



```

        </parameter>
        <parameter>
            <name>removeAbandonedTimeout</name>
            <value>60</value>
        </parameter>
        <parameter>
            <name>url</name>

<value>jdbc:microsoft:sqlserver://localhost;DatabaseName=ASSETDB;</value>
        </parameter>
        <parameter>
            <name>driverClassName</name>
            <value>com.microsoft.jdbc.sqlserver.SQLServerDriver</value>
        </parameter>
        <parameter>
            <name>username</name>
            <value>asset</value>
        </parameter>
        <parameter>
            <name>password</name>
            <value>asset</value>
        </parameter>
    </ResourceParams>

    <!-- Test entry for demonstration purposes -->
    <Environment name="simpleValue" type="java.lang.Integer" value="30"/>

    <!-- Editable user database that can also be used by
    UserDatabaseRealm to authenticate users -->
    <Resource auth="Container" description="User database that can be
    updated and saved" name="UserDatabase"
    type="org.apache.catalina.UserDatabase"/>
    <ResourceParams name="UserDatabase">
        <parameter>
            <name>factory</name>
            <value>org.apache.catalina.users.MemoryUserDatabaseFactory</value>
        </parameter>
        <parameter>
            <name>pathname</name>
            <value>conf/tomcat-users.xml</value>
        </parameter>
    </ResourceParams>

</GlobalNamingResources>

<!-- A "Service" is a collection of one or more "Connectors" that share
a single "Container" (and therefore the web applications visible
.
```

- .
-
15. Edit the C:\ISIC\tomcat\jakarta-tomcat-4.1.30\conf\server.xml file by replacing the lines highlighted in Example B-9 with the lines copied from the server.xml file in the previous step.

Example: B-9 Paste and replace the highlighted lines in server.xml

.

.

```
<Listener
className="org.apache.catalina.mbeans.GlobalResourcesLifecycleListener"
debug="0"/>

<!-- Global JNDI resources -->
<GlobalNamingResources>
  <Resource auth="Container"
    description="Database connection pool"
    name="jdbc/assetdb"
    type="javax.sql.DataSource">
  </Resource>
  <ResourceParams name="jdbc/assetdb">
    <parameter>
      <name>factory</name>
      <value>org.apache.commons.dbcp.BasicDataSourceFactory</value>
    </parameter>
    <parameter>
      <name>maxWait</name>
      <value>5000</value>
    </parameter>
    <parameter>
      <name>maxActive</name>
      <value>100</value>
    </parameter>
    <parameter>
      <name>maxIdle</name>
      <value>20</value>
    </parameter>
    <parameter>
      <name>removeAbandoned</name>
      <value>true</value>
    </parameter>
    <parameter>
      <name>removeAbandonedTimeout</name>
      <value>60</value>
    </parameter>
    <parameter>
      <name>url</name>
      <value>jdbc:db2j:C:/ISIC/db/assetdb</value>
```

```

    </parameter>
    <parameter>
      <name>driverClassName</name>
      <!-- <value>com.ibm.db2.jdbc.app.DB2Driver</value> -->
      <value>com.ibm.db2j.jdbc.DB2jDriver</value>
    </parameter>
  </ResourceParams>

  <!-- Test entry for demonstration purposes -->
  <Environment name="simpleValue" type="java.lang.Integer" value="30"/>

  <!-- Editable user database that can also be used by
    UserDatabaseRealm to authenticate users -->
  <Resource name="UserDatabase" auth="Container"
    type="org.apache.catalina.UserDatabase"
    description="User database that can be updated and saved">
  </Resource>
  <ResourceParams name="UserDatabase">
    <parameter>
      <name>factory</name>
      <value>org.apache.catalina.users.MemoryUserDatabaseFactory</value>
    </parameter>
    <parameter>
      <name>pathname</name>
      <value>conf/tomcat-users.xml</value>
    </parameter>
  </ResourceParams>

</GlobalNamingResources>

<!-- A "Service" is a collection of one or more "Connectors" that share
  a single "Container" (and therefore the web applications visible
  .
  .

```

16. Delete the c:\isic.log file.

17. Restart Windows.

Test ISIC with Microsoft SQL 2000

To test System Information Center to ensure that it is using the Microsoft SQL 2000 database, perform the following steps:

1. Open Internet Explorer and go to <http://localhost/ISIC>. This opens a window similar to the one shown in Figure B-9 on page 617.

Attention: The System Information Center administration Web interface is fully supported only with Microsoft Internet Explorer 6.0.

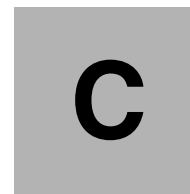
2. Log on to System Information Center.
3. Add an asset.
4. Log out of System Information Center.
5. Open c:\isic.log in a text editor.
6. Look for this entry:

Got Database MetaData for DB Microsoft SQL Server version = Microsoft SQL Server 2000

7. Close the log file.
8. System Information Center is now using Microsoft SQL 2000 database.

Remove Cloudscape database

After you verify that ISIC is correctly using Microsoft SQL 2000 for its database, you can use the **Delete c:\isic\db**command to remove the Cloudscape database if desired.



Software Delivery Center and System Information Center coexistence

This appendix describes the installation and customization steps required to install Software Delivery Center and System Information Center on a single server machine running Microsoft Windows 2000 Server or Microsoft Windows 2003.

Be aware that running Software Delivery Center and System Information Center on the same server is not a supported environment. However, it can be useful when setting up a test or staging environment or for demonstration purposes.

This procedure assumes the following:

1. Windows 2000 Server
2. Default installations of System Information Center and Software Delivery Center for all path locations
3. Tomcat 4.1.30
4. A local Windows user account with administrator rights named *admin*

Installing both programs on the same machine

To install System Information Center and Software Delivery Center on the same machine, perform the following steps:

1. Install the IBM Software Delivery Center program as described in 4.3.2, “Installing Software Delivery Center” on page 233.

Note: After downloading Apache Tomcat, make a backup copy of the of the jakarta-tomcat-4.1.30.zip file because the install program deletes it and it is required for the installation of System Information Center.

2. Install System Information Center as described in 3.2.3, “System Information Center installation” on page 97. Select the Quick installation type. Do not restart the machine after the installation.
3. Open the Windows Services Dialog by selecting **Start → Programs → Administrative Tools → Services**.
4. Locate the Apache Tomcat service as shown in Figure C-1 and stop it. Keep the services dialog open.

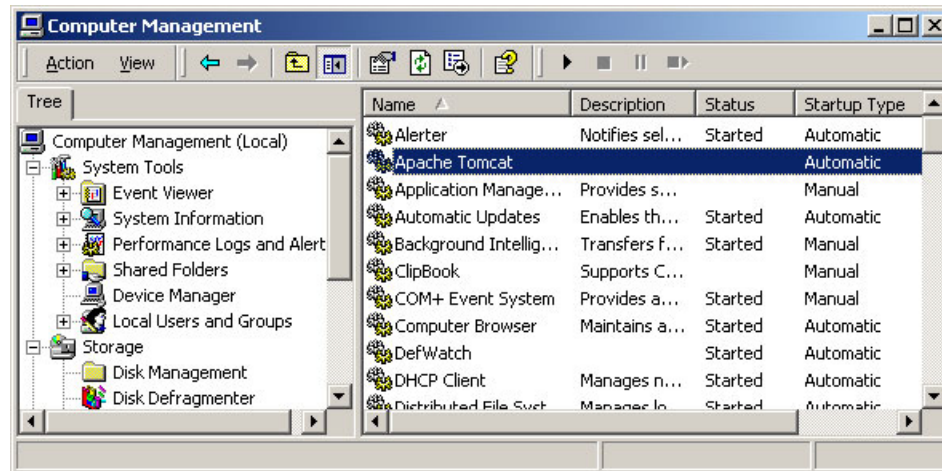


Figure C-1 Stopping Apache Tomcat service

5. Find and stop ISICTomcat4 Service. In addition, set the startup type to **Disabled** (Figure C-2 on page 629) for the ISICTomcat4 service. Keep the services dialog open.

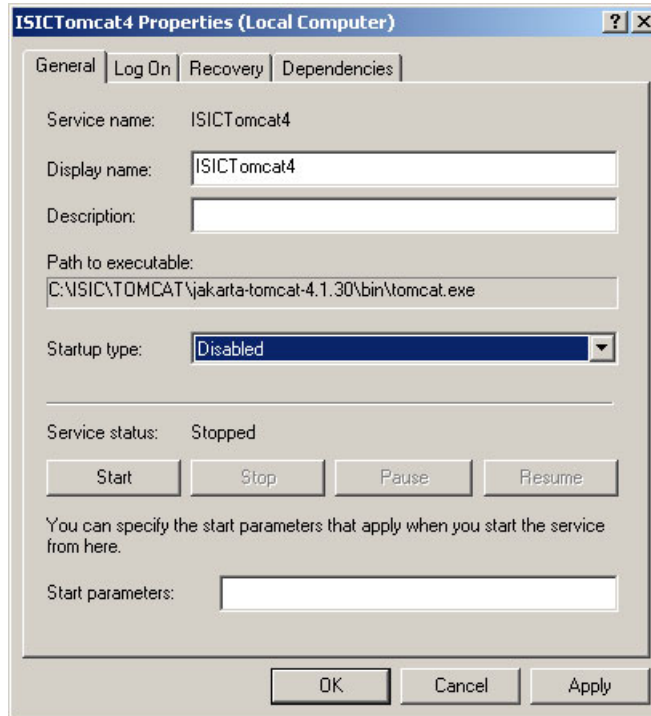


Figure C-2 Disabling ISICTomcat4 service

Note: Both System Information Center and Software Delivery Center install and configure a Tomcat service. One of these services must be disabled.

6. Copy the C:\ISIC\tomcat\jakarta-tomcat-4.1.30\webapps\isic.xml file to the C:\IBMSDC\TOMCAT413\webapps directory.
7. In the Services dialog, restart the Apache Tomcat service and wait a few minutes for the service and web applications to initialize.
8. Open your browser and enter <http://servername:8080/isic> to view the System Information Center logon page.
9. Open your browser and enter <http://servername:8080> to view the Software Delivery Center logon page.

Note: If you are using the System Information Center e-mailing feature, you will need to edit the `isic.properties` file in the `C:\ISIC\web\WEB-INF\classes` directory. The `url=` and the `audit.url=` lines must be updated to include the port 8080.

Note: When installing the local System Information Center agent, port :8080 must be specified at installation time.



D

System Information Gatherer scan uploads

This appendix documents a fix to the automatic System Information Gatherer scans not being uploaded to the System Information Center server.

The information in this appendix applies to any ThinkPad system running Microsoft Windows XP or Windows 2000 running System Information Center V1.1.

Problem description

When installing the System Information Center program, the administrator can customize some of the options (refer to 3.2.3, “System Information Center installation” on page 97). One customization option is to schedule automatic scans and specify the frequency with which the System Information Gatherer program uploads new asset scan information from the client machine to the System Information Center server as shown in Figure 3-17 on page 112. In that figure, the Automatically upload revised asset information box is checked, and the upload interval is set to 4 days.

However, when a System Information Center server is configured to automatically upload asset scans, and clients have installed the System Information Gatherer program (see 3.13, “IBM System Information Gatherer” on page 210), automatic scans fail to upload to the server at the appointed time.

The System Information Center server uses a configuration file named `isic.properties` to store default and customized product configuration data. The configuration file does not properly set up the asset scan information during System Information Center product installation. As a result, client computers are unable to automatically upload scheduled asset scans using the System Information Gatherer agent.

Solution

To correct this problem, the `isic.properties` file must be modified as follows:

1. Logon to the server where System Information Center is installed, select **Start** → **Run**.
2. Type **notepad.exe** and select **OK**.
3. In the Notepad menu bar, select **File** → **Open**.
4. Use the browse function to navigate to this directory:
`C:\ISIC\web\WEB-INF\classes`
5. Select the **isic.properties** file.
6. In the Notepad menu bar, select **Edit** → **Find**. The Find dialog box opens.
7. In the **Find what** field, type `url=`.
8. Select **Find Next**.
9. The line found will contain `url=http://yourservername/isic` (where `yourservername` is the computer name of the server with System Information Center installed). Delete the `/isic` portion of the line, making the line now read `url=http://yourservername`.

10. In the Notepad menu bar, select **File** → **Save**. Close Notepad.
11. From the desktop, select **Start** → **Run**.
12. Type **services.msc**.
13. The Services console opens, displaying a list of services. Find the ISICTomcat4 service. Right-click **ISICTomcat4** and select **Stop**.
14. When the service stops, right-click **ISICTomcat4** and select **Start**. This starts the Tomcat service. The System Information Center Web site should be available after approximately 30 seconds.

Client computers running the System Information Gatherer program that are configured to automatically upload asset scans can now upload scans. The time it takes for scans to appear on the server running System Information Center depends on the schedule setting that was specified during the installation and the amount of information the program is currently processing.

Abbreviations and acronyms

AES	Advanced Encryption Standard	FTP	file transfer program
ANSI	American National Standards Institute	GIF	CompuServe Graphics Interchange Format
API	application programming interface	GINA	Graphical Identification and Authentication
APS	Active Protection System	GMT	Greenwich Mean Time
ATAPI	Advanced Technology Attachment Packet Interface	GSK	Global Security Toolkit
BEER	Boot Engineering Extension Record	GUI	Graphical User Interface
BIOS	Basic Input/Output System	HDD	Hard Disk Drive
BSOD	blue screen of death	HPA	Hidden Protected Area
CA	Certificate Authority	HTML	Hypertext Markup Language
CAPI	cryptographic application programming interface	IBM	International Business Machines Corporation
CHS	cylinders, heads, sectors	IDE	Integrated Drive Electronics
CISC	Complex Instruction Set Computer	IE	Internet Explorer
CSS	Client Security Software	IIS	Internet Information Server
CSV	comma separated value	IP	Internet Protocol
DHCP	dynamic host configuration protocol	ISIC	IBM System Information Center
DLL	dynamic link library	ISO	international Standards Organization
DLT	digital linear tape	ITSO	International Technical Support Organization
ECC	error checking and correcting	IUB	ImageUltra Builder
EEPROM	Electrically Erasable Programmable Read Only Memory	JDBC	Java database connection
EFS	Encrypted File System	JDK	Java Development Kit
ESD	electronic software distribution	JNDI	Java Naming and Directory Interface
ESS	Embedded Security Subsystem	JRE	Java Runtime Environment
FFE	File and Folder Encryption	LBA	Logical Block Addressing
		LDAP	Lightweight Directory Access Protocol
		LPC	low pin count
		LTO	linear tape open

MBR	Master Boot Record	SMBIOS	Systems Management Basic Input Output System
MDAC	Microsoft Data Access Components	SIC	System Information Center
MFD	multiple file download	SQL	Structured Query Language
MSCAPI	Microsoft Crypto API	SSL	Secure Sockets Layer
MSI	Microsoft Software Installation	TAM	Tivoli Access Manager
NIC	Network Interface Card	TCG	Trusted Computing Group
NLS	National Language Support	TCO	total cost of ownership
NTFS	New Technology File System	TCPA	Trusted Computing Platform Alliance
OEM	Original Equipment Manufacturer	TFTP	Trivial File Transfer Protocol
OPSEC	Open Platform for Security	TVT	ThinkVantage Technologies
PARTIES	Protected Area Runtime Interface Extension Services	UCS	Universal Content Server
PCI	peripheral component interconnect	UDB	Universal Database
PKCS	Public Key Cryptographic Standard	USB	Universal Serial Bus
PKI	Public Key Infrastructure	UVM	User Verification Manager
PTA	Personal Trust Agent	VPN	Virtual Private Network
RAID	Redundant Array of Inexpensive Disks	WMI	Windows Management Instrumentation
RDM	Remote Deployment Manager	XML	eXtensible Markup Language
RISC	Reduced Instruction Set Computer		
ROI	Return on Investment		
RRU	Rapid Restore Ultra		
RSA	Rivest, Shamir, and Adleman		
RTE	Java Runtime Environment		
SCSI	Small Computer Systems Interface		
SDA	Software Delivery Assistant		
SDC	Software Delivery Center		
SDD	Secure Data Disposal		
SDK	Software Developer's Kit		
SMA	System Migration Assistant		
SMB	small, medium business		

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

IBM Redbooks

For information about ordering these publications, see “How to get IBM Redbooks” on page 639. Note that some of the documents referenced here may be available in softcopy only.

- ▶ *Using ThinkVantage Technologies: Volume 1 Creating and Deploying Client Systems*, SG24-7045-01

Other publications

These publications are also relevant as further information sources:

- ▶ *IBM Software Delivery Center Administrator's Guide:*
<http://www.ibm.com/pc/support/site.wss/document.do?ln docid=MIGR-57520>
- ▶ *IBM System Information Center Administrator's Guide:*
<http://www.ibm.com/pc/support/site.wss/document.do?ln docid=MIGR-57526>
- ▶ *Rescue and Recovery V2.0 User's Guide:*
<http://www.ibm.com/pc/support/site.wss/document.do?ln docid=MIGR-57317>
- ▶ *Rescue and Recovery Customization and Deployment Guide:*
<http://www.ibm.com/pc/support/site.wss/document.do?ln docid=MIGR-54502>
- ▶ *Access IBM Customization Guide:*
<http://www.ibm.com/pc/support/site.wss/document.do?ln docid=AIBM-T00LS>
- ▶ *Access IBM & Access Help Customization Guide:*
<http://www.ibm.com/pc/support/site.wss/MIGR-46027.html>
- ▶ *Client Security Software Installation Guide:*
<http://www.ibm.com/pc/support/site.wss/document.do?ln docid=MIGR-46391>
- ▶ *Client Security Software User's Guide:*
<http://www.ibm.com/pc/support/site.wss/document.do?ln docid=MIGR-46391>

- ▶ *Client Security Software Administrator's Guide:*
<http://www.ibm.com/pc/support/site.wss/document.do?ln docid=MIGR-46391>
- ▶ *Client Security Software with Tivoli Access Manager:*
<http://www.ibm.com/pc/support/site.wss/document.do?ln docid=MIGR-46391>
- ▶ *Client Security Password Manager User's Guide:*
<http://www.ibm.com/pc/support/site.wss/document.do?ln docid=MIGR-46391>
- ▶ *Client Security Software Deployment Guide:*
<http://www.ibm.com/pc/support/site.wss/document.do?ln docid=MIGR-46391>

Online resources and education

These Web sites and URLs are also relevant as further information sources:

- ▶ Introduction to IBM ThinkVantage Technologies: Security
<http://www.pc.ibm.com/training/txw14.html>
- ▶ Introduction to IBM ThinkVantage Technologies: Wireless
<http://www.pc.ibm.com/training/txw15.html>
- ▶ Introduction to IBM ThinkVantage Technologies: Migration and Recovery
<http://www.pc.ibm.com/training/txw16.html>
- ▶ Using the IBM ThinkVantage Technologies
<http://www.pc.ibm.com/training/ezi10.html>
- ▶ IBM ImageUltra Builder Workshop
<http://www.pc.ibm.com/training/txi06.html>
- ▶ IBM Rescue and Recovery with SMA Workshop
<http://www.pc.ibm.com/training/txi08.html>
- ▶ Implementing IBM Client Security
<http://www.pc.ibm.com/training/txi20.html>
- ▶ Implementing and Securing a Wireless LAN
<http://www.pc.ibm.com/training/txi21.html>

How to get IBM Redbooks

You can search for, view, or download Redbooks, Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy Redbooks or CD-ROMs, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Index

A

- Access Connections
 - overview 6
- Access Help 418–420
 - customizing 419
 - overview 5
- Access IBM 406–417
 - Configure 408
 - customization tool 411–417
 - customizing 410
 - Get Help & Support 409
 - Learn 408
 - overview 5
 - Protect & Recover 408
 - Rescue and Recovery 420
 - Stay Current 409
 - user interface 408
- Access IBM Message Center 421–429
 - Access Support 422
 - enabling 422
 - local message 422
 - Web messages 422
- Access Support 422
 - enabling 422
- access-config.ini 415
- access-text.ini 415
- Add Query Column 198
- Add Query Table 202
- Add Users 164
- admin.key 525
- Adobe Acrobat 6.0 Professional 559–567
- Adobe Systems Incorporated 559
- All Assets
 - Assets 144
 - Reports 168
- All Groups 163
- All Reports 188
- All Users
 - Reports 185
 - User Management 158
- anti-hammering 574
- Apache Tomcat 119
 - download 97

- installation 97
- security settings 119–121
- Software Delivery Center 220, 223
 - defined 223
 - downloading 223, 234, 236
 - installation 234
 - logs and manual 402
 - version requirement 236
- application and policy setup 499–508
 - application policy 501
 - passphrase policy 507
 - supported applications 500
- archiving backups 50–52
- Asset Device Drivers 145
- Asset History 145
- Asset Summary 170

B

- backing up encrypted files 56
- backing up your system 45–50
- backup considerations 39–41
 - delete all backup files 40
 - delete or archive old backup files 40
 - deleting old backup files 40
 - including and excluding files in backups 603
 - where to save backups 39
- base backup image 16
- Basic Authenticating Proxy 433
- biometrics devices 450
- BMGR32 599
- Boot Manager Control 599

C

- centrally managed usage 432
- cfgmod 597
- Change Owner 146
- chip and key settings 508–515
- chip settings 509–510
 - disable chip 510
 - security chip status 509
- Client Security Password Manager 447–448, 452, 483–487
 - configuring 484–487

- downloading the software 452
 - enabling 464
 - installing 483–484
 - limitations 452
 - overview 447, 484
- Client Security Software 444–447, 572
 - administrator console 524
 - components 444
 - downloading the software 452
 - File and Folder Protection 445, 489, 491, 577
 - fingerprint reader
 - installing 473
 - installation 457–483
 - installing prerequisite device drivers 458
 - mass deployment 475–479
 - mass configuration 477
 - mass installation 476
 - registering fingerprints 515–517
 - administrator 515
 - user 516
 - unattended installation 474–479
 - uninstalling 572
 - upgrading 480
 - User Verification Manager
 - aware 449
 - Lotus Notes 517–518
 - overview 445
 - replace Windows logon 500
 - using the policy editor 501
- Cloudscape 93
 - installation 97
 - Software Delivery Center 229
 - defined 222
 - installation 234–235
 - uninstall 618, 626
- column manipulation icons 192
- communicate 66
- Compare Revisions 147
- Compare Selected 148
- configure 65
- Create a new use 156
- Create Base Backup icon 36
- creating rescue media 37
- cryptographic microprocessor 444
- csec.ini 476–477
 - roaming 548, 557
 - sample 557
- csecwiz.exe 476, 533
- CSS

- See Client Security Software
- CSV File 207

D

- Data Maintenance 171
- Delete 150, 158
- delete all backup files 40
- Delete Group 165
- delete or archive old backup files 40
- deleting old backup files 40
- disable chip 510
- display type 189–190
- Distinct Asset Type 173
- Download Agent Installer 154
- Download XML file 150

E

- Edit 151, 160
- Edit Group 165
- EFS
 - See Encrypting File System
- egather2.exe 138–139
- Email Report 208
- Embedded Security Chip 444, 446–447, 449, 451, 453
 - clearing
 - ThinkCentre 456
 - ThinkPad 455
 - overview 444, 449
- Embedded Security Subsystem 443–589
 - Adobe Acrobat 6.0 Professional 559–567
 - Client Security Password Manager 447–448, 452, 483–487
 - configuring 484–487
 - enabling 464
 - installing 483–484
 - limitations 452
 - overview 447, 484
 - Client Security Software 444–447, 572
 - administrator console 524
 - components 444
 - File and Folder Protection 445, 489, 491, 577
 - fingerprint reader
 - installing 473
 - installation 457–483
 - installing prerequisite device drivers 458
 - registering fingerprints 515–517

- administrator 515
 - user 516
- unattended installation 474–479
- uninstalling 572
- upgrading 480
- User Verification Manager
 - aware 449
 - Lotus Notes 517–518
 - overview 445
 - using the policy editor 501
- components 444
- downloading the software 452
- File and Folder Encryption 448–449, 451, 487–491
 - configuring 488–489
 - considerations 451
 - enabling 464
 - installing 487–488
 - known issues 490–491, 575–577
 - limitations 490
 - overview 448
- overview 5
- policy
 - fingerprint 515
 - override 527
 - setting and control 491–508
- roaming profiles 534–559
 - prerequisites 535–536
 - setup 536–554
 - utilizing roaming clients 554–556
- Security Subsystem Administrator Utility 491–515
 - application and policy setup 499–508
 - application policy 501
 - passphrase policy 507
 - supported applications 500
 - chip and key settings 508–515
 - chip settings 509–510
 - key configuration 510–515
 - edit user settings 494–499
 - user enrollment 492–494
- troubleshooting 573
 - administrator utility 578
 - digital certificate 587
 - encryption 589
 - file and folder encryption 575
 - installation 577
 - Lotus Notes 588
 - Microsoft 581

- Netscape 585
 - ThinkPad specific 581
 - Tivoli Access Manager 587
 - user configuration utility 580
 - UVM-aware device 589
- enableroaming 559
- Encrypting File System 56, 81
- Entrust 445, 451, 465, 479, 500, 504
 - enabling support 500
- Enterprise Desktop Solutions 446, 450

F

FFE

See File and Folder Encryption

File and Folder Encryption 56, 81, 448–449, 451, 487–491

- configuring 488–489
- considerations 451
- downloading the software 452
- enabling 464
- installing 487–488
- known issues 490–491, 575–577
- limitations 490
- overview 448

File and Folder Protection 445, 489, 491, 577

- enabling 501

Filter 144

fingerprint reader 450, 568

- installing 473

G

Ghost 5

Groups

- members 164
- Reports 174

guiexcl 603–604

GUlexcl.txt 594

H

hwpw 478, 558

I

IBM Director 6

- overview 6

IBM HTTP Server

- logs and manual 402

IBM System Information Center

- Apache Tomcat 119
- IBM_SERVICE partition 23, 25, 27
- ibmexclcd 603–604
- ibminclcd 56, 81, 603–605
- IIS
 - Software Delivery Center
 - disable 232–233
- ImageUltra Builder
 - overview 5
- including and excluding files in backups 603
- incremental backup image 16
- individual (self-managed) usage 431
- InstallShield 221, 281
 - silent install 327
- Interrupt Current Background Tasks 196
- inventory file 136–137, 142
- inventory management 91
- isic.properties 632
 - required fields 131
 - tasks 197
 - viewing 194
- isig_ibm.exe 215
- isig_oem.exe 154, 211

J

- Java Update Recognizer 433
- Java Web Start 224, 276–277, 382, 394

K

- kal 478, 559
- key archive 478, 482, 573
- key configuration 510–515
 - change archive keys 514
 - change archive location 512
 - register with CSS roaming server 513
 - restore keys from archive 511
- kpl 478, 558

L

- Logs 175
 - task log 175
 - transaction log 175
- Lotus Notes 464, 500, 517

M

- machine-specifics.csv 415
- Macromedia RoboHelp 419

- managing backups 18
- Manually Add Asset 142
- mass configuration 477
- mass deployment 475–479
 - mass configuration 477
 - mass installation 476
- mass installation 476
- MaxNumberOfIncrementalBackups 16, 18, 592, 595
- MFD
 - See Multiple File Download
- Microsoft Challenge/Response (NTLM) Authenticating Proxy 433
- Microsoft Crypto API 445, 451
- Microsoft Internet Information Server 100
- Microsoft Software Installer 221, 269, 281
 - silent install 328
- MSCAPI
 - See Microsoft Crypto API
- MSI
 - See Microsoft Software Installer
- MSIEXEC 35
- Multiple File Download 430–432, 434
- My Assets
 - Assets 143
 - Reports 176
- My Details 157
- My Groups 163

N

- NetSEAT 570
- New Group 162
- newkp 478, 557–558

O

- Opera Web browser 13
- Operating System Summary 179

P

- Page Options 203
- PARTIES
 - See Protected Area Runtime Interface Extension Services
- PartitionMagic 490
- passphrase bypass 526–527
- password
 - Software Delivery Center

- initial 248, 295
 - new user 276, 306, 395
- PC Doctor 13
- PKCS
 - See Public-Key Cryptography Standard
- PKI
 - See Public Key Infrastructure
- policy
 - fingerprint 515
 - override 527
 - setting and control 491–508
- PowerQuest
 - DrivelImage 5
 - PartitionMagic 490
- Printable Report 209
- private1.key 525
- Protected Area Runtime Interface Extension Services 23, 26–27, 89
- protected folder 14
- PTA
 - See Verisign Personal Trust Agent
- Public Key Infrastructure 443–444, 560
- Public-Key Cryptography Standard 445, 451, 572–573
- pull infrastructure, setting up 288
- push infrastructure, setting up 288

R

- Rearrange report display output 190
- Redbooks Web site 639
 - Contact us xvii
- Refresh Result 198
- Register Asset 140
- registering fingerprints 496–497, 515–517
 - administrator 515
 - user 516
- registering smart card 496–497
- Remote Deployment Manager 7
 - overview 7
- Remove All Group Members 166
- replace Windows logon 500
- Reprocess 152
- Rescue and Recovery 420
 - archiving backups 50–52
 - backing up encrypted files 56
 - backing up your system 45–50
 - backup considerations 39–41
 - delete all backup files 40

- delete or archive old backup files 40
 - deleting old backup files 40
 - including and excluding files in backups 603
 - where to save backups 39
- backup methodology 16
 - base backup image 16
 - incremental backup image 16
- backup preferences
 - large enterprise users 41
 - mobile computer users 41
 - setting preferences 42–45
 - small business users 41
 - storage sensitive users 41
- base backup image 16
- components 15
- Create Base Backup icon 36
- creating rescue media 37
- environment and functions 12
- environment configurations 23–29
 - default installation 23
 - PARTIES area 26
 - PARTIES area and type 1C service partition 27
 - type 12 partition 28
 - type 1C IBM_SERVICE partition 24
- functions 14
- including and excluding files in backups 603
- incremental backup image 16
- installation 29–30
- installation process 22
- managing backups 18
- menu options 61–70
 - communicate 66
 - configure 65
 - Rescue and Restore 62
 - troubleshoot 69
- overview 3
- restoring individual files 73
- restoring your system 56–79
 - Rescue and Recovery environment 57–70
 - Windows environment 70–78
 - full system restore 71
 - individual files 73
- scheduler 596
- scheduling backups 52–55
- setting preferences 42–45
- silent installation 31–36
- system backup 38–56
- system requirements 20

- IBM systems 20
- OEM systems 21
- toolbar 58
- uninstall 38
- Rescue and Restore 62
- restoring individual files 73
- restoring your system 56–79
 - Rescue and Recovery environment 57–70
 - Windows environment 70–78
 - full system restore 71
 - individual files 73
- Retire 152
- Return 153
- roaming profiles 534–559
 - prerequisites 535–536
 - setup 536–554
 - utilizing roaming clients 554–556
- Robocopy 290–292
 - defined 290
- RRU command line interface 598
- RRUbackups 24, 45, 55
- RRUcmd 41, 598
- RSA SecurID Software Token 450

S

- scheduler 596
- scheduling backups 52–55
- sdcc.conf 272, 289
 - contents 272
- SDCAdmin 293, 295
- SDCAgent 223, 272–273
 - logs 402
- SDCSETUP.EXE 267, 269–272
 - attended installation 260
 - function 224
 - unattended installation 269
- Secure Data Disposal
 - overview 6
- SecurID 446
- security chip status 509
- security settings 115, 188
- Security Subsystem Administrator Utility 491–515
 - application and policy setup 499–508
 - application policy 501
 - passphrase policy 507
 - supported applications 500
 - chip and key settings 508–515
 - chip settings 509–510

- key configuration 510–515
- edit user settings 494–499
- user enrollment 492–494
- Self-managed Mode 431, 433–435
 - usage 431
- Send Application Log 195
- service partition 65
- Set Current Query as Default 198
- SM Mode
 - See Update Connector
 - Self-managed Mode
- SMA
 - See Software Migration Assistant
- smart card
 - registering 496–497
 - selection 506
 - settings 506
- SMB Client 436–437
 - configuring 437
- SMB LAN Mode 431, 433–441
 - SMB Client 436–437
 - configuring 437
 - SMB Server 436–437
 - configuring 437
 - usage 432
- SMB Server 436–437
 - configuring 437
- SMBus device driver 452, 459, 475
 - installation 459
- Software 178
- Software Delivery Assistant
 - overview 4
- Software Delivery Center 219–404
 - accessing the administrator's console 293–296
 - accessing the ISDC server 385
 - adding a distribution group 354
 - adding a new export group 337
 - adding a new group 297
 - adding a new software package 312
 - adding a new user 306
 - adding a schedule 367
 - adding/deleting a package/bundle in an export group 343
 - adding/deleting machines for a distribution group 361
 - adding/deleting new package/bundle 302
 - administrator's console, using 292–381
 - accessing the administrator's console 293–296

- creating a digital signature for a secure package 336
- exporting a portable catalog 351–354
- exporting/importing software packages/bundles 336–351
 - adding a new export group 337
 - adding/deleting a package/bundle in an export group 343
 - changing the export name and description 341
 - creating an XML file for an export group 345
 - deleting an export group 338
 - importing ISDC files from another server 348
 - searching for an export group 339
- finding help 381
- logging out of the administrator's console 381
- managing distributions 354–364
 - adding a distribution group 354
 - adding/deleting machines for a distribution group 361
 - changing the distribution group description 360
 - deleting a distribution group 357
 - searching for a distribution group 358
 - searching for a machine in a distribution group 362
- managing groups 296–305
 - adding a new group 297
 - adding/deleting new package/bundle 302
 - changing the group 301
 - deleting a group 299
 - searching for a group 300
 - updating user information 304
- managing machines 364–367
 - delete machines 364
 - searching for a machine 365
- managing schedules 367–375
 - adding a schedule 367
 - deleting a schedule 371
 - searching for a schedule 372
 - updating a schedule for pushed software 374
- managing software packages/bundles 312–336
 - adding a new software bundle 314
 - adding a new software package 312
 - deleting a software package/bundle 318
 - searching for a software package/bundle 319
 - software bundle definition information 335
 - software package definition information 322
 - updating software bundle information 321
 - updating software package information 321
- managing users 306–312
 - adding a new user 306
 - changing a user to a different group 311
 - deleting a user 308
 - searching for a user 309
 - updating user information 312
- using ISDC logs 375–381
 - deleting a log 378
 - searching for a log 379
 - viewing a log 376
- Apache Tomcat 220, 223
 - controlling the service 402
 - defined 223
 - downloading 223, 234, 236
 - installation 234
 - logs and manual 402
 - version requirement 236
- architecture considerations 225
 - customization considerations 229
 - hardware recommendations 230
 - large environments 228
 - small and medium environments 225
- building a software library 278–287
 - command line Export/Import interface 286
 - creating a folder structure 279
 - creating a portable catalog 285
 - creating a software bundle 285
 - creating a software package 280
 - importing files from another server 286
 - using a portable catalog 285
- changing the group 301
- changing the distribution group description 360
- changing the export description 341
- client
 - startup 402
- client applet overview 382
- Cloudscape 229

- defined 222
- installation 234–235
- components 222–224
 - client 223–224
 - server 222–223
- contacting a Software Delivery Center technical expert 404
- creating a catalog for an export group 345
- creating a digital signature for a secure package 336
- creating a secure package 336
- customization considerations 229
- deleting a distribution group 357
- deleting a group 299
- deleting a log 378
- deleting a machine 364
- deleting a schedule 371
- deleting a software bundle 318
- deleting a software package 338
- deleting an export group 338
- enabling and disabling the client agent 402
- exporting a portable catalog 351–354
- exporting/importing software packages/bundles 336–351
 - adding a new export group 337
 - adding/deleting a package/bundle in an export group 343
 - changing the export name and description 341
 - creating an XML file for an export group 345
 - deleting an export group 338
 - importing ISDC files from another server 348
 - searching for an export group 339
- finding help 381
- hardware recommendations 230
- IBM HTTP Server logs and manual 402
- IIS
 - disable 232–233
- infrastructure, setting up 287–292
 - server package directory replication tips 290
 - setting up a pull infrastructure 288
 - setting up a push infrastructure 288
- installation
 - client 259–278
 - attended installation 260
 - prerequisite software 259
 - testing ??–278
 - unattended installation 269–272
 - server 231–259
 - providing security 249–259
 - testing 244–249
 - Windows 2000 Server 231–232
 - Windows Server 2003 232–233
- installing a bundle 398
- installing an application 396
- Java Web Start 224, 276–277, 382, 394
- large environments 228
- launching the client applet 386
- logging out of the administrator's console 381
- managing distributions 354–364
 - adding a distribution group 354
 - adding/deleting machines for a distribution group 361
 - changing the distribution group description 360
 - deleting a distribution group 357
 - searching for a distribution group 358
 - searching for a machine in a distribution group 362
- managing groups 296–305
 - adding a new group 297
 - adding/deleting new package/bundle 302
 - changing the group 301
 - deleting a group 299
 - searching for a group 300
 - updating user information 304
- managing machines 364–367
 - deleting machines 364
 - searching for a machine 365
- managing schedules 367–375
 - adding a schedule 367
 - deleting a schedule 371
 - searching for a schedule 372
 - updating a schedule for pushed software 374
- managing software packages and bundles
 - deleting a software package 318
- managing software packages/bundles 312–336
 - adding a new software bundle 314
 - adding a new software package 312
 - deleting software package/bundle 318
 - searching for a software package/bundle 319
 - software bundle definition information 335
 - software package definition information 322
 - updating software bundle information 321

- updating software package information 321
- managing users 306–312
 - adding a new user 306
 - changing a user to a different group 311
 - changing user to a different group 311
 - deleting a new user 308
 - deleting a user 308
 - searching for a user 309
 - updating user information 312
 - user information 312
- obtaining support 404
- overview 4
- password
 - initial 248, 295
 - new user 276, 306, 395
- prerequisite software 259
- providing security 249–259
- Robocopy 290–292
 - defined 290
- sdcc.conf 272, 299
 - contents 272
- SDCAAdmin 293, 295
- SDCAgent 223, 272–273
 - logs 402
- SDCSETUP.EXE 267, 269–272
 - attended installation 260
 - function 224
 - unattended installation 269
- searching for a distribution group 358
- searching for a group 300
- searching for a log 379
- searching for a machine 365
- searching for a machines in a distribution group 362
- searching for a schedule 372
- searching for a user 309
- searching for an export group 339
- searching the library
 - for a software package 319
- setting up the Trusted Sites zone 403
- small and medium environments 225
- testing 244–249
- troubleshooting 401–403
- updating a schedule for pushed software 374
- updating user information 304
- user information 312
- using ISDC logs 375–381
 - deleting a log 378
 - searching for a log 379
 - viewing a log 376
- using the client applet 381–401
 - accessing the ISDC server 385
 - client applet overview 382–385
 - installing a bundle 398
 - installing an application 396
 - launching the client applet 386
- using the documentation 403
- using the software catalog 381–401
 - accessing the ISDC server 385
 - client applet overview 382–385
 - installing a bundle 398
 - installing an application 396
 - launching the client applet 386
- using the Web 404
- viewing a log 376
- Software for Selected Asset 145
- Software Not Used in 90 Days 179
- Start Task Scheduler 197
- Statistics 180
- Stop and Requeue Background Tasks 196
- Surplus 153
- sysregpwd 559
- system backup 38–56
- System Information Center 91–218
 - Admin 193
 - defined 193
 - Interrupt Current Background Tasks 196
 - Send Application Log 195
 - Start Tasks Scheduler 197
 - Stop and Requeue Background Tasks 196
 - Update File to Server 195
 - View Application Log 195
 - View Current Server Status 195
 - View Properties File 194
 - administrator account 129, 155
 - Administrator password 122, 129
 - alternative database support 607–626
 - DB2 608–618
 - Microsoft SQL Server 618–626
 - Apache Tomcat
 - download 97
 - installation 97
 - security settings 119–121
 - Asset Device Drivers 145
 - Asset History 145
 - Assets 133–154
 - All Assets 144
 - Change Owner 146

- Compare Revisions 147
- Compare Selected 148
- Delete 150
- Download Agent Installer 154
- Download XML file 150
- Edit 151
- Filter 144
- Information 144
- Manually Add Asset 142
- My Assets 143
- Register Asset 140
- Reprocess 152
- Retire 152
- Return 153
- Surplus 153
- Upload Asset Scan 135
- Users 145
- Cloudscape 93
 - installation 97
 - uninstall 618
- column manipulation icon 192
- components 94
- database integration 93
- demographic information 131, 141, 171, 173
- display type 189–190
- egather2.exe 138–139
- features 92–94
- Group management 161–166
 - Add Users 164
 - All Groups 163
 - Delete Group 165
 - Edit Group 165
 - Groups 164
 - My Groups 163
 - New Group 162
 - Remove All Group Members 166
- initial password 113, 122, 129, 155
- installation 96–123
 - custom install 107–117
 - modifying 124–128
 - quick install 104–107
 - testing 117–123
- Internet Explorer 95
- inventory file 136–137, 142
- inventory management 91
- isic.properties
 - required fields 131
 - tasks 197
 - viewing 194
- isig_ibm.exe 215
- isig_oem.exe 154, 211
- JDBC DB connection parameters
 - DB2 V8.2 608
 - SQL Server 2000 618
- location information 131, 140–141, 158
- logging on 128–132
- Microsoft Internet Information Server 100
- missing prerequisites 101
- Options 197–206
 - Add Query Column 198
 - Add Query Table 202
 - defined 197
 - Page Options 203
 - Refresh Result 198
 - Set Current Query as Default 198
- Output 206–209
 - CSC Fild 207
 - Email Report 208
 - Printable Report 209
- overview 4, 95
- Rearrange report display output 190
- Reports 95, 167–192
 - All Assets 168
 - All Reports 188
 - All Users 185
 - Asset Summary 170
 - column manipulation icons 192
 - Data Maintenance 171
 - display type 189–190
 - Distinct Asset Type 173
 - Groups 174
 - Logs 175
 - My Assets 176
 - Operating System Summary 179
 - Rearrange report display output 190
 - Software Not Used in 90 Days 179
 - Software 178
 - Statistics 180
 - Tasks 180
 - ThinkVantage Reports 181
 - Usage Information 186
 - Users 184
 - Workstation Security 186
- required fields 114, 131
- requirements 95
- security settings 115, 188
- Software for Selected Asset 145
- super-user account 129, 155

- System Information Gatherer 94, 210–215
 - Compare Revisions 147
 - installation
 - installation from product CD 211
 - installation from the Web 215
 - permanently installed client agent 211
 - temporarily installed client agent 210
 - overview 92, 94, 210
 - task log 175
 - Tasks 192–193
 - defined 192
 - transaction log 175
 - uninstall 626
 - user account 128, 155
 - User Management 155–161
 - All Users 158
 - Create a new user 156
 - Delete 158
 - Edit 160
 - My Details 157
 - User Details 158
 - User History 158
 - user name 130
 - user types 93, 111, 128, 155
 - administrator account 129, 155
 - super-user account 129, 155
 - user account 128, 155
 - verifying the version level 123
- System Information Gatherer 94, 210–215
 - Compare Revisions 147
 - data sources
 - SMBIOS 94
 - Windows Management Instrumentation 94
 - Windows Registry 94
 - installation
 - installation from product CD 211
 - installation from the Web 215
 - permanently installed client agent 211
 - temporarily installed client agent 210
 - isig_ibm.exe 215
 - isig_oem.exe 154, 211
 - overview 92, 94, 210
- System Migration Assistant
 - overview 6
- System Recognizor 433

T

- Targus 450, 568

- fingerprint reader 450, 568
 - install 473
- task log 175
- Tasks 180
 - defined 192
- TCG
 - See Trusted Computing Group
- TCPA
 - See Trusted Computing Platform Alliance
- technical assistance 404
- terminal services 536
- ThinkVantage Reports 181
- Tivoli Access Manager 446, 450, 453, 570–572
 - policy management 502
 - troubleshooting 587
- transaction log 175
- troubleshoot 69
- troubleshooting
 - Embedded Security Subsystem 573
 - administrator utility 578
 - digital certificate 587
 - encryption 589
 - file and folder encryption 575
 - installation 577
 - Lotus Notes 588
 - Microsoft 581
 - Netscape 585
 - ThinkPad-specific 581
 - Tivoli Access Manager 587
 - user configuration utility 580
 - UVM-aware device 589
 - Software Delivery Center 401
- Trusted Computing Group 444
- Trusted Computing Platform Alliance 444, 452, 480, 575
- TVT.txt 18, 34–36
 - values and settings 591
- type 1C IBM_SERVICE partition 24, 27

U

- Universal Content Server 430, 433–434
- Update Connector 429–441
 - centrally managed usage 432
 - individual (self-managed) usage 431
 - Java Update Recognizor 433
 - Multiple File Download 430–432, 434
 - overview 430
 - Self-managed Mode 431, 433–435

- usage 431
- SMB LAN Mode 431, 433–441
 - SMB Client 436–437
 - configuring 437
 - SMB Server 436–437
 - configuring 437
 - usage 432
- System Recognizor 433
- Universal Content Server 430, 433–434
- Upload Asset Scan 135
 - attach an inventory file 137
 - inventory this machine 136
- Upload File to Server 195
- Usage Information 186
- User
 - Reports 184
- User Details 158
- User History 158
- User Verification Manager
 - aware 449
 - change passphrase 498
 - Lotus Notes 517–518
 - overview 445
 - passphrase bypass 526–527
 - passphrase expiration 495
 - registering fingerprints 496–497, 515–517
 - administrator 515
 - user 516
 - remove user 498
 - replace Windows logon 500
 - reset user 497
 - storing Windows passwords 496
 - using the policy editor 501
- Users
 - Assets 145
- UVM
 - See* User Verification Manager

V

- Verisign Personal Trust Agent 447
- View Application Log 195
- View Current Server Status 195
- View Properties File 194

W

- Web-D xiii
- where to save backups 39
- Windows PE

- See* Windows Pre-installation Environment
- Windows Pre-installation Environment 12
- WinZip 221, 281
- Wise InstallManager 221, 281
- Wise InstallSystem
 - silent install 327
- with User Verification Manager 517
- Workstation Security 186

X

- xfercert 566
- XML 150



Using ThinkVantage Technologies: Volume 2 Maintaining and Recovering Client Systems

(1.0" spine)
0.875" <-> 1.498"
460 <-> 788 pages



Redbooks

Using ThinkVantage Technologies: Volume 2 Maintaining and Recovering Client Systems

**New Software
Delivery Center
ThinkVantage
Technologies**

**Simple software
distribution in
corporate
environments**

**Use of the
Technologies to
lower costs**

IBM® ThinkVantage™ Technologies bring your IBM PCs one step closer to being self-configuring, self-optimizing, self-protecting, and self-healing, saving you time and money throughout the life of your systems. In short, ThinkVantage Technologies let you focus your attention on your business, rather than on your computer.

ThinkVantage Technologies are software tools designed to help companies drive down IT support costs, especially those associated with managing and supporting systems after initial roll-out. These tools also help increase security and decrease the complexity of today's IT infrastructure.

This IBM Redbook is volume two of a two-volume set. It guides you through the process of maintaining, recovering, and securing ThinkVantage Technologies on IBM and third-party desktops and mobiles.

This edition adds a chapter on IBM Software Delivery Center. Software Delivery Center is a software delivery solution that uses Web-based tools and technology to deliver software components to computers distributed throughout a corporate enterprise.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks